Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 23 (2011) 586 – 593

Procedia Engineering

www.elsevier.com/locate/procedia

2011 International Conference on Power Electronics and Engineering Application

Study on the security models and strategies of cloud computing

Jianhua Che[a*], Yamin Duan[b], Tao Zhang[a], Jie Fan[a]

[a]*State Grid Electrics Power Research Insititute, No.8 Nanrui Road, Nanjing 210003, China*
[b]*Shijiazhuang University of Economics, No.136, Huaian East Road, Shijiazhuang 050031, China*

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 customers to understand the security status quo of cloud computing and contribute some efforts to improving the security level 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 security risks of cloud computing deriving from different organizations. Finally, we gave some security strategies from the perspective of construction, operation and security incident response to relieve the common security issues of cloud computing.

Keywords: Cloud computing; security model; risk analysis; security strategy

1. Introduction

Cloud computing is a new computing paradigm appeared in 2006, and the evolutionary offspring of parallel computing, distributed computing, utility computing and grid computing, and the developmental outcome of network storage, virtualization and load balance [1]. The main idea of cloud computing is to build a virtualized computing resource pool by centralizing abundant computing resources connected with network and present the service of infrastructure, platform and software. This network that offers various computing resources is called "*cloud*" [2]. As a supercomputing paradigm based on the Internet, cloud computing allows customers to dynamically share a mass of hardware, software and data resource, and charges according to their actual usage. Therefore, computing power can be sold and purchased as

* Corresponding author. Tel.: +086-25-83096338.
E-mail address: chejianhua@zju.edu.cn.

1877-7058 © 2011 Published by Elsevier Ltd.
doi:10.1016/j.proeng.2011.11.2551

merchandise easily by network in a low price, just like water, gas and electric power. Cloud computing is an innovatory thing similar to electric power changing from a single generator to a centralized electric power plant.

The concept of cloud computing has been introduced for several years, however, there are still various interpretations on what is cloud computing. Since the cloud computing specification of National Institute of Standards and Technology (NIST) has been proposed, the definition of NIST about cloud computing becomes the most authoritative one widely accepted by researchers. The cloud computing definition of NIST includes *five essential features*, *three service models* and *four deployment models* as figure 1 shown [3]. Herein, the *five essential features* includes virtualized computing resource pool, broad network access, rapid elasticity, on-demand self-service, measured service; the *three service models* are *Infrastructure as a Service (IaaS)*, *Platform as a Service (PaaS)*, *Software as a Servcie (SaaS)*; the *four deployment models* are *private* cloud, *community* cloud, *public* cloud and *hybrid* cloud.

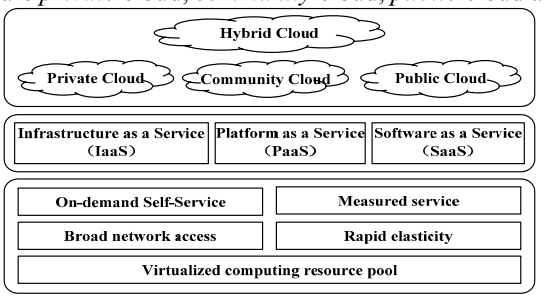

Fig.1. the NIST's definition model of cloud computing[1]

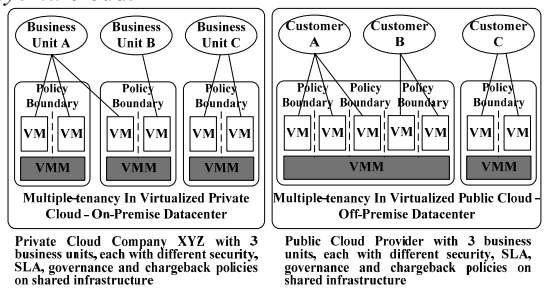

Fig.2. the multiple-tenancy model of cloud computing[4]

2. The Security Models of Cloud Computing

2.1. 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.

2.2. 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.

2.3. Jerico Formu'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 [6] 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.

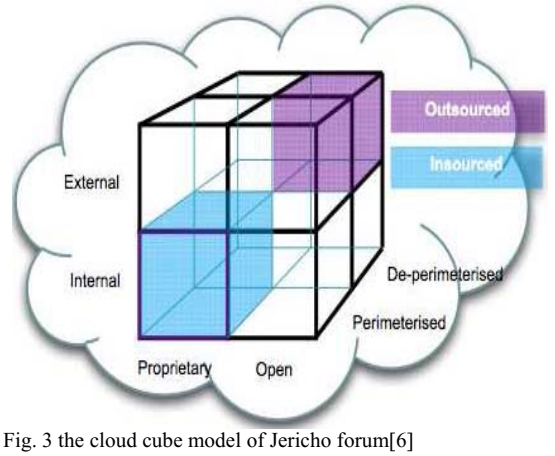

Fig. 3 the cloud cube model of Jericho forum[6]

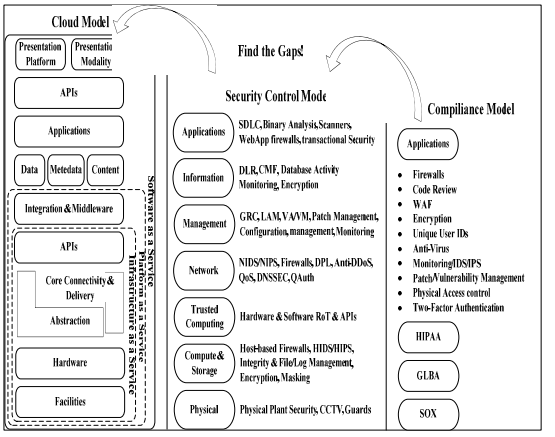

Fig. 4 the mapping model of cloud, security and compliance[4]

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 de-perimeterised 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.

2.4. 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.

3. The common security issue of cloud computing

3.1. Seven Security Issues of Cloud Computing Respectively by CSA and Gartner

Cloud Security Alliance (CSA) has published a white paper titled *Top Threats to Cloud Computing* by summarizing various security concerns of cloud computing in March, 2010 [7]. In this white paper, CSA has described seven security risks of cloud computing: 1) *abuse and nefarious use of cloud,* 2) *insecure interfaces and APIs*; 3) *malicious insiders*; 4) *shared technology issues*; 5) *data loss or leakage*; 6) *account or service hijacking*; 7) *unknown risk profile*.

Gartner, a global authoritative IT research and analyst firm, has made a widespread investigation, and summarized seven security risks of cloud computing [8]: 1) p*rivileged user access*; 2) r*egulatory compliance*; 3) d*ata location*; 4) d*ata segregation*; 5) r*ecovery*; 6) *investigative support*; 7) l*ong-term viability*.

3.2. Three Parties' Security Issues of Cloud Computing

We analyze the security risks of cloud computing from the perspective of customer, service provider and government as follows.

- *The security risks confronted by customers*

The security risks that customers need to confront in cloud computing environment include: 1) The downtime of cloud computing environment that brings great depress to the confidence of customers cannot be avoided totally; 2) The leak of commercial secrets that means a nightmare for customer cannot be avoided totally; 3) How to face the privilege status of cloud service provider and the security concerns such as fault elimination, damage compensation and business migration etc.

- *The security risks confronted by service providers*

The security risks that service providers need to confront in cloud computing environment include: 1) How to assure the long-term secure operation of the cloud data center and isolate the fault to reduce its influence to a smallest extent are the security risks that service providers have to face with; 2) How to fight against the numerous and aggressive network hackers is a disturbing security problem; 3) For customers with various demands, how to effectively and securely manage these customers and identify and block the malicious customers is another unavoidable task.

- *The security risks confronted by government*

The security risks that government administrators need to confront in cloud computing environment include: 1) How to enhance the security protection of a mass-scale data center is one important concern; 2) How to securely manage the numerous and various scale cloud service providers; 3) How to evaluate and rank the security level of cloud service providers and the security credit of cloud customers, and publish the proactive alarm of malicious programs.

4. Some security strategies of cloud computing

When constructing or migrating customer business to a cloud environment, its security must be assured. Here, we give several strategies to contribute a secure cloud environment. Regarding to the security risks of cloud computing, we proposed several security strategies as follows.

4.1. Securely Construction Strategies of Cloud Computing

4.1.1 Traditional Security Practice Mechanism

Traditional security practice such as the security protection of physical facilities, network, computer system, software application, and data still work in a cloud environment, and constructing a cloud environment should obey the common international information security standards such as ISO27001. Therefore, the traditional security practice mechanisms should be assured for a secure cloud environment.

4.1.2 Virtualization Security Risks Assessment

Regardless of a public or private cloud, the construction and deployment of a cloud environment cannot lack numerous virtualization products. Therefore, we need to assess the merits and drawbacks and security level of various virtualization technology resolutions and suite products, and choose the best one to reduce the security risks brought by virtualization.

4.1.3Development Outsourcing Risk Control

Constructing a cloud environment is a large-scale systematic engineering with heavy work load and many advanced technologies, so it is hard to take charge of all development work for an organization. A practical action is to handover partial development work to several outsourcing parties, which will introduce some security risks. Therefore, we should identify the security risks incurred by outsourcing service and establish strict control strategies to assure their quality level and security requirement.

4.1.4Portability and Interoperability

Customers must keep in mind that they may have to change service providers for the sake of unacceptable cost increase at contract renewal time, business operations ceasing by service providers, partial cloud service closure without migration plans, unacceptable service quality decrease, and business dispute between cloud customer and provider etc. Therefore, portability and interoperability should be considered up front as part of the risk management and security assurance of any cloud program.

4.2. Securely Operation Strategies of Cloud Computing

4.2.1Business Continuity Assurance

Rapid change and lacking transparency within cloud computing requires that business continuity plan and disaster recovery expertise be continuously engaged in monitoring the chosen cloud service providers. Regular inspections of a cloud service provider about cloud infrastructure and its physical interdependencies, disaster recovery and business continuity plans, contract documentation about security control action, recovery time objectives (RTOs), and access to data should be performed.

4.2.2Attack Proactive Alerting

Security incidents will be inevitable during in a cloud environment's operation. As cloud is an ultra-lager-scale distributed network system that contains a lot of physical infrastructure, host system, and business application, the range attacked by malicious people is very widespread and traditional attack proactive alerting mechanisms in small network environment may fail to work. Therefore, how to monitor the network access all the time and alert timely on the malicious intrusion should be resolved.

4.2.3 Data Leak Prevention

Sensitive data leak is an important security risk of cloud environment. There are two potential data leaking ways: static data leakage and dynamic data leakage. Static data leakage means that the data stored in data center, application memory and terminal memory is accessed and leaked by unauthorized users, dynamic data leakage means that the data being transformed in cloud environment is accessed and leaked by customer account hijacking or network channel wiretapping. Therefore, all static and dynamic data are facing the security risk of leakage and tamper, and how to resolve it should be concerned seriously.

4.2.4Security Accident Notification & Response

Once security incidents occurred in a cloud environment, cloud service providers should notify their customers at first time, so as to customers can evaluate the potential damage incurred by these security incidents. Furthermore, cloud service providers should start the emergency plan to response these security incidents, including application-level firewalls, proxies, application logging tools, disaster recovery project, and cloud service backup etc. Therefore, cloud service providers should create their respective standard security incident response mechanisms.

4.2.5 Security Incidents Audit

To avoid the same security incidents occurring again, cloud service providers should find out the reasons of security incidents. Auditing can contribute to the reason analysis of security incidents in cloud environment. However, traditional security auditing techniques (e.g. security log, compliance check tools) might not satisfy the auditing demand of cloud environment. Therefore, cloud service providers should develop some new security auditing approaches. In addition, as a new evidence-obtaining way, electric discovery is gradually accepted by court. Courts now are realizing that information security management services are critical to making decisions as to whether digital information may be accepted as evidence. While this is an issue for traditional IT infrastructure, it is especially concerning in Cloud Computing due to the lack of established legal history with the cloud.

5. 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, we surveyed the main existing security models of cloud computing, and summarized the main security risks of cloud computing from different organizations. Finally, we gave some security strategies against these common security issues of cloud computing. In the future, we will fulfil these security strategies with technology and management ways.

References

[1] Vaquero L.M., Rodero-Merino L, Caceres J., Lindner M. A break in the clouds: towards a cloud definition. In: ACM SIGCOMM, 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] Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing (Draft). NIST. 2011. http://www.production scale.com/home/2011/8/7/the-nist-definition-of-cloud-computingdraft.html#axz z1X0xKZRuf.

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

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

[8] Heiser J. What you need to know about cloud computing security and compliance, Gartner, Research, ID Number: G00168345, 2009.