Research on the Model for Cloud Security Based on SLA

Guo-Chun TANG　Yan-Ping WU
（Department of Information, OiongTai teachers' college, Haikou 571100, China）
E-mail: tangguochun1@163.com

Abstract: The cloud computing applications brings a new set of information security problems. The cloud security model based on SLA (Service Level Agreement) was studied. From the security challenges of cloud computing , cloud computing security threats was analyzed comprehensively, the service level agreements was expanded, the CSLA (Cloud Service Level Agreement) structure was proposed, the cloud security reference framework was designed, the cloud security level architecture and cloud services pricing and charging models was proposed.

Key words: Cloud security; Cloud computing; Cloud security framework; CLSA (Cloud Service Level Agreements)

1. Introduction

The new features of cloud computing applications has brought unprecedented security challenges to information security, security and privacy issues have become an obstacle and major bottleneck to popularize and promote cloud computing. At present cloud computing security is facing some challenges in three areas: (1) Cloud computing technology security challenges: including fake identity (primary threat facing cloud computing), Shared Risk (specific security risks of cloud computing), data security risks and privacy disclosure, cloud computing platform business continuity, unsafe interfaces. (2) Cloud management security challenges: including personnel management risks (internal personnel management risks, the risk management), responsibility for security risks,, compliance risk, operational risk management (multi -service model risk, continuous operational risk), safety monitoring risks. (3) Computing security legal risks: including major countries / economies on computer crime legislation, information security and privacy risk monitoring, computer forensics risk. In this paper , cloud computing security threats was analyzed comprehensively, the service level agreements was expanded, the CSLA (Cloud Service Level Agreement) structure was proposed, the cloud security reference framework was designed, the cloud security level architecture and cloud services pricing and charging models was proposed.

2. The architecture model of CSLA (Cloud Service Level Agreement)

To ensure the quality of service, One SLA (Service Level Agreement) usually is signed between users and service providers. The SLA definition from TMF (Tele Management Forum): SLA is a formal agreement negotiated by two entities, a legally binding contract, the respective responsibilities and other aspects of the consensus and agreements between the service provider and the customer. In short, CSLA is the guarantee terms and mishandling for QoCS (Quality of Cloud Service) signed between the cloud service providers and cloud service consumers. CSLA includes five parts: cloud service, cloud technology, cloud quality report, and cloud security, cloud business，as illustrated in Figure 1.

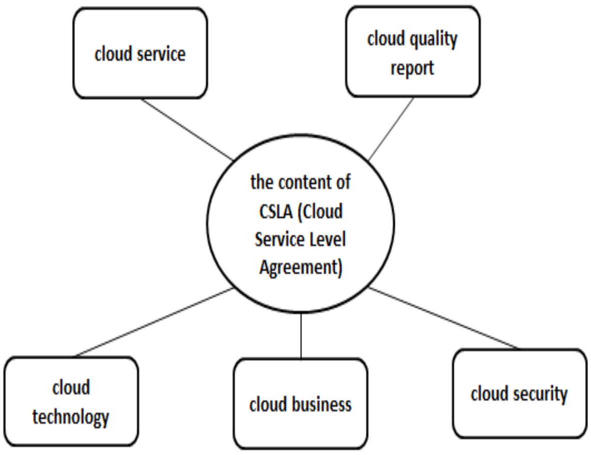

Figure 1 CSLA structure

Cloud service describes the negotiated cloud services, including cloud service information identity, cloud services, cloud service level, cloud services billing, contract modification or termination. Cloud component technology represents a common business measure of cloud technology parameters, targets set and performance monitoring. Cloud reports section refers to the cloud services quality monitoring report of consumers and providers, including the cloud services quality data and statistics specified in CSLA. Cloud Business section refers to the description that when the cloud service provider does not meet the promised cloud service level (ie. Service violation), the cloud service provider should compensate according content, methods, and irresistible factors in. Cloud security refers to the major cloud security service side.

3. Information security framework of Cloud services and the basic safety requirements of level protection

3.1 Information security framework of Cloud services

Cloud computing security issues are the shared responsibility between cloud service providers and cloud services users. Three modes of cloud services (IaaS, PaaS, SaaS) have the cloud services public safety issues, such as data security, encryption and key management, identity and access control, security event management, business continuity, and have their own cloud model security issues, and presents different security duties for cloud service providers and cloud service users. IaaS cloud service providers are responsible for the physical security, network security, environmental security and virtualization security controls. The cloud service users will bear the related IT systems and security controls, such as the operating system, applications and data. PaaS cloud service providers are in addition to the responsibility for solving the physical, network, and environmental safety issues underlying infrastructure, and should resolve your operating system, application interface security and other issues, and the cloud service users will bear the operating system on the application and data security. SaaS cloud service providers need to ensure the overall security of the SaaS services from infrastructure to the application layer, and are responsible for the physical and environmental security, applications and data related security control. The cloud service users will need to maintain information security associated with itself, including authentication username, password and terminal security. In view of this, this paper proposed the following cloud security framework, as shown in Figure 2.

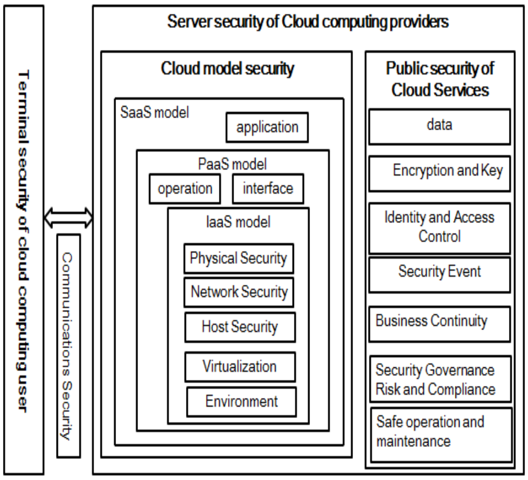

Figure 2 Cloud Security Framework

Security governance, risk management and compliance are a business-driven security point. Through the enterprise business and operational risk assessment to determine its strategy and governance framework, risk management framework, defining compliance and policy compliance, establishing information security document management system.

3.2 Some basic safety requirements of Cloud security level

In view of cloud computing security challenges faced by three, cloud security basic requirements for cloud services system is presented in Figure 3.

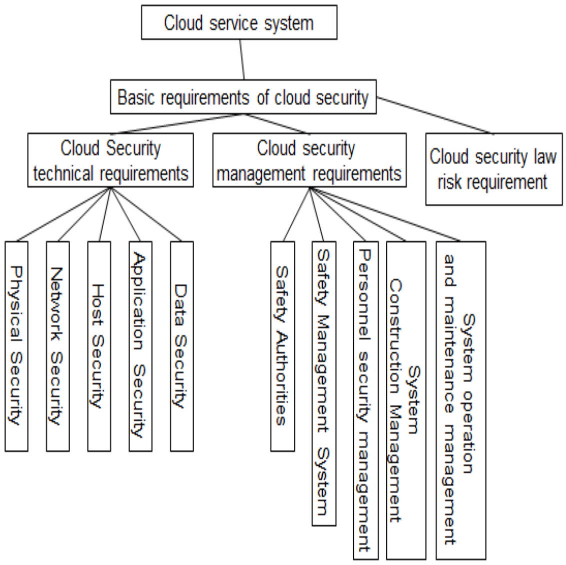
Cloud service system
Basic requirements of cloud security
Cloud Security technical requirements
Cloud security management requirements
Cloud security law risk requirement
Physical Security
Network Security
Host Security
Application Security
Data Security
Safety Authorities
Safety Management System
Personnel security management
System Construction Management
System operation and maintenance management

Figure 3 cloud security system basic requirements of cloud services

In view of cloud services system security requirements, this paper proposed a level of security to protect the cloud architecture. The level is summarized in Table 1.

Table 1 Cloud Security level Architecture

security level	object	security capabilities of cloud service providers	The level of supervision
The initial level (one security response)	General System	Monitoring and control, monitoring, operating conditions of the physical device by Borders and the corporate network gateway	Independent security from user
Growth level (Two Security Response)	General System	Adopting new monitoring and control technology, and can timely process related security issues	Partial safety supervision and inspection and guidance
Stereotypes level (Three Security Response)	Critical systems	At the enterprise level ,integrated monitoring and control technology, monitoring and control of automated management	Supervision and inspection
Specification level (Four Security Response)	Critical systems	Accurate measurement of cloud security risks Degree	Mandatory supervision and inspection
Optimization level (Five Security Response)	Extremely important system	Constantly improve cloud security strategy, Reduce security risks cloud, Constantly enhance the automatic monitoring and control capabilities	Special supervision and inspection

As discussed in Table 1, It is divided into five levels, and is respectively described from four aspects, such as security level, object, security capabilities of cloud service providers and the level of supervision. Cloud computing center security level of protection must be carried out within the framework of the construction, taking full account of new virtualization and operational security issues.

4. Cloud service system pricing and billing models based Cloud security as a service

When cloud services system is directly facing final consumers, the design of service pricing strategy is essential. Pricing strategy is directly related to the user experience and satisfaction, but also affects the cloud service provider's revenue. Cloud security is a factor that cloud service users are very concerned about, and directly determines the user of cloud services system availability and reliability. The cloud security as a service is the inevitable trend of cloud computing applications for users. To this end, the cloud service pricing and billing system should reflect the value of cloud security as a service for users. Cloud service system pricing system should be the clear, flexible, easy to understand and easy to select for individuals or enterprises users. and it’s clear features means that the application can provide the functionality and the corresponding functional safety, and how each should charge is at a glance to cloud billing service users; flexible features means the different combinations of the functionality and the corresponding functional safety should be truthfully reflected in the price; Understanding is that price policy should have specify, scientific and reasonable framework; facilitate selection refers to the option of different types, different needs of users according to their situation. Based on this, the paper presents one reference model of the pricing and billing for cloud services system, as shown in Figure 4.

In this pricing model, according to the order of accounts, planning, feature pack type, feature pack level and cloud security level, the former and the latter is a one to many relationship, means that an account can have multiple plans, a plan may correspond to more than functional packet type, a function package types can correspond to multiple feature pack, a feature pack may correspond to multiple cloud security level. Along with this expansion-many relationship, the user selects more and more flexibility, but the choices are the lower the convenience, operability of the application weaker.

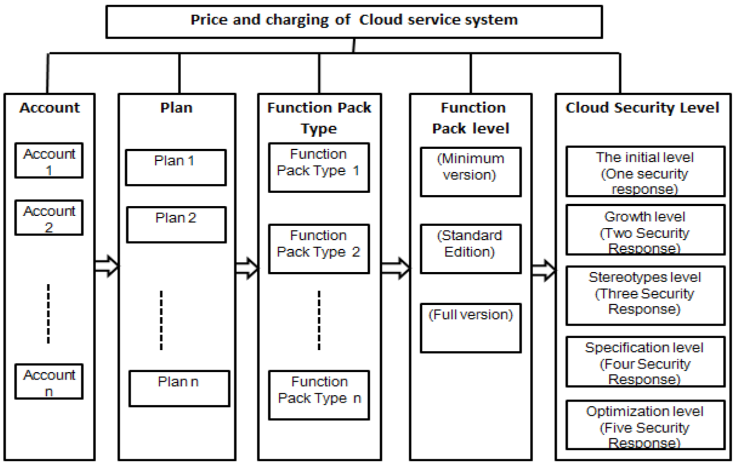
Price and charging of Cloud service system
Account
Account 1
Account 2
Account n
Plan
Plan 1
Plan 2
Plan n
Function Pack Type
Function Pack Type 1
Function Pack Type 2
Function Pack Type n
Function Pack level
(Minimum version)
(Standard Edition)
(Full version)
Cloud Security Level
The initial level (One security response)
Growth level (Two Security Response)
Stereotypes level (Three Security Response)
Specification level (Four Security Response)
Optimization level (Five Security Response)

Figure 4 price and charging models of cloud service system

Billing plans added to the concept of time, it is different with the function package types, but can also come through differentiated market segments to user choice. Flexibility of billing account is at minimum, but provides the most convenient package solution to the cloud service users. An account is often of the users of multiple plans; provide a variety of planned combination according to account the different needs. Cloud service providers can refer to the above pricing model, select the appropriate option for pricing.

5. Conclusion

With cloud computing becoming popular, openness makes cloud computing be faced with the serious security challenges. Security is a real problem and needs to be constantly examined and studied. This paper describes the cloud security challenges, a comprehensive analysis of cloud computing security threats, expands the service level agreements, proposes cloud service level agreements CSLA (Cloud Service Level Agreement) structure, designs cloud security framework, proposes price and charging model of cloud service system.

Acknowledgment

Supported by 2012 OiongTai teachers' college Project, Project Number: qtky201218

References

[1] Azlan Ismail, Jun Yan,Jun Shen. An offer generation approach to SLA negotiation support in service oriented computing. Computer Science Service Oriented Computing and Applications, 2010, 4(4):277-289.

[2] Security Guidance for Critical Areas of Focus in Cloud Computing, https:// downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf.

[3] Marco Comuzzia, Constantinos Kotsokalisb, George Spanoudakisa,Ramin Yahyapour. Establishing and Monitoring SLAs in complex Service Based Systems, IEEE International Conference on Web Services, 2009: 783-790.

[4] FENG Deng-guo, ZHANG Min, ZHANG Yan，et al.Study on Cloud Computing Security［J］.Journal of Software, 2011, 22(1) : 71-83.

[5] WANG Lin-song，LIU De-shan，GUO Jin. Design of Public Cloud Security Architecture [J]. Journal of Jilin University (Information Science Edition), 2013, 31 (2):166-169

[6] Fu Yingxun,Luo Shengmei,Shu Jiwu. Survery of Secure Cloud Storage System and Key Technologies [J]. Journal of Computer Research and Development, 2013, 50 (1):136-145

[7] Xu Yingying, GaoFei,Shang Fengying.New Cloud Security solutions and its key technologies [J]. Huazhong Univ.of Sci.&Tech. (Natural Science Edition),2012,40(Z1): 74-78