Security SLAs for IMS-based Cloud Services

Guo zhien
Department Of Computer Science and Technology
Tsinghua University
Beijing, China
Zhienguoguo@hotmail.com

Dai yiqi
Department Of Computer Science and Technology
Tsinghua University
Beijing, China
Daiyiqi@126.com

***Abstract*—For the actual use of existing security problems and lack of existing solutions for cloud computing, we introduce the SLA(Service Level Agreement) ideas to the security capability negotiations, which called sSLA(Security Service Level Agreement). The framework and data processes of sSLA were implemented on our IMS-based cloud systems, which were showed that this method can effectively eliminate the security concerns of the customers of cloud services.**

Keywords: cloud computing; IMS; Security;SLA

I. INTRODUCTION

With the rapid development of the Internet, the cloud computing is proposed to meet the high capability requirement of computing, storage, service[1]. It uses virtualization, dynamic resource management, QoS technology, service-oriented design ideas, to provide on-demand and easy dynamic expansion method to obtain any services for businesses and users. However, due to situation that the users and business critical data and information is on the cloud, security has been one of the important issues impact business and users to choose cloud computing[2].

To solve the security situation, the developers and providers of cloud computing services use some technologies such as the WS-Security architecture[3,4], PKI infrastructure to secure the communications between the service consumer and provider. However, studies suggest that the program can not effectively eliminate the security concerns of users and businesses on cloud computing services.

Service Level Agreement (SLA) [5]technology in the cloud computing services are widely used in the negotiation process between the user and the Service Provider the quality of service by a formal contract. The technology uses the SLA to require the SP to take measures to ensure the demand for the QoS parameters agreed on the specific business. Draw on the ideas, we introduce the security service level agreement (sSLA) mechanisms, and a trust third party which is supposed to supervise the actual service capacities to the consumers. Based on the design idea, we design and realize a set of sSLA mechanisms on the IMS-based cloud service systems.

To better illustrate the work, the paper is organized as follows: section II introduced the IMS-based cloud systems, which developed three services(messaging, conferencing, location). Section III gives the mechanisms of SLA of the cloud services. Section IV proposed the sSLA architecture and the data flow， and analyzed the scheme. Section V summarized the paper and discussed the future work.

II. IMS-BASED CLOUD SERVICE

IMS technology[6] which is combined with the communication network technology and Internet technology has the ability to support various integrated multimedia applications due to is openness, dependency and security. Meantime, the access independent and high Guarantees features make it appropriate to support cloud computing services. As illustrated in Fig.1, IMS-based cloud computing services are composed with system level, core-middleware level, user-middleware level and user presentation.

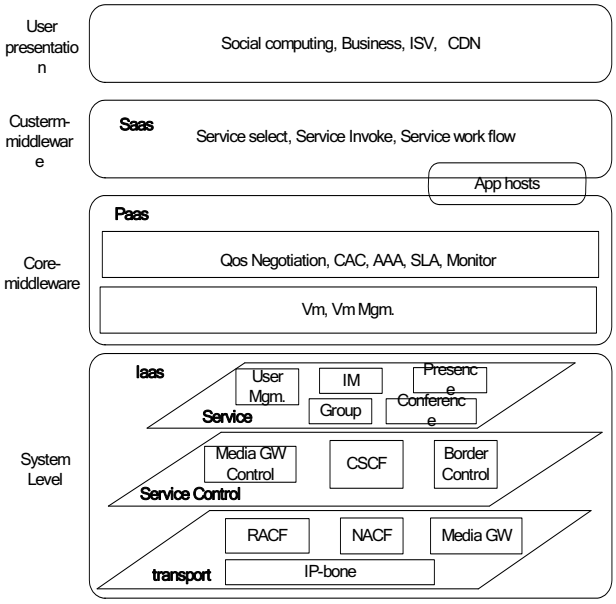

Figure 1. IMS-based Cloud Service

System level is composed mainly by IMS systems, which is at the bottom of the cloud systems. The IMS systems can be considered as the infrastructure of the cloud systems， which make it's the IaaS[7]. The IMS system contains service, control, barrier levels. Therefore, we need to virtualized the physical hardware resources based on the cloud system architecture. The word "physical hardware"

978-0-7695-4816-6/12 $26.00 © 2012 IEEE
DOI 10.1109/ChinaGrid.2012.14

does not means the real physical hardware, we can imagine that through the IMS-system, it virtualized the networks and its capabilities to the network users, as if it "divide" the network and capabilities to several pieces. The virtualized resource may include network processing, network storage, communication services such as CSCFs, presence, conference, IM, locations, and also the control abilities of the network such as NACF, RACF, etc.

The core-middleware is the platform as a service part of the cloud services, constructed based on the IMS-based IaaS. It's the software development and runtime environment, and can also provide the virtual machines and its management. The system users do not have to care about the underlying technical issues such as network, storage, operating system due to this level. Thus , the users can development and deploy their own applications.

Customer-middleware is the software as a service part of this system. It can provide the service the user needed through the Iaas and PaaS. Different customers can get different services by their Business demands and can also achieve the pay-as-needed service mode.

In this system, we implemented the IMS systems, and three services: IM, conference, location. Based on the system and service, we developed several web service in the SaaS level which virtualized the three services to six services in order to provide different customized services for the user, which exists security worries.

III. SLA IN CLOUD SERVICE

When people or enterprises buy network services, they always realize that the availability and performance issues in the cloud are in a weak position. The solution to this problem is that the negotiation to cloud computing services providers and signs a cloud computing SLA.

Cloud computing SLA is an agreement between the cloud services providers and users, similar to the traditional services SLA, the SLA includes the commitment of both security and QoS. The way to commitment: 1) commitment to the user: including availability, failure recovery, data retention commitments, et al.; 2) No commitment to the user: including the planned service disruption, force majeure, the SLA change, security and others; 3) user behavior limitations: including the legality of usage, the legality of software, and so on.

Cloud is a large number of on-demand supplies of virtual resources (such as hardware, software, development platforms and I / O services) of the resource pool. These virtual resources can be dynamically reconfigured based on different load in order to achieve more optimal resource utilization. This resource pool is usually the infrastructure resources services (IaaS), Platform resources services (PaaS) and software resource services (SaaS), and provider manage and develop the pay-as-model of IaaS, PaaS and SaaS in accordance with different SLAs. Therefore, cloud computing SLA can be divided into three categories of IaaS, PaaS and SaaS.

1) In low-level IaaS cloud computing services, the supplier shall ensure the services they provided; your mission is to determine how to measure performance of IaaS services provided by supplier. In IaaS, the speed of your application assigned to the server will be the most variability of the factors, and the availability will be determined by the speed of a new server replacing the failure server in the case of service failure of a server.

2) PaaS is the most problematic part of the SLA terms, because what you get is not a specific commitment to the hardware, but a commitment to a platform which includes a large number of physical hosts and software elements to a certain extent. Determine the number of response time variability may be required to establish a measurement point in the cloud, by this point you can measure the network delay by deducting the end-to-end application delay, so that one can determine the contribution of cloud computing application program.

3) In SaaS, virtual resources include almost everything, because the user does not need to provide any components. Therefore, the cloud computing service providers should have a completely control of cloud, and should prepare a non-network components SLA for all applications.

Cloud computing as a service model, the SLA is affected by the network performance, service quality standards, user-created application performance and cloud computing resources configuration parameters, the research of cloud computing SLA needs to consider these issues, and ultimately, one can obtain an agreement that can control the risk level and make sure that cloud computing services you experienced to meet the enterprise objectives.

IV. SECURITY SLA MANAGEMENT IN IMS-BASED CLOUD SERVICES

Based on the IMS-based cloud services described in section II, we proposed the sSLA scheme of cloud services in order to guarantee the security of the user's information. And the scheme was implemented in the system.

A. Lifecycle management of sSLA

The key problems of sSLA is lifecycle management, which focus on the whole service process from the production to the end of security service provider and consumers. As illustrated in Fig.2,the lifecycle of sSLA contains five main processes. The basic idea and main functions are described as follows:

1) Security Product Development: The stage is the stage of the development of new business and define the appropriate security template. The new security services were deployed to the service environment and the consumer can discover and invoke these services. The template should clearly provide the needs for security: Identify customer security requirements, Identify the security business features(such as security level, Encryption strength, etc). It should be noted that this process is a dynamic process, the provider of security services may often change the provision of its security service capabilities. Therefore, the security

template that must be displayed include a validity period of the representations, expired security template should not be used. The formal description of the security template and information modeling can refer to WSAL(Web service Level Agreement).

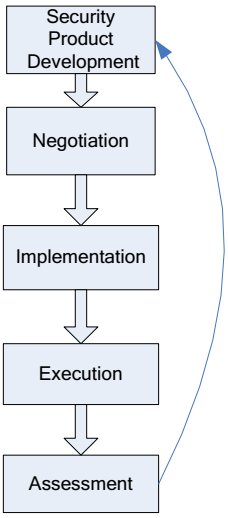

Figure 2. SLA Lifecycle of Security

2) Negotiation: The stage is the stage of the service consumer booked the security services they needed, and security service providers should verify the feasibility and generate orders. Verification process mainly including the verifying if the current system security capabilities can meet the needs of the user, such as the confidentiality strength, authentication security levels, etc. The basic idea is the service provider comprehensively analysis the security abilities of its security services, after several rounds of consultations to reach a formal sSLA, the specific process is indicated in Fig.3.

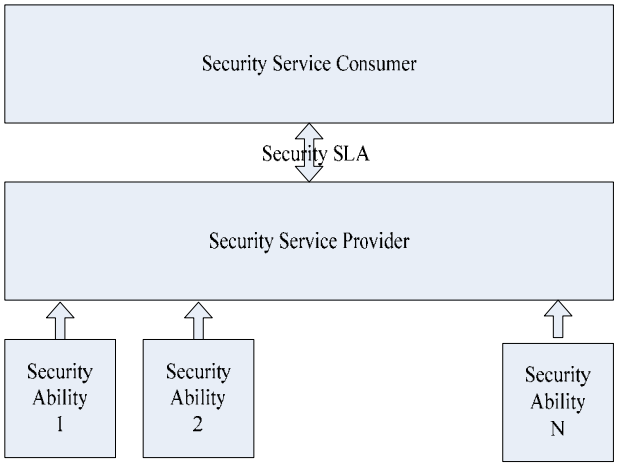

Figure 3. Security Negotiation

3)Implementation:This stage complete the process of the sSLA orders of the security services and users. It complete all the business configuration works before the security services actually delivered. After the configuration, the parameters that negotiated in the phase III were sent to the security services, then the transaction were activated and bind to the service.

4)Execution The stage is the actual use of the services of security services to consumers in acordance with sSLA. Maybe the users try to change the security capabilities during the execution process, however, it should be activated another negotiation phase.

5) Assessment The stage is to assess the the sSLA during the execution stage. It consists of two aspect of assessment. The first is from the users, they based on the negotiated security capabilities, parameters, and the actual implementation to determine whether the service meet their requirements. The second is from the service providers, it assess the overall security capabilities periodically and to improve its technologies and provide better security services

B. sSLA for IMS-based Cloud Services

We developed the sSLA scheme in the IMS-based cloud service environment. Without loss of generality, we assume there were two security service providers(SSP-A, SSP-B, etc) in the system, and the end users access the service providers through IMS Providers.

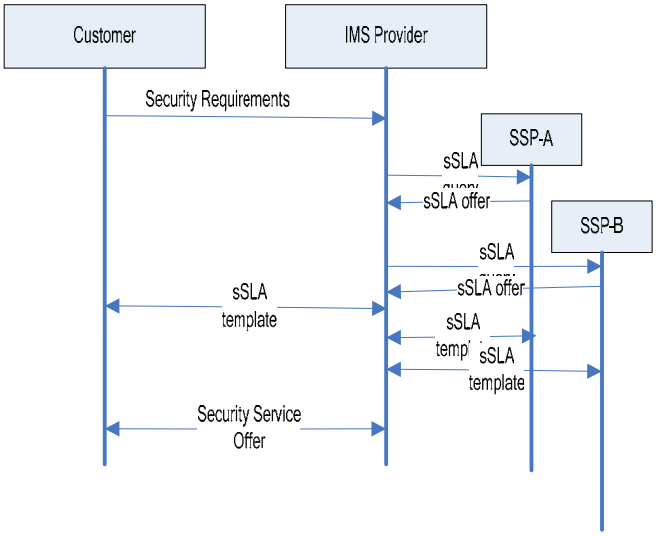

Figure 4. Message flow of sSLA for IMS-based Cloud Service

As Illustrated in Fig. 4. end users give their specific security requirement to the IMS provider through IMS signals. The IMS provider check the appropriate security service through the service delivery platform after the receive of the user request. Security service provider described its security capabilities to the IMS provider. Then the IMS provider choose several SSPs according to their

descriptions, and generate the sSLA template for the end user. If the users agreed with the results, then the contract was signed between the user and IMS provider. The provider serve the user according to the contract at specific security requirements.

Through this process, the user's security needs has rules to follow, and signed in the sSLA template clearly. In the one hand, it added a mandatory requirement on the service provider to protect the user's information, on the other hand, confirmed the user that their information were secured.

V. CONCLUSIONS

Security has always been one of the cloud services need to be taken seriously. By providing sSLA mechanism, enabling service providers need to make a tangible improvement in security capabilities and not just stay in the stage of the 'declaration'. Meanwhile, by the introduction of sSLA mechanism similar to QoS for the SP, it can also bring the revenue for the SP to provide a safe ability, thus it can promote SP's investment in the relevant field. By the means and mechanisms to allow users to have confidence that their data, the information is indeed to be protected, promoted the transfer of users to the cloud service platform, the development of this emerging field of the cloud services.

VI. REFERENCE

[1] M Armbrust, A Fox, R Griffith, AD Joseph, "A view of cloud computing", Communications of the ACM, vol 53(4), pp.50-58, Newyork, April 2010.

[2] Sean Carlin, Kevin Curran."Cloud Computing Security", International Journal of Ambient Computing and Inteligence IJACI . vol 3(1), pp. 14-19, April 2011.

[3] Matjaz B, Ivan Rozman, Bostjan Brumen," Comparison of performance of Web services, WS-Security, RMI, and RMI–SSL", Journal of Systems and Software, vol 79(5), pp. 689-700, My 2006.

[4] Thomas, I.; Warschofsky, R.; Meinel, C. ,"Whom to Trust? Generating WS-Security Policies Based on Assurance Information", 2011 9th IEEE European Conference onWeb Services (ECOWS), IEEE, pp. 65-72, 2011.

[5] Zhang Shu; Song Meina,"An architecture design of life cycle based SLAmanagement", The 12th International Conference on Advanced Communication Technology (ICACT), vol 2, pp. 1351-1355, 2010.

[6] Makaya, C., Dutta, A., Das, S. etc., "Service continuity support in self-organizing IMSnetworks", 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), IEEE,pp. 1-5, 2011.

[7] Ibrahim, A.S., Hamlyn-Harris, J., Grundy, J., "CloudSec: A security monitoring appliance for Virtual Machines in the IaaS cloud model", 2011 5th International Conference on Network and System Security (NSS), IEEE, pp. 113-120, 2011.