A SECURITY MECHANISM FOR CLOUD COMPUTING BASED ON TRUST PLATFORM MODULE

Cheng-Yuan Ku, Department of Information Management, National Chung Cheng University, Chia-Yi County, Taiwan, ROC, 886-5-2721500, cooperku@mis.ccu.edu.tw
Chien-Te Ho, Department of Sport, Health and Leisure, Tatung Institute of Commerce and Technology, Chia-Yi City, Taiwan, ROC, 886-5-3621100, greg0933362477@ms2.ttc.edu.tw

EXTENDED ABSTRACT

With the vigorous development of modern Internet, various network services make our daily life more convenient. In order to comply with the peak demand, many institutions must purchase enough software and hardware. But most of them are not in use during non-peak periods. The cloud computing concept solves the above-mentioned problem and gradually leads the trend of information technology use. Cloud computing is one of the hot issues on the Internet. It allows users to access the service via the Internet anytime and anywhere. Users do not even need the professional skills or own the hardware, software and equipment, they still can get the services and resources they need from cloud computing.

According to the definition from U.S. National Institute of Standards and Technology (NIST), cloud computing can be divided as the following three service modes: (1) software as a service (SaaS); (2) platform Services (PaaS); (3) infrastructure as a service (IaaS). SaaS is to provide the application software services through the Internet. The providers will deploy applications on their own servers and the users can obtain software services remotely in accordance with their own needs. Well-known SaaS vendors include Google, Salesforce and Microsoft. PaaS is to provide a platform of services. Platform users often utilize this service to deploy application of software on the cloud so that they do not need to create their own host or operating system. It contributes significant saving on the time required for software development. Famous PaaS providers include Amazon web services and Google App Engine. IaaS provides IT infrastructure as a service. Through outsourcing, IT infrastructure, including the operation of the storage, servers, firewalls and network components are provided by IaaS providers. IaaS is the most attractive mode of service for many businesses and companies. IaaS vendors include IBM Blue Cloud and Amazon.com. Whether it is based on the cost or the technical considerations, we can imagine why so many enterprises today want to invest in the cloud computing businesses. Though cost reduction and convenience provided by cloud computing, there exists many potential risks in this infrastructure. Therefore, most of enterprises are still wait-and-see. Cloud computing is built in a distributed environment in order to improve the computational efficiency, which also means the user's information or resources may be exposed to unknown threats and cause great challenges to information security. Actually, after users transfer their sensitive data to the cloud, they are unable to make sure whether the cloud service providers carefully and properly handle or save them [1-6].

In this abstract, we try to propose a security mechanism to provide protection for data in cloud by complying with ISO27000 standard. This information security management system is to ensure the following security features: confidentiality, integrity and availability. The security protocol we design, named CloudSec, is located in the application layer as shown in Fig. 1.

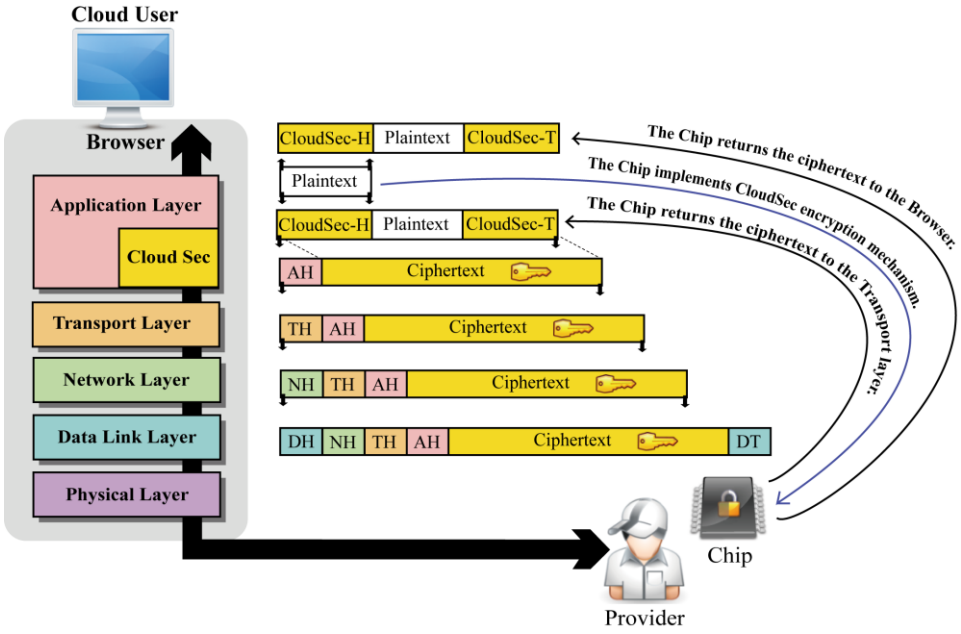

Figure 1. Protocol and packet format of CloudSec

With a security chip embedded in trusted third party (TTP) to assist in selecting, monitoring and auditing the cloud services, the confidentiality, integrity, and availability of data can be protected. Once the cloud computing customers login into the cloud service provider's portal, browsers pop up a message window asking users what feature of security is needed. If nothing is required, it will be handled like general web services. If they need availability, TTP selects the most reliable service providers. If it is integrity required, then TTP chooses two or more service providers and compare the consistency of the computing results. In addition, the CloudSec can achieve authenticity like IPSec's Authentication Header (AH) does. If the customers need confidentiality, then TTP must choose service providers who support CloudSec to provide confidential service like Encapsulation Security Payload (ESP).

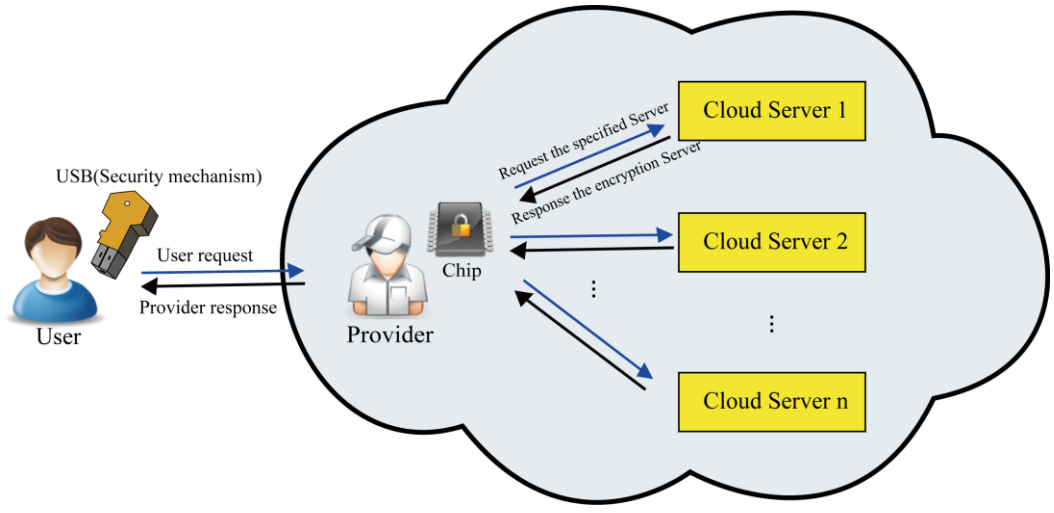

Figure 2. Architecture of security mechanism

Of course, TTP should ensure that these service providers follow CloudSec practices. In addition, the encryption and decryption processes within application layer use firmware validation with digital certificates to increase the authenticability. These tamper resistant devices such as smart card, USB or others, which include a security chip and store important private key, will monitor and audit all

computing procedures. It can ensure that cloud computing brokers and service providers even if the internal staff can not steal or eavesdrop the sensitivity information of customer. Then the service providers can obtain the trust of consumers because all sensitive information is protected. Even if the data is stored in the cloud database, the customers do not have to worry about security issues due to double protection from the application layer and database security. The overall operation of the above-mentioned concept is shown in Fig. 3.

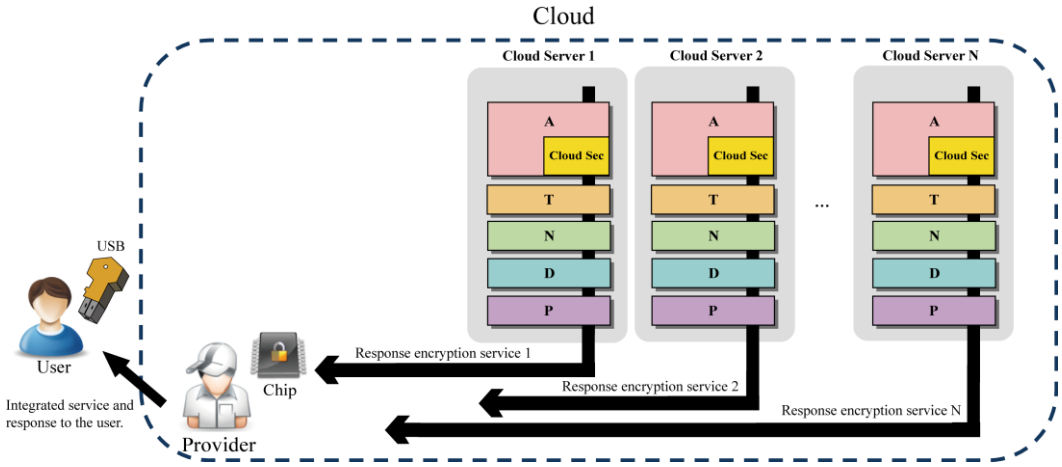

Figure 3. Distributed cloud computing services which support CloudSec

This abstract proposes a security mechanism for cloud computing, which provides data protection for customers. Through security analysis, it can resist many well known attacks including insider attack. We expect to implement a prototype system and test its performance in the near future.

ACKNOWLEDGEMENT

This research is supported by project NSC 101-2410-H-194-005 of National Science Council, Taiwan, R.O.C.

REFERENCES

[1] Nuno Santos, Krishna P. Gummadi, and Rodrigo Rodrigues, “Towards Trusted Cloud Computing,” Proceeding of HotCloud 2009, USA, June 2009.

[2] Imran Khan, Habibur Rehman, and Zahid Anwar, “Design and Deployment of a Trusted Eucalyptus Cloud,” Proceeding of Cloud Computing (CLOUD), 2011 IEEE International Conference on, pp. 380-387, Washington, DC, USA, July 2011.

[3] Xufei Zheng, and Yonghui Fang, “An AIS-based Cloud Security Model,” Proceeding of International Conference on Intelligent Control and Information Processing, August 13-15, 2010.

[4] Joel-Ahmed M. Mondol, “Cloud Security Solutions using FPGA,” Proceeding of Communications, Computers and Signal Processing (PacRim), 2011 IEEE Pacific Rim Conference on, pp. 747-752, 23-26 Aug. 2011.

[5] Dimitrios Zissis, and Dimitrios Lekkas, ”Addressing Cloud Computing Security Issues,” Future Generation Computer Systems, vol. 28, no. 3, pp. 583-592, March 2012.

[6] Flavio Lombardi, and Roberto Di Pietro, ”Secure Virtualization for Cloud Computing,” Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1113-1122, July 2011.