Cloud Computing System Based on Trusted Computing Platform

Zhidong Shen, Li Li
International School of Software
State Key Laboratory of Software Engineering
Wuhan University
Wuhan, China, 430079
zhidongshen@163.com, lli@whu.edu.cn

Fei Yan, Xiaoping Wu
School of Computer
Wuhan University
Wuhan, China, 430079
yfpostbox@yahoo.com.cn, wuxp2002@126.com

***Abstract*—Cloud computing provides people a way to share large mount of distributed resources belonging to different organizations. That is a good way to share many kinds of distributed resources, but it also makes security problems more complicate and more important for users than before. In this paper, we analyze some security requirements in cloud computing environment. Since the security problems both in software and hardware, we provided a method to build a trusted computing environment for cloud computing by integrating the trusted computing platform (TCP) into cloud computing system. We propose a new prototype system, in which cloud computing system is combined with Trusted Platform Support Service (TSS) and TSS is based on Trusted Platform Module (TPM). In this design, better effect can be obtained in authentication, role based access and data protection in cloud computing environment.**

Keywords—cloud computing; trusted service; trusted computing platform; trusted platform module

I. INTRODUCTION

Cloud computing has developed from the grid computing technology. Cloud computing is concerned with the sharing and coordinated use of diverse resources in distributed virtual organizations(VO), which is consisted of different organizes and systems. Cloud computing provides a facility that enable large-scale controlled sharing and interoperation among resources that are dispersedly owned and managed. Security is therefore a major element in any cloud computing infrastructure, because it is necessary to ensure that only authorized access is permitted and secure behavior is accepted. In a word, all members in the cloud and the cloud computing environment should be trusted by each other, and the members that have communication should be trusted by each other. Trust is the major concern of the consumers and provider of services that participate in a cloud computing environment.

Because the cloud computing is composed of different local systems and includes the members from multiple environments, therefore the security in cloud is complicate. In one side, the security mechanism should provide guarantees secure enough to the user, on the other side, the security mechanism should not be too complex to put the users into an inconvenient situation. The openness and flexibility of the computer and popular commercial operating systems have been important factors supporting their widespread adoption. However, that very same openness and flexibility have been proved to be a double edged sword, because it brings complexity, reduces trust degree and threat against security. So there should be a balance between the security and the convenience. The dependable and secure computing includes not only security and confidentiality, but also reliability, availability, safety and integrity [1,2,3]. In this paper, we propose a new way that is conducive to improve the secure and dependable computing in cloud. In our design, we integrate the Trusted Computing Platform (TCP), which is based on Trusted Platform Module (TPM), into the cloud computing system. The TCP will be used in authentication, confidentiality and integrity in cloud computing environment. We also design a software middleware, the Trusted Platform Software Stack (TSS), on which the cloud computing application can use easily the security function of TPM.

II. RELATED WORK ABOUT CLOUD COMPUTING SECURITY

Cloud computing developed from the grid computing technology and paid attention to provide distributed service to different users. A typical cloud model described by Frank Gillett [4] is shown in Fig.1. that model does not seem to address end-to-end management. Ultimately, the cloud service infrastructure must provide end-to-end service assurance to meet both service creation and service delivery platform user requirements. The service creators must be able to develop services rapidly using

978-0-7695-4077-1/10 $26.00 © 2010 IEEE
DOI 10.1109/ICICTA.2010.724

reusable and collaborating service components available globally. The infrastructure must also accommodate billions of users globally who will contribute to wildly fluctuating workloads.

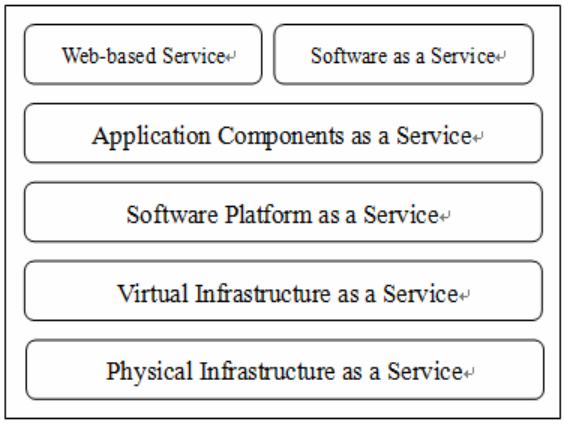

Figure 1. A kind of Cloud Computing Model

In this model, the cloud computing security can be provided as security services. Security messages and secured messages can be transported, understood, and manipulated by standard Web services tools and software. This mechanism is a good choice because the web service technology has been well established in the network-computing environment. Even the mechanism for the cloud computing security has many merits now, but there are still some disadvantages. For example, there is short of the mechanism on the hardware to support the trusted computing in cloud computing system. The trusted root in cloud computing environment has not been defined clearly. The creation and protection of certificates are not secure enough for cloud computing environments. In the cloud computing, many users participate in the VO and they join or leave VO dynamically. Other resources in the cloud computing environments are the same too. Users, resources, and the VO should establish the trustful relationship among themselves. And they will be able to deal with the changing dynamically. The VO includes distributed users and resource from distributed local systems or organizes, which have different security policies. According to this reason, how to build a suitable relationship among them is a challenge. In fact, the requirements for the security in cloud computing environment have some aspects in the follow:

- Confidentiality. The information belongs to different owners in the cloud computing resources should be open to the trusted objects. Unauthorized people or other entities should be forbidden from that information.
- Dynamic of the services. The cloud computing system should also be able to provide services to users dynamically. This dynamic mechanism gives the user convenience to use the services and resources in the cloud computing environment. Then the security can be treated as the dynamic services too.
- The trust among the participant. As described above, the participants, including users, local organizes and distributed resources, should build trust relationships among the entities that will have mutual operation to each other. The trusted relation is based on the authentication.
- Dynamically building trust domains. In the cloud computing system, participants need to organize dynamically to solve different problems. So the relationship among them changes dynamically too. Then the VO needs to establish dynamically the trust domain including the participants, such as the users and the resources, which span multiple organization or systems.

III. BUILD TRUSTED CLOUD COMPUTING ENVIRONMENT

A. Trusted Cloud Computing based on TCP

The Trusted Computing Group (TCG) provided the trusted computing technology. This distinguishing technology is arguably the incorporation of "roots of trust" into computer platforms. Because one of the biggest issues facing computer technology today is data security, and the problem has gotten worse because users are working with sensitive information more often, while the number of threats is growing and hackers are developing new types of attacks, many technology researchers advocate development of trusted computing systems that integrate data security mechanism into their core operations, rather than implementing it by using add-on applications. In this concept, TC systems would cryptographically seal off the parts of the computer that deal with data and applications and give decryption keys only to programs and information that the technology judges to be trusted. The TCG made this mechanism as their core criteria to define the technology specification. The word trust is defined as "A trusted component, operation, or process is one whose behavior is predictable under almost any operating condition and which is highly resistant to subversion by application software, viruses, and a given level of physical interference." TCP operates through a combination of software and hardware: manufacturers add some new hardware to each computer to support TC functions, and then a special TC operating system mediates

between the hardware and any TC-enabled applications. [5, 6]

The trusted computing mechanism can provide a way that can help to establish a security cloud computing environment. The model of trusted computing is originally designed to provide the privacy and trust in the personal platform and the trusted computing platform is the base of the trusted computing. Since the internet computing or network computing has been the main computing from the end of the last century, the model of trusted computing is being developed to the network computing, especially the distributed systems environment. The cloud computing is a promising distributed system model and will act as an important role in the e-business or research environments. As web service technology have developed quickly and have been used broadly, cloud computing system could evolve to cloud computing service, which integrates the cloud computing with web service technology. So we could extend the trusted computing mechanism to cloud computing service systems by integrating the TCP into cloud computing system. Trusted computing platform provide the basis for trusted transactions to occur, and trusted computing technologies must allow stakeholders to express policies and have those policies negotiated and enforced in any execution environment.

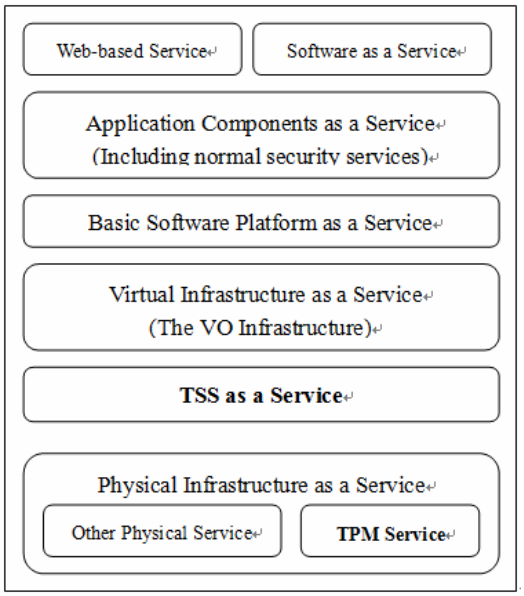

Figure 2. The Architecture of Cloud Computing Based on TCP

In Fig.2, the architecture of cloud computing based on TCP is described. The upper layer services in can lodge the security service provided by TPM through the TSS layer. The TSS layer stays on every trusted platform enabled by TCP. TSS can communicate directly with TPM and provide the interface to upper layer application components. The virtual infrastructure will be built dynamically and VO is built on it too.

B. Role Based Access Control Model in cloud computing environment

In the cloud computing system, there are a great number of users who hope to make the access to the cloud computing service. They do have their own goal and behavior. If the cloud computing systems hope to deal with them one by one, there will be a great hard work. In order to reduce the complication of the access control model, we can classify them into several classes or groups and make the access control criteria for these classes. So the users should firstly register themselves into one or some of the classes and get some credential to express their identities. When they make the access to the cloud computing resource or hope to get the cloud computing service, they should take their full ID, which includes their personal identities or the classes/group. Then the objective environment will have a relative simple way to control their accessing. In the TPM, the root of trust in integrity reporting is fulfilled. And the reporting could be delivered to the remote machine via the network. By using the remote attest function, the user in the TCP could to notify their identities and relevant information to the remote machine that they want to make access to. And each objective environment has the mechanism to clarify the accessing entity's information about their identity, role, and other information about the security. The user should bind their personal ID used for TCP, the stander certificate, such as X.509, took from the CA, and the role information together. And the cloud computing system has the according mechanism to verify this information about each user. The cloud computing service should present which role it will give the permission, when the cloud computing service notifies itself to the cloud -computing environment. So the user will able to know whether he could make access to that cloud computing service before his action. The hardware maintains a "master secret key" for each machine, and it uses the master secret to generate a unique sub-key for every possible configuration of that machine. As a result, data encrypted for a particular configuration cannot be decrypted when the machine is in a different configuration. When one machine wants to join the cloud computing, it will show its certificate and generate session key with other cooperators buy using the unique sub-key. If the configuration in the local machine is changed, the session-key will also be not useful. So in the distributed environment, we can use this function to transmit data to remote machine and

this data can be decrypted when the remote machine has certain configuration.

C. TSS and cloud computing system

TSS components are the major parts of the TCP enabled cloud computing。 It provides fundamental resources to support the TPM. In our design, TSS should be a bridge between the up-application and the low-hardware. As depicted in Fig.3, TSS includes two layers, the TSS service provider (TSP) and TSS core services (TCS). The applications call the function of TSP. TSP provides some basic security function modules. These basic modules send calls to TCS. Then TSS converts these calls to according TPM instructions. Since TPM is hardware, the TCG Device Driver Library (TDDL) is necessary. TDDL convert the calls from TCS to the TPM orders. After the TPM process the order, it will return the results up forward. Each layer gets results from low layer and coverts them to responding results that the up layer needs.

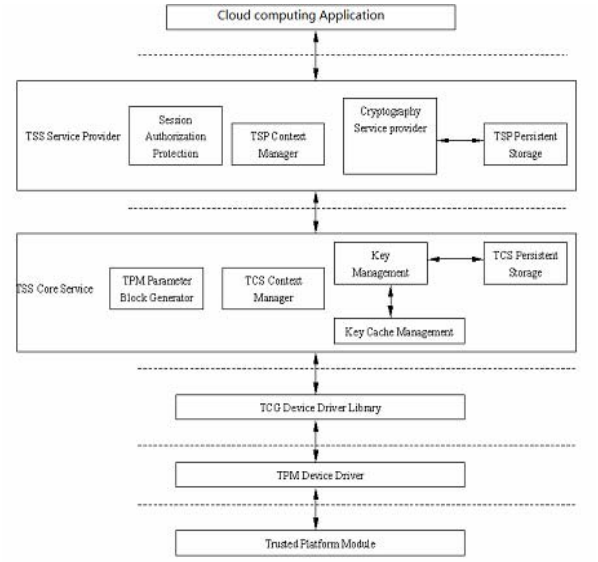

Figure 3. TSS Architecture for cloud computing based on TCP

IV. CONCLUSIONS

In this paper, we analyzed the security of cloud computing environment and described the function of trusted computing platform in cloud computing. The advantages of our proposed approach are to extend the trusted computing technology into the cloud computing environment to achieve the trusted computing requirements for the cloud computing. TCP with TPM is used as the hardware base for the cloud computing system. In our design, TCP provides cloud computing system some important security services, such authentication, role based access and data protection. The trusted hardware function will be lodged through the TSS which plays a link role to upper layer services. Trusted cloud computing is built on the trusted computing platform and can provide flexible security services for users.

ACKNOWLEDGEMENT

Our work is supported by the Research Fund for the Doctoral Program of Higher Education (No.20090141120024), the foundation of State Key Laboratory of Software Engineering (No.SKLSE2008-07-16), the Independent Research Projects of Wuhan University (No.6082023), and Hubei Municipal Natural Science Foundation (No. 2009CDB140). We also got help from researchers of laboratory of information security of the school of computer at Wuhan University.

REFERENCES

[1] Kevin Sloan, “ecurity in a virtualised world”, Network Security, August 2009, page(s)15-18.

[2] Jason Reid Juan M. González Nieto Ed Dawson, "Privacy and Trusted Computing", Proceedings of the 14th International Workshop on Database and Expert Systems Applications, IEEE, 2003.

[3] Algirds Avizienis, Jean-Claude Laprie, Brian Randell, and Carl Landwehr, “Basic Concepts and Taxonomy of Dependable and Secure Computing”, IEEE transactions on dependable and secure computing, vol.1, No.1, January-March, 2004.

[4] Frank E. Gillett, “Future View: The new technology ecosystems of cloud, cloud services and cloud computing” Forrester Report, August 2008.

[5] Trusted Computing Group (TCG), "TCG Specification Architecture Overview Specification Revision 1.2", April 28, 2004.

[6] "Trusted Computing Platform Alliance (TCPA) Main Specification Version 1.1b", Published by the Trusted Computing Group, 2003.

[7] Dr.Rao Mikkilineni, Vijay Sarathy, “Cloud Computing and the Lessons from the Past”, the 18th IEEE international Workshops on Enabling Technologies: Infrasturctures for Colloaborative Enterises, on page(s):57-62, 2009

[8] Balachandra Reddy Kandukuri, Ramacrishna PaturiV, Atanu Rakshi, “Cloud Security Issues”, 2009 IEEE International Conference on Services Computing, pages(s):517-520.

[9] N. Santos, K. P. Gummadi, and R. Rodrigues. Towards trusted cloud computing. In USENIX HotCloud, 2009.

[10] M. Smith, M. Schmidt, N. Fallenbeck, T. Doernemann, C. Schridde, and . Freisleben, “Secure On-demand Grid Computing,” Journal of Future Generation Computer Systems, vol. 25, no. 3, pp. 315–325, 2009.

[11] Tal Garfinkel, Mendel Rosenblum, and Dan Boneh, "Flexible OS Support and Applications for Trusted Comput-ing", the 9th Workshop on Hot Topics in Operating Systems (HotOS IX), USENIX, 2003.