2010 2nd International Conference on Signal Processing Systems (ICSPS)

The Security of Cloud Computing System enabled by Trusted Computing Technology

Zhidong Shen
International School of Software,
Wuhan University,
Wuhan, China, 430079
zhidongshen@163.com

Qiang Tong
School of Software,
Northeastern University,
Shenyang, China, 110004
qiang.tong@163.com

Abstract—**Cloud computing provides people the way to share distributed resources and services that belong to different organizations or sites. Since cloud computing share distributed resources via the network in the open environment, thus it makes security problems important for us to develop the cloud computing application. In this paper, we pay attention to the security requirements in cloud computing environment. We proposed a method to build a trusted computing environment for cloud computing system by integrating the trusted computing platform into cloud computing system. We propose a model system in which cloud computing system is combined with trusted computing platform with trusted platform module. In this model, some important security services, including authentication, confidentiality and integrity, are provided in cloud computing system.**

Keywords-cloud computing; trusted computing platform; trusted computing; trusted service

I. INTRODUCTION

Since distributed systems and network computing were used wildly, security has become an urgent problem and will be more important in the future. In order to improve the work efficiency, the different services are distributed in different servers that are distributed in different places. In contrast to the fast developing of distributed computing technologies, people have remained insufficient in the field of information security and safety. In recently, a new trend attracts people's attention. Users from multiple environment hope use the distributed computing more efficient, just like using the electric power. Then, cloud computing has become a new star for this demand. cloud computing is concerned with the sharing and coordinated use of diverse resources in distributed organizations --- cloud, 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 [5]. The dependable and secure computing includes not only security and confidentiality, but also reliability, availability, safety and integrity [10]. Considering these facts, 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. The TCP can improve the cloud computing security and will not bring much complexity to users. Because the TCP is based on relatively independent hardware modules, it does not cost too much resource of CPU, and can improve the performance of processing cryptographic computation. We also design a software middleware, the Trusted Platform Support Service (TSS), on which the cloud computing application can use easily the security function of TPM.

II. RELATED WORK ABOUT CLOUD COMPUTING SECURITY

A. *Current Security model of the cloud computing*

In order to archive security in cloud computing system, some technologies have been used to build the security mechanism for cloud computing. The cloud computing security can be provided as security services. Security messages and secured messages can be transported,

978-1-4244-6893-5/$26.00 © 2010 IEEE

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. The performance is reduced apparently when the cryptographic computing are processed. There are also lack of some mechanisms to register and classify the participants carefully, such as the tracing and monitoring for them. In the following section, we will analyze the challenge for the cloud computing security in deep.

B. *The challenge for the security in cloud computing*

In cloud computing environment, many users participate in the CLOUD and they join or leave CLOUD dynamically. Other resources in the cloud computing environments are the same too. Users, resources, and the CLOUD should establish the trustful relationship among themselves. And they will be able to deal with the changing dynamically.

The CLOUD 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, including confidentiality. multiple security policy, dynamic of the services., the trust among the entities, dynamically building trust domains.

In the next section, we will propose the mechanism of trusted computing platform and other related functions that aid to achieve the trusted cloud computing, which has a trusted computing environment.

III. TRUSTED COMPUTING TECHNOLOGY

A. *Trusted Computing Technology*

In recent years, increased reliance on computer security and the unfortunate fact of lack of it, particularly in the open-architecture computing platforms, have motivated many efforts made by the computing industry. In 1999, HP, IBM, Compaq, Intel, and Microsoft announced the formation of the Trusted Computing Platform Alliance (TCPA) that focused on building confidence and trust of computing platform in e-business transactions. In 2003, the Trusted Computing Group (TCG) was formed and has adopted the specifications developed by TCPA. The distinguishing feature of TCG 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 (TC) 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 [9]. 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."[1]

B. *The Trusted Computing Platform*

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. TCP provides two basic services, authenticated boot and encryption, which are designed to work together. An authenticated boot service monitors what operating system software is booted on the computer and gives applications a sure way to tell which operating system is running. It does this by adding hardware that keeps a kind of audit log of the boot process.

On the computer platform with TCP, the TPM is used to ensure that each computer will report its configuration parameters in a trustworthy manner. Trusted platform software stack (TSS) provides the interfaces between TPM and other system modules. The platform boot processes are augmented to allow the TPM to measure each of the components in the system (both hardware and software) and securely store the results of the measurements in Platform Configuration Registers (PCR) within the TPM.

IV. BUILD TRUSTED CLOUD COMPUTING SYSTEM USING TCP

As what we have discussed above, the trusted computing mechanism can provide a way that can help to establish a security 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.

In the network computing environment, trust will go on to envision a connected, digital world in which trusted entities would interact with one another in much the same way individuals and businesses interact in traditional commercial relationships. "The digital universe requires that parties to a common transaction be able to trust that their mutually agreed upon intents will be fulfilled and their rights protected. For true commerce automation to exist, trading partners must know what to expect from each other's systems."[8]. Trusted computing, therefore, must 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.

A. Authentication cloud computing environment with TCP

In cloud computing environment, different entities can appeal to join the CLOUD. Then the first step is to prove their identities to the cloud computing system administration. Because cloud computing should involve a large mount of entities, such as users and resources from different sources, the authentication is important and complicated. Considering these, we use the TCP to aid to process the authentication in cloud computing.

The TCP is based on the TPM. The TPM is a logic independent hardware. It can resist the attack from software, and even the hardware attack. The TPM contain a private master key which can provide protect for other information store in cloud computing system. Because the hardware certificate can store in TPM, it is hard to attack it. So TPM can provide the trust root for users.

Since the users have full information about their identity, the cloud computing system can use some mechanism to trace the users and get their origin. Because in the TCP the user's identity is proved by user's personal key and this mechanism is integrated in the hardware, such as the BIOS and TPM, so it is very hard to the user to make deceiving for their identity information. Each site in the cloud computing system will record the visitor's information. So by using the TCP mechanism in cloud computing, the trace of participants can be known by the cloud computing trace mechanism.

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 order to reach the goal of trusted computing, the users should come from the trusted computing platform, and take the security mechanism on this platform to achieve the privacy and security for themselves. The user has his personal ID and secrete key, such as the USB Key, to get the right to use the TCP. They can use the decryption function to protect their data and other information.

When the machine starts booting, the TC hardware computes the cryptographic hash of the code in the Boot ROM and it writes that hash into the tamper-resistant log. Before it brings in the next block of code, the code from the Boot ROM computes the hash of the next block and appends it to the end of the tamper-resistant log. In turn, each chunk of code adds to the log the hash of the next chunk that will load. This process continues until the entire OS is booted, at which point the tamper-resistant log contains a record that can establish exactly which version of which OS is running. The TC contains part called certifying. It is helpful for the TC hardware to know via its log what software configuration is running on a machine. TC can certify that a known OS version is running, and then that OS can certify the application's precise configuration. If you trust TC and the OS, then you can be confident that you know the application's configuration. A configuration certificate can be presented to any recipient—the user or the program running on another computer in the cloud computing environment—and the recipient can verify that the certificate is valid and up-to-date, so it can know what the machine's configuration is. This mechanism provides a way to help the participants in the cloud computing systems to build relationship among the ones that have mutual action.

The trusted computing platform's boot sequence is illustrated. The beginning of the boot is the BIOS boot block. 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. Moreover, a role hierarchy is introduced to reflect inheritance of authority and responsibility among the roles. If a user has a user-role certificate showing membership in role R, and a cloud computing service requires role r, the user should be able to get permission. On the other hand, the resource owners should also use this mechanism to express their identities, and get the rights to provide their resources to other users.

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 encryption is another major mechanism in our design. This function lets data be encrypted in such a way that it can be decrypted only by a certain machine, and only if that machine is in a certain configuration. This service is built by a combination of hardware and software application. 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.

The user login the CLOUD from the TCP, which is based on the Trust Platform Module (TPM), and get the certificate from the CA, which is trusted by the cloud. When the participant wants to communicate with remote entity, it will carry all the information, including the personal ID, certificate and role information. And the information between them is protected buy their session key.

C. Data Security in cloud based on TCP

With the TCP, the different entities can communicate in a security way. The TCP generate random numbers and then create session keys. The random keys created by physical hardware have the security characteristics better than those generated just by software programs. The security communication protocols use the system in cloud to call TSS to use the TPM. Then TPM provides the encryption key and session key to the communicators in cloud computing. With its computing capacity, TPM can burden some computation work from CPU and improve the performance.

The important data stored in the computer can be encrypted with keys generated by the TPM. When accessing to these data, the users or applications should pass firstly the authentication with TPM, and encryption keys are stored in the TPM, which makes it hard to attack these keys. To prevent the attack for integrity of data, the hash function in TPM is used. The TPM will check the critical data in a certain interval to protect the integrity of data. The processes of encryption and integrity check use TSS to call the function of TPM.

D. The Trace of the User's Behavior

Since the users have full information about their identity, the cloud computing system can use some mechanism to trace the users and get their origin. Because in the TCP the user's identity is proved by user's personal key and this mechanism is integrated in the hardware, such as the BIOS and TPM, so it is very hard to the user to make deceiving for their identity information. Before the distributed machine cooperates to do something, they should attest their local information to the remote site. When the user login the cloud computing system, his identity information should be recorded and verified at first. Each site in the cloud computing system will record the visitor's information. So if the TCP mechanism is integrated into the cloud computing, the trace of the participants, including the users and other resources, can be knew by the cloud computing trace mechanism. Then if the participants do some malicious behavior, they will be tracked and be punished. In order to achieve the trusted computing in the cloud computing system, we should have the mechanism to know not only what the participants can do, but also what the participant have done. So the monitoring function should be integrated into the cloud computing system to supervise the participants' behavior. In fact, reference monitors have been used in the operation system for more than several decades, and it will be useful in cloud computing too.

V. CONCLUSIONS

We have analyzed the trusted computing in the cloud computing environment and 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 and then fulfill the trusted cloud computing. TCP is used as the hardware base for the cloud computing system. In our design, TCP provides cloud computing system some important security functions, such authentication, communication security and data protection. Related methods for these implementations are proposed.

The TCP provides cloud computing a secure base for achieve trusted computing. But how to integrate well these hardware modules with cloud computing system is a challenging work and need more deep research. Now we are developing an model system of trusted cloud computing, which is based on the trusted computing platform and can provide flexible security services for users. We will make the actual design more practical and operational in the future.

ACKNOWLEDGEMENT

Our work is supported by the Fundamental Research Funds for the Central Universities (No.6082023), the foundation of State Key Laboratory of Software

Engineering (No.SKLSE2008-07-16), the Research Fund for the Doctoral Program of Higher Education(No.20090141120024), 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] 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

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

[3] Peter Wayner, “Cloud versus cloud – A guided tour of Amazon, Google, AppNexus and GoGrid”, InfoWorld, July 21, 2008

[4] Glen Bruce, Rob Dempsey, "Security in Distributed Computing", Published by Prentice Hall, Copyright Hewlett-Packard Company, 1997.

[5] 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.

[6] ISO/IEC. Information technology - Open Systems Interconnection - Evaluation criteria for information tech-nology, 1999. Standard ISO/IEC 15408.

[7] Martín Abadi, "Logic in Access Control", Proceedings of the 18th Annual IEEE Symposium on Logic in Com-puter Science (LICS'03), 2003.

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

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

[10] 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.

[11] Cloud Security Alliance: ‘Security Guidance − Critical Areas of Focus in Cloud Computing ’ , April 2009, 10 July 2009 http://www.cloudsecurityalliance.org/guidance/csaguide.pdf

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