Volume 2, Issue 12, December 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Framework for Security Based Cloud by using Trusted Computing

Hari Baaskar R*, Gomathi A
**Assistant Professor, Dept of CSE, Narasu's Sarathy Institute of Technology, TamilNadu.*
Associate Professor, Dept of CSE, Narasu's Sarathy Institute of Technology, TamilNadu.

Abstract- Cloud Computing in cloud environment consists of a vast area for storing data. The data can be shared through distributed resources. While transferring data through the cloud, security parameters like authentication, confidentiality, integrity, and role based access and data protection will affect. In this article, I proposed an architecture which consists of Trusted Computing Platform (TCP) with Trusted Platform Module (TPM) that solves the issues which arises during the data transfer in a cloud computing network.

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

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. Users from multiple environment hope use the distributed computing more efficient, just like using the electric power. 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.

The dependable and secure computing includes not only security and confidentiality, but also reliability, availability, safety and integrity. 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. (e.g. [2], [3])

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. 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. 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 reusable and collaborating service components available globally. 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. 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 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. 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: (e.g. [3])

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 Environment

A. *Trusted Cloud Computing*

Trusted Computing technologies, in the sense defined by the Trusted Computing Group, revolve around capabilities enabled by the addition of a hardware device called a Trusted Platform Module (TPM) to a computing system. TPMs are small embedded computing devices which provide a specific, standard set of operations to the host platform. These devices are typically built using small (8-bit) processors with embedded firmware to provide the operations, and since these devices serve as a hardware root of trust for the computing platform, it is vital that the operations work as defined and not be modifiable or 'hackable' by a user (although the specification provides a mechanism for the manufacturer to perform an authenticated firmware update). Trusted Platforms (systems incorporating a TPM) potentially have many interesting applications, and several re-searchers have considered what could be possible if a modified set of operations were provided by the TPM. Examples include using TPMs to provide count-limited objects, to instantiate random oracles, to support verifiable encryption and fair exchange, or to support privacy-preserving operations. Unfortunately, the previously described reasons why end-user updating of TPM firmware would destroy the basic trust in this hardware mean that directly experimenting with these applications of modified TPMs is impossible by people outside of the companies that manufacture the TPMs.

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.

C. *TSS Stack*

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. 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.

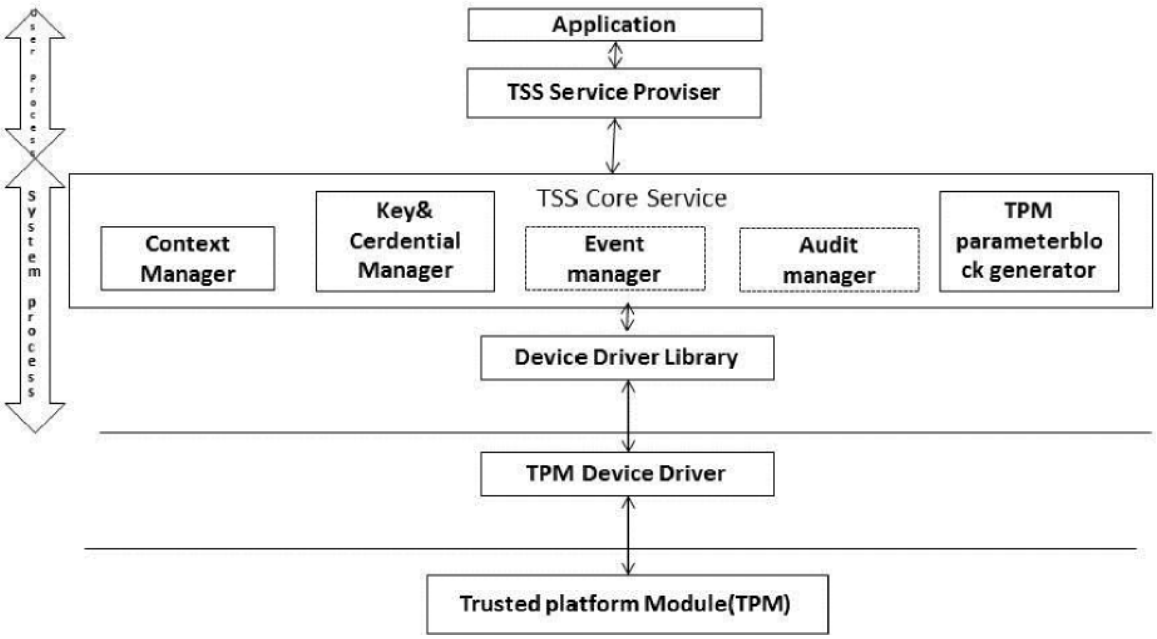

Figure 1. TSS Stack Structure

As shown in Figure 1 TSS Stack, the TSS stack is comprised of TPM device drivers; TSS core services (TCS) and the TSS service provider (TSP). The TPM device driver is a hardware specific driver typically provided by the TPM vendor. The device driver library interface provides a common standard TPM interface for all the applications. TSS Core Services (TCS) provides the infrastructure required to manage keys and credentials, serialization of commands to the TPM, and context, event & audit management. Applications communicate to the TCS using the TSS Service Provider (TSP) layer. The TSP is the topmost component in the stack and provides TPM services for applications.

IV. Build Trusted Cloud Computing System

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. 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. 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 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. (e.g. [4])

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. Conclusion

The proposed approach shows hardware based security architecture by using trusted computing platform (TCP) with trusted platform module (TPM) enabled system components which makes user data more secure and reliable. This architecture can be applied for a single user in a particular system alone, so we have to improve the security parameter and user mobility.

REFERENCE

[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] Kevin Sloan, *"Security in a virtualized world"*, Network Security, August 2009, page(s)15-1 8.
[3] Balachandra Reddy Kandukuri, Ramacrishna PaturiV, Atanu Rakshi, *"Cloud Security Issues"*, 2009 IEEE International Conference on Services Computing, pages(s):517-520.
[4] Frank E. Gillett, *"Future View: The new technology ecosystems of cloud, cloud services and cloud computing"*, Forrester Report, August 2008.
[5] Cloud Security Alliance: ~Security Guidance ~ Critical Areas of Focus in Cloud Computing ~, April 2009, 10 July 2009 http://www.cloudsecurityalliance.org/guidance/csaguide.pdf
[6] 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.

AUTHOR:

He is now working as Assistant Professor in Narasu's Sarathy Institute of Technology**.** He completed his Post Graduate from Anna University of Technology Coimbatore and Bachelor degree from Mahendra Engineering College. His area of interest is cloud computing, and he participated in several workshop and conferences.

She is now working as Associate Professor/Head of Computer Science and Engineering Department in Narasu's Sarathy Institute of Technology**.** She is doing her Research work in Anna University Chennai, completed her Post Graduate at Sona College of Technology, Salem and Bachelor degree at SRM Easwari Engineering College, Chennai. Her area of interest is data mining. She published her research papers in various reputed journals, participated in several workshops and conferences.

