Data Security Isolation Methods and Practices Based on Different Cloud Environments

Yu Cong, Wang Tingting, Wen Lei, Gao Ruohan, Li Yan

NARI Group co.,LTD., Nanjing, Jiangsu 211100, China

Keywords: Cloud environment, trust, data security.

Abstract: Since co-residency virtual machines in a cloud environment share the physical resources, making some malicious users stealthily obtain others' private information through detecting and analyzing the physical resources, which brings the potential threat of the Side-Channel-Attacks and challenged the isolation among co-residency virtual machines in a cloud environment. In view of this, this paper researches the virtual machine security isolation mechanism in cloud environment. In order to build a reliable cloud environment security system and solve the trust and data security problems of cloud environment, a cloud environment isolation mechanism based on trusted computing architecture is proposed and implemented. Combined with the mechanism of cloud environment itself, a research scheme is proposed from the isolation of network architecture. The validity of related models and schemes is verified by experiments and process analysis respectively.

1. Introduction

With the change of people's demand and the transformation of Internet service mode, cloud computing technology has been widely used. It is based on Internet technology, characterized by high performance and large scale. It provides users with computing resources and Shared resources through the principle of resource sharing and on-demand distribution. For cloud computing technology, its basis is virtualization technology [1,2], which builds a computing platform for users, thus allocating resources for each user and providing an independent virtual computing environment. With the rapid development and popularization of cloud computing technology, people gradually get used to and enjoy the convenience brought by various cloud applications in their daily life. The development of cloud computing technology not only conforms to the law of Internet development, but also is the inevitable trend of modern information technology progress.

However, as cloud computing is more and more widely used in People's Daily life, its security problems are gradually emerging in front of people. For cloud computing, the most important requirement of its security problem is to protect the security of users' virtual resources, that is, to ensure the security of virtual machines in the cloud environment. In the traditional research, the protection of virtual machine is mainly to prevent the malicious application on the virtual machine from penetrating attacks, affecting the security of the physical machine where the virtual resources are located. The security problem of cloud computing is mainly because the traditional security scheme cannot meet the characteristics of cloud environment. In the cloud environment, virtualization technology is taken as the implementation basis and on-demand allocation is taken as the resource sharing mode, which results in the lack of a trusted root of physical significance in the cloud computing environment compared with the traditional security technology solution.

This paper focuses on solving the problem of mutual trust. Trusted computing technology [3] is adopted to make up for the trust problem of cloud environment system. Trusted computing starts from entity trusted root and measures step by step to build a trust chain and transfer the trust relationship step by step. It is an important way to build an integrated trusted system from terminal to network.

  DOI: 10.25236/mmmce.2019.108

2. Measurement Authentication of Trusted Computing Techniques

In the measurement process of the trusted calculation, the trust chain is established and the trust relationship is extended to the whole system by starting from a trusted root and measuring and trust level by level[4].

As shown in figure 1, the system starts from the trusted root to measure the BIOS, LOADER, the start of the operating system, and the applications in the system, and transfers the permissions of the measures successively. After all the measures are passed, the whole system is measured step by step.

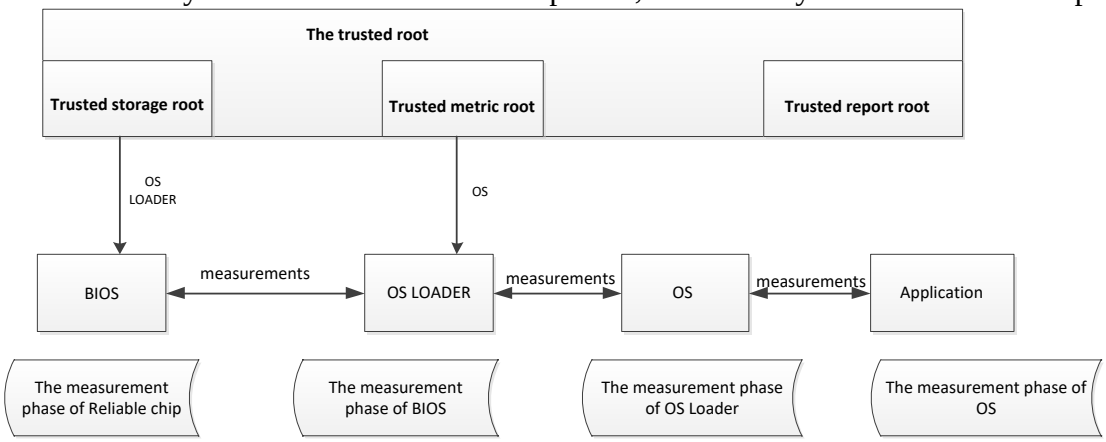

Fig. 1 Step by step Measurement of Trusted Computing

Among them, the trust root is the foundation of trusted computer system. In the definition of TCG, a trusted computing platform consists of three trust roots, that is, the trusted measure root RTM, the trusted storage root RTS, and the trusted report root RTR. As shown in figure 2:

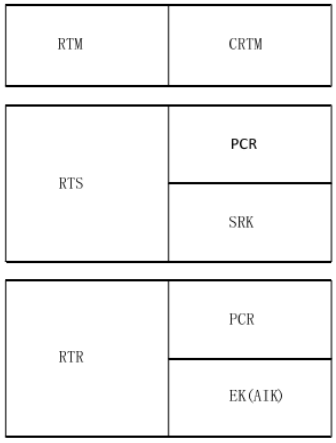

Fig. 2 Trusted Root Structure

3. Architecture of a Trusted Isolation Solution for a Cloud Environment

You can design an architecture diagram of a trusted isolation mechanism as shown in the figure. As shown in figure 3, it is horizontally divided into management area and computing area. The management area performs system management, security management and audit management of cloud computing environment, while the computing area manages related resources. Vertically speaking, computing area is divided into physical resource environment and virtual machine resource environment. The virtual machine resource environment obtains the allocated physical machines through the virtual machine manager, thus providing cloud computing virtualization environment for cloud users and supporting cloud users to apply in the virtualization environment. The management area manages the physical resource environment through the resource management environment, including resource security management server, cloud system management center, etc., to deal with

the deployment, management and allocation of physical resources, and provide resource support for the upper-level users' virtual environment. In the virtual application layer, the cloud application security management server is responsible for the management of virtual machine resources, the configuration of virtual computing environment and software deployment, and the operation of user applications. The terminal is connected to the environment via a boundary control device[5].

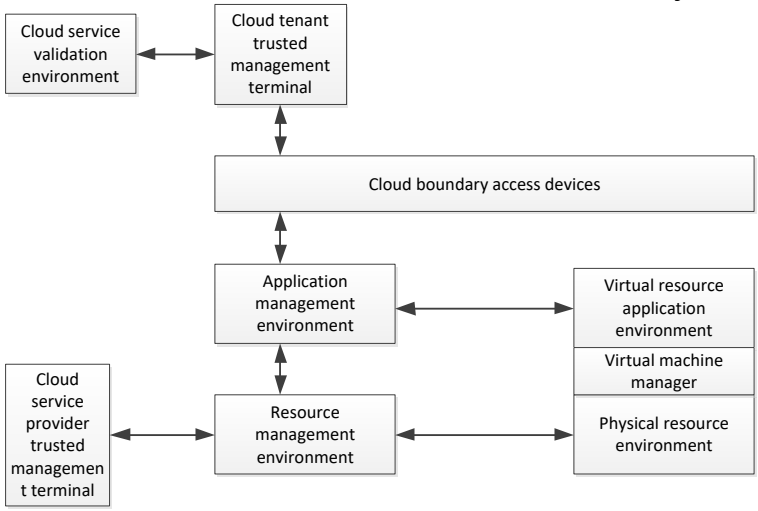

Fig. 3 Trusted Cloud Architectures Isolation Mechanism

4. The Trusted Benchmark Library Generates Tests

Firstly, on the computing platform, the host computer platform is calculated and measured according to the aforementioned trusted policies through the trusted audit mechanism of the host computer, and the terminal interface of the trusted verification server is logged in for viewing. The terminal display results are shown in figure 4:

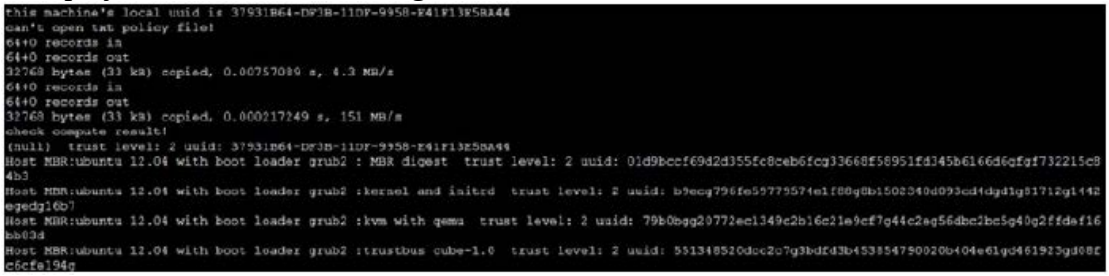

Fig. 4 Host Platform Reference Value Generation

During this process, the trusted metric program first performs IO operation, reads the host platform related information, and then calculates the key file summary value generation strategy. Here, the trust level is defined as 2 for the host platform, so the trust level output is 2 for the preset level.

Then, the trusted audit mechanism of the computing node sends the request to the trusted audit mechanism of the virtual machine, calculates the trusted policy of the virtual machine through the trusted audit mechanism of the virtual machine, and outputs the result. The trusted level of the virtual machine is set to 1, and the results are shown in figure 5 when viewed from the terminal interface of the trusted verification server.

Fig. 5 Virtual Machine Reference Value Generation

The user opens the trusted audit interface on his own terminal, and the trusted audit interface will send authentication request to the security audit server, which forwards the authentication request to the trusted audit mechanism on the computing node. Terminal display is shown in figure 6.

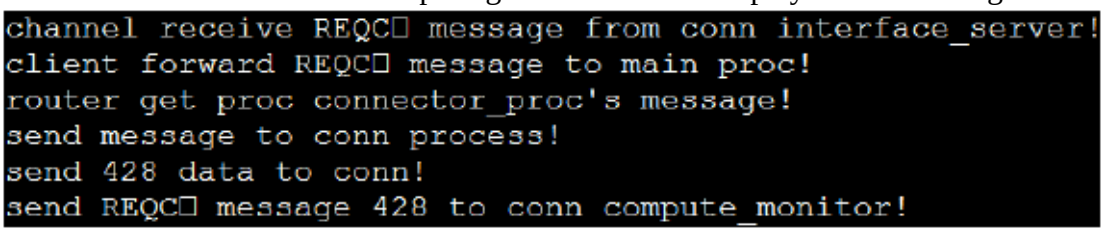

Fig. 6 Virtual Machine Reference Value Generation

The computing node audit mechanism receives the request message, gives the computing node information index to the security audit server, and then conducts the trusted measurement of the computing node. The calculated results are returned to the audit server as PCRP information. Terminal display is shown in figure 7.

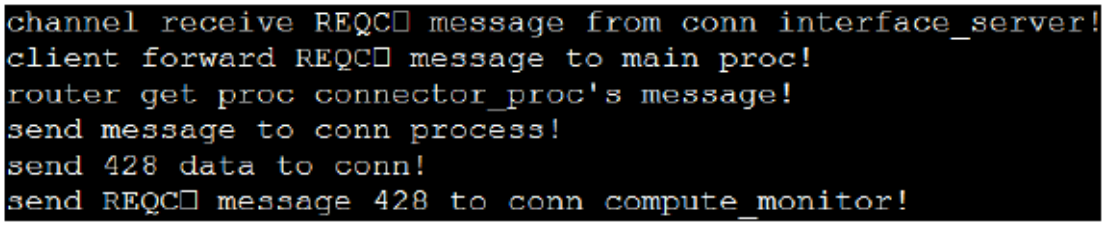

Fig. 7 Audit Server Forwards the Request Process

The security audit server forwards PCRP information to the cloud service validation environment. And send the index information PLAP to the trusted audit interface for users to check. As shown in figure 8:

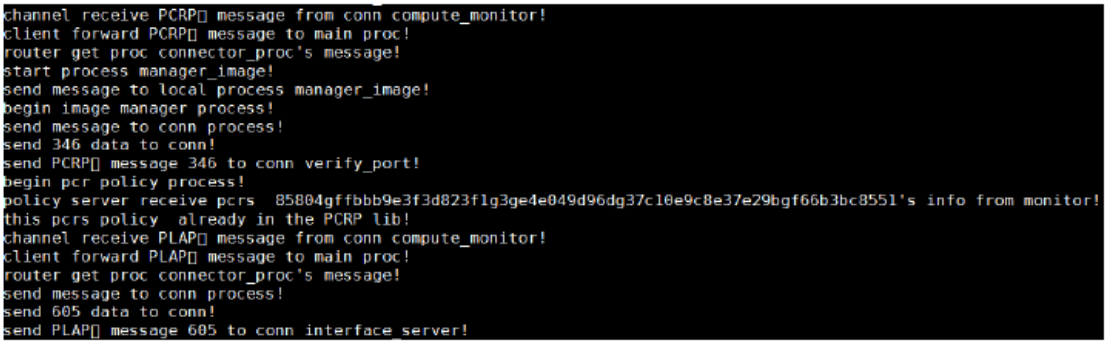

Fig. 8 Metric Computing Nodes Audit Mechanisms Host Process

The trusted audit interface gives the index information PLAP to the cloud service verification environment. The cloud service verification environment extracts messages from the local host benchmark database and compares them with PCRP messages, and returns the VERI information as the audit report to the trusted audit interface. As shown in figure 9:

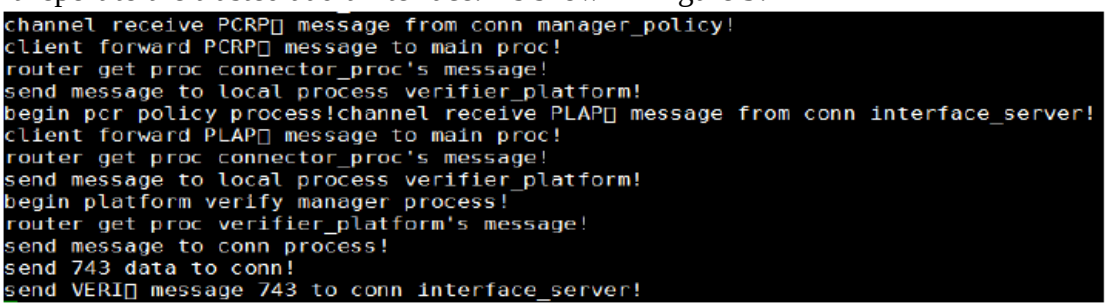

Fig. 9 Security Audit Server Workflow

After repeated tests, the trusted audit test results for the attack behavior of computing nodes and

virtual machine applications are summarized, as shown in the following Table 1.

Table 1 Compute Nodes and Virtual Machine Applications Attack Test Result

Type of aggression	Modify the content	Result of identification
Compute node bootstrap tampering	/boot/grub/grub.conf	Not credible
Compute node kernel tampering	/boot/vmlinuz-3.5.0-18-generic	Not credible
Virtual machine bootstrap tampering	/boot/grub/grub.conf	Not credible
Virtual machine kernel tampering	/boot/vmlinuz-3.5.0-18-generic	Not credible
Virtual machine security module application tamper	/boot/os_safe/whitelist	Not credible
Virtual machine application tamperin	/bin/ls	Not credible

5. Summary

The results show that when computing nodes and virtual machine applications are tampered with, they are judged to be untrusted. And the feedback is given to users. It can be seen from the results that when the trusted isolation mechanism proposed in this paper works normally, the trusted policy can be normally generated for computing nodes and virtual machines. Moreover, if the computing environment and application trusted mechanism are tampered with, the trusted audit mechanism will report the tampering behavior to the user in the trusted audit report provided to the user, so as to ensure the security of the system.

References

[1] D. Feng, M. Zhang, Y. Zhang, Z. Xu. Study on Cloud Computing Security. Journal of Software, Vol. 22 (2011) No.1, p.71-83.

[2] K. Hashizume, D. G. Rosado, E. Femádez-Medina and E. B. Fernandez. An analysis of security issues for cloud computing. Journal of Internet Services and Applications, Vol. 4 (2013) No.5, p.1-13.

[3] Wang Zhi, Jiang Xu-xian. Hyper Safe:a lightweight approach to pro-vide lifetime hypervisor control-flow integrity, Vol. 2 (2010) No.15, p.380-395.

[4] Serrano D, Bouchenak S, Kouki Y, et al. SLA guarantees for cloud services. Future Generation Computer Systems, 2016, 54(C):233-246.

[5] Salaun M. Practical overview of a Xen covert channel[J]. Journal in Computer Virology, Vol. 6 (2010) No.4, p.317-328.