2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing

Establishment of Security Levels in Trusted Cloud Computing Platforms

Fan Yang, Li Pan*, Muzhou Xiong, Shanyu Tang

(Computer School, China University of Geosciences, Wuhan 430074, Hubei, China)

Abstract—**Cloud computing, which provides online resources as a service to users, brings a technology revolution in IT world. However, the data security and privacy on cloud is an important issue, becoming the biggest barrier of cloud computing development. A Trusted Cloud Computing Platform (TCCP) based on remote attestation build a trusted cloud for tenant. The critical section is centralized Trusted Coordinator, taking the place of tenants to authenticate nodes individually in cloud computing platform. But, when a lot of tenants apply for nodes at the same time, Trusted Coordinator (TC) maybe can't deal with these requests quickly .To address this problem, we propose the establishment of security-level for different applications in TCCPs, which divides Trusted Coordinator into three, each responsible for authenticating different application kind. TC would implement different authentication policies, such as user password comparison, image hash verification and trusted chain measurement, according to different security levels.**

Index Terms: Cloud computing, Cloud security, TCCP, Security level.

I. Introduction

WITH the development of PC Internet and mobile Internet, it is in the rapid growth of the amount of information and data in the scientific, educational, commercial, national defense and other areas. So we should increase hard resources to meet the huge investment, but this is costly. In this case, in order to achieve cost savings and system scalability, cloud computing has been proposed. Cloud computing idea can be traced back to the 1960s. John M Carthy[1] mentioned that calculation would become a kind of public infrastructure sooner or later. This means that computing resource can be used as a circulation of commodities, like energy, service on-demand. Since March 2006, the Amazon launched Elastic Compute Cloud (EC2)[2] service, in August of the same year, Google CEO Eric Schmidt in the search engine Assembly first proposed the concept of "cloud computing". In October 2007, IBM and Google announced in collaboration about cloud computing, directed by Google engineer Bisciglia. Cloud computing came into use among several colleges and universities in the United States, and has been gradually into the public attention. Cloud computing attracted the attention of many people and quickly became focus of the industry and academia research.

Cloud computing spirit is the idea of everything as a server (XaaS). Cloud service providers will calculate the hardware and software resources providing as a service to the user. The most widely used definition of the cloud computing model is "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, services, storage, applications) that can be rapidly provisioned and released with minimal management effort or service provider interaction[3].". Cloud is divided into three deployments [3]: private cloud, public cloud, hybrid cloud. Three kinds of delivery mode: infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS). The prominent characteristic of cloud computing are multi-user renting and elasticity. Many users make use of resources to maximize cloud and different users can use the same resources. Overall, the cloud computing improves efficiency of the resource use, save the overhead of the network services conveniently.

Even though the benefits of cloud computing are clear, security is not up to the mark. If there is no security, these are no reliability in the data which are used by various cloud users. There is the need to develop proper security for the further implementation in the cloud[4]. Cloud computing still has a lot of open issues. Although there are many researchers devoting themselves to research this, but there is no an absolutely reliable and security model existing in current time. As everyone knows, cloud computing services and data storage are not in locality, so the environment which tenant will use is controlled by cloud server provider, thus it is unfair for tenants. Once the critical data is destroyed, lost or stolen, it will have a

Manuscript received May 31, 2013. This work was supported by National NSF of China (No.61003268), Key Science and Technology Research Project of Wuhan (No.201301050101014) and Fundamental Research Funds for the Central Universities (No.CUGL120283).

Fan Yang is a doctoral student major in trusted computing and cloud security.
Li Pan is a postgraduate major in cloud computing and cloud security.
(e-mail : lipan.wh.cug@gmail.com)

978-0-7695-5046-6/13 $26.00 © 2013 IEEE
DOI 10.1109/GreenCom-iThings-CPSCom.2013.398

IEEE computer society

significant impact, and cause irreparable loss, or even take the associated liability for tenants. The user's confidential data is controlled by the cloud service provider, so the trust-rank of cloud service provider should determine the user's choice directly. This is what is called “trusted but verify” [5] where cloud consumers should trust in their providers meanwhile cloud providers should deliver tools to help consumers to verify and monitor security enforcements. In recent years, the cloud platform security incidents occur frequently, these problems make the user doubtful about the security of the cloud platform, in the long run, the issue will seriously hinder the development of cloud computing.

The rest of the paper structure is as follows. In section Ⅱ, we explore previous efforts, and introduce the Trusted Cloud Computing Platform. Section Ⅲ introduces the architecture based on security-levels and detail design. Section Ⅳ describes the process of programming and build cloud platform. Section Ⅴ summarizes our conclusions and the future work.

II. RELATE WORK

Researcher Nuno Santos [6], who improved on the basis of the Terra [7] presents a secure server-based remote attestation scheme TCCP (Trusted Computing Cloud Platform). For the traditional trusted computing platforms such as Terra. The owner cannot prevent physical attacks on the host and the user cannot determine whether the datum run in a secure environment. TCCP is designed to ensure the integrity and confidentiality of cloud user’s data, and determines the absolute access rights for cloud user.

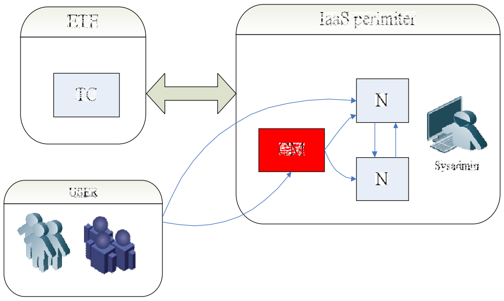

Figure 1: Architecture of TCCP

The architecture consists of two parts, a TC (Trusted Coordinator) in the ETE (External Trusted Entity) and infrastructure environment TCCP. When a user applies for computing node, the node under the management of CM (Computing Manager) was certificated by TC. TC must prove to nodes whether they are in trusted environment. If the node is trusted, then the user will get the access to node through the CM . In this architecture we assume that ETE is a trusted third party environment.

The model has pointed out a malicious administrator who can prevent unauthorized access to user data and damage of user data. TC need to respond a lot of node authentications and the authentication will affect the efficiency of the whole system, in particular for real-time authentication. Someone proposed remote attestation of trusted ring signature remote attestation[8] which alleviated these deficiencies. Hanzhang Wang[9] designed an architecture where some trusted nodes become a part of the Privacy CAs by introducing the DAA strategy based on the credible neutrality of chip features.

III. DETAILED DESIGN

Trusted Coordinator will be used to authenticate the computing nodes instead of the tenant, and ensure that the tenant's application will be deployed in a safe and controllable environment in Trusted Cloud Computing Platform. But the Trusted Coordinator approach certificates all computing nodes where would be deployed applications in the same way. So regardless of the level of security requirements, the implementation process and resource costs are the same, reducing the flexibility of deploying applications. Trusted Coordinator did not explain how to deal with multiple tenants applying for computing nodes at the same time. Trusted Coordinator is a critical part of the whole Trusted Cloud Computing Platform. When Trusted Coordinator becomes invalid or attacked, then the entire cloud platform cannot run well. Therefore, the efficiency and safety of the Trusted Coordinator affects the operation for the cloud computing platform.

To address these problems, combined with the idea of parallel processing, we propose a trusted cloud computing platform based on security level. According to applications requirements for the security level, we divided applications into three security levels. The highest security level as level1, mainly thinks over the security of data, including cloud storage, data backup, e-mail, e-commerce, cloud antivirus and so on. The level2 mainly takes into account the safety and efficiency sides both, including online business, search engine, online games, business management, CRM and so on. The level3, mainly considers the efficiency of services and the speed of data processing, including online music, online video and so on.

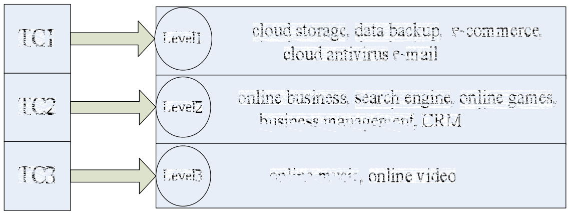
TC1
TC2
TC3
Level1
cloud storage, data backup, e-commerce, cloud antivirus e-mail
Level2
online business, search engine, online games, business management, CRM
Level3
online music, online video

Figure 2: Trusted Coordinator classification

According to different levels of security, Trusted Coordinator will be divided into three. Every one kind of TC is responsible for handling each level certification. For the level3 security requirements, Trusted Coordinator uses the password-base approach certification for computing nodes. Trusted Coordinator authenticates the computing nodes’ username and password, and authorizes to tenant. When a tenant no longer uses this node, Trusted Coordinator would delete the user name and password information. In living migration, the state of an executing VM is transferred between two nodes. Trusted Coordinator certificates the destination node and assigns it to the tenant, then removes application from source node to destination. For the level2, TC will calculate the hash value of virtual machines system image file. At the first time each node was initialized, the system image file's hash value as the original data was registered to Trusted Coordinator. When tenants apply for the computing nodes, the node sends its hash value of the current state to Trusted Coordinator. Trusted Coordinator will match the registered hash value with the current hash value, if the match succeeds, customer logins in the node, else continues to find the next trusted node. When the customer no longer uses the node, Trusted Coordinator withdraws the authorization. For the level1 of security requirements, Trusted Coordinator take the integrity measurement of entire platform, which is the value calculated as measurement list (ML for short). ML consists of a sequence of hashes including the boot sequence, BIOS, the bootloader and the software implementing. The value is stored in the memory of the TPM chip. From start-up, until the application is running, the process would have been the monitor by host TPM chip. The behavior of the host information should be collected by TPM chip. The process of authenticate the computing nodes are similar. As in Fig. 3, in step 1, user apply for computing nodes, in step 2 and step 3 Trusted Coordinator authenticates to computing nodes, in step 4 ,node returns the result to tenant .

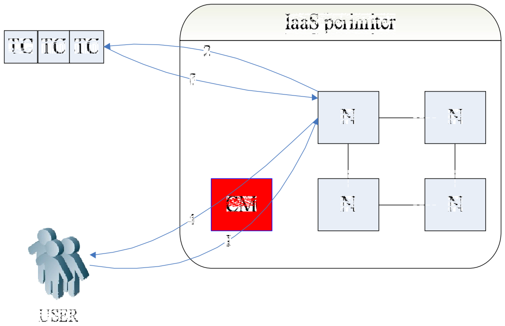

Figure 3: Process of authenticating the computing nodes.

Trusted Coordinator is divided into three for different security levels. Meeting the applications for deployment, Trusted Coordinator can be processed simultaneously. When one of Trusted Coordinator cannot run, it does not affect the normal work on the other Trusted Coordinators, which also improves the robustness of the system. Although we increase the number of Trusted Coordinator, but accelerate deployment of applications and moreover improve the flexibility of resource scheduling.

IV. EXPERIMENT AND PROGRAMMING

According to the experimental requirements and our own existing resources conditions, we combine the Opennebula[10] cloud platform with the virtual machine monitor Xen[11] to build our cloud computing platform. Opennebula is designed specifically for Linux VM. It is an open community project in a cloud component, which is completely open source. Opennebula physical machine is at the server and the devices generate new virtual layer that can support a cluster server implementation and enhance the effectiveness of the virtual machine. Xen is currently very popular as a para-virtualized virtual machine monitor in the open source community. Our cloud platform architecture is shown as in Fig. 4.

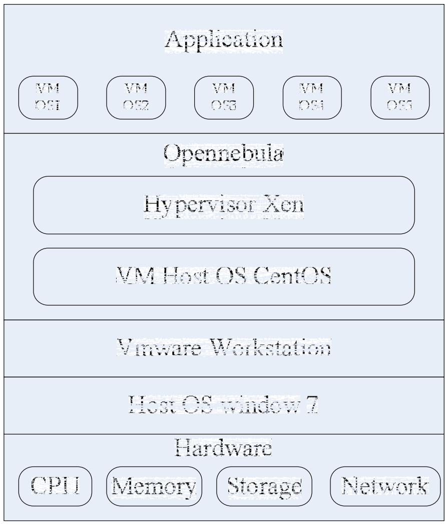

Figure 4: Architecture of our cloud platform.

The whole cloud platform is divided into multiple layers. The bottom which is the resource pool includes a variety of resources for the allocation and scheduling of upper layer which is the host. In order to improve the utilization rate of limited resources on lower layer, we should be assisted by virtualization of virtual machine software with limited resources. In these experiments, two virtual machines were created, and installed with CentOS (version 5.9) system. Combining Opennebula (version 3.8.3) with Xen (version 4.2.1), we built a small cloud environment. The Xen installation includes YUM warehouse update, kernel compilation and modification of startup items. The construct of Opennebula includes related package installation, Opennebula compilation, node creation, virtual network creation, virtual machines creation and other processes. The top is the application layer, and the security levels of the applications determine the whole platform authentication policy in this article.

After building the cloud platform, we program and realize the certification process of each security level. For the level 3, the simplest authentication is based on user's name and password, Trusted Coordinator generates a random password, and then stores username and password in the database. At the same time it will use 1024-bit RSA algorithm to encrypt password and send the ciphertext to customers. Thus, we complete the response to the tenant request. For the level 2, the process of security certification is based on the system image file. First of all, we calculate the system image file's hash value by SHA1 algorithm, and then get a 160-bit hash value. Finally, the Trusted Coordinator matches the hash value of the node with the original hash value provided when registering the node. The Trusted Coordinator determines whether the node is security by measuring the integrity of the system image file. For the level 1, due to its lack of TPM chip, so we did not realize yet.

Next is testing of SHA1 algorithm. Because the virtual machine image file are very large, so that calculate image file hash value may cost a lot of time. The following table I show measuring the time of the SHA1.

TABLE I
TIME COST OF SHA1 ALGORITHM TEST

Size of image file	Time of calculation
10MB	0.2200s
20MB	0.4100s
30MB	0.6300s
40MB	0.8200s
60MB	1.2400s
80MB	1.6500s
100MB	2.0700s
200MB	4.1100s
400MB	8.1500s

The TC spends time on certification process, include the transmission time, time of calculate the hash value and some other time-delay. We can control or improve the time of calculate the hash value.

V. Conclusion

Cloud computing is the most popular service model in current, and its security issues cannot be ignored. In this paper, we improve TC function and make it specific based on the structure of the original TCCP. Depending on the application requirements for security diversities, the application is divided into three levels. The level1 is the highest level, which follows in descending order. According to the level of security, TC will take different security certifications for nodes which deploy different applications. In level1, TC will measures the integrity of the measurement list (ML), that is, from the underlying hardware to the application layer, we establish a chain of trust. TC validates the integrity of the chain of trust. In level2, TC measures the integrity of the system image file. In level3, TC just checks the correctness of the password for the nodes. The proposed scheme can improve the efficiency of TC certification, saving hardware and software resources on certification process. If one TC cannot run, it does not affect the others.

VI. FUTURE WORK

Our architecture also has some disadvantages. When one TC broke down, the TC which is responsible for one security level of certification cannot be run normally. To be able to resolve such problem we need to take into account the TC migration. Other grades' TC which is responsible for other security level is dispatched to the problem TC or adds an active backup function TC to replace the faulted one. We also consider the structure optimization of TC, maybe like a tree structure. First we create a TC as a root of tree, and then according to security level, create some child nodes which are responsible for certifications. Each child node is separated into multiple leaf nodes responsible for the specific implementation of the certification process. From horizontal comparison, the structure can deal with different levels of security to do parallel processing. From vertical comparison, the structure also can deal with the same level for different users on doing parallel processing. It will greatly improve the efficiency of certification. Last, we would improve the efficiency of SHA1 algorithm, reduce the time of calculate hash value.

References

[1] Wikipedia.JohnMcCarthy(computer scientist) [EB/OL]. (2008210207)[2008212210]. http://cn.wikipedia.org/wiki/John_McCarthy(computer_scientist).

[2] Amazon elastic compute cloud (AmazonEC2).2009. http://aws.amazon.com/ec2/.

[3] NIST SP800-145. The NIST Definition of Cloud Computing (Draft) [S] .2011-01.

[4] Mohamed Al Morsy, John Grundy, Ingo Muller. An Analysis of The Cloud Computing Security Problem[C].In Proceedings of APSEC 2010 Cloud Workshop.

[5] D.K.Holstein, Stouffer.K. Trust but Verify Critical Infrastructure Cyber Security Solutions. HICSS 2010,pp.1-8.

[6] Santos N Krishap, Gummadi Rodrigo Rodrigues. Towards Trusted Cloud Computing .2010[2010-11-11].http://www.mpi-sws.org/~gummadi/papers/trusted_cloud.pdf.

[7] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh. Terra: A Virtual Machine-Based Platform for Trusted Computing. In *Proc. of SOSP'03*, 2003

[8] LIU Jiqiang,ZHAO Jia,ZHAO Yong. Study of Remote Automated Anonymous Attestation in Trusted Computing[J].CHINESE JOURNAL OF COMPUTERS,Vol 32,No 7,July 2009.

[9] Hanzhang Wang.Trusted cloud computing platform model : study and improvement[D].University of Science and Technology of China.

[10] OpenNebula project [EB/OL] [2008212231]. http://www.opennebula.org/doku.php.

[11] William von Hagen.Professinal Xen Vitualization[M].Wiley Publishing,Inc