[Volume 3 issue 6 June 2015]
Page No.1018-1024 ISSN :2320-7167

INTERNATIONAL JOURNAL OF MATHEMATICS AND COMPUTER RESEARCH

The Trusted Computing Model for Providing Security in Cloud Computing

Dr. P. Nageshwar, Dr. I Nagaraju, M Anil Kumar
E-mail-tejanagesh@gmail.com

Abstract
Cloud computing is a catch-all phrase that covers virtualized operating systems running on virtual hardware on untold numbers of physical servers. It is a paradigm where tasks are assigned to a combination of connections, software and services accessed over a network. The "cloud" term has consumed High Performance Computing (HPC), Grid computing and Utility Computing. It provides people the way to share discrete resources and services that belong to diverse 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, a method to build a trusted computing environment for cloud computing system is by integrating the trusted computing platform into cloud computing system with a model system in which cloud computing system is united with trusted computing platform and trusted platform module. The security necessities in cloud computing environment is the discovery of the vulnerabilities in the landscape of clouds, detection of security solutions, and finding evidence that early adopters or developers have grown more concerned with security with the proposed model. With this model, some important security services including authentication, integrity and confidentiality are provided in cloud computing system.

Key Words: cloud computing, trusted computing platform, trusted computing, trusted service.

INTRODUCTION

Cloud computing is concerned with the sharing and coordinated use of varied resources in distributed organizations cloud, which is consisted of different organizers 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 thus a major element in any cloud computing infrastructure, because it is necessary to make sure that only authorized access is permitted and secure behavior is accepted. 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. Certainty is the major

concern of the consumers and provider of services that share in a cloud computing environment.

CLOUD COMPUTING ISSUES

The basic areas of cloud receptiveness are similar to the standard issues that surround networking and networked applications. The issues specific to cloud architectures consist of network control being in the hands of third parties and a likely for sensitive data to be available to a much larger range of third-parties, both on the staff of the cloud providers, and among the other clients of the cloud.

Few of the hindrances associated with cloud computing are:
Internet with high speed is required: Cloud computing recital in slow speed internet connection is weird. Slow connections like dial-up make cloud computing a sting for the user or it can be impossible for the users to enjoy cloud computing on slow connections. Data Silos: All the data in Cloud computing is stored on Cloud. It is the duty of the user to make sure of the data which is stored on the cloud is secure. *Dependency and Flexibility*: No influence on maintenance level and fix frequency Quality problems, especially backup, restore and disaster recovery. Possible lower rate of business IT innovation and the customization is not possible. Hidden cost structure due to highly flexible usage of cloud services. *Integration Woes*: Deeper knowledge is required for implementing and managing and it is hard to integrate with the equipments hosted.

SECURITY 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. Even the mechanism for the cloud computing security has many virtues now, but there are still some drawbacks. For example, there is small of the mechanism on the hardware to sustain the trusted computing in cloud computing system.

TRUSTED COMPUTING MODEL

Trusted computing 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 amount of entities, such as users and resources from different sources, the authentication is important and dense. Considering these, the TCP is used to help to process the verification in cloud computing. The TCP is based on the TPM.

The TPM is a logic self-governing hardware. It can resist the attack from software, and even the hardware attack. The TPM contain a private master key which can provide guard for other information store in cloud computing system. Because the hardware certificate can store in TPM, it is firm 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 outline the users and get their origin.

B.-Goal Based Access Control Model in cloud computing environment

For reducing the impediment of the access control model, the users can be classified into a number of classes or groups and make the access control criteria for these classes. So they should at first register themselves into one or some of the classes and get some credential to express their identities. When they make 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 attain 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 subsequently block and appends it to the end of the tamper-resistant log. In turn, each lump of code adds to the log the hash of the next lump 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 operating system 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 operating system version is running, and then that operating system can certify the application's specific configuration. If you trust TC and the operating system, then you can be confident that you know the application's design. 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 routine provides a way to help the participants in the cloud computing systems to build relationship among the ones that have shared action. The trusted computing platform's boot sequence is illustrated. The start of the boot is the BIOS boot block. In the TPM, the basis of trust in integrity coverage is fulfilled. And the reporting could be delivered to the remote machine via the network. By using the remote bear out function, the user in the TCP could to considerate their identities and relevant information to the remote machine that they want to make access

to. And each objective environment has the mechanism to illuminate 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 accountability 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 state 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 mixture of hardware and software application. The hardware maintains a "master secret key" for each machine, and it uses the master secret to produce 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 illustrate 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 associate 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 by 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 onerous 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 go by firstly the authentication with TPM, and encryption keys are stored

in the TPM, which makes it hard to assault these keys. To prevent the attack for integrity of data, the hash function in TPM is used. The TPM will check the serious data in a certain interval to protect the integrity of data. The processes of encryption and integrity check use TSS to call the purpose of TPM.

D.- Tracing User's Identity

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.

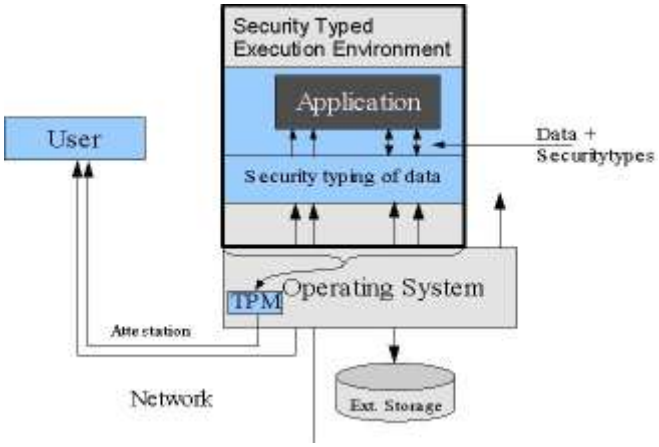

Figure 1. Trusted computing model

CHARACTERISTICS ANALYSIS

Some information security issues that regarding the service and application of cloud computing are analyzed. Some possible solution for remedy the shortcoming or the security problem of cloud computing are also presented such as user authentication, device

authentication, and the establishment of secure communication channel. The proposed suggestions not only focus on the cloud side to present the assurance for the client side, but also the verification and authentication on both sides. Moreover, those requirements of data confidentiality and integrity are also addressed and measured to avoid the occurrence of those needless illegal problems that issued in the perspective of information security.

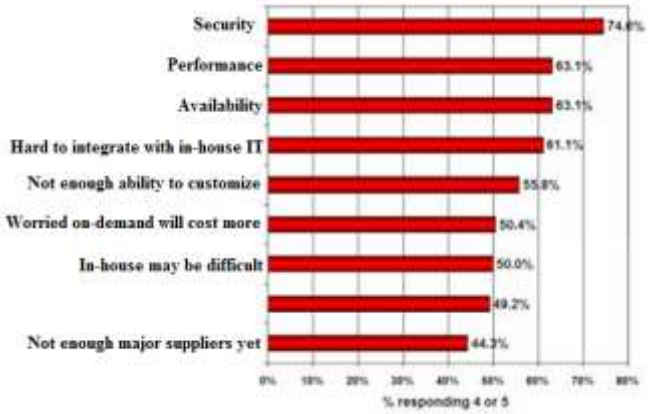

Figure 2. Performance characteristics

CONCLUSION

The trusted computing in the cloud computing environment and the function of trusted computing platform in cloud computing is analyzed. The recompense of proposed approach are to expand the trusted computing technology into the cloud computing environment to achieve the trusted computing requirements for the cloud computing and fulfill the trusted cloud computing. TCP is used as the hardware base and some important security functions such as authentication, communication security and data shield for the cloud computing system. A secure base for achieving trusted computing is also provided. But more profound research is needed to know how to integrate well the hardware modules with cloud computing system. Developing a model system of trusted cloud computing is planned, this will be based on the trusted computing platform and can provide supple security services for users.

REFERENCES

1. Mike Kavis, "Real time transactions in the cloud", http://www.kavistechnology.com/ blog pg=789. accessed on April 12, 2009.
2. Greg Boss, Padma Malladi, Denis Quan, Linda Legregni, Harold Hall, "Cloud Computing", http://www.ibm.com/deveIopers work/websp here/zones/h ipods/Ii brary. html, pp. 1-4 , October 2007
3. MICHAEL BELL, “Introduction to Service-oriented Modeling”, Service-oriented Modeling: Service Analysis, Design, and Architecture. Wiley& Sons, 3.ISBN 978-0-470- 14111-3, 2008.

4. W. M. BULKELEY, “IBM, Google, Universities Combine ‘Cloud’ Foces”, Wall Street Journal October 8,2007 http://online.wsj.com/public/article print/SB119180611310551864.html

5. From “NSF’S Cyber infrastructure Vision for 21stCentury Discovery,” NSF Cyber infrastructure Council, September 26th, 2005, Ver.4.0, pg 4.

6. Wikipedia, “Cyber infrastructure”, http://en.wikipedia.org/wiki/Cyberinfrastructure

7. http://www.cca-forum.org/, accessed February 2006.

8. Mike Ricciuti, “Stallman: Cloud computing is stupidity'”, http://news.cnet.com/8301-1001_3-10054253-92.html

9. J. J. Rehr, J. P. Gardner, M. Prange, L. Svec and F. Vila, “Scientific Computing in the Cloud”, Department of Physics, University of Washington, Seattle [13] Laboratório Nacional de Computação Científica, “Using Clouds to address Grid Limitations”, Av. Getúlio Vargas, 333 – Quitandinha

10. Sales force, http://www.salesforce.com/

11. Google App Engine, http://appengine.google.com