Augmentation Data Security Aspects of Cloud Computing

G. Rakesh Reddy[1] , Dr. M. Bal Raju[2]
[1]*Research Scholar, JNTUH, India*, gaddameedireddy@gmail.com
[2]*Principal-Professor,India*,drrajucse@gmail.com

Abstract: Cloud computing environments consisting of different modules that handle the security and trust issues of key components. One of the modules is responsible for authentication and identity management. This paper focuses on the issues related to the data security aspect of cloud computing. This paper surveys recent research related to single and multi-cloud security and addresses possible solutions. It is found that the research into the use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. This work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user. Dealing with “single cloud” providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. A movement towards “multi-clouds”, or in other words, “interclouds” or “cloud-of-clouds” has emerged recently.

Keywords: Authentication, Cloud Computing, Cloud Storage, Data Security.

INTRODUCTION

This integrates features supporting high scalability and multi-tenancy. Moreover, cloud computing minimizes the capital expenditure. This approach is device and user-location independent. According to the different types of services offered, cloud computing can be considered to consist of three layers. IaaS or Infrastructure as a Service (*IaaS) is the lowest layer that* provides basic infrastructure support service. PaaS –the Platform as a Service (*PaaS)* layer is the middle layer, which offers platform oriented services, besides providing the environment for hosting user’s applications. SaaS - Software as a Service (*SaaS)* is the topmost layer which features a complete application offered as service on demand. **SaaS** ensures that the complete applications are hosted on the internet and users use them. The payment is being made on a pay-per-use model. It eliminates the need to install and run the application on the customer’s local computer, thus alleviating the customer’s burden for software maintenance.

In **SaaS**, there is the Divided Cloud and Convergence coherence mechanism whereby every data item has either the “Read Lock” or “Write Lock”. Two types of servers are used by SaaS: the Main Consistence Server (MCS) and Domain Consistence Server (DCS). Cache coherence is achieved by the cooperation between MCS and DCS. In SaaS, if the MCS is damaged, or compromised, the control over the cloud environment is lost. Hence securing the MCS is of great importance.

In the **Platform as a service approach (PaaS)**, the offering also includes a software execution environment. As for example, there could be a PaaS application server that enables the lone developers to deploy web-based applications without buying actual servers and setting them up. PaaS model aims to protect data, which is especially important in case of storage as a service. In case of congestion, there is the problem of outage from a cloud environment. Thus the need for security against outage is important to ensure load balanced service. The data needs to be encrypted when hosted on a platform for security reasons.

Infrastructure as a service (IaaS) refers to the sharing of hardware resources for executing services, typically using Virtualization technology. With IaaS approach, potentially multiple users use available resources. The resources can easily be scaled up depending on the demand from user and they are typically charged for on a pay-per-use basis. The resources are all virtual machines, which has to be managed. Thus a governance framework is required to control the creation and usage of virtual machines. This also helps to avoid uncontrolled access to user’s sensitive information.

SECURITY IS A MAJOR CONCERN

We are stepping into the era of cloud computing. Cloud computing is a new type of IT service in which customers make use of the cloud computing infrastructures such as CPU capability, network and storages provided by cloud service providers (CSP). Cloud computing can help to reduce IT cost of small and medium enterprises (SME) in that they need not to buy their own IT infrastructures and employ an IT team again. Meanwhile, as the cost of traditional internal IT infrastructure is becoming a heavy burden to SME, cloud computing can also help to make them more competitive. However, when it comes to transfer their businesses to cloud, people tend to worry about the privacy and security. Is CSP trustworthy? Will the concentrated resources in cloud be more attractive to hackers? Will the customers be locked in to a particular CSP? All these concerns constitute the main obstacle to cloud computing.

Cloud Computing has many new characteristics compared with traditional computing mode. Cloud Security Alliance (CSA) describes these characteristics as: abstraction of infrastructure, resource democratization, services oriented architecture, elasticity/dynamism of resources and utility model of consumption & allocation; NIST summarizes these characteristics as: on-demand self-service, ubiquitous network access, resource pooling, rapid elasticity and pay per use . Since these cloud facilities are shared resources and generally located in the data center of CSP, they are under the full control of CSP. Security devices in cloud are also owned and controlled by CSP. On the other hand, customers have no control over the facilities on which their businesses run. This mode of management is not what customers expect, especially when the security policies are enforced on the cloud facilities. No one is willing to lose control over the security of his own business, or has his privacy exposed to others. There should be a shared security responsibility between CSP and customers. In other words, there should be a security duty separation in cloud computing between CSP and customers. The principle of security duty separation must be based on what services CSP provide to customers, in short, what you serve, what you secure. There are three typical cloud service delivery models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

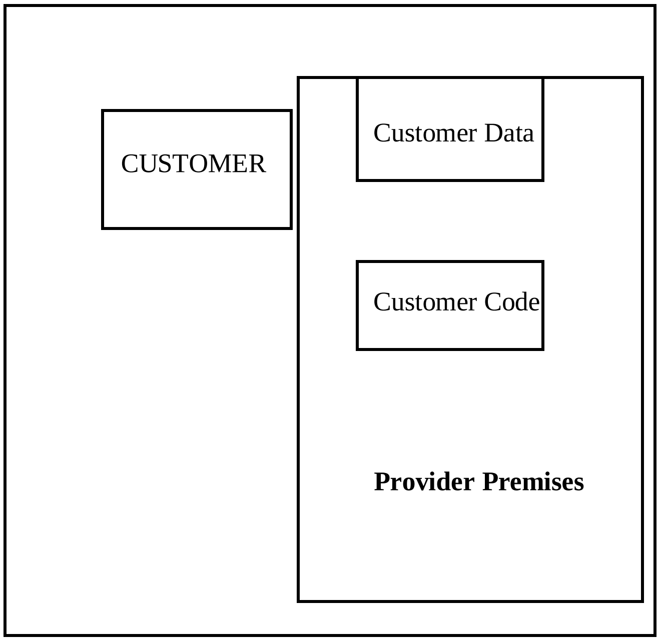

Fig 1: Data Storage Scenario in Cloud Computing

The interrelationship and logical boundaries of these three cloud service delivery models were depicted in the Cloud Reference Model illustrated in figure 1. Because these three service delivery models offer different levels of service, the security level that CSP assure to customers should also be different. CSA believes that CSP should take on the greatest amount of security responsibility in SaaS model and the least amount of security responsibility in IaaS model, while in PaaS model, security responsibility must be carefully leveraged by the CSP and customers.

TRUSTED PLATFORM FOR COMPUTING (SECURITY RISKS INVOLVED)

Cloud computing though provides a very dynamic and profitable structure; however it introduces significant concerns about privacy, security, data integrity, and intellectual property management, audit trails, and other issues. Because of the control that consumers of cloud services to providers, successful initiatives rely on a high degree of trust between a Client (Organization or university) and a supplier, including confidence in the provider's long term viability.

Security Policy Control

For the cloud computing to go main stream, it must offer IT organizations the ability to enforce corporate policy. This policy control ranges from the simple daily policy issues (like enforcing rules to ensure strong passwords) to the more complex (like conducting security related forensics). Many cloud providers fail to offer the kind of tough policy control that many organizations require.

Trusted Computing Group

Trusted Computing Group (TCG) is a not- for-profit organization formed to develop, define and promote open, vendor-neutral, industry standards for trusted computing building blocks and software interfaces across multiple platforms. The main idea of TCG is to assure computing platform trusted based on hardware protected cryptograph module named Trusted Platform Module (TPM) and related software stacks. TPM is a hardware chip that consists of a few cryptographic units and secure storage units. TPM protects its stored objects such as cryptograph keys in shielded location that can be accessed only by protected capabilities. TPM can also protect particular platform state information in its platform configuration registers (PCR).

A platform is regarded as trusted if it always behaves as expected. This expectation can be assured by a transitive trust mechanism: a computing platform can only boot from Core Root of Trust Measurement (CRTM), and CRTM is supposed to be trusted. After that, CRTM conveys system control to next executables only when it believes the code is trusted, and the trust boundary is extended. This process is iterated to form a trust chain as CRTM->BIOS->OS Loader->OS-> Applications, over which a platform is assured to be trusted. Some significant researches have been performed and a few of them can be applied in real system. Another important mechanism of trusted computing platform technology is platform attestation. Attestation is a mechanism by which a computing platform proves to a third party that it is trusted. The challenge to attestation is to define a set of reasonable and measurable metrics that can be used to determine whether a computing platform is trusted. People have presented several approaches for platform attestation, such as property based attestation, behavior and memory status based attestations, etc.

Multi-tenancy Trusted Computing Model

Cloud computing is a bilateral service model in which there are two entities: CSP and customers. Customers rent for software, platform or infrastructure services from CSP. CSP can be self-interested, untrustworthy and possibly malicious. Firstly, they are owned by CSP and organized to provide cloud services to customers, so they should be managed by CSP to satisfy the service level agreement (SLA) between CSP and customers. Secondly, as they are the platforms that customers store their data in or run their businesses on, they should supply customers with proper mechanisms to manage and secure their data or applications. In other words, they should be designed to accept and enforce the security policies from customers, which must not be tampered by CSP or other customers. From this perspective, cloud computing should have the capability to compartmentalize each customer and CSP and support security duty separation. The key point to compartmentalization and security duty separation between CSP and customers is to define clear and seamless security responsibility boundaries for CSP and customers, and these boundaries depend on the cloud service architecture and service delivery models.

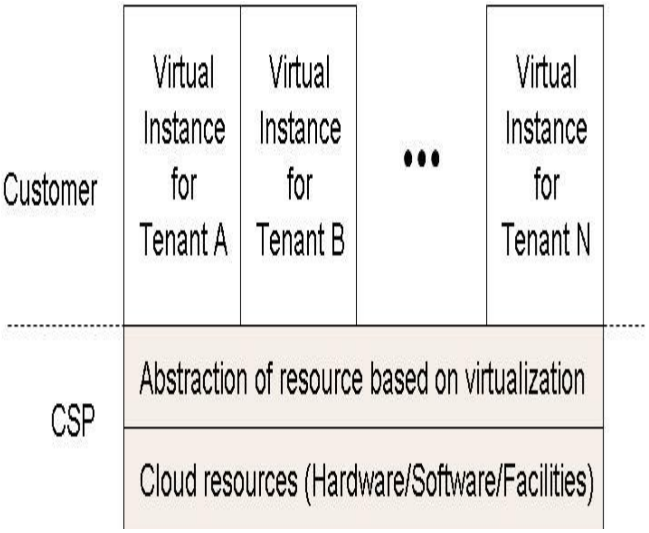
Customer
Virtual Instance for Tenant A
Virtual Instance for Tenant B
•••
Virtual Instance for Tenant N
CSP
Abstraction of resource based on virtualization
Cloud resources (Hardware/Software/Facilities)

Fig 2: shows typical multi-tenancy cloud service architecture.

Multi-tenancy trusted computing environment model (MULTI-TENANCY TRUSTED COMPUTING ENVIRONMENT MODEL) is a security duty separation model designed mainly for IaaS, and its purpose is to assure that CSP will secure the infrastructures they provide as services and that customers must build trusted virtual instances for themselves. Both sides will not exceed to other's authorities Figure 3 is an example of IaaS. The Host OS in the shadow part may not exist in other IaaS architecture.

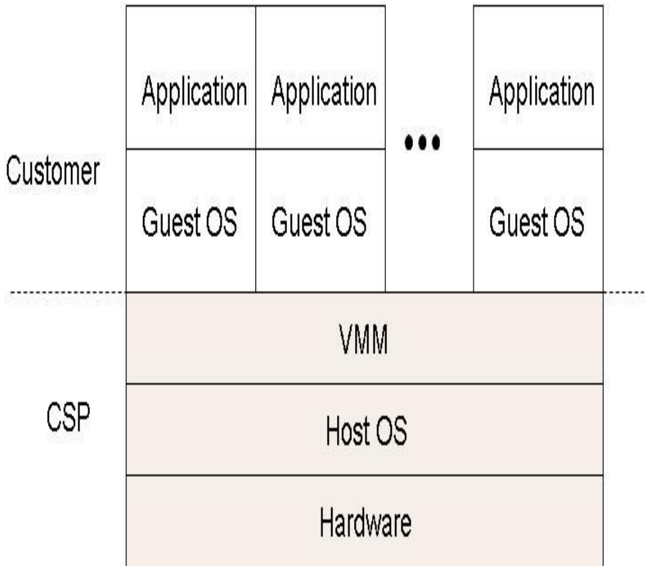

Fig 3: An IaaS model example

Customers rent virtual instances from CSP to run their own operating systems and applications. In this scenario, CSP should secure the services they offer, that is, they should provide trusted infrastructures for customers. On the other hand, according to the security duty separation principle, customers should be responsible to assure that their guest operating systems and applications are trusted. MULTI-TENANCY TRUSTED COMPUTING ENVIRONMENT MODEL is a two-level hierarchy transitive trust chain model which supports the security duty separation, as illustrated in figure 4.

In MULTI-TENANCY TRUSTED COMPUTING ENVIRONMENT MODEL, we have three entities as follow:

- Customers, who rent cloud services from CSP.
- CSP, who provide IaaS services.
- The Third Party Auditor, optional but recommended, who is responsible to verify whether the infrastructures provided by CSP are trusted on behalf of customers.

As illustrated in figure 4, the first level of transitive trust chain in MULTI-TENANCY TRUSTED COMPUTING ENVIRONMENT MODEL is from CRTM up to the loading of each virtual instance; this level of trust chain is to assure the infrastructures trusted. CSP assume the responsibilities to keep infrastructures trusted. The second level of transitive trust chain is from the boot of guest OS up to applications, sometimes even up to a higher VM environment such as JVM, and this level of trust chain is to assure that each virtual instance is trusted.

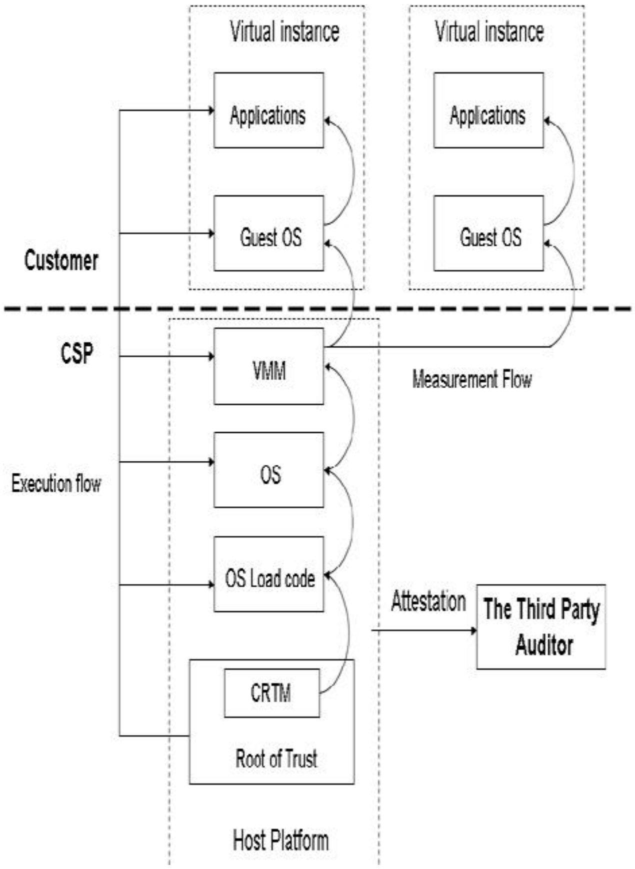

Fig 4: Multi-tenancy trusted computing environment model

CONCLUSION

It is clear that although the use of cloud computing has rapidly increased; cloud computing security is still considered the major issue in the cloud computing environment. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. Furthermore, data intrusion leads to many problems for the users of cloud computing. The purpose of this work is to survey the recent research on single clouds and multi-clouds to address the security risks and solutions. We have found that much research has been done to ensure the security of the single cloud and cloud storage whereas multi-clouds have received less attention in the area of security. We support the migration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user.

REFERENCES

[1] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, *On Technical Security Issues in Cloud Computing*. IEEE, 2009.

[2] Greg Boss, Padma Malladi, Denis Quan, Linda Legregni , HaroldHall,“CloudComputing”,http://www.ibm.com/developerswork/ websphere/zones/hip ods/library.html, October 2007, pp. 4-4

[3] A.J. Feldman, W.P. Zeller, M.J. Freedman and E.W. Felten, "SPORC: Group collaboration using untrusted cloud resources", OSDI, October2010, 1-14.

[4] S.L.Garfinkel,"Email-based identification and authentication: An alternative to PKI?", IEEE Security and Privacy, 1(6), 2003, pp. 20-26.

[5] S.L. Garfinkel, "An evaluation of amazon’s grid computing services: EC2, S3, and SQS", Technical Report TR-08-07, Computer Science Group, Harvard University, Citeseer, 2007, pp. 1-15.

G. Rakesh Reddy, B.Tech(CSE), M.Tech(IT), Research Scholar, JNTUH, and Assistant professor in **Jaya Prakash Narayan Educational Society Group of Institutions – School of Engineering,** Bhageeratha Colony, Mahabubnagar, Andhra Pradesh. His areas of Research include cloud computing, networks, information security and he has published papers in various journals.

Dr. M.B.RAJU, B.E (ECE), M.Tech.(CSE), Ph.D(CSE), Principal at VidyaVikas Institute of Technology. His areas of research include image processing, wireless Networks, information Security and Web Application Wireless Network, Data Mining ,Net Work, Web Application, Operating System and has organized a National and international level Conferences. He has published and presented papers in National and international level seminars and Journals.