Journal of
Information Technology & Software Engineering

Imran et al., J Inform Tech Softw Eng 2012, 2:4
DOI: 10.4172/2165-7866.1000e107

Editorial Open Access

Establishing Trust in Public Clouds

Jogesh K Muppala[1]*, Deepak Shukla[1], Subrota K Mondal[1] and Pranit Patil[2]

[1]*Department of Computer Science & Engineering, Hong Kong University of Science & Technology, Hong Kong, China*
[2]*Department of Computer Engineering, Veermata Jijabai Technological Institute, Mumbai, India*

Abstract

Virtualization technology enables a cloud to deliver cost-effective and scalable public services, making the cloud attractive especially to small and medium enterprises (SMEs). Securing trustworthiness in these "virtualized" environments is a non-trivial task and poses significant security threats for users' data and/or applications; the most critical threat being the "malicious insider's threat", the primary reason for lack of trust between a cloud provider and its customers.

Introduction

Cloud computing is a new business computing paradigm that is based on the concepts of virtualization, multi-tenancy, and shared infrastructure [1]. It is an effort to nudge the business computing model towards a "Pay-as-you-go" approach from the traditional "Own-and-Use" model. The Holy Grail is to eventually establish all types of computing as the fifth utility. A cloud system can be deployed in multiple ways depending on the business needs of an enterprise, either as a public, private or a hybrid implementation. Recently, other derivative deployment models like Community clouds and private rental clouds where an enterprise can rent a modular data center can also be seen [2]. Cloud services can be consumed in three ways viz. Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) with decreasing service abstraction levels respectively.

The benefits of clouds are realized through resource sharing. The basic idea is to share large pools of resources like compute cycles or virtual CPUs (VCPUs), storage, software services etc. This very idea of resource sharing gives rise to significant security concerns for a user, especially with respect to his/her data and/or applications which are hosted in the cloud provider's data centers. This security and privacy issue becomes grave in case of the IaaS deployment model which allows a user to set up their virtual infrastructure in clouds [3]. IaaS has the lowest abstraction level and allows a user to create their virtual infrastructure by choosing the desirable configuration in terms of OS, storage space, number of VCPU's, RAM size etc. A cloud provider is only responsible up to the hypervisor level, for security and maintenance of the infrastructure.

We consider only the IaaS model for analysis in this paper as it has the least abstraction amongst all the cloud offerings and allows a user to choose or employ security mechanisms as per their desired levels. There are significant security risks for sensitive data and/or applications hosted in clouds [4]. The rest of the paper is organized as follows: Section 2 discusses related work done in the context of cloud security esp. those dealing with threats related to the virtualized software stack and insider's attacks. Section 3 describes our views on the definition of trust in cloud computing.

Related Work

Security and its trustworthiness have become prime concerns in recent cloud research. Jansen [5], discussed about insider's access, issues with migration to cloud services and the lack of control of some components. He also sheds some light on the requirements of data isolation, encryption and user authentication which are generally desirable properties of a reliable system. Al Morsy et al. [6], briefly investigated IaaS security challenges viz. VM operating system's security, securing VM images repository and virtual network security as well. Finally, they recommend that cloud security solution should support integration and coordination at different layers.

Dawoud et al. [7], specifically point out security threats that can be sourced from a host in addition to threats from other VM's. Also, they propose a layered IaaS security model to help assess the security requirements at each layer. A different approach in the form of "Advanced Cloud Protection System (ACPS)" was proposed by Lombardi et al. [4]. ACPS aims at effectively monitoring the integrity of guest and infrastructure components while remaining transparent to the users. Griffin et al. [8], proposed a new architecture in the form of "Trusted Virtual Domain (TVD)" which is an abstracted secure environment that can provide various forms of attestations with isolation, confidentiality and immutability for virtual resources.

Correia et al. [9], described the use of TPM, both in hardware and software as a mechanism to establish trust amongst remote systems and as a critical tool for creating trustworthy cloud systems. However, while the TPM mechanism is capable of contributing to the creation of trustworthy clouds, the insider's threat still remains an unaddressed challenge. Zhang et al. [10], did significant work in the area of cloud security by proposing a new Cloud architecture named "CloudVisor", which displaces the hypervisor and runs in the privileged mode, while the hypervisor or VMM along with management VM runs in the guest mode. This significant change in architecture of virtual resource management guarantees good protection for all the communication between a guest VM and VMM by separating resource management and security services.

Though CloudVisor has the capability of making VM to VMM communication very secure, it does not increase the visibility into cloud operations, but only adds an extra layer of virtualization (nested virtualization), which in turn makes it even more difficult to log system and operational details for auditing purposes. Tracking back an event to clear details is very crucial for forensic investigations, external audits etc. Without these mechanisms, it would be impossible to tackle cyber

***Corresponding author:** Jogesh K Muppala, Associate professor, Department of Computer Science & Engineering, Hong Kong University of Science & Technology, Hong Kong, China, Tel: +852-2358-6978; E-mail: muppala@cse.ust.hk

Received September 15, 2012; **Accepted** September 21, 2012; **Published** September 24, 2012

Citation: Muppala JK, Shukla D, Mondal SK, Patil P (2012) Establishing Trust in Public Clouds. J Inform Tech Softw Eng 2:e107. doi:10.4172/2165-7866.1000e107

crime cases that take place in the clouds. Therefore, we believe that we need simple and efficient methods that can monitor and record VM operations that will make forensic investigations easy and also feed clients with sufficient details with the help of these logs. This will eventually increase their visibility into the cloud operations and hence the overall trust.

Ren et.al. [11], while discussing various types of security requirements like Data Service Outsourcing security and computation outsourcing security emphasized the need of trustworthy public cloud solutions. The unsuitability of public cloud infrastructures in their present form for business applications is clearly demonstrated by Hoffman et.al. [12], The reasons cited for public clouds not being trustworthy and appropriate for large enterprises were inappropriate SLA's, occasional outages, performance variability of clouds and risk of reputation loss.

Trust in Cloud Computing

Components of trust in cloud computing

The components of trust are a set of individual information security goals that together are responsible and contribute to a user's overall trust on an information security system or mechanism. The following are the four main aspects of trust as identified by [13] and represent a holistic approach towards ensuring trust and its goals:

Security: In securing trustworthiness sophisticated cryptographic methods play a key role and these methods are extremely complicated and/or extravagant for an illicit individual to access or to do any harm. The goal is to prevent any unauthorized access to information and/or the applications that are using the information.

Privacy: Only authorized persons are allowed to access the cloud. Defense against unauthorized access of personal or confidential information (personally identifiable information (PII)) is mandatory.

Accountability: It is critical to accept the ownership or responsibility of all the actions in a standardized way as regulated by OECD, APEC and PIPEDA. This is of paramount importance in enabling *auditability* and transparency in an organization.

Auditability: With effective controls in place for accountability that records and tracks each individual action on the service provider's side, it becomes easy to audit any event and trace any action back to the owner. Both internal and external audits are crucial in establishing trust and transparency in cloud services.

Preventive and Detective Controls

Trust establishment can be interpreted in terms of *Preventive Controls* and *Detective Controls* [13]. Preventive controls are meant to reduce or eliminate the probability of specific undesirable events from occurring in the future and are used as a precautionary step in ensuring overall security and trust. These controls mainly include techniques like active system monitoring which try to discover anomalous behavior of a system or employee. We term these types of controls as *Active Controls* or *Active Security Mechanisms* due to their nature and goals of implementation.

Detective controls, on the other hand, react to an incident of security breach or any event that does not comply with organizational policies and regulations, in order to find out the root cause of the event. We call these controls as *Passive Controls* or *Passive Security Mechanisms*.

As discussed above, it is clear that ensuring and implementing trust involves both aspects of security viz. taking sufficient precautions to prevent any security incidents by employing preventive controls and reacting to the incidents with appropriate actions using detective controls. Therefore, we believe that in order to achieve the ultimate goal of trustworthy clouds, it is essential to implement the right blend of these controls that are relevant to a customer's business and security goals.

Implementing Trust

To make Clouds trustworthy, it is apparent that all the four components of trust viz. Security, Privacy, Accountability and Auditability must be ensured completely. The goals of security and privacy have been addressed to a great extent by using techniques like data encryption (both in storage and network transit), multi-factor user authentication, key rotation, and role-based access for a group of users [1]. Accountability is supported by providing access logs on client's request, security processes, and risk and compliance agreements in the form of whitepapers [14]. In case of providing Auditability, individual administrative actions may not be logged and therefore can be very difficult to trace back to the source of the event in case anything goes wrong.

Accountability and Auditability are inter-related in the sense that without appropriate and complete accounting mechanisms or procedures, it is impossible to audit any unwanted incident and identify the culprit. Moreover, even if the actions are logged at the cloud provider's side, it may be accessible by the same administrative staff whose actions are being monitored and therefore could be modified for obvious reasons. Hence, we need a mechanism that will enable clients to have clear visibility into critical Cloud operations that are related to their own resources and therefore can put in sufficient confidence.

A summary of the mechanisms employed to implement individual components of trust are shown in (Table 1). Accountability and Auditability are mainly monitored on a periodic basis e.g. weekly or monthly and therefore, in their present form, provide only a consolidated summary of past events and present security controls being used. They do not enable a client to have sufficient visibility into the service provider's operations and the concomitant low levels of trust. Therefore, it is essential to introduce additional controls to completely address this issue of trust.

Trust Component	Mechanisms Adopted
Security	Physical Security, Firewalls, Intrusion Detection Systems, Remote Attestation using Public-Key Infrastructure etc.
Privacy	Role-based access, Multi-factor authentication, VM Isolation, Key Rotation, data and VM encryption etc.
Accountability	System Logs that mainly focus on server's status and overall network status reports. Service-level Agreements, practices as per the International regulations viz. Payment Card Industry (PCI) and Certification Authorities like VeriSign etc.
Auditability	Internal and External Audits

Table 1: Mechanisms Used To Implement Trust Components

Conclusion

Establishing trust in public clouds among the users is a very important requirement. Given the current state of the affairs, significant progress needs to be made in order to achieve this goal in practice.

Only then the widespread adoption of the public clouds among SMEs would take off.

References

1. Mell P, Grance T (2011) The NIST Definition of Cloud Computing. NIST 1-7.
2. http://en.wikipedia.org/wiki/Cloud_computing#Deployment_models
3. http://en.wikipedia.org/wiki/Cloud_computing#Infrastructure_as_a_Service_.28IaaS.29
4. Lombardi F, Di Pietro R (2010) Secure virtualization for cloud computing. Journal of Network and Computer Applications 1-10.
5. Jansen WA (2011) Cloud Hooks: Security and Privacy Issues in Cloud Computing. 44th Hawaii International Conference on System Sciences 1-10.
6. Morsy MA, Grundy J, Müller I (2010) An Analysis of the Cloud Computing Security Problem. In Proceedings of APSEC 2010 Cloud Workshop 1-6.
7. Dawoud W, Takouna I, Meinel C (2010) Infrastructure as a service security: Challenges and solutions. Hasso Plattner Inst 1 – 8.
8. Griffin JL, Jaeger T, Perez R, Sailer R, Van Doorn L, et al. (2005) Trusted Virtual Domains: Toward secure distributed services. Workshop on Hot Topics in System Dependability.
9. Rocha F, Abreu S, Correia M (2011) The Final Frontier: Confidentiality and Privacy in the Cloud.
10. Zhang F, Chen J, Zang B (2011) CloudVisor: Retrofitting Protection of Virtual Machines in Multi-tenant Cloud with Nested Virtualization. Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles 203-216.
11. Ren K, Wang C, Wang Q (2012) Security Challenges for the public cloud. IEEE Internet Computing 69-73.
12. Hoffman P, Woods D (2010) Cloud Computing: The Limits of Public Clouds for Business Applications. IEEE Internet Computing 90-93.
13. Ryan KKL, Peter J, Miranda M, Siani P, Markus K, et al. (2011) TrustCloud: A Framework for Accountability and Trust in Cloud Computing.
14. (2011) Amazon Web Services: Overview of Security Processes. whitepaper.