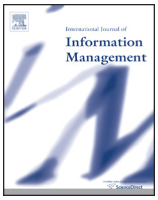
Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt



Data and infrastructure security auditing in cloud computing environments

Hassan Rasheed*

Taif University Deanship of Information Technology, Saudi Arabia

ARTICLE INFO

Article history:
Available online 3 December 2013

Keywords:
Cloud computing
Security audit
Data integrity
Standards compliance

ABSTRACT

For many companies the remaining barriers to adopting cloud computing services are related to security. One of these significant security issues is the lack of auditability for various aspects of security in the cloud computing environment. In this paper we look at the issue of cloud computing security auditing from three perspectives: user auditing requirements, technical approaches for (data) security auditing and current cloud service provider capabilities for meeting audit requirements. We also divide specific auditing issues into two categories: infrastructure security auditing and data security auditing. We find ultimately that despite a number of techniques available to address user auditing concerns in the data auditing area, cloud providers have thus far only focused on infrastructure security auditing concerns.

1. Introduction and motivation

Cloud computing has become one of the dominant IT paradigms of the current age: fulfilling the need of users for dynamic, high-capacity computing capabilities in diverse applications such as business intelligence and data archiving while essentially creating business value for cloud providers out of (what was at least initially) surplus computing resources. With all emerging technologies, however, the longevity of the paradigm will be determined by the way in which certain challenges are met.

One of those chief challenges for cloud computing, and one which has made many organizations hesitant to adopt cloud solutions is security. The European Network and Information Security Agency (ENISA, 2009) surveyed concerns regarding cloud computing security and among the top ten risks, two of them (loss of governance and compliance risks) were traced to the same vulnerability: namely, that audit is not available to customers. Within the context of cloud computing, therefore, the term security auditing actually entails two separate issues: the first is having the cloud provider take appropriate means to ensure that data or infrastructure is secure (the 'security'); the second is making it possible for the customer to verify that those security controls are indeed in place and working as promised (the 'auditing'). It is possible that a Cloud Service Provider (CSP) could have the first without the second (security with no auditing). For example: a cloud provider that attempts to ensure data integrity through the use of backups. The control is in place but the user may have no way to easily verify or audit the backups that the cloud provider is making. Audit is an important concern because it is a means through which the customer can attest to the way in which their technology resources are being handled. Our discussion of security auditing will focus on customer and third-party auditing of cloud provider security controls and methods – not on the more general issues of cloud security or technology auditing.

In this paper, we will attempt to look at the general subject of cloud security auditing with the aim of providing answers to the following critical questions: (1) what are the specific auditing concerns which must be addressed to ensure broader adoption of cloud computing technologies, (2) what is the current state of cloud audit in current offerings and (3) how many of the lingering audit issues could be resolved using existing research approaches and how many demand still further work. In order to do that, we will examine user requirements for cloud auditing security along with some of the existing research solutions to get an idea of what could realistically be integrated in cloud auditing security in the near future (as opposed to more unresolved issues that will require more long-term solutions). These two will be contrasted against what cloud service providers are currently offering (i.e. vendor solutions for cloud security auditing).

In our analysis, we will look at audit issues which could potentially arise in all of the various cloud offerings: Software as a Service, Platform as a Service, Storage as a Service and Infrastructure as a Service. We will subdivide these concerns, however, into infrastructure security auditing and data security auditing. Infrastructure security is important to all of the different cloud service layers: a customer developing an application on a CSP provided

* Tel.: +966 536895637.
E-mail address: hsrasheed@acm.org

0268-4012/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ijinfomgt.2013.11.002

development stack, for instance, may have the same concerns about how virtual machine images and snapshots are stored as a customer who is using complete virtual servers.

Data security issues, however, will be most critical for those users above the infrastructure level: users relying on cloud databases, software development platforms, or complete applications. If a cloud customer has their own virtual cloud infrastructure then in most cases they will have the ability to implement their own systems to ensure data auditability because they have complete virtualized servers and direct access to install or setup whatever applications they desire. It is when the user does not have that level of access – and consequently much of what happens to their data is transparent – that their is more planning necessary to maintain auditability.

2. User requirements for cloud security auditing

We divide the broad scope of user security needs with respect to cloud computing auditing into two sub-areas: infrastructure security and data auditing. The infrastructure auditing concerns deal with the systems that are used to process data and the security controls that are in place to protect those systems. These concerns are distinguished by being agnostic to the actual nature of the business or work being performed and merely ensuring that a secure environment is available for business to be conducted. Data auditing concerns have to do with the preservation of the data itself: its confidentiality, integrity and availability. The data is distinguished by being the information that is stored and processed on the infrastructure systems mentioned previously and is inherently tied to the nature of the business itself.

2.1. Infrastructure auditing needs

Because overall security in the IT industry is frequently driven by best practice standards, user concerns for cloud infrastructure security also seem to be driven by those standards. Two of the most widely used and important standards for enterprise infrastructure security are International Standards Organization security standard (ISO 27001) International Organization for Standardization (ISO) (n.d.) and Payment Card Industry Data Security Standard (PCI DSS) PCI Standards Security Council (2010).

2.1.1. Payment card industry data security standard

PCI DSS (PCI Standards Security Council, 2010) is a frequently used security standard in IT because achieving certification is a prerequisite to being able to handle customer credit card information. The standard consists of 11 core requirements in six main areas: building and maintaining a secure network, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks and maintaining an information security policy. Organizations wishing to gain certification against the requirements of this standard must get an assessment from a security specialist approved by PCI DSS.

Because of the ambiguity of previous versions of PCI DSS regarding virtualization and multi-tenancy, version 2.0 (PCI Standards Security Council, 2010), was changed to clarify these issues. In particular, the 2.0 standard establishes that virtual components are also included under the heading of system components to which the standard applies. It also changed the previous requirement that each server implement only one primary function, so that it now allows for a single hardware server to host multiple virtual machines with different functions as long as each of the virtual machines has only one primary function. This is a critical change to allow merchants to become PCI certified using multi-tenant cloud offerings.

Despite these changes, however, there remain aspects of the standard which may be difficult for cloud customers to meet. In discussing an architecture for security in public cloud offerings, the authors in Prafullchandra et al. (2011) outline risk factors for each of the core PCI DSS provisions. These risk factors have been discussed in detail in Rasheed (2011), but we will summarize the most significant of them into seven categories: virtualized network devices requiring greater documentation to demonstrate effective network separation, automatically provisioned systems using default settings (risks from two core areas fall into this category), exposure of volatile memory when it is written to disk, disclosure of private data on public networks, managing vulnerability patching on dynamic virtual systems, hypervisor-resident access control methods (risks from three different core areas fall into this category) and maintaining audit traces for all machine activity.

Of these concerns some are easier to resolve than others. We will divide these concerns into three types based on the difficulty of resolution: easy, moderate and difficult. The first one, for instance, requiring greater documentation for effective network separation would merely require the cooperation of the cloud service provider (CSP) in allowing access to some of their network architecture diagrams. And because there are CSPs beginning to this such as Amazon (as will be discussed in detail in an upcoming section), there is a relatively simple resolution to this risk. The second risk regarding automatic system provisioning is also easy to resolve: the cloud customer merely needs to use the services of a provider which allows customers to import their own customized images to create virtual machines, rather than using base images provided by the CSP. The risk of volatile memory being written to the disk is actually not specific to virtual machines (although it is more prevalent): many modern operating systems have the capability for a user to suspend the session, writing volatile memory to disk and powering off the machine. The risk is higher with virtualization, however, because a single server may be responsible for managing snapshots of many virtual machines. The resolution difficulty for this risk is therefore moderate because the managing hypervisor will need to be one that supports granular access control for virtual machines and encrypts backups. The risk of disclosing private data is also easy to resolve, because the card processor can simply ensure that all data transmitted over the network is encrypted. There may be some need to determine what constitutes a ‘public network’ if there are multiple virtual machines running on a public cloud host, but in the worst case the processor can satisfy the requirement by encrypting traffic even between peer servers.

Managing vulnerability patching could be handled easily if the individual machines are responsible for pulling their own updates using the service provided by a specific operating system (e.g. Windows Update, Red Hat Network, etc.). If, however, the cloud customer will need to update multiple software packages and thus wants to push updates and patches to their virtual machines this will depend upon the configuration options they have with their service provider. Depending on the CSP this could be a difficult risk to resolve optimally. There are, however, CSPs such as IBM (IBM, n.d.) that do offer private patch servers. The risk regarding hypervisor-resident access control is of moderate difficulty to resolve: the customer will need to ensure that the CSP they are using has an access control system in place whereby access privileges are limited by job function and that access to the hypervisor and virtual machines are governed by that access control system. Lastly, the security risk for data logging is also of moderate difficulty to resolve: the cloud customer must ensure that the hypervisor running their virtual machines has logging capability, that it is enabled and that those logs could be obtained if needed for certification purposes.