International Journal of Information Management xxx (2013) xxx–xxx

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 xxx

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 Published by Elsevier Ltd.
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.

Please cite this article in press as: Rasheed, H. Data and infrastructure security auditing in cloud computing environments. *International Journal of Information Management* (2013), http://dx.doi.org/10.1016/j.ijinfomgt.2013.11.002

2.2. Data auditing needs

We will focus on four essential data challenges that fall under the topic of data security auditing: data integrity, data confidentiality, data lineage, data provenance and data remnance. Data integrity means the "the preservation of data from unauthorized changes" (Mather, Kumaraswamy & Latif, 2009) and this must be ensured for both data residing in a storage medium or being transferred over the network. Data confidentiality is the need for users to "preserve data from unauthorized disclosure" (Mather et al., 2009): this property must also be achieved for data resident in a storage medium and being transferred over a network.

Traditionally, in much of the data processing literature data lineage has been used interchangeably with provenance. Bose and Frew (2005), for example defines lineage as "the origins and processing history," of objects and processes. Within the specific area of cloud computing, however, lineage has also taken on the additional meaning of referring to the ability to track exactly where the data was located at any given time and being able to follow the path of data (Mather et al., 2009). This is of special concern in cloud computing architectures because such systems may dynamically move virtualized systems and data for performance and scalability reasons and some of the data may have compliance regulations stating in which geographic areas the data can be stored.

Data provenance is defined in Mather et al. (2009) as the ability to demonstrate that the data is computationally accurate and was correctly calculated based on a certain delineated method. In Simmhan, Plale and Gannon (2005) it is defined as ". . .information that helps determine the derivation history of a data product, starting from its original sources," which includes both preceding data elements used in the derivation as well as the derivation process. This issue is more complex than integrity because it also encompasses ensuring and verifying that changes made in an authorized manner are fundamentally correct.

Data remnance is the possibility that some residual portions of data may remain after it was erased or removed (Mather et al., 2009). The risk is that such remnants could be inadvertently exposed to a unauthorized third party. It is therefore a confidentiality issue, but focused on retaining the confidentiality of data which was intended to be removed.

3. Techniques for data security

In the previous section, we provided an overview of the important issues in data auditing which may be of concern for cloud service users. In this section we provide a brief overview of some of the recent techniques proposed in those same areas of data auditing. Special attention will be given to approaches specifically proposed for use in cloud environments or which could be easily adapted to cloud environments.

3.1. Data confidentiality and integrity

Cryptography is a tool frequently used to ensure data confidentiality, privacy and integrity. In di Vimercati, Foresti, Jajodia, Paraboschi and Samarati (2007) the authors design an access control system for use in outsourced data storage (such as storage as a service offerings) that relies on issuing cryptographically derived access tokens to users. A number of approaches also propose techniques for querying and searching data that resides encrypted on the cloud server (Cao, Wang, Li, Ren & Lou, 2011; Li et al., 2010; Wang, Cao, Li, Ren & Lou, 2010).

There has also been some recent work on applying the concepts of remote data integrity checking to enable a storage customer to verify the integrity of their data stored in a public cloud. In Wang et al. (2010), Wang, Chow, Wang, Ren and Lou (2011) and Wang, Wang, Ren, Lou and Li (2011), the authors develop an approach for privacy-preserving third party data integrity checking that relies on a challenge protocol to verify pre-calculated cryptographic hashes of file segments; the proposed scheme also supports batch data auditing. Zhu et al. (2011) proposes a similar integrity checking mechanism but assumes the Third Party Auditor (TPA) as a trustable delegate of the original data owner and thus does not provide controls for preventing the original data contents from being disclosed to the TPA.

3.2. Data remnance

Data remnance in the cloud has received very little attention compared to the other user security concerns. There has been some work on proofs of secure erasure with mobile embedded devices (Karvelas, 2013; Perito & Tsudik, 2010). Many of assumptions used by such proofs, however – such as assuming that the storage device has fixed memory of known size – do not hold for the cloud scenario and thus there is still much work required on data remnance. In lieu of such approaches, therefore, the assumption of the cloud provider as an untrusted agent is even more significant: if erasure cannot be proven and the client has no access to the storage medium then it becomes even more important that the data which is given to the CSP is in encrypted form to begin with.

3.3. Data lineage and provenance

In Simmhan et al. (2005) the authors present a survey of data provenance techniques and systems along with a taxonomy of provenance approaches based on four main aspects: the subject of the provenance data (i.e. data or process), the representation of the data, its storage and dissemination. The majority of the systems surveyed were systems for distributed processing of scientific data. Only one – Provenance Aware Service-oriented Architecture (PASOA) (Groth, Luck & Moreau, 2005) – proposes an open protocol for data provenance that could potentially be leveraged for provenance infrastructures in the cloud computing domain. Among other capabilities, the system supports collecting data on the inputs and outputs of service invocation which must be agreed upon by both the client and the service provider. All provenance messages are assigned a unique ID which can be used to construct a process oriented provenance trace of the original workflow.

In Bose and Frew (2005) a survey of data lineage/provenance approaches is presented, in which techniques are classified based on how changes are introduced into the data: command line base data processing, script and program-based data processing, workflow system based data processing, query-based data processing and service-based data processing. However, the issue of tracking the physical location where data was processed was not discussed in the surveyed approaches and thus this aspect of data lineage has yet to be addressed with approaches compatible with the cloud computing environment. However, judging by the breadth of the available approaches for general data provenance, extension to also collect data about the physical location of the processing server should be a straight-forward modification.

4. Provider security capabilities

4.1. Security and compliance at leading cloud providers

In determining the spectrum of CSP security offerings, we looked at the top ten public cloud storage providers based on a recent survey by Gartner (Ruth & Chandrasekaran, 2012): Amazon Web Services, AT&T, Google, HP, IBM, Internap, Microsoft, Nirvanix, Rackspace and Softlayer. Of these, all also had Infrastructure as a

Please cite this article in press as: Rasheed, H. Data and infrastructure security auditing in cloud computing environments. *International Journal of Information Management* (2013), http://dx.doi.org/10.1016/j.ijinfomgt.2013.11.002

Service offerings except for Microsoft (who only supports IaaS services by providing software to its resellers) and Google whose IaaS is still in beta testing at the time of writing.

4.1.1. Infrastructure security

All of the companies we surveyed provided detailed information about their security controls and processes as well as the compliance certifications they have received such as PCI DSS, ISO 27001 and Safe Harbor. All of the companies also provide additional security services for their clients as add-ons to the basic service. For a few of the larger tech companies in the list (HP, IBM) this includes custom-developed security platforms that are made available to customers. For example, HP provides a technical white paper (HP, n.d.) which gives an overview of its TippingPoint IPS technology which is primarily responsible for the security of its servers, network hardware and data centers. In the paper they also discuss a CloudArmour solution which is a user-configurable IPS and firewall for VMs running in their enterprise level cloud offering. Other providers such as Amazon, AT&T, Rackspace and Internap just provide add-on services such as managed firewalls, intrusion detection/prevention or identity and access management as modular, independent security services. Yet another model for providing additional security services was the use of specialized partners to provide third-party security as a service. Softlayer, for example offers customers a free "PCI Compliance" account with McAfee Secure (a service that provides website monitoring and security certification).

Only one company (Amazon) supplemented the discussion of their own security certifications with detailed information about how their customers could achieve standards compliance using their public cloud offering. Like most other CSPs, they offer a page describing their security controls and certification; but they go further in detailing frequently asked questions by their customers regarding PCI DSS and ISO 27001 (Amazon Web Services, n.d.-a, n.d.-b). They also offer to provide customers with a set of documents to assist them in obtaining their own certification which includes: the attestation of PCI compliance for AWS, high-level documentation such as the description of the in-scope environment and more detailed documentation such as a detailed matrix of PCI DSS controls describing who is responsible for each individual control. They provide a general rule regarding the balance between the security responsibilities of CSP and customers saying, "for the portion of the PCI cardholder environment deployed in AWS, your QSA (Qualified Security Assessor) can rely on our validated service provider status, but you will still be required to satisfy all other PCI compliance and testing requirements, including how you manage the cardholder environment that you host with AWS" Amazon Web Services (b). AWS also asserts that several customers have achieved PCI DSS certification, although it is not clear which parts of their infrastructure were hosted on AWS.

Also AWS offers some guidance regarding the ISO 27001 standard. However, perhaps because the requirements for that standard are more high-level, no compliance pack is made available which details where the responsibility for certain controls lie. To illustrate this point, for example, PCI DSS requires things such as the following: building and maintaining a secure network, protecting cardholder data, implement strong security measures and regular testing and monitoring of networks (PCI Standards Security Council, 2010). ISO 27001, on the other hand, requires systematically evaluating information security risks, implementing information security controls and risk management and adopting an overarching management process for security controls (International Organization for Standardization (ISO)).

4.1.2. Data security

CSP support for auditing data security is currently very limited. In fact, the only CSP supporting real-time auditing of any sort appears to be Amazon with its CloudWatch API (Amazon Web Services, n.d.) and, as discussed previously in detail (Park, Spetka, Rasheed, Ratazzi & Han, 2012; Rasheed, 2011), this API only really supports auditing performance statistics for various AWS offerings. CloudAudit (Hoff, Johnston, Reese & Sapiro, 2010), an industry-wide effort to standardize on a way to present security compliance documentation seems to have made no further progress after an RFC (request for comments) submitted to the IETF in 2010. Furthermore, even basic support for data security in software, platform and storage level cloud offerings is also very limited. The lone exception appears to be Amazon's support for encryption of data through a Java API for its S3 storage-as-a-service offering. This partially resolves some confidentiality issues, but only in the case where the data is not regularly updated.

5. Related work

In Zhou, Zhang, Xie, Qian and Zhou (2010), the authors discuss the cloud security issues of availability, confidentiality, data integrity, control and audit in addition to privacy issues. There is a significant discussion of how various CSPs are meeting the security challenges of the various areas, especially for the areas of availability, confidentiality, data integrity and control. The discussion of auditing challenges is more general. The authors advocate for auditing to take place in a software layer within the virtual operating system and that such a system should provide minimal-overhead monitoring of events and logs.

In Subashini and Kavitha (2011), a survey is presented of security issues arising in service oriented architectures (and consequently cloud computing platforms because of their reliance on service orientation). The authors divide security issues based on the cloud service level at which they occur: Software as a Service, Platform as a Service and Infrastructure as a Service. In total fourteen broad security issues are outlined for Software as a Service cloud offerings including: data security, network security, data integrity and data segregation. The concerns listed for Platform as a Service and Infrastructure as a Service are more general, however, and no specific issues are detailed. Data auditing is not listed as one of the security concerns at any service level and there is only a brief mention how current cloud offerings address the security issues which are raised.

In Chow et al. (2009) the authors provide an overview of the security issues in the area of cloud computing by dividing them into three categories: traditional security issues that are also problematic in cloud computing, availability issues and issues arising from third party data control. Among the six data control issues listed is the difficulty of performing audits. They also outline two research directions which could be used to alleviate some of the data control issues and provide various types of auditability. The first is the notion of a trusted monitor residing on the cloud server which can audit the servers actions and provide verifiable proofs of compliance to the data owner. The second is for data to be self-describing, self-protecting and capable of creating a secure virtual environment for data access consistent with an embedded usage policy.

The authors in Chen, Paxson and Katz (2010) perform a general analysis of cloud computing security issues, arguing that most of the security issues related to cloud computing were first confronted in the main-frame time-sharing computing era but that multi-party trust and the need for mutual auditability are security issues unique to the current formulation of cloud computing. The research presented by Kaufman (2009) examines some of the

Please cite this article in press as: Rasheed, H. Data and infrastructure security auditing in cloud computing environments. *International Journal of Information Management* (2013), http://dx.doi.org/10.1016/j.ijinfomgt.2013.11.002

legal and regulatory issues over whether the customer or the cloud service provider is responsible for maintaining data security for information stored in the cloud. In Jansen and Grance (2011) the authors survey the security and privacy issues related to cloud computing and provides some guidelines for organizations considering utilizing cloud service offerings.

6. Conclusion

Despite its significant growth, there are still some obstacles to the more widespread adoption of cloud computing services. For many companies the most significant concern is security and specifically the lack of auditability. We have examined cloud computing auditing from three perspectives: user auditing requirements, technical approaches for security auditing and current cloud service provider capabilities for meeting audit requirements. User auditing requirements were further divided into infrastructure security auditing and data security auditing. Many of the infrastructure auditing requirements are driven by the need to achieve compliance with an IT security standard. For that reason we profiled the infrastructure auditing requirements of the PCI DSS standard version 2.0 (PCI Standards Security Council, 2010). While most of the risks are easy to overcome with the co-operation of the CSP a few such as patch management may present challenges depending on user requirements and provider infrastructure and configuration. Data auditing issues included confidentiality, integrity, data remnance, data provenance and data lineage. There are a number of applicable approaches in each of these areas which could serve the data auditing needs of cloud service users with the exception of data remnance which appears to be an open issue within public cloud offerings. While most of the leading cloud providers have begun to provide significant detail about their own internal infrastructure security and compliance, only one carefully addressed questions regarding how users of public cloud offerings could also achieve standards compliance. Unfortunately, among the cloud providers surveyed we did not find any with solutions for user data security auditing. However, because the cloud services market is driven and shaped by customer demands, if such auditing features become a critical service differentiator for a sufficient number of customers then CSPs will likely begin to offer them.

References

Amazon Web Services. (n.d.-a). Amazon CloudWatch. Retrieved February 2013, from: http://aws.amazon.com/cloudwatch/

Amazon Web Services. (n.d.-b). ISO 27001 Certification. Retrieved February 2013, from: https://aws.amazon.com/security/iso-27001-certification-faqs/

Amazon Web Services. (n.d.-c). PCI DSS Level 1 Compliance. Retrieved February 2013, from: https://aws.amazon.com/security/pci-dss-level-1-compliance-faqs/

Bose, R., & Frew, J. (2005). Lineage retrieval for scientific data processing: A survey. *ACM Computing Surveys*, *37*(1), 1–28.

Cao, N., Wang, C., Li, M., Ren, K., & Lou, W. (2011). Privacy-preserving multi-keyword ranked search over encrypted cloud data. In *Proceedings IEEE INFOCOM 2011, 10–15 April 2011* (pp. 829–837). Shanghai, China: IEEE.

Chen, Y., Paxson, V., & Katz, R. H. (2010). *Whats new about cloud computing security? Technical Report UCBEECS-2010-5*. Berkeley, CA, USA: Department of Electrical Engineering and Computer Sciences, University of California at Berkeley. Retrieved from: http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., et al. (2009). Controlling data in the cloud: outsourcing computation without outsourcing control. In *Proceedings of the 2009 ACM workshop on cloud computing security* (pp. 85–90). Chicago, IL: ACM.

di Vimercati, S. D. C., Foresti, S., Jajodia, S., Paraboschi, S., & Samarati, P. (2007). A data outsourcing architecture combining cryptography and access control. In *Proceedings of the 2007 ACM workshop on computer security architecture* (pp. 63–69). Fairfax, VA, USA: ACM.

Groth, P., Luck, M., & Moreau, L. (2005). A protocol for recording provenance in service-oriented grids. In *Principles of distributed systems: 8th International conference, OPODIS 2004, 15–17 December, Grenoble, France* (pp. 124–129). Berlin, Heidelberg: Springer.

Hoff, C., Johnston, S., Reese, G., & Sapiro, B. (2010). *Cloudaudit 1.0 – automated audit, assertion, assessment, and assurance api (a6) (Internet-draft)*. Fremont, CA, USA: IETF Network Working Group.

HP. (n.d.). HP cloudsystem: Integrating security with hp tipping point (technical white paper). Palo Alto, CA, USA: Author. Retrieved February 2013, from: http://h20195.www2.hp.com/V2/GetPDF.aspx/4AA4-4247ENW.pdf

IBM. (n.d.). IBM infrastructure as a service (IaaS): Details: Security. Armonk, NY, USA: Author. Retrieved February 2013 from: http://www-935.ibm.com/services/us/en/cloud-enterprise/tab-details-security.html

International Organization for Standardization (ISO). (n.d.). International organization for standardization. Retrieved June 2011, from: http://www.iso.org/

Jansen, W., & Grance, T. (2011). *Guidelines on security and privacy in public cloud computing: Special Report 800-144*. Gaithersburg, MD: National Institutes of Standards and Technology (NIST). Retrieved from: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909494

Karvelas, N. P. (2013). *Proofs of secure erasure*. Athens, Greece: Masters thesis, University of Athens.

Kaufman, L. M. (2009). Data security in the world of cloud computing. *IEEE Security and Privacy*, *7*, 61–64.

Li, J., Wang, Q., Wang, C., Cao, N., Ren, K., & Lou, W. (2010). Fuzzy keyword search over encrypted data in cloud computing. In *Proceedings IEEE INFOCOM, 2010, 14–19 March 2010* (pp. 1–5). San Diego, CA, USA: IEEE.

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud security and privacy: An enterprise perspective on risks and compliance*. O'Reilly Media, Inc.

Park, J. S., Spetka, E., Rasheed, H., Ratazzi, P., & Han, K. J. (2012). Near-real-time cloud auditing for rapid response. In *Advanced information networking and applications workshops (WAINA), 26th international conference on 26–29 March 2012* (pp. 1252–1257). Fukuoka, Japan: IEEE.

PCI Security Standards Council. (2010). *Payment card industry (pci) data security standard – requirements and security assessment procedures version 2. 0*. Wakefield, MA, USA: Author. Retrieved from: https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

Perito, D., & Tsudik, G. (2010). Secure code update for embedded devices via proofs of secure erasure. In D. Gritzalis, B. Preneel, & M. Theoharidou (Eds.), *ESORICS 2010 proceedings of the 15th European conference on research in computer security 2010, Athens, Greece* (pp. 643–662). Berlin, Heidelberg: Springer.

Prafullchandra, H., Owens, K., Richter, C., McAndrew, T., Overbeek, D., Chaubal, C., et al. (2011). *PCI-compliant cloud reference architecture. HyTrust, Savvis, Coalfire Systems*. VMWare and Cisco Systems. Retrieved from: http://www.hytrust.com/downloads/ht_wp_pcidss_ref_arch.pdf

Rasheed, H. (2011). Auditing for standards compliance in the cloud: Challenges and directions. In *Proceedings of the 2011 international Arab conference on information technology (ACIT 2011), 10–13 December*. Riyadh, Saudi Arabia: ACIT.

Ruth, G., & Chandrasekaran, A. (2012). *Critical capabilities for public cloud storage services*. Stamford, CT: Gartner, Inc. Retrieved from: http://www.gartner.com/technology/reprints.do?id=1-1D9C6ZM&ct=121216&st=sg

Simmhan, Y. L., Plale, B., & Gannon, D. (2005). A survey of data provenance in e-science. *SIGMOD Record*, *34*(3), 31–36.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1–11.

The European Network and Information Security Agency (ENISA). (2009). *Cloud computing: Benefits, risks and recommendations for information security*. Heraklion, Greece: Author. Retrieved from: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

Wang, C., Cao, N., Li, J., Ren, K., & Lou, W. (2010). Secure ranked keyword search over encrypted cloud data. In *Distributed computing systems (ICDCS), 2010 IEEE 30th international conference on June 2010* (pp. 253–262). IEEE.

Wang, C., Chow, S. S., Wang, Q., Ren, K., & Lou, W. (2011). Privacy-preserving public auditing for secure cloud storage. *IEEE Transactions on Computers*.

Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. (2011). Enabling public verifiability and data dynamics for storage security in cloud computing. *IEEE Transactions on Parallel and Distributed Systems*, *22*(5), 847–859.

Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010). Security and privacy in cloud computing: A survey. In *Semantics knowledge and grid (SKG), 2010 sixth international conference on 1–3 November 2010* (pp. 105–112). Beijing, China: IEEE.

Zhu, Y., Wang, H., Hu, Z., Ahn, G. J., Hu, H., Stephen, S., et al. (2011). Dynamic audit services for integrity verification of outsourced storages in clouds. In *Proceedings of the 2011 ACM symposium on applied computing, SAC'11* (pp. 1550–1557). New York, NY, USA: ACM.

Hassan Rasheed, received his Ph.D. in Computer Engineering from the University of Florida in 2009. He is currently an Assistant Professor at Taif University in Taif, Saudi Arabia. His previous academic and industrial affiliations include the Air Force Research Lab, Morgan State University and the University of Florida. His research interests include information and network security, business intelligence and text analytics.

Please cite this article in press as: Rasheed, H. Data and infrastructure security auditing in cloud computing environments. *International Journal of Information Management* (2013), http://dx.doi.org/10.1016/j.ijinfomgt.2013.11.002