Deloitte.

Managing Fraud Risks in a Cloud Computing environment

A Whitepaper

May 2016

www.deloitte.com/in

Introduction

Cloud computing is increasingly being adopted by organizations worldwide due to its ease, cost benefits and flexibility in usage. India too is not lagging behind on this global trend and the cloud computing market in the country is pegged at around USD 838 million (as of end of 2015[1]). However, despite the benefits, cloud computing has also exposed individuals and organizations to various security and fraud related threats. The anonymity and scale provided by the cloud environment makes it very attractive for fraudsters to exploit. Various studies reveal that as much as USD 3 billion has been lost to frauds perpetrated over cloud computing networks in the last few years.[2]

There are challenges in applying existing digital forensic practices in investigating issues in cloud networks. Most tools currently used for digital forensic investigations are largely intended for offline investigations with the assumption that the storage media under investigation is within the control of an investigator. Limited tools and methodologies that can assist in extraction and analysis of potential evidence (in a manner acceptable in legal proceedings) are significantly dependent on the service models or deployment model opted on a cloud infrastructure and the way a cloud service provider is managing those models. Non-availability of expert advice and inadequate oversight, right from the initial stages of planning a migration to a cloud infrastructure, can expose a user to legal or compliance issues later.

This whitepaper attempts to sensitize organizations to the various risks associated with different cloud computing models, and builds the case for developing a robust cloud computing environment with forensic-ready investigation infrastructure.

We hope you find this whitepaper useful. We look forward to your feedback and support.

Regards

Rohit Mahajan
APAC Leader
Partner and Head- Forensic
Financial Advisory
Deloitte India

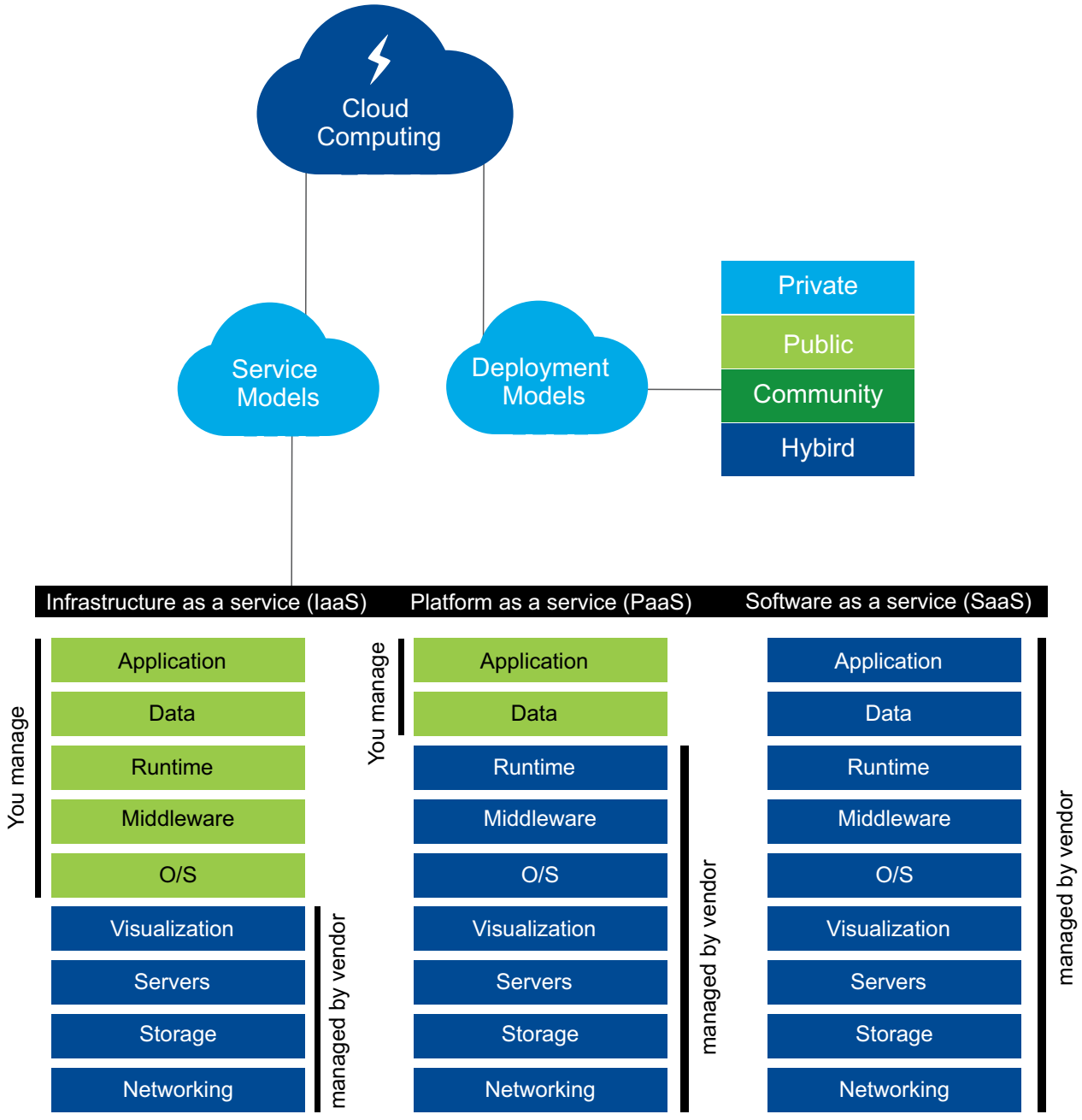
Jayant Saran
Partner
Forensic
Financial Advisory
Deloitte India

1. Source: http://articles.economictimes.indiatimes.com/2015-01-19/news/58231846_1_cloud-services-cloud-computing-cloud-management

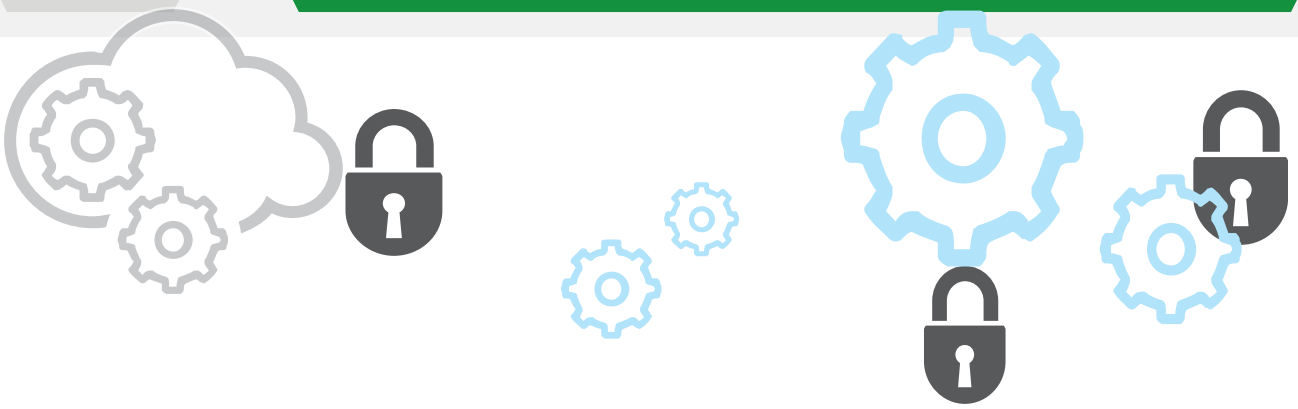
2. Source: http://www.theregister.co.uk/2011/05/14/playstation_network_attack_from_amazon/

Understanding the current cloud computing environment

Cloud Computing, typically, consists of three service and four deployment models. The characteristics define the capabilities/ benefits available to users, whereas the service and deployment models define the possible means of utilizing cloud service. From a fraud risk perspective, a large number of challenges may arise from the way cloud computing is deployed at organizations. This could also be because each type of deployment model allows a varying degree of resource sharing and corresponding security limitations.



Deployment model	Extent of resource sharing & Risks
Private Cloud	Minimum. The infrastructure is operated solely for an organization, managed by self or third parties.
Community Cloud	High. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns.
Public Cloud	Very high. Infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
Hybrid Cloud	Depend upon customization. The cloud infrastructure is a composition of two or more clouds entities.



Potential hurdles in managing fraud risks associated with cloud computing

When an organization adopts a cloud solution managed by a third-party, dependencies get created with the Cloud Service Provider (CSP), with respect to legal liability, the risk universe, incident escalation, incident response, and other areas. The actions of the CSP and fellow cloud users can impact the organization in various ways. Some of the key challenges identified include[3]

Difficulty in integrating enterprise risk management programs. Cloud service providers and their customer organizations are likely to have separate enterprise risk management (ERM) programs to address their respective universe of perceived risks. In practice, we have observed only a small number of cases (involving very high-value contracts) where CSPs have attempted to integrate parts of their ERM programs with those of their customers.

Inclusion of risks faced by the CSP. The universe of risks confronting an organization using third-party cloud computing is a combination of risks the individual organization faces along with a subset of the risks that its CSP is facing. The organization therefore has to doubly guard itself.

Lack of transparency. A CSP is unlikely to divulge detailed information about its processes, operations, controls, and methodologies from a risk management standpoint. For instance, cloud customers have little insight into the storage location(s) of data, algorithms used by the CSP to provision or allocate computing resources, the specific controls used to secure components of the cloud computing architecture, or how customer data is segregated within the cloud.

Security and compliance concerns. Depending on the processes cloud computing is supporting, security and retention issues can arise with respect to complying with regulations and laws including various data privacy and protection regulations enacted in different countries. Examples of these data privacy and protection laws would include the USA PATRIOT Act, the EU Data Protection Directive, Malaysia's Personal Data Protection Act 2010, and India's IT Act.

Non-Availability/ Accessibility to certain critical information. In the cloud, data is located on hardware outside of the direct control of an organization. Depending on the cloud solution used (SaaS, PaaS, or IaaS), a cloud customer organization may be unable to obtain and review network operations or security incident logs because they are in the possession of the CSP. The CSP may be under no obligation to reveal this information or might be unable to do so without violating the confidentiality of the other tenants sharing the cloud infrastructure.

High-value cyber-attack targets. The consolidation of multiple organizations operating on a CSP's infrastructure makes it a more attractive target than a single organization, thus increasing the likelihood of attacks. Consequently, the inherent risk levels of a CSP solution in most cases are higher with respect to confidentiality, data integrity and availability.

Risk of data leakage. A multi-tenant cloud environment in which user organizations and applications share resources presents a risk of data leakage that does not exist when dedicated servers and resources are used exclusively by one organization. This risk of data leakage presents an additional point of consideration with respect to meeting data privacy and confidentiality requirements.

3. Source: http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf

How these hurdles can impact investigations on the cloud

Complexity of the cloud infrastructure and the volatility of data create various challenges for digital forensic investigations. These include:

- **Recovery of deleted data:** Cloud providers share resources among many tenants. In a non-cloud environment, a deleted document will usually exist in a dedicated memory location, until it is overwritten. In a cloud environment, due to the dynamic nature of storage media management, a data set once deleted, may soon be overwritten.
- **Authorization and access to data:** This depends on the service level agreement (SLA) defined between a client and the service provider.
- **Challenges with system architecture:** Different cloud providers have their own system architecture and deployment models for clients. Whether details related to these are shared for forensic data collection and analysis would depend on the SLA.
- **Authentication & chain of custody:** The distributed and dynamic nature of cloud computing makes authentication (Hash Verification) and chain of custody verification difficult.
- **Privacy protection:** Unless it is a private cloud, it may be difficult to ensure that only data required by an investigator is identified and the privacy of other tenants is protected.
- **Jurisdictional and geolocation issues:** The data could be hosted on a server outside the national borders and hence the legal jurisdiction of the investigating agency can be questioned.
- **Dependencies with multiple clouds systems:** Collection and correlation of evidence lying across multiple CSPs may be a challenge. A customer may have a storage solution with one CSP (e.g. Dropbox), computing resource with another (e.g. Amazon) and all emails with another (e.g. Google). Activities like log analysis, recreation of crime event etc. may be difficult.
- **Meta data, log formats and time zones:** You may have multiple logs formats, different metadata for evidences from different time zones, further complicating the process of evidence gathering.
- **Data mirroring:** Data mirroring over multiple machines lying in different geographies introduce another set of difficulties for a forensic investigator.
- **Seizure/ confiscation of a computing resource:** This would be a challenge as multiple tenants are operating on a single resource.
- **Data on virtual machine (VM) environments:** Once decommissioned or moved to another VM environment, may pose another set of challenges such as the fact that the moment a VM is shut down, all evidence including logs and metadata gets washed out.
- **Other technical, legal and organizational challenges:** NIST has identified 65 such challenges for investigators conducting digital forensics in a cloud environment. However, it does not propose solutions at this stage as the focus is on developing a clear and accurate understanding of the challenges.

Managing fraud risks on the cloud through forensic readiness

It is important that companies assess their fraud risks on the cloud. To achieve this they need to understand inherent risks and gaps in the control mechanism and prepare a forensic readiness program. In the absence of adequate controls and forensic readiness, it may not be possible to collect any data that can be processed for discovering evidence.

Forensic readiness refers to the level of preparation an organization has to respond to forensic investigations in the future. These could be in response to internal and regulator driven investigations with sufficient provisions and support obligations in the SLA with the CSP. Depending on the type of incident, the nature of investigation and methodology for gathering evidences may differ. The SLA and service level objectives (SLO) should adequately address all possible issues that can come up during an investigation process. Some of the specific challenges in different service models identified by the Cloud Alliance Group[4] are as below:

- **Software as a Service (SaaS) model:** In this model the customer possesses no control over the operating infrastructure such as the network, servers, operating systems or source code of the application in use, thus limiting customers' forensic capabilities. In most cases, SaaS environment demands that the forensic examiner rely on Application Logs. As such, the required forensic functionality must be specified in the service level objectives (SLOs) incorporated into the Service Level Agreement between the company and the CSP.SLOs may include requirements for notification, identification, preservation, and access to potential evidence sources.
- **Platform as a Service (PaaS) Environment:** One of the main advantages of the PaaS model is that the customer controls the developed software application. However, the PaaS model still requires coordination with the CSP as the actual operation of this application will occur within the CSP's infrastructure. As a result, the customer must clearly identify the responsibilities of the CSP when the need for a forensic investigation arises. As such, required forensic functionality must be specified in the SLO incorporated into the SLA.
- **Infrastructure as a Service (IaaS) Environment:** Compared with SaaS and Paas, an IaaS deployment model offers a greater range of potential evidence sources under control of the customer. However, some (perhaps essential) data like DNS Logs, Host Operating System Logs, management portal logs etc might only exist in the CSP infrastructure. This requires that the customer clearly document in SLA the responsibilities of the CSP when the need for a forensic investigation arises.

The amount of accessible evidence may also be severely constrained by cost, technology (e.g., available storage space), multi-tenancy, privacy implications and other factors relevant to a particular CSP's infrastructure. For these reasons, it is critical that the customer understand the sources of potential digital evidence that will be available from the CSP, limitations on volumes of data, and retention periods. To avoid misunderstandings and potential litigation, these understandings should be documented in SLOs within the SLA.

4. Source: Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. https://cloudsecurityalliance.org/download/mapping-the-forensic-standard-isoiec-27037-to-cloud-computing

Identifying an appropriate fraud risk management model for cloud environments

Some of the important aspects to consider before finalizing SLAs and SLOs from a forensic readiness standpoint include:

Conclusion

Cloud infrastructure poses very different sets of challenges for digital forensics investigations. Most of these challenges can be overcome by bringing in suitable provisions in SLA/ SLO and make the cloud infrastructure into a state of forensic readiness. This will not only help a digital forensic examiner in invoking required provisions for collection and examination of digital evidence but also ensure that the required environment is in place for responding to incidents, if any, occur.

Contacts

Rohit Mahajan
APAC Leader
Partner and Head- Forensic
Financial Advisory
Deloitte India
Tel: +91 22 6185 5180
Email: rmahajan@deloitte.com

Jayant Saran
Partner
Forensic
Financial Advisory
Deloitte India
Tel: +91 124 679 2000
Email: jsaran@deloitte.com

Sebastian Edassery
Director
Forensic
Financial Advisory
Deloitte India
Tel: +91 80 6627 6157
E-mail: edasserys@deloitte.com