REVIEW

2(5), November 1, 2012

ISSN 2278–5469 EISSN 2278–5450

Discovery

Cloud Security: Analysing the risks involved in Cloud computing environments

Anju Yadav☼, Kavita Rani, Anu Sheoran, Gurpreet, Neha Gupta, Juhi

Computer Science Engineering, Dronacharya College of Engineering, Gurgaon, Haryana, India

☼Corresponding author:
Anju Yadav, Computer Science Engineering, Dronacharya College of Engineering, Gurgaon, Haryana, India, E-Mail: anjuyadav5408@gmail.com

Publication History
Received: 10 September 2012
Accepted: 13 October 2012
Published: 1 November 2012

Citation
Anju Yadav, Kavita Rani, Anu Sheoran, Gurpreet, Neha Gupta, Juhi. Cloud Security: Analysing the risks involved in Cloud computing environments. *Discovery*, 2012, 2(5), 29-33

General Note

Article is recommended to print as color digital version in recycled paper.

ABSTRACT

There is a growing development of using cloud environments forever growing storage and data processing requirements. However, adopting a cloud computing paradigm has positive as well as negative effects on the data security of service consumers. This paper primarily aims to highlight the major security issues existing in current cloud computing environments. We carry out a study to explore the security mechanisms that are compulsory by major cloud service providers. We also plan a risk analysis approach that can be used by a future cloud service for analyzing the data security risks before put his confidential data into a cloud computing environment.

1. INTRODUCTION

Cloud computing security (sometimes referred to simply as "cloud security") is a growing sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Cloud security is not to be confused with security software offerings that are "cloud-based" (a.k.a. security-as-a-service).

In a cloud computing environment, the original computing infrastructure is used only when it is needed. For example, in order to process a user request, a service provider can draw the required resources on-demand, perform a specific job and then resign the not required resources and often arrange them after the job is complete. Contrary to traditional computing paradigms, in a cloud computing environment, data and the application is controlled by the service provider. This leads to a natural concern about data safety and also its protection from internal as well as external threats. Usually, in a cloud computing paradigm, data storage and computation are performed in a single datacenter. There can be various security related advantages in using a cloud computing environment. However, a single point of failure cannot be assumed for any data loss. As shown in Figure 1, the data may be located at several geographically distributed nodes in the cloud. There may be multiple points where a security breach can occur. Compared to a traditional in house computing, it might be difficult to track the security breach in a cloud computing environment.

In this paper, we present the advantages and disadvantages (in the context of data security) of using a cloud environment. We take out a small study on major cloud service providers to examine the major security issues. We examine the security mechanisms that are used by major service providers. Our study supports that in the context of data security trust is a major element which is missing in the currently existing computing models. We consider a requirement of trust management mechanism between the cloud service provider and users. espite the fact that service providers use various mechanisms to maintain high level of data security, we find a general need of trust (in the context of confidential data) among the cloud service users. In order to build a better trust mechanism, we present a risk analysis approach that can be primarily used by the perspective cloud users before putting their confidential data into a cloud. Our approach is based on the idea of trust model, principally used in distributed information systems. We extend the general idea of trust management and present its use in analyzing the data security risks in cloud computing.

The contributions of this paper can be summarized as follows:

1. We examine the major security issues in cloud computing paradigms.
2. We also carry out a study of major cloud service providers to explore the security mechanisms in the context of security issues.
3. Further, we also present a risk analysis approach that can be used by a prospective cloud service user to evaluate the risk of data security.

2. SECURITY ISSUES AND CHALLENGES

There is a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing Software-, Platform, or Infrastructure-as-a-Service by the cloud) and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information. The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist. However, in a typical scenario where an application is hosted in a cloud, two broad security questions that arise are:

– *How secure is the Data?*
– *How secure is the Code?*

Cloud computing environment is generally assumed as a potential cost saver as well as provider of higher service quality. *Security, Availability, and Reliability* are the major quality concerns of cloud service users. Gens et. al., suggests that security in one of the prominent challenge among all other quality challenges.

2.1. Security Advantages in Cloud Environments

Current cloud service providers operate very large systems. They have sophisticated processes and expert personnel for maintaining their systems, which small enterprises may not have access to. As a result, there are many direct and indirect security advantages for the cloud users. Here we present some of the key security advantages of a cloud computing environment.

2.1.1. Data Centralization

In a cloud environment, the service provider takes care of storage issues and small business need not spend a lot of money on physical storage devices. Also, cloud based storage provides a way to centralize the data faster and potentially cheaper. This is particularly useful for small businesses, which cannot spend additional money on security professionals to monitor the data.

2.1.2. Incident Response

IaaS providers can put up a dedicated forensic server that can be used on demand basis. Whenever a security violation takes place, the server can be brought online. In some investigation cases, a backup of the environment can be easily made and put onto the cloud without affecting the normal course of business.

2.1.3. Forensic Image Verification Time

Some cloud storage implementations expose a cryptographic check sum or hash. For example, Amazon S3 generates MD5 (Message-Digest algorithm 5) hash automatically when you store an object .Therefore in theory, the need to generate time consuming MD5 checksums using external tools is eliminated.

2.1.4. Logging

In a traditional computing paradigm by and large, logging is often an afterthought. In general, insufficient disk space is allocated that makes logging either non-existent or minimal. However, in a cloud, storage need for standard logs is automatically solved.

2.2. Security Disadvantages in Cloud Environments

In spite of security advantages, cloud computing paradigm also introduces some key security challenges.
Here we discuss some of these key security challenges:

2.3.1. Data Location

In general, cloud users are not aware of the exact location of the datacenter and also they do not have any control over the physical access mechanisms to that data. Most well-known cloud service providers have datacenters around the globe. Some service providers also take advantage of their global datacenters. However, in some cases applications and data might be stored in countries, which can judiciary concerns. For example, if the user data is stored in X country then service providers will be subjected to the security requirements and legal obligations of X country. This may also happen that a user does not have the information of these issues.

2.3.2. Investigation

Investigating an illegitimate activity may be impossible in cloud environments. Cloud services are especially hard to investigate, because data for multiple customers may be co-located and may also be spread across multiple datacenters. Users have little knowledge about the network topology of the underlying environment. Service provider may also impose restrictions on the network security of the service users.

2.3.3. Data Segregation

Data in the cloud is typically in a shared environment together with data from other customers. Encryption cannot be assumed as the single solution for data segregation problems. In some situations, customers may not want to encrypt data because there may be a case when encryption accident can destroy the data.

2.3.4. Long-term Viability

Service providers must ensure the data safety in changing business situations such as mergers and acquisitions. Customers must ensure data availability in these situations. Service provider must also make sure data security in negative business conditions like prolonged outage etc.

2.3.5. Compromised Servers

In a cloud computing environment, users do not even have a choice of using physical acquisition toolkit. In a situation, where a server is compromised; they need to shut their servers down until they get a previous backup of the data. This will further cause availability concerns.

2.3.6. Regulatory Compliance

Traditional service providers are subjected to external audits and security certifications. If a cloud service provider does not adhere to these security audits, then it leads to a obvious decrease in customer trust.

2.3.7. Recovery

Cloud service providers must ensure the data security in natural and man-made disasters. Generally, data is replicated across multiple sites. However, in the case of any such unwanted event, provider must do a complete and quick restoration.

2.4. Security Issues in Virtualization

Full Virtualization and Para Virtualization are two kinds of virtualization in a cloud computing paradigm. In full virtualization, entire hardware architecture is replicated virtually. However, in Para virtualization, an operating system is modified so that it can be run concurrently with other operating systems. MM (Virtual Machine Monitor), is a software layer that abstracts the physical resources used by the multiple virtual machines. The VMM provides a virtual processor and other virtualized versions of system devices such as I/O devices, storage, memory, etc. VMM Instance Isolation ensures that different instances running on the same physical machine are isolated from each other. However, current VMMs do not offer perfect isolation. Many bugs have been found in all popular VMMs that allow escaping from VM (Virtual machine). Vulnerabilities have been found in all virtualization software's, which can be exploited by malicious users to bypass certain security restrictions or/and gain escalated privileges. Below are few examples for this:

(a) Vulnerability in Microsoft Virtual PC and Microsoft Virtual Server could allow a guest operating system user to run code on the host or another guest operating system.

(b) Vulnerability was found in VMware's shared folders mechanism that grants users of a guest system read and writes access to any portion of the host's file system including the system folder and other security-sensitive files.

3. RISK ANALYSIS

In order to create awareness among the users of cloud computing regarding the serious threats and vulnerabilities involved in cloud computing environments, a study on various risks is imperative. In the sections below, we discuss the different risks.

3.1. Security Risks

The state of preventing a system from vulnerable attacks is considered as the system's security. Security risks involved with the governmental use of cloud computing have various risk factors. Seven important identity factors for risk in a cloud computing model are: Access, Availability, and Network load, Integrity, Data Security, Data Location and Data Segregation.

3.1.1. Access

The data in a private organization allows only the authenticated users to access the data. The access privilege must be provided only to the concerned customers and auditors in order to minimize such risks. When there is an access from an internal to external source, the possibility of risk is more in case of sensitive data. Segregation of the data is very important in cloud computing as the data is distributed over a network of physical devices. Data corruption arises if appropriate segregation is not maintained. Currently, there are no federal policies addressing how Government information is accessed.

3.1.2. Availability

Availability plays a major role in cloud computing since the needs of the customers should be attended on time. A research from the University of California had tracked the availability and outages of four major cloud vendors. It was found that overload on the system caused programming errors resulting in system crashes and failures. Due to the lack of backup recovery Apple, Mobile Me, Google Gmail, Citrix and Amazon s3 reported periods of unavailability ranging from 2 to 14hrs in a span of just 60 days. This resulted in a loss of confidence among the customers and the vendors. Natural disasters can also present significant risks.

3.1.3. Network Load

Cloud network load can also prove to be detrimental to performance of the cloud computing system. If the capacity of the cloud is greater than 80%, then the computers can become unresponsive due to high volumes. The computers and the servers crash due to high volume motion of data between the disk and the computer memory. The percentage of capacity threshold also poses a risk to the cloud users. When the threshold exceeds 80%, the vendors protect their services and pass the degradation on to customers. It has been indicated that in certain cases the outage of the system to the users are still not accessed. Flexibility and scalability should be considered pivotal when designing and implementing a cloud infrastructure. Money and time also plays an important role in the design of the infrastructure. Customers will always have expectations on the durability and the efficiency of the system. Going forward the customers will also demand the need of interoperability, ability to switch providers and migration options. Another risk factor of cloud computing is the implementation of the application programming interfaces (API).

3.1.4. Integrity

Data integrity affects the accuracy of information maintained in the system. In a cloud computing model data validity, quality and security affect's the system's operations and desired outcomes. The program efficiency and performance are addressed by the integrity. An apt example for this would be that of a mobile

phone service provider who stored all the customer's data including messages, contact lists etc in a Microsoft subsidiary. The Provider lost the data and the cloud was unavailable. The customers had to wait until they got the necessary information from the cloud and the data was restored.

3.1.5. Data Security

Another key criterion in a cloud is the data security. Data has to be appropriately secured from the outside world. This is necessary to ensure that data is protected and is less prone to corruption. With cloud computing becoming an upcoming trend, a number of vulnerabilities could arise when the data is being indiscriminately shared among the varied systems in cloud computing. Trust is an important factor which is missing in the present models as the service providers use diversified mechanisms which do not have proper security measures. The following sub section describes the risks factors in cloud environments.

3.2. Privacy Risks

Several complex privacy and confidentiality issues are associated with cloud computing. In this section, we dwell on some of these different privacy risks involved in cloud computing environments. There are no laws that block a user from disclosing the information to the cloud providers. This disclosure of information sometimes leads to serious consequences. Some business users may not be interested in sharing their information, but such information is sometimes placed in the cloud and this may lead to adverse impacts on their business. For example, recently when Facebook changed its terms of service, the customers were not informed about it. This made it possible to broadcast the information of the Facebook customers to others if the privacy options were not set accordingly. This amplifies the importance of reading and understanding the Terms of Service and the Privacy Policy of the cloud providers before placing any information in the cloud. If it is not possible to understand the policy or it doesn't satisfy the needs of a user, the user can and must always opt for a different cloud provider. Several organizations have analyzed the issues of privacy and confidentiality in the cloud computing environment. These analyses have been published by a Privacy Commissioner, an industry association and a commercial publisher. Domestic clouds and trans-border clouds are two distinct cloud structures. Certain privacy issues are specific to each cloud structure. In a domestic cloud structure, the complete cloud is physically located within the same territory. This gives rise to fewer privacy issues such as whether the data is collected, used and stored in an appropriate manner and whether the data is disclosed to authorize recipients only. Another privacy issue in the domestic cloud structure is related to the rights possessed by the data owners to access their data. The circumstances under which the data owner can access and correct the data should be defined clearly. The above privacy issues can also be extended to all other cloud computing environments in general. Trans-border cloud structures have their cloud transferred across the borders. This gives rise to more privacy issues. The best example for a trans-border cloud operator is the Google Docs. People from different parts of the world store data in Google Docs. When data is transferred between different organizations located at different countries, serious privacy issues could occur. The privacy principles regulating trans-border dataflow defined by the different countries should be given importance by the cloud providers. For example Australia's National Privacy Principle 9 deals with trans-border data flows and is different from privacy regulations of other nations. Another example is where a health care provider uses a transborder cloud computing product to store and/or process patient data, they would have to ensure that the transfer is permitted under the relevant privacy law .We examined the Google Docs' Privacy Policy, which must be read in conjunction with Google's general Privacy Policy. Several noteworthy provisions were observed in it.

3.3. Risk Analysis Approach

The cloud computing service providers use various security mechanisms to ensure that all the security risks are fully taken care of. However, there are two broad questions:

– *How to estimate the risk to data security before putting a job into the cloud?*
and
– *How to ensure customers that their data and programs are safe in provider's premises?*

3.3.1. Need of a Risk Analysis Approach

The service users need a clear communication about the methods adopted by the service providers to maintain security. Current security technology provides us with some capability to build a certain level of trust in cloud computing. For example, SSL (Secure Socket Layer), digital signatures, and authentication protocols for proving authentication and access control methods for managing authorization. However, these methods cannot manage the more general concept of *Trustworthiness*. Gambetta et. al. define trust as *"trust (or, symmetrically,* Towards Analyzing Data Security Risks in Cloud Computing Environments 261 *distrust) is a particular level of the subjective probability with which an agent will perform a particular action, both before [we] can monitor such action and in a context in which it affects [our] own action"*. Based on this definition, we can say that trust is a subjective property and is affected by those actions that we cannot monitor.
Three kinds of trust models have been discussed in distributed computing:

– *Direct Trust;*
– *Transitive Trust; and*
– *Assumptive Trust*

In a cloud computing paradigm, where the data and programs cross the organizational boundaries, transitive trust and assumptive trust can be crucial for certain type of applications. A direct trust model in a cloud exists in cloud computing environments, when there is a common trust entity that performs all original entity authentications and the generation of credentials that are bound to specific entities.

3.3.2. Risk Assessment Using Trust Matrix

Although no single unit of measure is adequate to the definition of trust, several dependent variables (such as data cost), can be used to describe it. We select following two trust variables to build the trust matrix:

(a) *Data Cost*
(b) *Provider's History*

The reason for selecting these trust variables is explained here:
In cloud environment, data can be assigned a cost by the users based on the criticality of the data. The data criticality needs to be computed by the service users. There may be multiple factors that affect the data criticality. Confidential business data can be critical and therefore we can assign it a higher cost as compared to less critical data. Similarly, service provider history can be a possible parameter to estimate the risk. History includes a provider's profile of past

services. If users are dissatisfied with a particular service, they can record their experience. If a service provider do not possess a good history of data security (e.g. there is a past record of security failures), then it may also decrease the trust factor. However, other variables can also be used for building the trust matrix. Some of these variables can be Encryption support, Service Cost, Monitoring support etc.

3.3.2.1. Variable Parameters

Along with trust variables, few parameters used in measuring trust can be applied to fine-tune these trust variables. The parameters which we choose in this category are:

(a) *Data Location*
(b) *Regulatory Compliance*

As we have explained in section 2, data located at the sites which are geographically or politically sensitive would likely to have lower trust than other locations. Similarly, if a service provider is assuring the customers using a centralized regulating authority, it will lead to an increase in trust level among the service users. We make use of variable parameters as a support mechanism in the trust matrix. It is used as a validation factor that provides a support in the risk analysis.

3.3.3. Risk Analysis

We capture the relationship using a trust matrix where the axes represents the variables used. The variables used should be meaningfully related to each other. Figure 1, represents an example trust matrix with area representing the Low Risk/High Trust zone and, High Risk/Low Trust zone. This can be explained as:

– x axis represents the data cost.
– y axis represents the service provider's history.
– z axis represents the data location.

Now, it is obvious that a high data cost with poor service provider history combining with a very sensitive location will result in a higher risk/lower trust. *High trust zone* signifies the region of high trust. It can specify the security risk for the current transactions and also for future transactions with that service provider. Similarly, *low trust zone* signifies the region of low trust. As a risk preventive approach, we also define here a *trust action*, which can be taken as part of a preventive or reactive measure. For example, an added level of authentication and/or verification can be used for the activities which are related to the low trust zone. We have used these variables in a common cloud computing scenario, where we have some past statistics about the service provider. The method has been used to measure the trust and will be used for all future transactions. Based on this method, we were able to define the trust actions, for all future transactions with the service provider.

4. CONCLUSION

In an emerging discipline, like cloud computing, security needs to be analyzed more frequently. With advancement in cloud technologies and increasing number of cloud users, data security dimensions will continuously increase. In this paper, we have analyzed the data security risks and vulnerabilities which are present in current cloud computing environments. The most obvious finding to emerge from this study is that, there is a need of better trust management. We have built a risk analysis approach based on the prominent security issues. The security analysis and risk analysis approach will help service providers to ensure their customers about the data security. Similarly, the approach can also be used by cloud service users to perform risk analysis before putting their critical data in a security sensitive cloud. At present, there is a lack of structured analysis approaches that can be used for risk analysis in cloud computing environments. The approach suggested in this paper is a first step towards analyzing data security risks. This approach is easily adaptable for automation of risk analysis.

DISCLOSURE STATEMENT

There is no financial support for this research work from the funding agency.

ACKNOWLEDGEMENT

We thank friends for their timely help, giving outstanding ideas and encouragement to finish this research work successfully.

REFERENCES

1. Amazon elastic compute cloud (2008), http://aws.amazon.com/ec2/
2. Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I.: Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for delivering Computing as the 5th Utility. Future Generation Computer Systems 25, 599–616 (2009)
3. Development (2002), http://www.sun.com/blueprints
4. Diego, G.: Can we trust Trust? Oxford: Trust Making and Breaking Cooperative
5. Hayes, B.: Cloud Computing. Communications ACM 51, 9–11 (2008)
6. http://cloudcomputing.syscon.com/read/612375_p.htm
7. http://www.cloudsecurityalliance.org/guidance/ (Accessed 2 July 2009)
8. http://www.microsoft.com/technet/security/bulletin/ms07-049.mspx
9. http://www.robertwrose.com/vita/rose-virtualization.pdf
10. John, H.: Security Guidance for Critical Areas of Focus in Cloud Computing (2009),
11. Llanos, D.R.: Review of Grid Computing Security by Anirban Chakrabarti.
12. Microsoft Security Bulletin MS07-049 (2007),
13. Overview of Security Processes (2008)
14. Public Key, http://en.wikipedia.org/wiki/Public_key_certificate
15. Queue 5, 45 (2007)
16. Relations (1990)
17. Rose, R.: Survey of System Virtualization Techniques (2004),
18. Twenty Experts Define Cloud Computing (2008),
19. Two Factor Authentication, http://en.wikipedia.org/wiki/
20. Weiss, A.: Computing in the Clouds. NetWorker 11, 16–25 (2007)
21. Xen Multiple Vulnerabilities (2007), http://secunia.com/advisories/26986/