2nd International Conference on Multidisciplinary Academic Research
(ICMAR-2019), Bali, Indonesia
ISBN: 978-0-6482404-5-7
Asia Pacific Institute of Advanced Research (APIAR)
www.apiar.org.au

TOWARDS CLOUD COMPUTING SECURITY IN ORGANIZATIONS

Nader Shahata
National Institute of Informatics, Tokyo, Japan
Corresponding Email:nader@nii.ac.jp

Abstract

In the last few years, the cloud computing technology has grown from being a promising business concept to one of the fastest growing segments of the IT industry. The main concern of cloud computing is to deliver hosted services over the Internet. These services include three major categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a service (SaaS). Cloud computing is rapidly growing as a service used by many individuals and organizations internationally. For individual users, cloud computing allows them to access many services from the Internet without the need to store or run applications on their computers. For organizations, cloud computing helps to maintain huge data- centres so that they can adopt a lean and mean approach to their business. This research focuses on three major aspects of information security in cloud computing: information security issues of using cloud computing, the incident response policy to change and address these issues, and the organizations strategies to reduce the risks of adopting of cloud computing.

***Keywords*:** Cloud Computing, Security, Privacy, Internet.

1. Introduction and Purpose

Security issues in cloud computing have been growing in recent times. Corporations and individuals are concerned about how security can maintained in the cloud. In terms of those security issues or threats, a lot of professionals or experts have concluded some remediation for these security threats.

1.1 Loss of Governance

By using cloud computing the customer will lose their governance. They cede control to the Cloud Provider (CP) and that will lead to several of issues that may affect security. At the same time, service level agreement (SLAs) may not offer a commitment to supply such services on the part of the cloud provider, thus leaving a gap in security defenses.

1.1.1 Remediation:

- Cloud Provider should build a security steering council, and clearly define roles and responsibilities (Krešimir & Željko , 2010).
- Some essential security issues and responsibilities should be defined in the service level agreements (SLAs) between Cloud Provider (CP) and customers.
- Customers also should define security related responsibilities for their employees when they are using the cloud service.

1.2 Malicious Insiders

It is well known that most of the information security threats are come from inside of organizations, which is called malicious insider. There are three reasons for this kind of threat.

The first one is the convergence of IT service has enlarged the threat to cloud consumers; the second reason is the single management for customer; and the last reason is the lack of transparency into provider process and procedure.

1.2.1 Remediation

- Cloud provider should strictly manage the whole process of the supply of their cloud service to customer; and the customer should make a sufficient assessment for their supplier.
- The human resource department of organizations should determine the requirement for employee, and make this as part of legal contracts.
- Organizations should also practice all of the information security and management. Organizations also should make incidence policy for security breach.

1.3 Date Integrity

When the developer analyses the databases for cloud computing integrity issues constantly crop up. One of the issues is understanding the rules and logic that applied to the construction of the database (Linthicum 2009). Another issue is data backup. If you move an application to a cloud-based provider, it is important to know how to back up the data. This can be to traditional backup media which will need storing off-site, or you can take advantage of the physically-diverse locations to store the backups in a totally different place.

1.3.1 Remediation

Organizations should apply strong API access control for all of the sensitive data. Encrypt and protect integrity of data in transit, storage, management and destruction with a strong key generation system. They should also contractually specify provider's responsibilities for data backup, retention and deletion.

1.4 Availability of a Service/ Single Point of Failure

Many organizations worry about the availability of services in the Cloud. In 2008, there were many companies like App Engine of Apple, and Gmail of Google encountered the availability failure by many reasons. Normally, there are two main reasons for the failure of service unavailability. One is single internet service provider; the other one is that the cloud service provider is the only one provider, which is so-called single point failure. So, if this single provider encounters a failure, definitely, the business of their customer would be affected. Even if it has multiple data centres in different geographic regions using different network providers, or the company may even go out of business (Armbrust, 2009).

1.4.1 Remediation

Customers use the same service from more than one clouding service providers. Customers contractually cooperate with network providers who could provide customers with multiple internet access points to ensure the continuous network connection. Customers put this situation into their own information security plan.

1.5 Lack of Standardization

Cloud standards need to emerge to promote general adoption. But there are gaps in both industry-specific and IT standards that make it hard to standardize and automate cloud computing. The gaps are caused by two reasons. The first reason is consumers only want their favourite technology to be supported in the production of cloud computing standards; the other reason is when consumers have seen the benefits of cloud delivery, they want as quickly as possible to migrate to a standard. But the cloud computing as a new raised technology, it is quite hard to make this possible.

1.5.1 Remediation

Even though there is no complete and unified standard for Cloud Computing, and it is very hard to standardize Cloud Computing. There are many potential standards which are one or some aspects of Cloud Computing and widely accepted, these standards also called Open Standards, such as "Standards for moving applications between several Cloud platforms" and "Standards for describing resource/performance capabilities and requirements" and so on. So Cloud Computing companies could reference those standards. There are also some organizations that promote the use of best practices for providing security assurance within Cloud Computing, and promote the standardization of Cloud Computing, such as "Cloud Security Alliance", "The European Telecommunications Standards Institute (ETSI)" , "National Institute of Standards and Technology (NIST)".

1.6 Data Confidentiality and Auditability

Because most of the current cloud services are being provided by public networks, so, the system is facing the threats of more attacks, which threatens data confidentiality. Besides this, the auditability of data is also needed. Cloud computing auditing and Software as a Service (SaaS) become a major issue in the cloud. Therefore, IT auditors need to understand the cloud technologies then they need to identify the key risks based on risk-based approach (RBA) to improve effectual audits for cloud technology, however; the Risk base approach (RBA) in practice for the cloud is very complicated. IT audits of cloud computing and SaaS have a framework for assisting an effective risk assessment for this technology (Singleton, T 2010).

1.6.1 Remediation

- A Customer contractually requires the provider for the protection for their sensitive data and clearly indicates the service provider's responsibilities.

-Providers use the technologies that have been well understood and have been proved to be safe, such as encrypted storage, Virtual Local Area Networks, and network middle boxes (e.g. firewalls, packet filters); Customers should also should have the awareness to actively protect their sensitive information. For instance, before placing the sensitive data in a Cloud, they could encrypt it (Krešimir & Željko, 2010).

-There also is an organization called Cloud Audit is specially for auditing Cloud Computing Company. This organization is officially under the auspices of the Cloud Security Alliance.

1.7 Bugs in Large-Scale Distributed Systems

It is difficult to remove errors in these very large scale distributed systems. And normally, these bugs cannot be rebuilt in smaller configurations, so the debugging must be done at scale in the production data centers (Armbrust , 2009).

1.7.1Remedation

According to the study of Patrick Reynolds (USENIX 2006),visualization is one of the best ways to dealing with bugs in Distributed System. So, Cloud Computing service providers could set virtual machines and virtual environment for their Cloud Computing.

1.8 Software Licensing

Currently, the licenses of software are used to restrict the computers on which the software can run. But the traditional licensing model which is for commercial software does not suit cloud computing, cloud computing providers relied on open source software (Armbrust 2009), which are not widely used. So, the licensing model is another problem for cloud computing.

1.8.1Remedation

For making the licenses fit Cloud Computing, Commercial software companies could change their licensing structure (Armbrust, 2009). For example, they could make the licenses redistributable.

2. The Organizations Strategies to Reduce the Risks of Adopting of Cloud Computing:

There are about three risks categories that are related to cloud computing in organizations. These risks are: Policy and organizational risks, technical risks and legal risks.

2.1 Policy and organizational risks:

These risks are defined to be business related IT risks that might be found an organization when applying cloud computing service providers. These risks include:

- Loss of business reputation: The customer's bad behavior can be one of the reasons of giving a bad impact to the cloud computing in an organization. For example, IP addresses that might have a spam-prevention service included in, may cause some limitations to the applications types that can be found in the cloud (Armbrust,M., 2009)..
- Cloud service termination or failure: One of the issues that might raise here is that the financial viability which considered being a critical issue to deal with cloud computing services could be terminated as a result of financial matters. The termination will not only affect the clients but it can also down streaming the clients as well.
- Compliance challenges: Leaving customers unclear with the processes and the procedures of the provider is one of the results of the lack governance. So that, the providers of cloud computing should clear about illustrating these procedures in order to ensure that customers are on the right track and are getting appropriate guidelines (ENISA 2009).
- Lock-in: (Armbrust 2009)states that lock-in is one of the main things that jumps to the customer's mind when talking to its relation to cloud computing service providers. (Armbrust 2009).defines lock-in as "the inability of a customer to move their data and/or programs away from a cloud computing service provider" (Arrmbrust 2009). The customers here are on various types of risks like: reliability problems and the increase of prices.

2.2 Technical Risks

In this section, we will focus on the risks that are related with IT that have a direct technical impact on the cloud computing systems. These impacts can affect the host customer programs. The availability of service and distributed denial of service are two examples of these risks.

- Availability of service: This risk considers being the number one barrier to the growth of cloud computing (Armbrust 2009). (Armbrust 2009)states that there are some good companies such as Google (which sponsoring the Gmail service) has reported problem such power outages for many hours. This threat might happen and leads to a negative impact to such a company. For the customers who are far away from the cloud provider, the network performance could be a problem for them too. (Smith 2009) believes that the applications communication in long distances could be in a low speed or even not existed if there is no appropriate network performance (Smith 2009).
- Distributed denial of service: When the industry is in the process of developing, there is a high possibility for the attackers to threaten the cloud computing systems considering the services in its system is going toward a single interface. Threats like viruses could be

spread and may affect the data of other organizations that are located in the same environment.

2.3 Legal Risks

In this session, we will be focusing on the risks that are related to IT but from a legal perspective. Changes of jurisdiction and Data Privacy are two examples of these risks.

- Changes of jurisdiction: If any of the countries do not follow the international agreements, the customer data will be a subject to enforced disclosure. (Soghoian 2009)says there is no choice for an organization that works internationally, but to focus on international data management that are associated by a cloud computing model. The risks of cloud computing will grow rapidly when applying different jurisdictions.
- Data privacy: Data privacy is one of the important issues that we have to mention when talking about cloud computing. One of cloud computing risks when working with a group of organizations is spreading an organization's data to multiple locations and overlapping with another organization's data.

3. Mitigation Strategies:

3.1 Audit Control

There are some challenges when we are executing audits into the cloud environment. The providers of auditing cloud could be expensive. One solution might raise here which is sponsoring an external audit, but the presence of a formally adopted framework and a proper identified scope is important.

To ensure the effectiveness of the security programs to be compatible with the set regulations, organizations have to follow several recommendations in order to do so; these recommendations include:

- Organizations have to understand their legal duties.
- Organizations have to get the ability of classifying and labelling their data and systems.
- External risk assessment has to be applied.

Also, there are several recommendations that audits of cloud computing implementations should focus on:

- The client environment.
- The provider environment.
- The cloud itself, which consider being the link between the previous two.

3.2 Policies and Procedures:

Here our concern will be towards the development and maintenance of a huge number of used documents in order to make sure that the services of cloud computing are implied within the organizations' policies. To do that, organizations have to focus on three issues: several levels of security, legal work of the business, the assurance and security of the professionals. One of the important items that should be included in the documentation between the consumer and the provider of the cloud computing is service level agreements. Service level agreements will identify the customer needs, provides a clear framework, understanding of complex issues, decreases of conflict items and deletes unexpected possibilities.

3.3 Other forms of Governance:

There are some other tools that could allow the customers to work in a helpful environment, these tools include:

- Promoting cloud standards: The customers will be able to migrate data between service provider using an application called cloud application programming interface.
- Applying Brokers/Markets: The consumers of cloud computing will be benefit from implementing a market system for cloud services that can give the participants the opportunity in locating their providers. Due to the absence of such a system, the brokers can buy capacity from the providers of cloud computing and then sub-lease it to the customers.

Conclusion

Cloud computing is one of the current technologies which grow in the recent time. This technology has some issues in the light of information security. This research focuses on three major points: security issues of cloud computing, the incident response policy that change and address these issues, and risks management and mitigation strategies of cloud computing. In order to work within safe and successful implementations, organizations have to estimate the current risks and put some mitigation strategies to deal with them in the future. However, the customers of cloud computing need to make sure that the effective policies are acceptable in the management of data.

References

i. Armbrust,M.,Fox,A.,Griffith,R.,Joseph,A.,Katz,R.,Konwinski,A.,Lee,G.,Patterson,D.,Rabkin,A.,Stoica,I.,Zaharia,M. 2009. *Above the Clouds: A Berkeley View of Cloud Computing*. Electrical Engineering and Computer Sciences:University of California at Berkeley. [Online] Available at:http://www.eecs.berkeley.edu/Pubs/TechRpts/2009 /EECS-2009-28.pdf

ii. Krešimir, P &Željko, H, 2010. *Cloud computing security issues and challenges*. Institute of Automation and Process Computing, Faculty of Electrical Engineering Osijek, pp. 344-349.

iii. Linthicum, D., 2009. *Understanding Data Integrity Issues in the Context of Cloud Computing*. [Online] Available at: ebizq.net, http://www.ebizq.net/blogs/linthicum/2009/10/understanding_data_integrity_i.php

iv. Securing Europe's Information Society (ENISA) 2009. *Cloud computing: benefits, risks and recommendations for information security*. [Online] Available at: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

v. Singleton, T 2010. *IT Audits of Cloud and SaaS*. ISACA.org, [Online] Available at: http://www.isaca.org/Journal/Past-Issues/2010/Volume-3/Pages/IT-Audits-of-Cloud-and-Saas.aspx

vi. Smith, J 2009. *Fighting physics: A tough battle. Communications of the ACM',*pp. 60-65. [Online] Available at:http://cacm.acm.org/magazines/2009/7/32092-fighting-physics-a-tough-battle/fulltext

vii. Soghoian, C. 2009. *Caught in the cloud: Privacy, encryption, and government back doors in the Web 2.0 Era, Social Science Research Network*. [Online] Available at: http://ssrn.com/abstract=1421553

viii. USENIX 2006.*Pip: Detecting the Unexpected in Distributed Systems*. [Online] Available at: http://www.usenix.org/event/nsdi06/tech/full_papers/reynolds/reyn