International Journal of Engineering & Technology, 7 (3.27) (2018) 223-226

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Analysis of Risks and Security Requirements in Public Cloud

A. Banushri[1*], R.A. Karthika[2]

[1]*Research Scholar, Department of Computer Science & Engineering, Vels Institute of Science, Technology & Advanced Studies (VISTAS).*
[2]*Associate Professor, Department of Computer Science & Engineering, Vels Institute of Science, Technology & Advanced Studies (VISTAS). E-mail:karthika.se@velsuniv.ac.in*
**Corresponding author E-mail:banushri.annamalai@gmail.com*

Abstract

To enjoy the full benefits of cloud computing, it is necessary to have built-in security, privacy, compliance and legal requirements for the cloud implementation and use. Each industry has its own risk levels that it could work within. A company, which is planning to use public cloud services, should be conscious of the regulations and industry risks and need to monitor it and abide by the same. This is due to multi-tenant and open to all nature of public cloud. A thorough risk analysis must be done initially with a public cloud provider. The main objective is to identify the existing vulnerabilities and to implement the measures to counter those threats. There are a variety of risks such as vendor lock-in, non-compliance, poor provisioning, unauthorized access, loss of control, Service Level Agreement (SLA) violations, Internet attacks, etc. To alleviate the risks, there are several measures that could be deployed. This paper deals with mitigation mechanism, security requirements and various risks associated with public cloud.

Keywords: *Risk assessment, mitigation mechanism, service level agreement, security requirements, public cloud.*

1. Introduction

Cloud computing is a technology that is intended to allow open accessibility and enriched data sharing. The data is uploaded into a cloud and stored in a data center, which is accessed by the users. In a fully cloud based model, the data are created in the cloud, stored and accessed via a data center from the cloud by the user. The most observable risk is that accompanying with the storage of the data [6]. Those data are warehoused and retained by a third party cloud providers such as Microsoft, Amazon, Google and so on. This action has numerous risks accompanying with it [11]. It is important to safeguard the data, while uploading the data into data center to make sure that the data do not get stolen on the way into the database. It is necessary to ensure that the data stored in the data center should be encrypted all times. Access to those data should be controlled, which is applied to the hosting company including data center administrators. In addition, applying security to a data resource is the safeguard given to that resource during its use. If we use a system which provides improved accessibility and gives platform for multi-node access, then we should take in account, the risks associated with it.One way of element of control is in the form of access control, which provide a degree of risk mitigation. The area of risk associated with the use of content is not only present in the cloud computing, but also in the traditional network computing [1]. The risk is theoretically greater in cloud network because the information is stored outside your corporate walls. Some of the challenges with data security are Snooping, Unauthorized discovery, Spoofing, Accidental or Malicious deletion, denial-of-service attacks [12].The lack of privacy and security within the cloud environment is contested over whether those problems are real or perceived. However, the analysts of IT industry recommended that this is a real problem and should be astounded to permit complete deployment of cloud. Encryption is a vibrant component of protection policy of the data. In cloud, data confidentiality is a way to protect messages or data from being used or understood by unintended users of the cloud [6]. Encrypting the data is the common way to achieve data confidentiality. The data is encrypted with a key and the algorithm and the encrypted data is called cipher text. Linking security policies, to the access control method, use of content, offers a way of continuing protection of data. To relieve security risks, this type of data security must be integrated into the use of cloud computing [9].

2. Types of Cloud Computing Risks

According to Gartner, different cloud computing risks are, Regulatory Compliance, Privileged User Access, Data Segregation, Data Location, Investigative Support, Recovery, and Long-term Viability [10]. The other types of risks are Vendor Lock-in, Loss of Control, Resource Scarcity or Poor Provisioning, Multi-Tenant Environment, Failure of Supply chain, Inadequate SLA, Malware and Internet Attacks, Management of Cloud Resources, Network Outages, Physical Infrastructure ,Software and Application Licensing Risks,etc.

Vendor Lock-In Risk: [7]

As a user, there is a risk of going through a bothersome process, when migrating from one provider to another. The user has to decide on a SLA (Service Level Agreement), while accepting a cloud and categorizing Service Provider for using the Services. The custom apps will be developed for the cloud platform. Creating application environment or a backup service will be of

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

low priority. Migrating data to the new surroundings would be time-consuming and expensive, even if you get a backup [5] [2].

Issues with vendor lock-in of SaaS and mitigation mechanism

SaaS (Software as a Service) Providers have general purpose environment and the users might develop certain platform specific tools which could be used on the cloud. Your corporate data cannot be deciphered by other providers, since it might be stored in a proprietary format. To mitigate this issues, we have to make sure that the APIs provided by the vendors are well-suited for usage on other public clouds. You should be able to port your custom tools to a different provider. You must be able to export your data in Standard formats such as Excel, Oracle or text, which could be used on another site.

Issues with vendor lock-in of PaaS and mitigation mechanism

PaaS (Platform as a Service) environment might be unique for all the providers. There are not many Standards for PaaS APIs (Application Program Interface).To mitigate this issue, we have to make sure that the PaaS provider gives a development environment which is supported by other PaaS providers. To port to another platform, use Standard APIs, which makes it easier.

Issues with vendor lock-in of IaaS and mitigation mechanism

Data storage format and access procedures might make it different to move one provider to other. To mitigate this issue, test the back up of VMs (Virtual Machines) with OS and user data and copy it to an internal network or another platform. Make sure that the VMs could be restored and booted up.

Loss of Control Risk

There are various issues related to the fact that the provider controls the network and infrastructure. When IT services are organized, and which are used from a third-party platform, the provider controls the security, network, hardware resources and datacenter. The SLAs might not be appropriate to the end-user necessities. The responsibility of the Consumer and the Provider are different for SaaS, PaaS and IaaS services. In all these cases, the consumer does not have control over the infrastructure. Further, some providers might outsource the part of some services such as power maintenance, datacenter, etc. These changes makes it more difficult to meet the SLA terms for the Providers [11].

Poor Provisioning or Resource Scarcity Risk

In a public cloud, there might be several problems, which are related to infrastructure resources. When multiple users are conflicting for a static set of bandwidth, server and storage resources, it will lead to a situation where the supply would become insufficient. The available resource pool may also be inappropriately provisioned. The cloud provider might have organized less amount of resources. To meet user requirement in real-time, the dynamic resource scheduling policies are to be provided. Sometimes, the algorithm might not function properly or might mistakenly assign the similar logical resource to multiple users, which is intended for a single user. There could be some hardware failure, which leads to non-availability of resources in the pool [6].

Multi-Tenant Environment Risk

Multiple users access the same logical or physical resource in multi-tenancy. In this environment, a tenant could also access, alter, copy, or delete the data of a co-tenant. Such unsecure access to data might be devastating for the targeted cloud consumer. It will also hurt the status of the cloud provider and create loss of confidence amongst other consumers. Any occurrence of un-authorized access will lead to hazardous defamation for the cloud provider, which in-turn will influence all cloud users.

Failure of Supply Chain Risk

Cloud Providers use service partners for various aspects such as Service monitoring, network bandwidth, physical security, etc. The providers must abide by the state of affairs of the third-party vendors. Any failure on part of the partners or the vendors will impact the consumer, the provider and end-users. There might be a Service outage, corruption or unacceptable performance, data loss. Figure 1 shows the reach or scope of outsourced services.

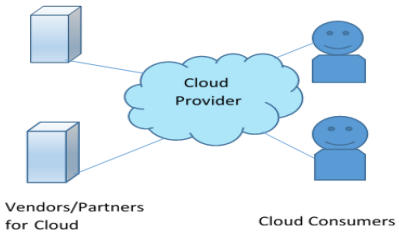

Fig. 1: Scope of outsourced services

Inadequate SLA Risk

SLAs (Service Level Agreement) directive the estimated service availability, security and performance.SLAs essentially be able to meet the user and compliance requirements. The document helps to create responsibility areas and settle difference of opinion. An inadequate SLA could turn out to be inadequate for the user load management or inappropriate for compliances by business verticals. In some cases, service provider may be assimilated by another provider. In such cases, inadequate SLAs may need to be substituted, leading to alternative discussion and risk of non-compliance [2].

Malware and Internet Attack Risk:[3][7]

In a cloud, anyone can open an account, as the level of Selection is minimal. Because of this, the malicious users could create their account and might launch attacks. These attacks could be engaged to disable a particular customer site or disable the entire cloud service within the cloud. The two common forms of Internet attacks are:

Economic denial of sustainability (EDoS) attacks

These are the attacks which could use up cloud resources, and therefore increase costs for other cloud users to the stages that they cannot pay anymore for the resources.

Distributed denial of service (DDoS) attacks

This is a kind of an attempt by hackers to disable a network or services for users. It is an effort made by one or more hackers to indeterminately or temporarily interrupt services by server overload. One of the most frequently used procedures is to saturate the target server or network with plenty of external communication requests. Because of this, it cannot respond to genuine user traffic or it could respond so leisurely, that it becomes basically useless.

Network Outages Risk

One of the key cloud risks is network outage. During an outage, the most recent data changes could not be accessed from other sites, because the updates might not have been replicated. For those who used the cloud for customer services, or for E-commerce, it results in hard sales losses. During an outage, there might not be adequate synchronization to redirect requests to other cloud providers or to another datacenter [12].

Physical Infrastructure Risk

There could be various security risks in the physical infrastructure of IT assets and data center. Some of the physical risks are:

- Theft of the equipment, which belongs to the customers and is located at the hosting provider or at the data center of the cloud.
- The physical scanning of visitors may be defective and somebody can enter the data canter with items which could damage the IT hardware.
- Malicious insiders and employees, who have confidential access and could damage the equipment in the datacenter [3].
- There can be power outages and complications in the power backup mechanisms (UPS, diesel generator, etc.)
- The Precision Air Conditioning (PAC) is acute and any failures would cause an increase in the surrounding temperature and influence the delicate IT equipment in the datacenter.

Besides, the datacenter must be located in a safer region. It should be away from the high-activity areas such as banks, airports, stadiums, refinery pipelines and freeways. It should be in a less seismic region, so as to be less obstructed by earthquakes. To make sure proper security of the physical properties, the SLA should obviously list out all the responsibilities of the consumer and the cloud provider.

Software and Application Licensing Risk

The main problem in the cloud is to control the use of licenses for database, middleware, applications, development tools, OS, etc. Conventionally, there are three categories of licenses. They are:

- Licenses based on user count.
- Licenses based on Devices.
- Enterprise-wide License.

We should know the number of users and resources contained by each server to get a sufficient number of licenses. But, in the cloud, the number of Servers used for a service or an application and the amount of resources in each depends on the user load. Each server could have a flexible amount of memory or CPU.There are various risks related to the user of licensed software in a cloud. They are:

- Cloud providers increase the server farm horizontally (more servers added) and vertically (resources is added in each server) to meet performance SLAs and to meet user load.
- It is ineffective to check the usage count, as the amount of resources may differ.

The solution is to work with the application vendors and the cloud providers to decide on the license count requisite. This will eliminate the risk of violating license agreements. [2]

Table 1: Risks in Cloud Environment & Influence on Customer Business

S.No	Risks	Impact of the Risk
1	Vendor Lock-in	High
2	Failure of Supply Chain	Medium
3	Failure of Cloud providers	Medium
4	Loss of Management Control	Medium
5	Not meeting Regulatory Compliances	High
6	Shortfall of Cloud Resources	Low
7	Data Integrity issues	High
8	Incompatible SLA	Medium
9	Failure of Cloud Resource	High
10	Violating Software License Agreement	High
11	Service non-availability	Medium

3. Risk Assessment and Management

The first thing we must do, is a through risk analysis with a public cloud provider. The objective is to pinpoint the potential and existing vulnerabilities. Then, we need to implement the methods to counter the threats. There are various measures that we can deploy to mitigate risks. It is necessary to have updated backup copies of cloud data at an alternate Cloud provider's site or within your corporate network. If there is service outage or data damage at the primary site, it is necessary to make a plan to quickly switch to another public cloud or to an internal IT environment [4].
Risk Management involves the following tasks:

- Risk identification.
- Risk analysis and evaluation.
- Selection of counter measures.
- Deployment of appropriate counter measures.
- Continuous monitoring to evaluate effectiveness of the solution [1].

4. Security Requirements in a Public Cloud

There are various risks related to privacy and data security in the cloud because of essential multi-tenancy and ease of accessing services. Cross-examine your service provider on essential hazards of keeping data at a shared location and about the risk-mitigation measures. Some of the security requirements in a public cloud are: [8]

Privileged User Access

Consumers need to know the data access mechanisms which is executed at the cloud provider's site.
How are the activities of administrators managed?
What are the administrators hiring and training programs?
Who can get to the data with privileged administrator rights and what are their qualifications and experience?
How does the provider control data access?
Answers to all these questions are useful for compliance verification, audits and fixing problems.

Regulatory Compliance

Even though the data is in a public cloud, the customers are ultimately legally responsible for their process compliance and data security. Providers are exposed to compliance requirements and external audits. Cloud providers who refuse to undergo the inspection should not be used for critical services.

Investigative Support

Your cloud provider should be prepared to and technically capable of providing end-to-end help for inquest of breaches, problems or illegal access. The providers must be able to show where and how the activities are logged. The logs should be maintained separately for each customer. The vendor should readily and successfully complete such inquiries and discovery requests in the past.

Data Location

As a consumer, you might not know where the replicated data copies and backup are stored. But for certain data, such as health,

personal and financial information, you are required to act upon country or local privacy policies, and should keep the data within a geographical boundary. Your cloud provider must be agreeable to act in accordance with your business needs.

Data Separation

As a consumer, you should know how cloud providers keep data separate for different customers in a multi-tenant Cloud. You should know whether the data is encrypted and how the key are managed? How the encryption is designed, implemented and tested?

Service Recovery

Make sure your provider imitates the data and provides services in case the major site is down. Find out the time to restore services and the data loss if any, in case the chief site goes down.[13]

Long- Term Business Sustainability

Preferably your provider should not go broke, be financially in a close-fitting corner or close down the business. Be sure and know how to move your data to another cloud provider. You should know how to have a backup at another public cloud of your data for redundancy.[14]

5. Conclusion

Each industry vertical has its own risk levels and government protocols that it must work within. There are privacy, Security, compliance and legal issues to factor in when selecting a public cloud provider. The objective of Security and risk analysis is to identify prevailing and possible vulnerabilities. The risk is managed by various tasks such as Risk identification, analysis and evaluation, selecting the counter methods and deploying the suitable counter methods to mitigate the risks. This paper analysis different types of risks and deals with mitigation mechanism, security requirements associated with public cloud.

References

[1] Khan AU, Oriol M, Kiran M, Jiang M & Djemame K, "Security risks and their management in cloud computing", *IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom)*, (2012), pp.121-128.

[2] Luna J, Suri N, Iorga M & Karmel A, "Leveraging the potential of cloud security service-level agreements through standards", *IEEE Cloud Computing*, Vol.2, No.3,(2015), pp.32-40.

[3] Priyanka Reddy, G. S., & Surendar, S. M. A. (2017, January 1). A review article on performance comparison of CNTFET based full adders. *Journal of Advanced Research in Dynamical and Control Systems*.

[4] Djemame K, Armstrong D, Guitart J & Macias M, "A Risk Assessment Framework for Cloud Computing", *IEEE Transactions on Cloud Computing*, Vol.4, No.3, (2016).

[5] Benfateh A, Gharnati F & Agouti T, "ISA-based model for risk assessment in cloud computing environment", *5th International Conference on Multimedia Computing and Systems*, (2016), pp. 377-383.

[6] Durga MG, "Study on data security mechanism in cloud computing", *2nd International Conference on Current Trends in Engineering and Technology (ICCTET)*, (2014), pp.13-17.

[7] Alani MM, "Securing the Cloud: Threats, Attacks and Mitigation Techniques", *Journal of Advanced Computer Science and Technology*, (2016).

[8] Castiglione A, Choo KKR, Nappi M & Narducci F, "Biometrics in the cloud: Challenges and research opportunities", *IEEE Cloud Computing*, Vol.4, No.4,(2017), pp.12-17.

[9] Patil TA, Pandey S & Bhole AT, "A review on contemporary security issues of cloud computing", *1st International Conference on Intelligent Systems and Information Management (ICISIM)*, (2017), pp.179-184.

[10] Gartner Security and Risk Management, 2018, (Internet Source).

[11] Bouchaala M, Ghazel C, Saidane LA & Kamoun F, "End to End Cloud Computing Architecture Based on A Novel Classification of Security Issues", *IEEE/ACS 14th International Conference on Computer Systems and Applications*, (2017), pp.303-310.

[12] Sharma PK, Kaushik PS, Agarwal P, Jain P, Agarwal S & Dixit K, "Issues and challenges of data security in a cloud computing environment", *IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, (2017), pp.560-566.

[13] A Mukanbetkaliyev, S Amandykova, Y Zhambayev, Z Duskaziyeva, A Alimbetova (2018). The aspects of legal regulation on staffing of procuratorial authorities of the Russian Federation and the Republic of Kazakhstan Opción, Año 33. 187-216.

[14] G Cely Galindo (2017) Del Prometeo griego al de la era-biós de la tecnociencia. Reflexiones bioéticas Opción, Año 33, No. 82 (2017):114-133