PROCEEDINGS OF SCIENCE

A Study on Security Risk in Cloud Computing

Lijun Chen
Institute of software ecology and artificial intelligence, South China Institute of Software Engineering of Guang Zhou university
Guangzhou, 510990, China
E-mail: 372158286@qq.com

Xiaoru Chen
South China Institute of Software Engineering of Guang Zhou University
Guangzhou, 510990, China
E-mail: 479170369@qq.com

With the rapid development of the global economy and internet technology, cloud computing technology has been advanced at a rapid pace. Cloud computing technology is a new development model for large-scale computing after distributed computing, parallel computing and grid computing. In the in-depth application of cloud computing services, cloud programs continue to expand. Due to the popularity of cloud computing services, cloud service security has become an important factor affecting its application and development. Cloud computing technology will be a public resource shared among computing resources, storage resources and others; it has also led to the lack of transparency and less control of IT assets, resulting in many business concerns about data loss and destruction. At present, the main risks to cloud computing lie in sharing, insecure interfaces, privileged user visits, identity counterfeiting, data security, management and legal affairs. To reduce or eliminate the main risks of cloud computing, encryption technology is adopted, with the introduction of strict identity authentication mechanism, strengthen management and safety supervision, as well as improvement on information security laws, regulations and other countermeasures.

ISCC2017
16-17 December 2017
Guangzhou, China

1. Introduction

Network security problems related to cloud computing services can be divided into two categories: security technology problems encountered by cloud service providers and data security problems of customers using cloud services [1], with the shared responsibility. Cloud service providers must ensure that the hardware infrastructure is secure enough. They also need to protect customers' data and applications. Users must also take measures to consolidate their applications and use more effective cryptographic authentication measures. In fact, when an enterprise deploys an application to the cloud, it does not have the ability to protect hardware facilities and important data. As a result, the potentially important data of the enterprise may receive threats by internal attacks. According to the latest report of the cloud security alliance, internal attacks are the sixth biggest threats to cloud services [2]. Therefore, the cloud service provider must make sure that the employees who have access to the cloud server are qualified after being thoroughly inspected. In addition, the cloud data center should constantly monitor all suspicious activities.

The risk of cloud service is quite difficult to deal with. It could be possible that no result comes up after lots of work has been done, or it is too late to find the result out. . Some IT companies even choose to forego the use or sale of cloud services. In the last five years, this has been increased by more than 100%. While cloud computing offers many benefits, most IT company providers are aware of the security risks ,so they charge in advance in all cases to avoid payment delay.

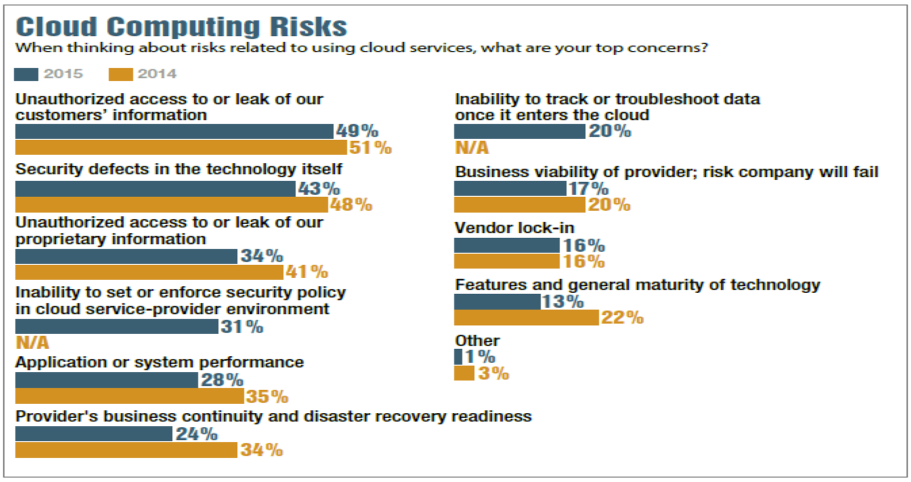

Figure 1: Cloud Computing Risk

From the survey in Figure 1, the biggest cloud service risk potentially comes from the IT people around the world. The top three are mainly about threats caused by unauthorized visit.

This paper presents the relevant study and findings as follows. Section 2 provides an overview of the two major topics of cloud computing and risk management. Section 3 demonstrates a review of the work on the previously proposed cloud computing risk management framework. Section 4 introduces the advantages and disadvantages from various aspects. Section 5 is about the result and discussion. Section 6 makes the conclusion suggestions for future work.

2. Background

2.1 Cloud computing

Cloud computing is not a revolutionary proposition, but a new concept that incorporates many existing technologies and provides a configuration tool that most people are able to use. Every unit of the cloud applications can be purchased and makes it easy to use big data and hosting applications. In other words, as long there is access to the internet, cloud applications can be reached. The rapid development of cloud computing technology leads to difficulty in understanding by the public.. However, there are four important attributes that differentiate cloud computing from traditional computing [3]:

- Service basis
- Flexibility and Scalability
- Sharing over the world
- Charge by traffic

Cloud computing includes many aspects of hardware and software, and no solution can work as the entire cloud service. Cloud computing applications now typically include a combination of the following models, as shown in Table 1:

1	Infrastructure as a Service (IaaS): IaaS solutions provide enterprises or governments with hardware resources to meet the needs of users such as CPU, memory, operating system and storage.
2	Platform as a Service (PaaS): PaaS provides users with application development tools that allow for test, deployment, and application maintenance.
3	Software as a Service (SaaS): SaaS is a software deployment model that acts as a power company on a meter's scale, and the cloud computing service is charged on a flow basis or on a time basis. Vendors use software for service delivery.

Table 1: The three models of clouds

2.2 Cloud computing risk

Most businesses are aware of the benefits of the emerging cloud computing, and they are investigating if they should risk taking applications and data into the cloud. In fact, many businesses are acting now, although data security remains as a very serious problem, as shown in figure2.

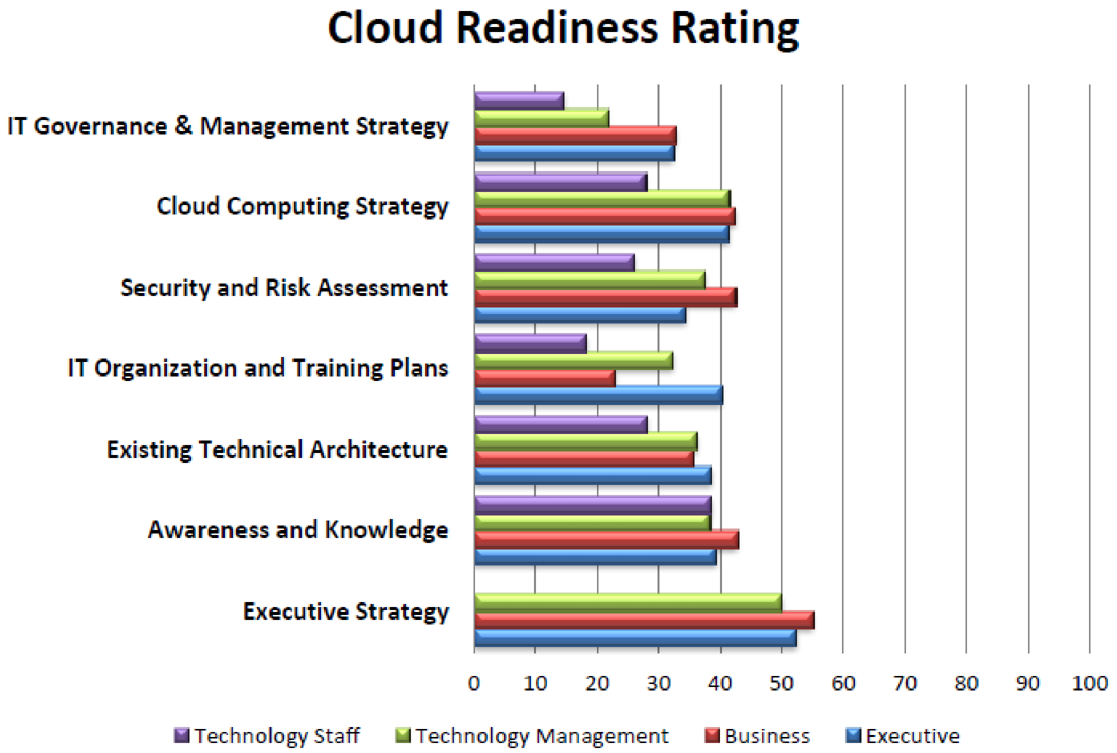

Figure 2: Security and Risk

The Shared nature of cloud computing and the nature of on-demand customization, in addition to bringing efficiency to the enterprise, also introduce new security risks, which may not be worthwhile for the enterprise to take. Here are 12 security threats that the cloud security alliance (CSA) used to point out:

(1) Data leaks

There are many data in the cloud environment facing the same threat of traditional enterprise network, but with a large amount of data stored in the cloud server, cloud providers will become a main target for hackers. In the occurrence of an attack, the severity of the potential damage depends on the sensitivity of the leaked data. Disclosure of personal financial information may make headlines, but the leak of health information, trade secrets and intellectual property can be more devastating.

Companies may incur fines or even face legal or criminal charges once data breaches happen. The cost of data breaches and customer notifications can also be astronomical. Other indirect effects, such as brand image decline and loss of business, will further affect the company for several years.

Cloud service providers typically deploy security controls to protect the cloud, but ultimately, the responsibility to protect their own cloud data falls on the client companies. CSA recommends companies adopting multi-factor authentication and encryption measures to prevent data breaches.

(2) Certificate theft and authentication are like a dummy

Data leaks and other attacks are usually the result of lax authentication, weak password, key or credential management. Companies often are bogged down during identity management when they try to allocate proper permissions based on user roles. To make it even worse, they sometimes forget to revoke permissions to users when a job function changes or when a user leaves.

(3) The interface and API are black

Every cloud service and cloud application now provides apis (application programming interfaces). The IT team uses interfaces and apis to manage and interact with cloud services, which can be done through service initiation, management, configuration, and monitoring.

From authentication and access control on encryption and behavior monitoring, security and availability of cloud services relies on the security of API. As companies may need to open up more services and credential, the risks of third party applications built on these interfaces and apis increases accordingly. Weak interfaces and leaky apis will leave businesses exposed to many security issues, and confidentiality, integrity, availability and reliability will be tested.

(4) System vulnerabilities are exploited

The loopholes in the computer operating system, or the loopholes that can be used by hackers in computer programs are now nothing new. However, with the emergence of multiple customers in the cloud computing, the problem caused by system vulnerabilities can be serious. Companies using the cloud need to share memory and database, opening another possibility of hacking.

(5) Account hijacking

The use of phishing, internet fraud and system software vulnerabilities is still an easy way of hacking. For cloud services nowadays, new content is added to such threats. Because hackers can use cloud services to capture user activity, manipulate transactions, and modify the relevant data. Using cloud computing to launch new attacks is also easy.

(6) Malicious insiders

The threat of unit insiders comes with many masks: current employees or departing employees, internal system administrators, contractors, business partners with units, etc. The malicious actions can be stolen from pure data and developed into retaliatory companies. In a cloud computing environment, malicious insiders can completely destroy the organization's entire infrastructure of the organization, or modify its important data. This security depends entirely on systems made by cloud computing service providers such as encryption systems, and the security risks are huge.

(7) Advanced persistent threat of parasites

APT is short for advanced continuous threats. CSA compares APT to an attack of "parasitic" form. APT penetrates the system, initiates attacks, and then quietly gets the data or intellectual property for a long time. The attack or steal is of no difference from a parasite.

(8) Permanent data loss

Now, with the maturity of cloud computing services and the rise of cloud services, the permanent loss of data due is already difficult. However, malicious attackers may have removed cloud data to threaten corporate businesses, and cloud data centers are powerless against natural disasters such as earthquakes and fires [4].

(9) Insufficient investigation

For any enterprise, it is conceivable that cloud services can be used without understanding the cloud-computing environment and its associated threats. It requires detailed and thorough investigation to decide whether the company's applications migrate to the cloud-computing environment, or to collaborate with another company through the cloud. Companies that do not scrutinize cloud service contracts may not notice the terms of the cloud service providers' liability when data is lost or leaked to hackers.

(10)Misuse of cloud computing services

Cloud services could be used by hackers to initiate criminal activities, such as using cloud computing to crack encryption keys, initiate DoS attacks, and send unwanted spam and phishing scams.

(11)DoS attack

DoS is the short name of distributed denial of service, which has existed for a long time. But due to the emergence of cloud services, this type of attack gets easier because the DoS attacks usually affect the availability and reliability of the application, and the application speed will be slow. Finally, being unable to open or timeout tips can make the hacker's attack more serious. A DoS attack is just like a traffic jam when commuting. There is nothing can be done but sitting in the car.

(12)Technology sharing leads to danger

The vulnerability of network sharing technology poses a huge security threat to cloud services. With cloud service providers sharing the system server and database server infrastructure, application platform and enterprise applications, if anyone places a security vulnerability, all the relevant parties may be affected. A small vulnerability or configuration error can damage the entire cloud service provider's system. [5]

3. Cloud computing risk management framework

In this article, cloud computing is considered as an innovation that a variety of organizations are planning to make use of. It is believed that risk may affect the deployment of innovation, especially cloud computing. Figure 3 displays the cloud risk map as below.

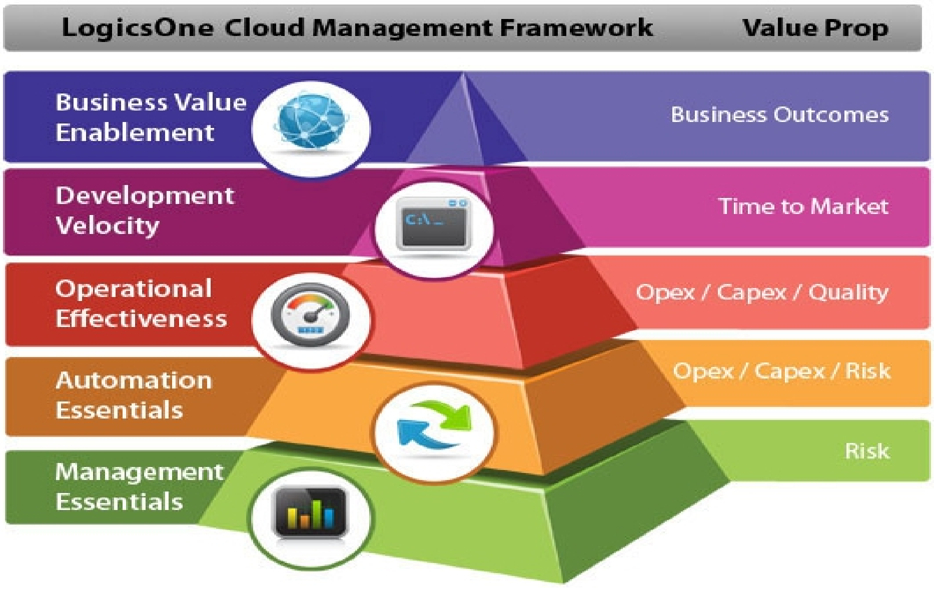

Figure 3: Risk Diagrams for Cloud Computing

3.1 Risk management for cloud consumers

For consumers of cloud services, multiple units adopt a private cloud strategy. This strategy enables avoiding risks on data privacy, basic budget funding, and related outsourcing cloud computing. Each infrastructure unit has been recently implemented with a private cloud services (SFU Vault), using the industrial standard technology to provide a flexible, safe and redundant environment to host its own services and applications. SFU Vault is a private cloud service owned and managed by SFU, which replaces high-risk foreign public cloud services such as Dropbox [6].

Mixed or public cloud services can be performed under the condition that the analysis in this paper proves that the mentioned services are mature enough, all costs considered, the remaining risk is acceptable, and they are determined to clear from the perspective of business. Each unit will consider cloud technology in the following order:

(1) Private cloud

It is recommended to solve the cloud-computing problem in a private cloud, if the full business case well proves this option.

(2) Community cloud

The solutions that reside in our province shall be prioritized, and then within China, to minimize judicial problems.

(3) Hybrid cloud

A hybrid cloud environment platform, application, software or specific goals for solution shall be considered, with the premise that the data is on all the unit systems and the data transmission will not put PII data at risk.

(4) Public cloud

It must be clear that while cloud computing is at risk, the public cloud solution shall be the best or even the only option.

3.2 Cloud computing technology for provider risk management

The following content or situation should be minimized. See table 2 below:

1	Availability (e.g., 99.999% of services and data)
2	Performance (e.g., expected response times vs. maximum response times)
3	Security/Privacy of the Data (e.g., encrypting all stored and transmitted data)
4	Logging and Reporting (e.g., audit trails of all access and the ability to report on key requirements/indicators)
5	Disaster Recovery Expectations (e.g., worse-case recovery commitment, recovery time objectives (RTO), maximum period of tolerable disruption (MPTD))
6	Location of the Data (e.g., ability to meet requirements/consistent with local legislation)
7	Data Format/Structure (e.g., data retrievable from provider in readable and intelligent format)
8	Portability of the Data (e.g., ability to move data to a different provider or multiple providers)
9	Identification and Problem Resolution (e.g., helpline, call center, ticketing system)
10	Change Management Process (e.g., changes – updates or new services)
11	Dispute Mediation Process (e.g., escalation process, consequences)
12	Exit Strategy with expectations on the provider to ensure smooth transition.

Table 2: Cloud Computing Technology for Provider Risk Management

4. Advantages and disadvantages of the risk management framework for cloud computing

Nowadays, cloud computing has not yet had a sound risk management framework. Due to the complexity of cloud computing environment and conditions, there are many reasons for making the framework more effective. Table 3 shows the benefits of the cloud computing risk management framework. Table 4 shows the weaknesses of the cloud computing framework.

(1) Table 3 shows the benefits of cloud computing

1	Cost reduction - Cloud services bring together computing resources such as all

	applications and databases, optimizing the server mix of hardware and software and dramatically enhancing the efficiency and utilization of the entire cloud-computing infrastructure.
2	Greater flexibility and scalability - As the cloud computing can dynamically change in size, the rapidly growing needs of applications can be met, without increasing investment on hardware devices.
3	Rapid Deployment of the applications - The biggest benefit of cloud computing is that it eliminates the need for a configuration environment and quickly builds up the applications without the necessity of purchasing hardware and software. The new server can be dialed up and imaged through a self-serve control console. Better yet, with a private cloud, the service provider can dial up a new server with a single call or support ticket.
4	Scaling the programs as needed - As the business applications grow or shrink, business owners can add as many disks, memories, and CPU capacities as necessary.
5	Maintenance cost reduction: Cloud computing services allow organizations to deploy fewer hardware and outsourcers, share computer skills, or network technicians. Because of the use of cloud services, businesses need fewer physical resources even without need for servers, and they do not need as many computer technicians as before, greatly reducing their maintenance cost.

Table 3: Benefits of Cloud Computing

(2) Here are the drawbacks of cloud computing, as shown in Table 4:

1	Service interruption This is one of the most significant drawbacks of cloud computing. There is no cloud provider that is immune to server outages. The cloud service system is internet based, which means that all your access is very dependent on the internet connection. Moreover, as with any hardware cloud, there may be a part of hardware failure on the cloud platform, resulting in cloud service interruption.
2	Low security and poor privacy Important business data or programs must address security and privacy, and the lesson of what happened in Code Space (hackers attacked the AWS EC2 console and permanently deleted sensitive data, forcing the company to close) shall always be learnt.
3	Vulnerability. In cloud services, every component is exposed in the internet, which means anyone can access it, and hackers make it easier to get started. Of course, a computer or server without access to the internet is completely safe, however impossible. Since it is cloud computing, it must allow the device to access the internet.
4	Limitation on control and flexibility. Cloud users of the provider's infrastructure functions and operations have not gained full control but only deal with a simple configuration and data management. Cloud provider's user agreement and management policies will also limit the customer's operating authority.
5	Cloud computing platform dependencies This dependency, also known as vendor lock-in, is another key weakness of cloud services. Since cloud service providers can not operate cross-platform, it is impossible for enterprises to migrate from one cloud platform to another. Even if the

	migration is possible, the cost will be high, in addition, the relocation also endangers the sensitive data.

Table 4: Cloud Computing Abuse

The cloud computing has powerful benefits. No matter for public or private cloud, the application, performance, security and compliance requirements, are what IT account for. The deployment of appropriate open cloud computing can save capital and enable better IT services as well as higher reliability.

5. Results and discussion

(1) All companies of either big or small business, are aware of the benefits of cloud computing and scalability. Cloud computing allows for increase in (or smaller) operation, also can enhance cost effectiveness. However, with the increase of cloud computing usage, cloud computing security is encountering more challenges.

(2) Water hole attacks of cloud

As Neeraj Khandelwal explained: "as each unit in the fight against spam and phishing aspects do better and better, tunnel attack is the latest attack methods in hacking toolkits, hackers through a web browser secretly to all these trusted web application attack."

The water hole attack has three steps. First, hackers have detailed reconnaissance and research on their targets, and they have found that target employees often visit trusted websites. Second, hackers put a vulnerability on a trusted site. Finally, when the employees visit trusted websites, the vulnerability is exploited by hackers.

The solution is to mask the vulnerability: frequently update and fix all software and limit suspicious access points.

(3) The government and other spies

"If a government department wants to access my data, they have to come to me and tell me what they want," said cloud security experts. Once the application is transferred to the cloud, all visibility is now gone - they go straight to the cloud provider and cut the unit off the loop.

If someone is going to solve this problem, cloud computing shall be used wisely: get its benefits, but do not allow anyone (or even a cloud provider) to access the encryption key. This is the best practice as recommended.

(4) Data privacy laws

VPS of speed technology solutions- Marcello Burgio and Jim McInnes, observed that cloud computing enables enterprises to achieve cross-regional capabilities. However, the reality is, in many cases, the state must abide by various laws that allow companies to take full advantage of various products of cloud computing.

The architecture of the cloud environment is the key, and the rules of data store shall be well followed in related countries. Typically, there must be laws and regulations concerning cloud security solutions. In fact, encryption makes it much easier. A cloud encryption solution can prevent data leakage from the computer. Most rules, including strict EU rules, prove that this is a good solution.

(5) Liability for Breaches

"Our use is to promote the migration of companies to the public cloud, and when you move your applications and data to the cloud, you will not be able to evade responsibility," said Amit Cohen of FortyCloud. Amazon Web Service's own security center explains that the cloud provider has secured the underlying infrastructure and the client must secure everything on the infrastructure.

What does this mean for units that are ready for migration to the cloud? Are there concerns about their responsibilities? [7]

Cloud computing has many advantages, except eliminating responsibility through cloud computing. Just as the operator is responsible for the data security of information center, he is also responsible for the security of the virtual world. That is, he must use key cryptographic techniques to ensure that only he can manage the data. The cloud provider is only responsible for infrastructure, while the operator is still responsible for the application and important data.

How easy or complex is cloud computing? Is there feasible solution?

The choice of cloud is the best choice to save money and energy, which means that people it is unnecessary to buy hardware. Of course, the solution must have the highest degree of security. This requires innovation, whose responsibility for innovation lies entirely in the providers of the cloud. In short, the best solution should be for all the benefits in a very short time.

Therefore, it is required to safeguard the computer from application vulnerabilities, but not to except using encryption keys. In addition, relevant national laws and regulations should be abided by, and encryption technology should be used to make the work easier.

6. Conclusion and future work

To summarize, cloud computing provides a virtual hardware infrastructure for government and enterprise, which can store all kinds of data and run corresponding applications. Although the advantages of cloud computing are well known, it meanwhile brings new challenges, due to the fact that the cloud operators don't need the unit code to manipulate a variety of data for the client. Encryption primitives and protocols are being studied in this paper, based on cloud computing, with the attempt to find the balance among security, efficiency, and functionality.

References

[1] Hu Xiaojing, *Challenge for University Library Managers Caused by Cloud Services* [J]. Academic Journals, 2016 (4): 7-12.

[2] MAO is gong. *The library is thinking in the era of cloud computing center.* Computing information technology BBS, 2015(6): 351:41.

[3] Yang Lifang, *the construction of modern library in the cloud computing environment* [dao. Construction of library. 2014(9): 7:9.

[4] Hu Aiping. *Construction and management of cloud library* [J]. Intelligence theory and exploration, 2016(6): 29, 30.

[5] Sun Jiawei. *Thoughts of university library in the era of cloud computing.* Digital library BBS, 2014(6): 351-4.

[6] Xue Guofei. *Application of cloud computing services in the construction of digital library in universities* [J]. Books and archives, 2016(29): 372, 373.

[7] Zhang Mingchao. *A preliminary study on the construction model of university experimental platform based on "cloud computing age"* [J]. Library science research, 2016(11):39-42.