J. Inf. Technol. Appl. Manag. 27(6): 89~99, December 2020
https://doi.org/10.21219/jitam.2020.27.6.089

ISSN 1598-6284 (Print)
ISSN 2508-1209 (Online)

The Security Establishment for Cloud Computing through CASE Study

Myeonggil Choi*

Abstract

Cloud computing is rapidly increasing for achieving comfortable computing. Cloud computing has essentially security vulnerability of software and hardware. For achieving secure cloud computing, the vulnerabilities of cloud computing could be analyzed in a various and systematic approach from perspective of the service designer, service operator, the designer of cloud security and certifiers of cloud systems. The paper investigates the vulnerabilities and security controls from the perspective of administration, and systems. For achieving the secure operation of cloud computing, this paper analyzes technological security vulnerability, operational weakness and the security issues in an enterprise. Based on analysis, the paper suggests secure establishments for cloud computing.

Keywords : Cloud Systems, Security Vulnerability, Cryptography, Hardware Weakness, Key Management

Received : 2020. 11. 06.　　Revised : 2020. 12. 28.　　Final Acceptance : 2020. 12. 30.

※ Following are results of a study on the "Leaders in Industry-university Cooperation+" Project, supported by the Ministry of Education and National Research Foundation of Korea.

* Corresponding Author, Professor, Dept.of Business Administration, Chung-Ang University, 84 HeukseoRo, DongjakGu, Seoul, 06974, Korea, Tel : +82-2-820-5454, e-mail : mgchoi@cau.ac.kr

1. Introduction

The security issues that arise from the technical and administrative characteristics of the clouds. The issues are need to be analyzed by the cluster service designers, service operators, cluster security authentication and security technologies. This paper aims to security risks of cloud from the perspective of integral approach including technology, and administrative views.

Administrative security issues that exist in public clouds is required. Cloud security issues are known partially from a technical point of view through the literature. But integrated analysis should be conducted from the integrated views of management issues and technical issues. The security issues posed by administrative characteristics of the cloud are based on the cloud service designers and service operators surrounding the cloud service, cloud security certification and security architects [Choi, 2014].

It is necessary to systematically analyze the unknown technical security problems and administrative security problems that exist in the public sectors. The problem of security of cloud is analyzed from the perspective of technology. However, there is a lack of systematic analysis of security risks derived from the operational and management problems in which administrative and technical problems are integrated [Kim and Choi, 2019].

Most of organizations have limited human resources and budgets to voluntarily solve all computing services. In a particular situation, some of the services for citizens are cloud operators that provide services to the general user. There seems to be an advantage in terms of cost-effectiveness of this service. However, in order for public institutions to use the cloud efficiently, existing security certification schemes need to supplement the overlooked aspects. In this study, we propose an administrative security policy, and an institutional security policy for the cloud that can complement such points. In this study, the proposed integrated policy options are based on the trust of the private and public sectors to fine-tune information security policies and enforce good faith obligations between service providers and service users. For achieving the aims of the study, this study conduct a case study. From the case study, we would like to an integrated way for secure cloud computing.

2. The Features and the Advantages of Cloud Service

2.1 The Feature of Cloud Computing Services

The cloud service provides a virtual machine, a network, and a storage resource provided by a cloud operator via a network with users. Users connect to cloud systems remotely over a network to use computing resources such as computer systems, software systems, storage systems. Cloud services allow users to use the system as much as they like and pay only for the capacity, so users can use the system at the minimum cost and minimize waste of computing resources [Kim and Choi, 2020].

The advantages of cloud system are that even when it is difficult or unpredictable to predict the demand for the use of computing resources, the flexibility of using the computing resources to provide smooth services is flexible and depends on the usage. The advantage is that we can ensure service continuity from the user's point of view and make efforts to minimize the costs associated with using computing. Cloud service operates largescale computer resources from the perspective of a cloud service provider, but has the advantage of realizing economies of scale that can manage resources efficiently.

The cloud computing has various configuration but has common architecture. The architectures of cloud computing are distributed computing, virtualization, system management, service platform security, billing, and user authentication.

First, distributed computing is a technology that allocates a single computing resource to users by connecting multiple resources such as multiple computers, networks, story servers, and software into one resource. Second, virtualization is a technology that provides services to users through networks, such as servers, storage, and networks, and is a core function of cloud services. Third, system management dynamically allocates resources to individual systems participating in the cloud, and improves the availability of the entire individual system. Fourth, the service platform provides an interface to the user using a cloud service. Fifth, the cloud service provides a policy to manage the amount of use, authentication and security services for cloud users.

2.2 The Advantages of Cloud Computing

We briefly review the advantage of cloud computing. First, the total cost of ownership is decreased. Cloud service providers can provide computer resources to users at low cost with economies of scale [Hwang and Choi, 2017]. Second, Cloud computing can dynamically allocate computing resources in response to computing resource demands. Cloud services flexibly respond to service demands even when it is difficult to accurately predict the number of service users and computer resource usage, or when service usage increases only during a specific period. Third, Cloud service providers provide maintenance services to systematically manage security vulnerabilities or updates. Forth, the service providers provide a variety of information protection services such as control services for cyber terrorism and vulnerability attacks, and flexible responses.

3. The Security Threats of Cloud Service

3.1 The Risk of Cloud Service

Cloud Security Alliance (CSA) presents cloud security threats as both technical and non-technical threats. Technical threats consist of technical threats and virtualization threats. Non-technical threats consist of management threats and legal and institutional threats. CSA presents seven security risks that threaten cloud computing. Security Threats Abuse or immoral use of Cloud Computing, use of insecure interfaces and APIs, malicious insiders, threats to shared technologies, threats to data loss and leakage, threats to hijack user accounts and services, and risky unknown security settings [CSA, 2011].

Second, Virtual machines can invade other virtual machines. Third, Virtual machines can access network and storage devices. Access to networks and storage devices poses a threat. Forth, the guest operating system can use the system with host privileges for management and use purposes. In this case, it is possible to acquire the authority to threaten the entire system. Fifth, all functions including virtual machine image creation and management, state control (start, pause, stop, etc.), migration, snapshot creation, virtual machine monitoring, and policy application must be managed efficiently. Sixth, the hypervisor configures the virtual network and patches the modules. The hypervisor must be able to control the equipment used in the virtual machine.

3.2 The Vulnerabilities of Cloud Service

The vulnerabilities of cloud service are summarized as following ; The privilege of guest operation systems can be upper granted. The users of virtual PC and virtualization server guest operating system can execute a specific code on a host operating system or on another user's operating system (OS) The vulnerability has been discovered that can act as a threat that can raise the user's privilege level. 2) The shared folder of the virtual machine, VMware has a vulnerability that allows a guest OS user to access, read or write to the system folder or security-sensitive files of the host OS. 3) Virtualization security problems cause breaches and vulnerabilities. Hypervisor infection, which is essential for running the host OS and cloud service, can potentially damage multiple virtual machines utilizing the hypervisor at the same time. 4) The virtual machines are interconnected, so an attacker can move from one virtual machine to another. Attackers can use the path to spread malicious behaviors such as packet sniffing, hacking, DDos attacks, and malicious code propagation. 6) Existing network security technologies (firewall, IPS, IDS) make it difficult to detect anonymous attackers in a virtualized environment. 7) Virtual machines residing on different physical platforms can move to different physical platforms, so an infected virtual machine can easily infect other physical platforms. Virtual machines infected with malicious code and virtual machines that have not been applied with security patches can easily spread malicious code to other physical platforms. Real-time live migration, which moves a virtual machine to another physical platform in real time, can transfer malicious code to a physically separate platform.

The vulnerability of hardware in cloud service has been analyzed and presended as following; 1) The fatal vulnerability of hardware design has been analyzed. Critical security vulnerabilities were found in some CPU architectures of major manufacturers such as Intel, ARM, and AMD. This issue was discovered in 2017 and was made public in January 2018. Major commercial operating system companies such as Windows, Linux, and Mac OS responded to the vulnerability by patching software. It is known that this problem can exploit the vulnerability of out-of-order execution and speculative execution used by the CPU, thereby leaking information in memory. The problem is shown in ⟨Table 1⟩.

⟨Table 1⟩ The vulnerability of hardware design

type 1 (spectre)	bounds check bypass	CVE-2017-5753
type 2 (spectre)	branch target injection	CVE-2017-5715
type 3 (melt down)	rogue data cache load	CVE-2017-5754

Spectre is a vulnerability in which a user program steals the memory of another user program, and does not leave traces of logs or access. It was named to mean ghost. Meltdown is a vulnerability that allows user programs to access the operating system privilege area. Meltdown can access the cache memory abnormally from the kernel. It can defeat any security system. An operating system patch has been released to prevent Specter and Meltdown. However, after patching the operating system, the server performance deteriorated. This security threat is a hardware design problem, so operating system patches cannot be a fundamental solution. Therefore, hardware design error is a threat that can threaten all computers and IT infrastructure. However, even after the operating system has been patched, additional threats related to design errors continue to be discovered by academia and industry.

4. Security Threats in the Operation of the Cloud System

4.1 Security Risk Embedded in Cloud Technology

This study derives and analyzes the security problems that can occur in cloud operations through in-depth interviews with cloud certification experts, cloud service providers, and cloud users.

While the cloud user accesses the virtual machine and performs tasks, the cloud system must provide encrypted communication between the user and the virtual machine. However, it is difficult to use a CC-certified hardware VPN due to the characteristics of virtual machines.

The virtual machine of the cloud system has the characteristic that the location changes from time to time. Therefore, it is not easy to used physical VPN for secure communication. For the secure communication the of cloud system, a virtual VPN is created. The virtual VPNs are not clear to secure the password because of absence of the verified password module.

4.2 Cryptography Policy of Cloud Computing

4.2.1 The Absence of Key Management Process in Cloud-Enabled Organizations

A key management policy is required for the secure use of the cloud used by the organization. Basically, key management should be done at the user's responsibility. Therefore, if the user loses the key, all data, which is previously encrypted and stored in the cloud, cannot be recovered. Data stored in the cloud may be lost due to loss or damage of keys.

To solve this problem, the cloud administrator manages the user keys. In order to solve the key management problem, it is necessary to establish a key management process policy.

4.2.2 Cloud Service Provider User'S Encryption Key Management

The cloud service provider operates a master key that encrypts the user's key. It was investigated that the cloud administrator actually owns and manages the root key required to store the user's key. Although the operator has no intention of malicious access to data, a security incident can occur if the administrator's equipment is exposed to security threats.

As a result of the investigation, the user is not provided with information or knowledge about the algorithm or system structure of the cloud encryption operation mode from the service provider. The user does not have knowledge and information about the existence and management method of the encryption/decryption key of the cloud system being used.

In the past, information leakage or security-related accidents in cloud systems were caused by administrator mistakes or rule violations rather than technical weaknesses. Therefore, the lack of knowledge related to the administrator's cloud security method is likely to cause an accident.

4.2.3 Administrator's Encryption Key Consignment Problem

The users cannot manage their encryption key, so entrust the key to the service provider. The cloud provider is completely managing the data, and there is no key management policy and guidelines. Administrators and users of most organizations entrust their encryption keys and master keys to cloud users and manage them. The cloud security of the organization is entirely determined by the management of the cloud service provider.

Technical and administrative measures such as log recording and audit of user key usage and access are required. It is necessary to divide the master key to prevent leakage or theft of the administrator key.

If the authority of the root key is required, the separated root key must be physically located in the same location and the root authority must be used. Periodic key replacement is required for the master key, root key, and encrypted master key.

4.2.4 Key and Password Backup Policy Establishment and Key Management Automation

The backup policy for user keys, passwords, files, and related data are established. But, there are no policies agreed upon by the organization. It is necessary to audit the key backup regularly and to check the background of personnel related to the key. Regular training is required for key management requirements and procedures for cloud providers, and it is necessary to develop a guideline for establishing the number of job changes and procedures for key-related personnel.

Key management should be fully automated and should not expose keys to administrators. System design is required so that the administrator's intervention is impossible in the key generation process.

4.3 Cloud Operation Management

4.3.1 Security Continuity Management

Private cloud providers are concerned that it is difficult for service providers to take responsibility for themselves if they do not violate security device regulations, regulations, and security rules. Even with certification, it is difficult to see if a security management certification project includes a breach management system or if breach event management is indeed effective. Even without a cloud operator who is legally responsible, some organizations can harm trust and assets. As a result, it is difficult for external administrators to manage directly, which can lead to trust issues.

4.3.2 The Absence of Cloud Auditor

In the current cloud architecture, there is no independent auditor. An independent third party auditor is needed. The audit of the cryptographic operating system is not smooth in the investigation of various security incidents, and investigation and support for compliance and audit response.

4.3.3 Service Provider's Internal and External Audit Procedures and Organization Needs

NIST SP 500-292 suggests that auditing bodies and organizations are needed to monitor cloud providers [NIST, 2011]. It is necessary to have professional audit personnel for policy or commerce such as the "compliance officer" of a financial institution. Personnel in charge of auditing should check whether the internal control standards to be observed by executives and employees are observed, and monitor compliance when establishing contracts or policies.

5. Case Study for Cloud Computing in K Cooperation

K Corporation is a public institution that operates social infrastructure and can make reservations for use through its website. As a business feature, it is a public service whose usage increases rapidly during a specific period. Whenever the service usage increased, it caused traffic overload on the homepage, causing service outages several times. To solve this problem, it was considered to use the cloud for the reservation system, but the current information disclosure level is violated. The cloud cannot be used for this part. Therefore, at present, a cloud system is introduced and operated on a trial basis for public relations pages or knowledge suggestion services that do not violate the information disclosure level.

5.1 The Economics Evaluation for Cloud System

K Corporation is evaluating the economics of cloud as follows.

- Up 37% reduction compared to self-deployment (5 years, based on 2 servers)
- The maintenance cost : 7% average maintenance rate applied, including operating personnel expenses and incidental expenses
- Cloud leased line (SSL VPN) usage fee (KRW 6 million per year) is excluded from the calculation as a common fee.

5.2 Advantages/Shortcomings After Introducing a Cloud System

K Corporation analyzes the advantages and disadvantages of cloud as shown in ⟨Table 3⟩.

⟨Table 2⟩ The Effect of Knowledge Presentation System(unit : million won)

	In house	Cloud	Difference
5 year	• 96 - purchase : 48 - maintenance : 48	• 60/month - lease : 48 - operation : 12	36 (37% saving)
8 year	• 125 - purchase : 48 - maintenance : 77	• 96/month - lease : 77 - operation : 19	29 (23% saving)

⟨Table 3⟩ The Advantages and Shortcomings of Introducing Cloud Systems

Advantages	• Real-time system construction and expansion without going through the purchase process • No need to secure spare equipment (parts) and upper space • System expansion and return according to plan (Auto-Scaling) • Cloud provider keeps the latest patches and settings • Use of standardized system and application environment
Shortcomings	• Concerned about self-deployment and cost increase compared to operation during long-term (6 years or more) • Cloud unsupported S/W (Unix, Oracle, etc.) system conversion unavailable • Need for on-premises system maintenance and integrated operation and management with systems operated by cloud providers

5.3 Cyber Terrorism and Security Issues

The K Corporation manager was not informed of the key management method from the cloud provider and the fact that the company managed the keys of K Corporation. Cloud providers regularly submit reports on security policies and service status.

The management supervision and security procedures have not been reflected on the cloud afteer the introduction of the cloud. There are insufficient guidelines or business processes for using the cloud.

It is necessary to divide the roles of the cloud service provider and the organization. Cloud service providers provide services and report system monitoring and operation management to the Corporation. However, the organization is not conducting service use and service level assessment.

It can be exposed to hard disk device threats that are not fully encrypted. An entirely unencrypted hard drive can contain files stored on an encrypted disk or USB area using the AutoRecovery folder. Full disk encryption can solve this problem.

The second business continuity. Private cloud providers are concerned that it is difficult for service providers to take responsibility for themselves if they do not violate security device regulations, regulations, and security rules. Even with certification, it is difficult to see if a security management certification project includes a breach management system or if breach event management is indeed effective. Even without a cloud operator who is legally responsible, some organizations can harm trust and assets. As a result, it is difficult for external administrators to manage directly, which can lead to trust issues.

The third vulnerability is the absence of cloud auditors. There are currently no isolated auditors in the cloud structure. An independent external auditor is required. Auditing cryptographic operating systems is not sufficient to investigate and respond to various security incidents and to support compliance and auditing.

However, current cloud administrators have all administrative roles. In principle, organizations need to manage their data directly. The cloud service provider should only provide infrastructure and service structure. Many organizations rely solely on cloud providers to configure and operate their services. Cloud providers

have absolute security rights to users, and cloud owners can also access the cloud, which can lead to cloud security vulnerabilities. There is no clear definition of the individual roles and responsibilities of service providers and users, providers and external audit procedures and organizations. To monitor cloud providers, we need an audit organization and an organization. We need a policy, such as a financial institution's "Compliance Officer" or a regular business professional auditor. Auditors confirm compliance with internal control standards that employees must comply with and monitor compliance as contracts or policies are established.

The fifth vulnerability is authenticate user. For secure cloud services, administrators need to be able to access only designated IPs or PCs. Role-Administrator access control is required, but problems can occur due to the lack of secure authentication devices. When DRM is provided to a DB/information system installed in the cloud, there is a problem that DRM provider cannot receive user information because SSO and SSL are applied. If the user is authenticated using a hardware security machine (HSM), the DRM service provider is fine. However, in the absence of an HSM, the physical computer on which the virtual machine is created can be an issue when accessing cloud computing.

The sixth vulnerability is collaboration between managers and users. Cloud security requires cloud service providers and users to collaborate for cloud security. However, the current cloud administrator has all of the administrative roles. In principle, the organization should manage the data directly. The cloud service provider must provide only the infrastructure and service structure. Many organizations depend entirely on cloud providers to organize and operate their services. Cloud providers have absolute security privileges for their users, and cloud holders also have access to the cloud, which can lead to cloud security vulnerabilities. There is no clear definition of the individual roles and responsibilities of service providers and users.

5.4 The Issues of Physical Devices

Cloud users are anxious about the physical location of their cloud systems. When storing data using a cloud computer, the storage location is not fixed. Some users hope that cloud services will be located within the physical area of the organization. The biggest concern about the cloud is related to the location of data storage. Providing cloud services at the physical location of the organization is likely to enhance security.

6. Conclusion and Implications

Although the cloud stores personal information and institutional information, there is a problem of key management because definition of key management is not clear. For secure key management, it is necessary to establish a distributed key management system and a key management system combined with the public domain. In the future, detailed procedures related to key generation, key storage, key deletion, and periodic key changes are needed in preparation for the future expansion of cloud use. Secure key management requires introduction of HSM and PKI scheme.

The cloud service requires cloud auditor and audit system. Thanks to the password operating system, there is a need for an independent auditor delegated its own authority to investigate various security incidents. Establishment of a survey and support system for compliance and audit response is required. Encryption algorithms and protocols

This study not only confirmed the necessity of introducing and activating the cloud in public institutions during the interview process of field officials, but also suggesting the need for security reinforcement measures.

Korea needs strict laws and institutional guidelines related to cloud. Therefore, the use of secure cloud is not spreading in our country. The problems and policy suggestions presented by this study will play a key role in helping organizations strengthen cloud security and distribute secure information in the future.

References

〔1〕 Choi, M. and Song, J., "Social Control through Deterrence on the Compliance with Information Security Policy", *Soft Computing*, Vol. 22, 2018, pp. 6765-6772.

〔2〕 Choi, M., "Information Security Management as a Bridge in Cloud Systems from Private to Public Organizations", *Sustainability*, Vol. 7, No. 9, 2015, pp. 12031-

12051.

〔3〕 Cloud Security Alliance(CSA), The Security, Trust & Assurance Registry (STAR), 2011. Available online: https://cloudsecurityalliance.org/star

〔4〕 Hwang, K. J. and Choi, M., "Effects of Innovation-Supportive Culture and Organizational Citizenship Behavior on E-government Information System Security Stemming from Mimetic Isomorphism", *Government Information Quarterly*, Vol. 34, 2017, pp. 183-198.

〔5〕 Kim, J. and Choi, M., "A Study of Personal Characteristics Influencing Cloud Intention", *Journal of Information Technology and Management*, Vol. 26, No. 3, pp. 135-157.

〔6〕 Kim, Y. and Choi, M., "A Study of Personal Characteristics Influencing Platform Business", *Journal of Information Technology and Management*, Vol. 27, No. 2, 2020, pp. 61-72.

〔7〕 Moon, Y., Choi, M., and Amstrong, D. J., "The Impact of Relational Leadership and Social Alignment on Information Security System Effectiveness in Korean Governmental Organizations", *International Journal of Information Management*, Vol. 40, 2018, pp. 54-66.

〔8〕 NIST SP 800-56c, Recommendation for Key Derivation through Extraction-then-Expansion, 2011.

Author Profile

Dr. Myeonggil Choi

He earned Ph.D. at KAIST (Korea Advanced Institute of Science and Technology). and has researched in the information security and IT Business Entrepreneurship. He currently served as a professor in the department of Business Administration, at Chung-Ang University, Seoul. His paper appeared in Government Information Quarterly(GIQ), International Journal of Information and Management(IJIM), International Journal of Entrepreneurial Behaviour & Research.