Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 581563, 5 pages
http://dx.doi.org/10.1155/2015/581563

Research Article

Decision Making for the Adoption of Cloud Computing for Sensor Data: From the Viewpoint of Industrial Security

Chang Jin Koo[1] **and JeongYeon Kim**[2]

[1] *Microsoft Customer Support and Service, 15010 NE 36 Street, Redmond, WA 98052, USA*
[2] *Sangmyung University, 20 Hongjimun 2-gil, Jongno-gu, Seoul 110-743, Republic of Korea*

Correspondence should be addressed to JeongYeon Kim; jykim@smu.ac.kr

Received 16 November 2014; Accepted 2 December 2014

Academic Editor: Damien Sauveron

Utilizing cloud computing platform to meet the new business requirements brought several business and technical benefits including cost-saving, high scalability, and business risk reductions. The new requirements of sensor-based systems for computing and communication also need cloud platforms. Based on the survey results of Korean companies, we analyze important factors of decision making for cloud platform adoption. Survey results show the cost efficiency is the most important factor for cloud platform adoption. With the economic benefits of cloud computing utilization, we provide basic arguments on data sharing issue with infrastructure providers, which requires additional investments to implement data management policies in cloud computing environment.

1. Introduction

Cloud computing, that is, utilizing service or infrastructure providers to meet the organization's required IT functionalities, is a new trend of IT services [1, 2]. From the business and technical viewpoints, there are several reasons for the popularity of cloud computing. The most compelling background of cloud computing adoption is "cost-saving" impact based on the fact that cloud platform makes it possible to reduce up-front investment and operating cost [3].

Increasing numbers of physical sensors and new requirements of sensor-based system also make business units consider cloud platforms to get the benefits of cost-saving. New concept of sensor-cloud infrastructure, virtualizing physical sensors as a virtual sensor on the cloud computing and provisioning them based on users' need, is suggested and widespread recently.

On the contrary, shifting the responsibility of IT services to cloud computing providers has several considerable topics for the business owners. In practice, the most critical factor would be the complicated Service Level Agreement. With the service usage agreement, customers of cloud computing should understand the cost allocation mechanism for service usage and the compensation plan for service outages.

Besides, many survey results on cloud computing adoption show customers concern on the sharing sensitive data with their cloud computing provider and it is counted as one of the main blocking factors of cloud computing adoption. Customers should estimate their security and privacy level for digitalized data before the decision for utilizing cloud infrastructure. Considering that poor data management practices in organization are the root cause of data leaking [4–7], implementing additional security policies on sensitive data is regarded as an inevitable requirement of cloud computing adoption. It needs additional investment though.

In this paper, we compare the business benefits of cloud computing adoption and required security investment to prevent intangible property leaking from the industrial viewpoint. Our approach is to review the benefits and additional required investment caused by adoption of cloud computing with rational arguments and actual survey results. We will compare them within few conceptualized situations to get the expected net business gain.

Most of cloud computing related researches are about technical benefits or implement methods replacing current IT functionalities. Technological categorization is widely used such as Software as a Service, Platform as a Service and

Table 1: Data protection policy according to firm size.

Size (employees)	PC user security guideline	Internal data management plan	Wireless LAN management guideline	External network usage management
5~9	73.5%	60.2%	28.1%	25.2%
10~49	73.6%	62.4%	35.9%	34.5%
50~249	84.4%	65.6%	44.5%	45.9%
250+	87.3%	71.5%	50.0%	42.7%
Total	75.5%	62.4%	34.8%	33.1%

Infrastructure as a Service, or private cloud, public cloud, and hybrid cloud. In Software as a Service (SaaS), the capability provided to the customer is to use the provider's applications running on a cloud infrastructure. The customer does not manage or control the underlying cloud infrastructure. In Platform as a Service (PaaS), the capability provided to the customer is to deploy consumer created or acquired applications onto the cloud infrastructure. The customer does not manage or control the underlying cloud infrastructure but has control over the applications or its configurations. In Infrastructure as a Service (IaaS), the capability provided to the customer is to provision fundamental computing resources. The customer does not manage or control the underlying cloud infrastructure but has control over operation systems and selected computing components. In the other categorization, private cloud refers to the cloud infrastructure operated only for an organization while public cloud refers to the cloud infrastructure made available to the general public. Besides, hybrid cloud refers to the cloud infrastructure having different compositions from private or public cloud types. However, the technical category does not represent the economic impacts of cloud computing. Some researches on the issue propose to classify applications into "wholesale" and "retail" cloud applications [3]. Wholesale cloud applications facilitate large-scale data integration and rapid and low fixed cost activities including new start-ups, or outsourcing IT functionalities. Retail cloud applications focus consumers moving their application and contents from PC to cloud platforms. The applications also make it possible to use them in many mobile devices, which transform the customer's methods to socialize, communicate, and consume the content.

We will focus on the commercial customers utilizing cloud platform for wholesale applications. In the following, we give a short description of survey results on data security and cloud computing in Korea IT environment. Then, we discuss the cost benefits of utilizing cloud computing and considerable decision making factors.

2. Surveys on Security and Cloud Computing

By adopting provided cloud platform, organization gets benefits of cost-saving, business agility, efficiency, and resource consolidation. Consumer of cloud platform also extends the benefits by focusing more on business opportunities with reserved capability.

With the service providers' technical issues, customers of cloud platform have business related and organizational issues for running business in cloud computing [8, 9]. The major concern on cloud computing is how to share computing resource for sensitive data. Considering the fact that sensitive information is routinely leaked from subcontractors of outsourced tasks with poor data management practices, the concerns of data security should be resolved before utilizing cloud computing [7, 10, 11].

The Verizon Business breach report blog (https://securityblog.verizonenterprise.com/) reported in 2008 [12] interesting facts on data security issues. External criminals were considered as the greatest threat with 73% of survey responses but achieve the least impact with 30,000 compromised records. On the contrary, inside criminals were considered as the least threat with 18% of survey responses but achieve the greatest impact with 375,000 compromised records. Partners were middle in both (73.39% and 187,500). To prevent data breaches, they suggested that service provider must be compliant with PCI DSS (Payment Card Industry—Data Security Standards).

However, infrastructure providers cannot mandate specific data protection policies between simultaneous resource users and each customer has to implement their own data protection policies on sensitive data stored in cloud environment. Additional security policy implementation requires more investment for data management while adopting cloud computing brings cost-effectiveness at early stage of adoption.

2.1. Survey Results on Security Policy.

The survey results of KISA (Korea Internet and Security Agency) conducted in 2013 [13] are a good reference for the status of security investment and cloud computing usage in Korean company. The survey was conducted with companies having more than 5 employees and at least 1 network connected computer in Korea. Final 5243 samples consist of 1,590 companies with 5~9 employees (30.3%), 1,766 companies with 10~49 employees (33.7%), 1,060 companies with 50~249 employees (20.2%), and 827 companies with more than 250 employees (15.8%).

The survey results from the sample show 75.5% or 62.4% of the organizations have PC or internal data management related guidelines but the positive reply ratios on data management are different in wireless or external network access management such as 34.8% or 33.1% as described in Table 1.

Even though security guidelines on important IT areas are not ready, security related budget compared to total IT budget shows the current limitation of Korean companies for the

Table 2: Security related budget % compared to IT total budget (Korea).

Security budget %	2011	2012
No investment	73.3%	54.1%
~1%	13.6%	28.5%
~3%	6.0%	10.9%
~5%	3.4%	3.2%
~7%	1.2%	0.7%
~10%	1.6%	2.0%
10+%	0.3%	0.5%
No data/response	0.5%	0.0%
Total	75.5%	62.4%

Table 3: Adoption rate of cloud computing service.

Size (employees)	Current using	To use within 1-2 years	To use as long term plan	To consider with cost comparison	No plan
5~9	5.90%	1.30%	2.90%	5.80%	84.10%
10~49	9.60%	0.70%	3.20%	7.10%	79.50%
50~249	9.70%	1.40%	5.70%	9.30%	73.90%
250+	9.90%	1.90%	9.30%	9.70%	69.30%
Total	7.80%	1.10%	3.30%	6.60%	81.20%

investment on data security. Table 2 shows the security related budget is almost under 1% of total IT budget (28.5%) or 0% (54.1%). KISA reported a big improvement in 2012, where companies with no investment on security area dropped from 73.3% to 54.1% of total sample, but only few companies have the security related budget more than 3% of total IT budget even in 2012.

Responses on the reasons of not having a security investment plan are the following. The main cause of no investment decision is that the company did not experience big impacts after security incidents:

(i) No damage from data leakage (64.5%).

(ii) No budget (35.8%).

(iii) No interest in security (29.2%).

(iv) No information on data management (28.9%).

(v) Already invested (12.7%).

(vi) Others (2.8%).

Contradictory to the investment for security, company identifies digitized data, intangible assets, and paper documents as top 3 items of valuable IT assets. The hardware such as servers, PCs, or facilities is still regarded as one of the important IT assets, but the response ratio recognizing intangible components of IT such as human resource as an important factor is also remarkable. Figure 1 shows the overall responses on valuable IT assets as the 1st and the 2nd selection.

2.2. Survey Results on Cloud Computing Adoption. The KISA survey shows only the 7.8% of the surveyed companies were already using cloud computing. Considering the future plan, the positive responses of utilizing cloud computing were increased to 19.8% of responses. Some of them had a short team plan (1-2 years) and some of them had a long term plan, while 81.2% of replies said they does not have any plan for cloud computing adoption. Table 3 shows the percentages of responses to cloud computing adoption and the transition cost to cloud computing is the most important factor for decision making.

3. Business Benefits versus Required Investment for Security

Cloud platform saves initial investment and operational cost of IT, but it also requires additional investment on data management scheme. The analysis of KISA survey results shows clearly that cost is the most important factor for the decision making of cloud computing adoption.

3.1. Initial Investment and Operational Benefit. The benefits of cloud computing adoption can be calculated by comparing traditional IT investment and cloud computing investment including future operation costs.

For new IT system, traditional IT investment has one time initial investment for new functionality and continuous operation cost every financial period. Cloud computing does not need any initial investment but it also has continuous operation cost. We can summarize the benefits of cloud computing adoption as required initial investment and sum of operation cost differences during expected operation period. The future saving from the difference of operation cost should be converted to current value. Also, the expected benefits should be considerably positive for decision making of cloud computing adoption.

Table 4: Adoption rate of cloud computing service.

Item	ICAMP (US)	IPA (Japan)
IT environment	University campus	Commercial company.
Damage investigation time	Calculate after damage recovery	The same as left.
Data collection method	Direct survey or interview	The same as left.
Recovery cost	Internal employee's hourly payment (labor + facility)	Internal employee's hourly payment (labor focus).
Operational damage estimation	User impact—users' hourly payment or tuition	Weighted estimation with usage of IT functionality.
Property damage calculation	28% of additional labor (internal employees + users)	Including obvious property damage only. FMS (facility management system) based damage calculation may be included.
Damage on company's brand image	52% of (recovery cost + operational damage + property damage)	N/A.
Damage on company's stock price	N/A	N/A.

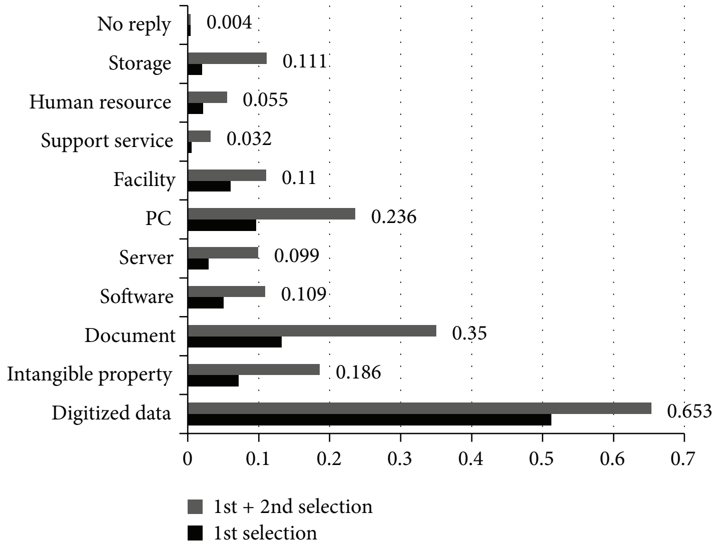


Figure 1: Selection as valuable IT asset.

For existing functionalities, same considerations can be applied except the one time initial investment for new IT functionality. However, converting current IT functionality to cloud platform needs amount of efforts in practice and the migration includes several considerations. One of them is the compatibility issue caused by keeping old version of software, which is not executable in cloud environment.

3.2. Additional Investment for Data Management. Another issue for the migration to cloud infrastructure is data security or protection to share sensitive data with service providers. Considering current investment in Korean companies, it may require additional investment for better security solutions on the overall data management schemes including employees' behaviors. Companies having important intangible properties stored as digitized data should review their policy for data privacy management and protection methods before deciding utilization of cloud computing.

Proper level of security for cloud platforms is hard to be clearly defined and mandatory investment on security depends on companies' current data management policies. More investment or complicated security plan would be better for valuable data. Korean companies have average 2% security investment of total IT budget according to KISA survey results, while U.S. companies spent 8% of total IT budget on data security.

The estimating required investment on security can be another research topic for cloud computing adoption. However, we can refer to the damage estimation method caused by data leaking [14, 15]. Table 4 shows well known property damage evaluation method caused by data security issue.

According to the survey results, most Korean companies having data leakage experiences replied they do not have any severe damage on IT operation or intellectual property. If survey participants have more information on listed damage estimation methods in Table 4, the results may be different.

4. Discussion

In this paper, we reviewed the benefits of utilizing cloud platform and challenges for running business in cloud computing in terms of data security. The survey results on secured data management and cloud platform adoption for selected Korean companies help us to understand the current status of adopting new platform and blocking factors of migration to cloud platform in Korea.

Survey results from KISA show that the cost efficiency by utilizing cloud platform is the main decision making factors. Besides, the results also provide us with several blocking issues of utilizing cloud platform such as no urgent demands with useful applications or concerns of service outage. The most critical blocking issue from potential cloud platform customers is the security issue caused by sharing sensitive internal data with infrastructure provider. Contradictory to the worries on data protection, Korea companies do not have a plan to increase the investment on security area. The average investment on security area remains 2% level of total IT budget.

The survey results show decision maker in Korean company should deliberate on proper data security level for the organization before the decision on cloud platform utilization. Proper definition of data privacy and required data protection policy is basic approaches on it. After setting up the appropriate security planning and investment, companies can consider the migration to cloud platforms and realize the benefits of it for their business.

Especially for new IT operations in sensor-based system, IT service providers also consider new challenges such as sensing latency and energy consumption, where utilization of cloud platform is inevitable. Business agility could be one of the most considerable benefits of using cloud platforms for this scenario and it could be an additional research topic for economic analysis.

Disclosure

Chang Jin Koo is the first author.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2015-H8501-15-1018) supervised by the IITP (Institute for Information & Communications Technology Promotion).

References

[1] M. Armbrust, A. Fox, R. Griffith et al., "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[2] J. Staten, *Hollow out the MOOSE: Reducing Cost with Strategic Rightsourcing*, Forrester Research, 2009.

[3] E. Bayrak, J. P. Conley, and S. Wilkie, "The economics of cloud computing," *The Korean Economic Review*, vol. 27, no. 2, pp. 203–230, 2011.

[4] R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, *A Survey on Security Issues in Cloud Computing*, Cornell University Library, Ithaca, NY, USA, 2013.

[5] P. Mell and T. Grance, *The NIST Definition of Cloud Computing*, 2011.

[6] R. T. Mercuri, "Analyzing security costs," *Communications of the ACM*, vol. 46, no. 6, pp. 15–18, 2003.

[7] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: State-of-the-art and research challenges," *Journal of Internet Services and Applications*, vol. 1, no. 1, pp. 7–18, 2010.

[8] Y. S. Gurjar and V. S. Rathore, "Cloud business intelligence—is what business need today," *International Journal of Recent Technology and Engineering*, vol. 1, no. 6, pp. 81–86, 2013.

[9] H. R. Motahari-Nezhad, B. Stephenson, and S. Singhal, "Outsourcing business to cloud computing services: opportunities and challenges," *IEEE Internet Computing*, vol. 10, 2009.

[10] L. J. Camp and S. Lewis, Eds., *Economics of Information Security*, vol. 12 of *Advances in Information Security*, Springer, New York, NY, USA, 2004.

[11] R. T. Mercuri, "Analyzing security costs," *Communications of the ACM*, vol. 46, no. 6, pp. 15–18, 2003.

[12] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, 2011.

[13] KISA, "Survey on industrial Security activities in 2013," http://isis.kisa.or.kr/board/index.jsp%20?pageId=bbsId=15itemId=43pageIndex=1.

[14] Computer Crimes and Intellectual Property Section (CCIPS), /http://www.justice.gov.

[15] T. Takemura, M. Osajima, and M. Kawano, "Economic analysis on information security incidents and the countermeasures: the case of Japanese internet service providers," in *Advanced Technologies*, pp. 73–89, INTEH, 2009.

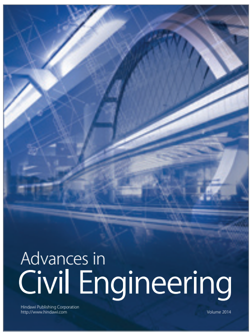
Journal of
Engineering

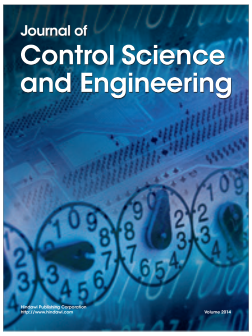
The Scientific World Journal

International Journal of
Rotating Machinery

Journal of
Sensors

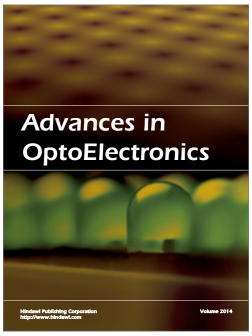
International Journal of
Distributed Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science and Engineering

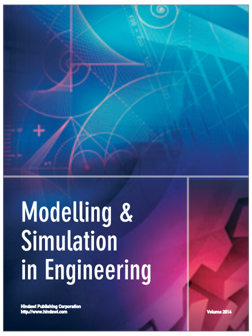
Journal of
Robotics

Journal of
Electrical and Computer Engineering

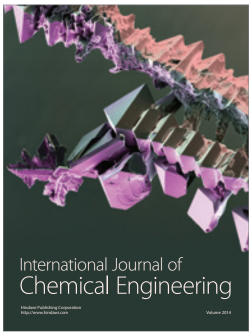

Advances in
OptoElectronics

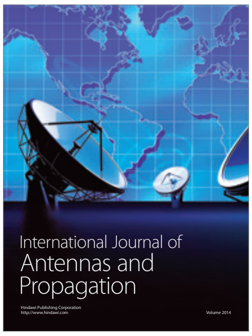
VLSI Design

International Journal of
Navigation and Observation

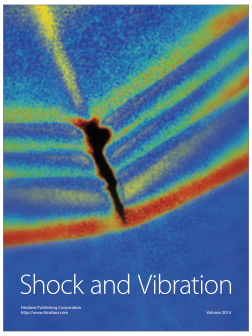

Modelling &
Simulation
in Engineering

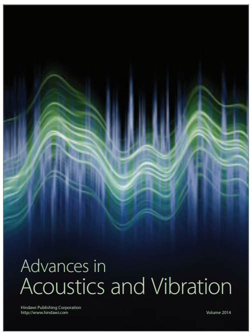
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration