The Difference of Awareness between Public Institutions and Private Enterprises for Cloud Computing Security

Junseok Oh[1], Young Bae Yoon[2], Jong Ryeol Suh [3] and Bong Gyou Lee[4,*]

[1, 2, 4]Yonsei University, [3]Korea Internet & Security Agency
{[1]jseok, [2]charismaox, [4]bglee}@yonsei.ac.kr, [3]simonsuh@kisa.or.kr

Abstract

Cloud computing has become one of the important technologies for reducing cost and increasing productivity by efficiently using IT resources in companies. The cloud computing system has mainly been built for private enterprise, but public institutions, such as governments and national institutes also have plans to introduce the system in Korea. Various researches have pointed out security problems as a critical factor to impede the vitalization of cloud computing services, but they only focus on the expected security threats and their correspondents for solving problems. Cloud computing security area is classified into managerial, physical and technical area in the research. The research derives the influence of security priorities in each area on the importance of security issues according to the recognition of workers in private enterprise and public institutions by ordered probit model. The ordered probit model is used to analyze the influences and marginal effects of awareness for security importance in each area on the degree of security priority. The results show workers in public agencies regard the technical security as the highest priority, otherwise the physical and managerial security are considered as the critical security factors in private enterprise. This research compared the difference of recognitions for the security priority in three areas between workers in private enterprise which are using cloud computing services and them in public institutions that has never used the services. It contributes to the establishment of strategies in aspect of security by providing guidelines to companies or agencies which want to introduce the cloud computing systems.

Keywords: *Cloud Computing, Security, Ordered Choice Model*

1. Introduction

The cloud computing has become one of the core technologies in order to contributes in organizational productivity and effectiveness improvement by sharing the computing resources in different devices. In the cloud computing environment, people use the IT resources and pay the price for the usage to the providers [1]. Due to this advantage, the cloud computing is recognized as the alternative that may overcome the restriction of the existing system. The cloud computing was introduced in Korea as an enterprise service of major companies in 2008. In addition, Korean government established a cloud computing activation plan: growing the size of local cloud computing market from 67.39 billion won in 2009 to 2.5 trillion won in 2014, by introducing the public section of the cloud computing. The cloud computing becomes the spotlighted technology for boosting IT industry and it is considered the main technology to increase national competiveness [2].

The security is one of the important issues in cloud computing due to the basic attribute of outsourcing [3]. So, the security problems have to be considered for introducing cloud computing, but extremely complicated and high level security confrontation may lead to an

obstacle of a financial burden to the service providers and inconvenience to the service users. Therefore, it is necessary to establish a security strategy to stability, efficiency and the usability of the guarantee services. Although many researches indicated security problems as the most threatening factor for vitalizing the cloud computing, the anticipated security threats and confrontation techniques were simply mentioned or technological solutions are only described in the researches. The perception gap for the security in the private enterprise, which uses the cloud computing, and in the public institution, which plans to be introduced it, is analyzed in this research. For the analysis, the actual perceptions of workers in private enterprises and public institution are investigated in three security sectors which are managerial, physical and technical security. The research could be applied as a guideline for establishing security strategies for introducing cloud computing by analyzing the perception gap of security importance.

2. Related Works

2.1. Cloud Computing Service

The cloud computing is a new computing paradigm in which IT resources are not installed in a user's terminal, but they are remotely borrowed the computing of the terminal [4] [5]. In cloud computing environment, people get high performance computing services regardless of the terminal specification and storage space because computing resources and Software can be rented from cloud service providers. The major enterprises have provided business cloud computing services since 2008 in Korea. The cloud computing is expanded into the personal services in 2010. The Korean government plans to cut down IT operation costs and increase world market share by introducing public cloud computing for the next five years [2]. Therefore, governmental departments lead research about constructing infrastructures, excavating service models, and developing technologies [6].

2.2. Cloud Computing Security

The security threats may easily occur to cloud computing since the threats are complex and the rental environment for IT resources are highly exposed to the diverse attack on computer networks. Gartner and ENISA discussed that the security problems should be solved at first to provide reliable cloud computing services [7] [8]. Eun [4] proposed the necessary security technologies for each cloud computing components which is divided into server, software, storage, network and terminal. Ryu [9] and Eun et al. [10] divided security technologies for cloud computing into platform, storage, network and terminal. CSA [11] addressed twelve domains for successful control of cloud computing security.

A few researches suggested combination of managerial, physical and technical security area for cloud computing services. Lee [12] analyzed the security technologies on cloud computing in terms of managerial, physical and technical security area. Kim [13] suggested appropriate managerial, physical and technical security elements based on overseas cloud computing security guidelines and the ISO 27001 to solve the specific security issues for cloud computing environment. The existing research about cloud computing security presents various security threats and confrontation techniques considered when providing services. However, most researches describe technological threats and countermeasures instead of presenting considered security strategies.

3. Research Model and Sample Data

3.1. Research Model

The relationship between variables is generally analyzed by the regression method. When the dependent variable has specific data type such as count and dummy, different models can be used for the analysis. The ordered choice model is one of models specified for the ordered data in the dependent variable. It is a selection model which is used as the dependent variable it contains discrete data associated with selection. There are two types of ordered choice model as ordered logit model and ordered probit model. The ordered probit model is used to analyze the relationship in this research. The ordered probit model is used cumulative distribution function instead of utility function to obtain the values of selection probability [14].

Formula (1) shows the relationship between a dependent variable and independent variables in the ordered probit model following the normal regression equation. Let y* represents an unobservable response variable and it captures the importance level of security for the ith individual. Here, x is a vector of independent variable and ßis a vector of estimated parameters. The importance outcome can be expressed as a function of a vector of independent variable xi using the following linear relationship.

$$y^* = \beta\, x_i + \varepsilon_i \ \left[\varepsilon_i \sim N(0,1)\right] \tag{1}$$

Generally, y* is unobserved, but y is observed and divided into number of J ranges. It is assumed that errors ε i is the standard normal distribution. Formula (2) shows the relationship between categorized criteria y* and observed response y.

$$\begin{aligned} y_i &= 0, if \ \ y^* \le \mu_0 \\ &= 1, \ if \ \ \mu_0 \prec y^* \le \mu_1 \\ &= 2, \ if \ \ \mu_1 \prec y^* \le \mu_2 \\ &\quad \vdots \\ &= J, \ if \ \ \mu_{j-1} \prec y^* \end{aligned} \tag{2}$$

The probability of ordered probit model can be combuted as follows Formula (3). Here, μ values indicate the cut values of each categogy and it is assumed that Φ(·)is the standard normal distribution cumulative function.

$$\begin{aligned} &\Pr ob(H_i = 0) = \Phi(-\beta' K_i) \\ &\Pr ob(H_i = 1) = \Phi(\mu_1 - \beta' K_i) - \Phi(-\beta' K_i) \\ &\Pr ob(H_i = 2) = \Phi(\mu_2 - \beta' K_i) - \Phi(\mu_1 - \beta' K_i) \\ &\Pr ob(H_i = J) = 1 - \Phi(\mu_{j-1} - \beta' K_i) \end{aligned} \tag{3}$$

The probit model uses the log-likelihood function to present goodness of fit of the model. The general expression for the log-likelihood function is given as ;

$$\log L = \sum_{i=1}^{n}\sum_{j=0}^{J} Y_{ij} \log[\Phi(\mu_j - \beta' K_i) - \Phi(\mu_{j-1} - \beta' K_i)] \qquad (4)$$

Because the coefficient of analyzed result can not predict the intensity of independent variable toward dependent variable, the marginal effects should be calculated to expresss the intensity. The probability of marginal effect on specific dependent variables can be calculated by partial differential formula (1) as a dependent variable. The marginal effect equation as follews;

$$\frac{\delta \Pr ob(y=j)}{\delta x_k} = \frac{\delta}{\delta x_k}[F(\mu_j - \sum_{k=1}^{K}\beta_k x_k) - F(\mu_{j-1} - \sum_{k=1}^{K}\beta_k x_k)] \qquad (5)$$

$$= [F'(\mu_{j-1} - \sum_{k=1}^{K}\beta_k x_k) - F'(\mu_j - \sum_{k=1}^{K}\beta_k x_k)]\beta_k$$

3.2 Research Variables

The dependent variable is defined as the awareness of importance in cloud computing security and independent variables are the awareness of importance in areas which is classified managerial, physical and technical security. The demographic independent variables are added gender, age, job tenure, and number of employees.

Table 1. Research Variables and Operational Definition

	Variables	Operational Definition
Dependent Variable	Importance of Cloud Computing Security	Importance to take advantage of managerial, physical, technical security for cloud computing service
Independent Variables	Importance of Managerial Security	Importance to take advantage of political, institutional, personal method for cloud computing service
	Importance of Physical Security	Importance to control of physical factors related service facility and materials for cloud computing security
	Importance of Technical Security	Importance to remove the security threatens take advantage of technology for cloud computing security

4. Analysis Results

4.1. The Awareness for Cloud Computing Security Importance in Public Institution Workers

In the aspect of cloud computing security, public institution workers recognize the importance of technical security. The importance of the security sectors variables is highly presented: managerial security 4.42, physical security 4.20 and technical security 4.47 respectively. The analysis results show technical security, age and job tenure are statistically significant at 5% significant level in public institution. In other words, the older and working longer public institutions workers, the more cloud computing security importance recognized. For the analysis results about detailed factors in cloud computing security, technical security is significant in public institution. Specially, in the case of public institutions, the coefficient of technical security is statistically significant as 1.0724, and this indicates that it is the most effective variable in the importance of cloud computing security. The coefficient of physical

security (0.0763) and managerial security (-0.2753) indicate to be effective sequentially in the awareness of cloud computing security importance but they are insignificant. In the case of the public institutions, the odds ratio of technical security is 2.9255, meaning that the importance of technical security is 2.9 times higher regarding the awareness of odds in technical security importance than the awareness of cloud computing security importance. With the same method, physical security is 1.8 times, managerial security is 0.8 times higher in odds ratio.

Table 2. Analysis Results on the Awareness of Cloud Computing Security Importance in Public Institution Workers

Independent Variables	$\hat{\beta}$	**exp($\hat{\beta}$)**	**t**	**P**
Importance of managerial security	-0.2753	0.7594	-1.4	0.162
Importance of physical security	0.0763	1.0793	0.37	0.71
Importance of technical security**	1.0724	2.9225	4.46	0
Gender	-0.1169	0.8897	-0.39	0.695
Age**	0.0639	1.0660	2.05	0.041
Job tenure**	-0.0652	0.9369	-2.52	0.012
Number of employees	-0.0031	0.9969	-0.03	0.974
cut1				4.8142
cut2				6.5216
LR chi-square				29.80
Log likelihood				-74.223337

Table 3 shows the results of marginal effects change in the recognition of cloud computing security importance for workers in public institutions. When the gender changes from male to female, the proportion of cloud computing security 'very importance' has 3.1% increases. Also, cloud computing security is recognized very importantly, as age increased, and job tenure and the size of the working place decreased. As the subjective awareness in the importance of technical security increased, proportion of marginal effects that cloud computing is 'very important' increased 26.6%. Besides this, physical security increases 1.9%, and managerial security decreases 6.8%. So, the workers in public institutions consider that cloud computing security is 26.5% higher important for one increase of technical security, and marginal effect of technical security has the highest association with the importance of cloud computing security.

Table 3. The Marginal Effect Changes of Recognized Cloud Computing Security Importance in Public Institutions Workers

	Prob(Y=3) Normal	**Prob(Y=4) Important**	**Prob(Y=5) Very important**
Importance of managerial security	0.0841	-0.0159	-0.0681
Importance of physical security	-0.0233	0.0044	0.0189
Importance of technical security	-0.3276	0.0621	0.2655
Gender	0.0349	-0.0052	-0.0297
Age	-0.0195	0.0037	0.0158
Job tenure	0.0199	-0.0038	-0.0161
Number of employees	0.0009	-0.0002	-0.0008

4.2. The Awareness for Cloud Computing Security Importance in Private Enterprise Workers

The private enterprise workers put the importance of physical security as the first security priority. The importance of the security sectors variables is highly presented: managerial security 4.29, physical security 4.04 and technical security 4.55.

Table 4. Analysis Results on the Awareness of Cloud Computing Security Importance in Private Enterprise Workers

Independent Variables	$\hat{\beta}$	exp($\hat{\beta}$)	t	P
Importance of managerial security**	0.3766	1.4574	2.98	0.003
Importance of physical security**	0.4233	1.5271	3.27	0.001
Importance of technical security	0.1173	1.1245	0.86	0.39
Gender	0.1642	1.1785	0.81	0.416
Age	0.0224	1.0227	1.36	0.174
Job tenure	-0.0149	0.9852	-0.68	0.5
Number of employees	-0.0517	0.9496	-0.81	0.421
cut1				3.8134
cut2				5.3341
LR chi2-square				27.60
Log likelihood				-196.54798

The analysis results show gender, age, job tenure and the number of employee are not statistically significant, but importance of physical and managerial security are statistically significant at 5% significance level. The coefficient of physical security is statistically significant as 0.4233, and this indicates that it is the most effective variable in the importance of cloud computing security. The managerial security is identified as the second most important variable (0.3766). The odds ratio of physical security is 1.5271, meaning that the importance of physical security is 1.5 times higher regarding the awareness of odds in physical security importance than awareness of cloud computing security importance.

Table 5 shows the results of marginal effects change in the recognition of cloud computing security importance for workers in private enterprises. When the gender changes from female to male, the proportion of cloud computing security ‘very importance’ has 4.5% increases. The other socio-demographic variables have same signs as them in the results for the public institutions but they have different magnitudes.

Table 5. The Marginal Effect Changes of Recognized Cloud Computing Security Importance in Private Enterprise Workers

	Prob(Y=3) Normal	Prob(Y=4) Important	Prob(Y=5) Very important
Importance of managerial security	-0.1177	0.0105	0.1072
Importance of physical security	-0.1323	0.0118	0.1205
Importance of technical security	-0.0367	0.0033	0.0334
Gender	-0.0529	0.0079	0.0450
Age	-0.0070	0.0006	0.0064
Job tenure	0.0047	-0.0004	-0.0042
Number of employees	0.0162	-0.0014	-0.0147

In the case of marginal effects for the security area variables, as the importance of physical security increased, the proportion of marginal effects that cloud computing is 'very important' increased 12.0%, managerial security is increased 10.7%, and technical security is increased 3.3%. So, workers in private enterprises consider that cloud computing security is 12.0% higher important for one increase of physical security, and marginal effect of physical security has the highest association with the importance of cloud computing security.

5. Conclusions

The cloud computing is introduced for improving effectiveness of businesses and group productivity in private enterprises and public institutions. The current research in security of cloud computing just describe problems and technical correspondents. However, the analysis for security priority and countermeasure is necessary to help the establishment of the security strategies for cloud computing systems. Therefore, this research analyzed the difference of awareness for the security of cloud computing in private enterprises and public institutions by ordered profit model.

The workers in public institutions estimated the importance of technical security, physical security and managerial security in sequence, while the people in private enterprises recognized physical, managerial and technical security. This result shows that the workers in the public institutions seem to highly recognize technical security which is emphasized in research reports or press releases because they do not have experiences in tasks using cloud computing. However, people that perform their tasks in private enterprises evaluated physical and managerial security as highly important security issues in the cloud computing. It is because they experienced that the security for the installation of facilities or infrastructures has to be considered and the problems were solved by institutional supports. Therefore, public institutions which want to introduce the cloud computing services have to pay more attention to the establishment of strategies for physical and managerial security. They also have to train the workers for improving consciousness in the importance of security.

The public institutions and private enterprises consider the introduction of cloud computing for the maximization of resource effectiveness. However, each group has limitations in time and capital for investing in cloud computing system. Therefore, each group needs to choose the suitable countermeasure for their state and finish the system construction. This research is the case study for finding considerable factors and it is referred as a guideline for minimizing the trial and error constructing the cloud computing security system in public institutions. However, more variables for the security in cloud computing are found in other research. So, it is necessary to perform the research in the comparison between two groups with detailed factors in three areas which are used in this research.

Acknowledgements

This research was supported by the KCC(Korea Communications Commission), Korea, under the CPRC(Communications Policy Research Center) support program supervised by the KCA(Korea Communications Agency) (KCA-2012-0902-1)

References

[1] S. J.Kim, "Information Security Plan on Cloud Computing: Information Security Management System", Management Consulting Review, vol. 2, no. 2, **(2010)**.
[2] Korea Communications Commission and Korea Internet Security Agency, Information Security guide for Cloud Services, KCC & KISA **(2011)**.

[3] S. K.Eun, "Cloud Computing Security Technology Trends", Review of Korea Institute of Information Security and Cryptology, vol. 20, no. 2, **(2010)**.
[4] E. Y. Choi, B. J. Han, D. H. Shin, H. C. Jung, and KISA Security R&D Team, "A Study for enhancing Mobile Cloud Computing Security", Proceedings of 2011 Korean Society for Internet Information Summer Conference, **(2011)** June 22-24; Cheju, Korea.
[5] Korea Communications Commission, KCC Open the Cloud Service Test Bed, **(2010)** November 11.
[6] Gartner, Assessing the Security Risks of Cloud Computing **(2008)**.
[7] European Network and Information Security Agency, Priorities for Research on Current and Emerging Network Technologies, Crete **(2010)**.
[8] J. S. Ryu, "Cloud Computing as Green IT and Security Issues", The Graduate School of Computer Information Communications, Korea University **(2010)**.
[9] S. K. Eun, N. S. Cho, Y. H. Kim and D. S. Choi, "Cloud Computing Security Technology", Electronics and Telecommunications Trends, vol. 24, no. 4, **(2009)**.
[10] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 **(2009)**.
[11] K. J. Lee, "The Study on the Issue of Cloud Computing Security and the Plans for the Personal Information Protection", Department of Information Security, The Graduate School of Information & Communications, Sungkyunkwan University **(2010)**.
[12] D. H. Kim, "A Study on the improvement and application of Information Security Management System for Cloud Computing Security", Department of Information Security, The Graduate School of Information & Communications , Sungkyunkwan University **(2011)**.
[13] K. E. Train, "Discrete Choice Methods with Simulation", Cambridge University Press, Cambridge **(2009)**.

Authors

Junseok Oh is a Research Professor at Communications Policy Research Center in Yonsei University. He received B.E degree from Information Engineering in Hansung University and M.S degree from Computer Science in Chungbuk National University in 2002 and 2004. He also received MSCE and PhD from the Pennsylvania State University in 2006 and 2010. His research interests are ubiquitous computing, cloud services, data mining, and the econometrics analysis.

Young Bae Yoon is a Master student at Graduate School of Information in Yonsei University. He received B.S. degree in Air Transportation from Korea Aerospace University in 2002. His research interests are cloud services, information technology evaluation and security.

Simon(Jong Ryeol) Suh received the MBA Graduate school of Business, Yonsei University in 2004, Republic of Korea. Currently, he is studying Graduate Program in Technology Policy PhD course, Yonsei University. Also, He is a President of Korea Internet and Security Agency(KISA).

Dr. Bong Gyou Lee who is a professor at Graduate School of Information has served as a director of Communications Policy Research Center(CPRC) in Yonsei University since 2009. Dr. Lee received a B.A. from the Department of Economics at Yonsei University and M.S, Ph.D. from Cornell University. During 2007 and 2008 he served as Commissioner of the Korea Communications Commission.