The Establishment of Security Strategies for Introducing Cloud Computing

Young Bae Yoon[1], Junseok Oh[2] and Bong Gyou Lee[3]
[1] Republic of Korea Air Force, Ministry of National Defense, Seoul, Korea
[e-mail: charismaox@gmail.com]
[2] Communications Policy Research Center, Yonsei University, Seoul, Korea
[e-mail: jseok@yonsei.ac.kr]
[3] Graduate School of Information, Yonsei University, Seoul, Korea
[e-mail: bglee@yonsei.ac.kr]
*Corresponding author: Bong Gyou Lee

Received January 2, 2013; revised February 26, 2013; accepted March 19, 2013; published April 30, 2013

Abstract

Cloud computing has become one of the most important technologies for reducing cost and increasing productivity by efficiently using IT resources in various companies. The cloud computing system has mainly been built for private enterprise, but public institutions, such as governments and national institutes, also plans to introduce the system in Korea. Various researches have pointed to security problems as a critical factor to impede the vitalization of cloud computing services, but they only focus on the security threats and their correspondents for addressing the problems. There are no studies that analyze major security issues with regard to introducing the cloud computing system. Accordingly, it is necessary to research the security factors in the cloud computing given to public institutions when adopting cloud computing. This research focuses on the priority of security solutions for the stepwise adoption of cloud computing services in enterprise environments. The cloud computing security area is classified into managerial, physical and technical area in the research, and then derives the detailed factors in each security area. The research derives the influence of security priorities in each area on the importance of security issues according to the identification of workers in private enterprise and public institutions. Ordered probit models are used to analyze the influences and marginal effects of awareness for security importance in each area on the scale of security priority. The results show workers in public institutions regard the technical security as the highest importance, while physical and managerial security are considered as the critical security factors in private enterprise. In addition, the results show workers in public institutions and private enterprise have remarkable differences of awareness for cloud computing security. This research compared the difference in recognition for the security priority in three areas between workers in private enterprise, which use cloud computing services, and workers in public institutions that have never used the services. It contributes to the establishment of strategies, with respect to security, by providing guidelines to enterprise or institutions that want to introduce cloud computing systems.

Keywords: Cloud Computing, Cloud Security, Security Strategies, Ordered Choice Regression, Ordered Probit Model

The preliminary version of this paper was presented in the APICIST 2012

http://dx.doi.org/10.3837/tiis.2013.04.015

1. Introduction

Cloud computing has become one of the core technologies to increase productivity by sharing computing resources in different devices [1]. In the cloud computing environment, users consume the IT resources and pay a usage price to the computing resource providers [2]. This advantage has recognized cloud computing as the alternative that may overcome problems of the existing system. These problems include low computing performances by limited computing resources, overhead and maintenance charges for periodically upgrading IT infrastructures, and difficulty in service extensions [3]. Cloud computing services were introduced in Korea as enterprise services to major companies in 2008. The personal cloud services have been employed since 2010 and various enterprises have adopted cloud computing in order to improve their productivity [4]. In addition, the Korean government established a cloud computing activation plan to increase the market size for local cloud computing from 67.39 billion won in 2009 to 2.5 trillion won in 2014, by introducing the public section of cloud computing [4]. Private enterprises and public institutions recognize cloud computing as the important technology for enhancing business efficiency. Cloud computing has become the spotlighted technology for boosting the IT industry. Also, Korean government expects that cloud computing will become the main technology to increase national competiveness [5]. Cloud computing is not free from security compromises due to the fundamental features including partial or whole outsourcing [6]. Because of the various security problems, which can be complexly derived in the cloud computing environment, it is important to provide a trustworthy service by removing security threats. However, extremely complicated and high level security issues may create a financial burden on the service providers and an inconvenience to users of the service. Therefore, it is necessary to establish a security strategy to guarantee the services' stability, efficiency, and usability to the utmost limit.

Although much research has identified security problems as the most threatening factor for employing cloud computing, the anticipated security threats and confrontation techniques were simply mentioned or technological solutions are only described in the research. The ultimate objective of cloud computing to private enterprise and public institutions is to increase productivity and effectiveness, and to strengthen competitiveness; as a result, investment in security has to be considered at the introducing step. Thus, it is required to select a security measure to confront cloud computing security threats and prepare a base to evaluate the importance to counteract effectively. The perception gap for security in the private enterprise, which uses the cloud computing, and in the public institution, which plans to introduce it, is analyzed in this research. For the analysis, the actual perceptions of private enterprise and public institution workers are investigated in three security sectors which are managerial, physical, and technical security. This research can be applied as a guideline for establishing security strategies when public institutions and private enterprises introduce cloud computing by analyzing the perception gap of security importance.

2. Related Research

2.1 Status of Cloud Computing Services

Cloud computing is a new computing concept in which IT resources are not installed in a local terminal. Instead, the resources are provided to subscribers as types of services [7] [8]. In the cloud computing environment, the service subscribers are able to do high performance computing work regardless of the terminal's performance and storage space because of the computing resources that are provided by cloud computing service providers [7].

The major enterprises in Korea, such as SK C&C, KT, and Samsung SDS, have provided cloud computing services for businesses since 2008. The quality of cloud computing services is under valued compared to the services in the U.S. and other advanced countries. The services are diversified and their qualities are improved based on world-class IT infrastructures in Korea [7]. The Korean government plans to reduce IT operation costs and increase the world market share by introducing public cloud computing for the next five years [4]. As a result, related government ministries are leading research about constructing infrastructures, excavating service models, and developing technologies [8].

2.2 Research on Cloud Computing Security

Security threats can easily occur to cloud computing services because IT resources are highly exposed to diverse attacks on computer networks due to the unique environment of the cloud computing services. For example, information for service subscribers is not safe from the attacks by hackers such as phishing and pharming. The information is stored in servers of service providers instead of the subscriber's computer. The hackers are able to easily obtain private information, business information, and computer or network information of subscribers because the information of all subscribers are stored and managed into the servers of the service providers. A total number of 244 people in IT enterprises have pointed out security problems of prior decision in the implementation of cloud computing according to International Data Corporation (IDC) investigations [9]. Gartner and European Network and Information Security Agency (ENISA) recommend that the security problems should be solved first in order to provide reliable cloud computing services [10] [11]. Eun [4] defined the components of cloud computing as server, software, storage, network, and terminal. He also proposed required security technologies for each cloud computing component as shown in **Table 1**. Ryu [12] and Eun et al. [13] divided security components of cloud computing into platform, storage, network, and terminal. They provided similar technologies for cloud computing as the technologies in **Table 1**. The representative companies in the cloud computing area have introduced the technical services for cloud computing security. For instance, the company Amazon introduced authentication function, backup, EC2 security, S3 security, and Simple DB security for Amazon Web Service (AWS) which is their representative cloud computing service [14].

Table 1. Required cloud computing security technology for each components

Criteria	Server	Software	Storage	Network	Terminal
Security Technology	Operation system & Hypervisor Security Technology	Application certification, User certification & payment technology	Access control, Encryption technology	Encryption & Anti-Denial of Service technology	Preventing Malicious code, Privacy protection technology

Lim [15] proposed eight critical factors for cloud computing services with the respect to security regarding privacy and data encryption, user certification and access control, and data integrity. Gartner [10] assessed the security risks of cloud computing and suggested seven specific security proposals: privileged user access, regulatory compliance, data location, data segregation. CSA [16] addressed twelve domains for successful control of cloud computing security.

Limited research has suggested a combination of managerial, physical, and technical security for cloud computing services. Kim [2] argued that security technology is not clear for solving cloud computing security problems and that the establishment of response systems with respect to managerial, physical, and technical areas. Lee [17] analyzed security technologies to prevent personal information extrusion on cloud computing in terms of managerial, physical, and technical security areas. Kim [18] suggested appropriate managerial, physical and technical security elements based on overseas cloud computing security guidelines, Information Security Management System (ISMS) in the ISO 27001, and ISMS developed by Korea Internet and Security Agency (KISA) to solve the specific security issues in the cloud computing environment. Existing research in cloud computing security describes various security threats and confrontation techniques. However, most of the research focuses on technological threats and counter-measures instead of presenting a security strategy which can be applied to managerial, physical, and technological sectors in an organizational structure. Additionally, limited references and resources were used in previous concerning security strategies to public institutions or private enterprises that want to introduce cloud computing.

3. Research Model and Empirical Settings

3.1 Research Model

This work has expanded the research model that analyzed the importance of cloud computing security in three aspects. Similar to the previous research, the five point Likert scale: not very important, not important, normal, important, very important, is used as a measurement standard of dependent variables, and the dependent variable has an ordered dummy value. When the dependent variable has an ordered number, the ordered choice model should be used instead of a general linear regression model. The ordered choice model is able to recursively deal with the survey responses investigated with the Likert scale. The ordered choice model is based on the normal choice model, which is used as the dependent variable, contains discrete data associated with choice. There are two types of ordered choice models as the ordered logit model and the ordered probit model. The ordered probit model is used to analyze the importance of the cloud computing security in this research. The ordered probit model uses a cumulative distribution function instead of a utility function to obtain the values of selection probability in the ordered logit model [19] [20].

Formula (1) shows the relationship between the ordered dependent variables and the independent variables in order to analyze the relationship based on linear regression. However, the ordered probit model uses a latent factor as the dependent variable. Let y* represent an unobservable response variable (latent variable) that captures the importance level of the i^{th} individual, x is a vector of the independent variable, and β is a vector of estimated parameters. The importance outcome can be expressed as a function of a vector of dependent variable x_i using the following linear relationship.

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

In general y^* is not observed, but y is observed instead of y^* and divided into the number of

J ranges. It is assumed that errors ε_i is the standard normal distribution, the ordered probit model is shown in the following formula (2). Formula (2) shows the relationship between categorized criteria y* and observable response y. Also, μ means threshold value for each category of the selection.

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

Green [17] showed the example of the ordered choice model. The dependent variable in the example is the value of a self-reported health assessment. The value for the dependent variable is between 0 and 4. The independent variables x are age, household income, education level, household kids, and married. Married and kids variables have binary values. After the estimation with the health dataset in Green’s research, the equation for the example is obtained as follows:

$$\begin{aligned} Health^* &= 1.97882 - 0.01806 Age + 0.25869 Income + 0.03556 Edu \\ &\quad + 0.06065 Kids - 0.03100 Married + \varepsilon \\ y &= 0, \; if \;\; y^* \le 0 \\ y &= 1, \; if \;\; 0 < y^* \le 1.14835 \\ y &= 2, \; if \;\; 1.14835 < y^* \le 2.54781 \\ y &= 3, \; if \;\; 2.54781 < y^* \le 3.05639 \\ y &= 4, \; if \;\; y^* > 3.05639 \end{aligned} \tag{3}$$

The parameter effects are explained in the coefficients in other regression base models. However, the probability of each selection is computed on the basis of the threshold values and cumulative distribution. The probability of selection can be obtained on the basis of the above dependent variable definition and the probability function. It is assumed that $\Phi(\cdot)$ is the standard normal distribution cumulative function and the probability for each response belongs to each category is as follows:

$$\begin{aligned} \mathrm{Pr}ob(H_i = 0) &= \Phi(-\beta' K_i) \\ \mathrm{Pr}ob(H_i = 1) &= \Phi(\mu_1 - \beta' K_i) - \Phi(-\beta' K_i) \\ \mathrm{Pr}ob(H_i = 2) &= \Phi(\mu_2 - \beta' K_i) - \Phi(\mu_1 - \beta' K_i) \\ &\;\;\vdots \\ \mathrm{Pr}ob(H_i = J) &= 1 - \Phi(\mu_{j-1} - \beta' K_i) \end{aligned} \tag{4}$$

The general expression for the log-likelihood function, which is indicates the suitability of the model, is given as:

$$\log L = \sum_{i=1}^{n}\sum_{j=0}^{J} Y_{ij} \log[\Phi(\mu_j - \beta' K_i) - \Phi(\mu_{j-1} - \beta' K_i)] \qquad (5)$$

It is not able to predict the intensity of the independent variable toward the dependent variable from the coefficients in the analysis results. The concept of marginal effects has to be introduced in order to compute the degree of impact of the independent variables on the dependent variable. The probability of marginal effect on a specific dependent variable can be calculated by the partial differential formula (1) as a dependent variable. The marginal effect equation is as follows:

$$\frac{\delta \Pr ob(y=j)}{\delta x_k} = \frac{\delta}{\delta x_k}[F(\mu_j - \sum_{k=1}^{K}\beta_k x_k) - F(\mu_{j-1} - \sum_{k=1}^{K}\beta_k x_k)] \qquad (6)$$
$$= [F'(\mu_{j-1} - \sum_{k=1}^{K}\beta_k x_k) - F'(\mu_j - \sum_{k=1}^{K}\beta_k x_k)]\beta_k$$

3.2 Characteristics of the Sample

The data for the research were collected through a web survey during March 2012. A total number of 298 workers in private enterprises and public institutions responded to the web survey. Seven responses were removed because they had missing data, therefore 291 samples are used for the analysis. The relevant socio-demographic and behavioral characteristics of the data are presented in **Table 2**.

Table 2. Demographic composition of sample

		Private Enterprise **n=205 (%)**	**Public Institutions** **n=86 (%)**	**Pooled** **n=291 (%)**
Gender	Male	159(77.6)	64(74.4)	223(76.6)
	Female	46((22.4)	22(25.6)	68(23.4)
Age	20-29 years	69(33.7)	10(11.6)	79(27.1)
	30-39 years	94(45.9)	48(55.8)	142(48.8)
	Over 40 years	42(20.4)	28(32.6)	70(24.1)
Job tenure	5 years under	145(70.7)	29(33.7)	174(59.8)
	5 -10 years	28(13.7)	22(25.6)	50(17.2)
	10-15 years	21(10.2)	12(14.0)	33(11.3)
	Over 15 years	11(5.4)	23(26.7)	34(11.7)
Persons at Work	1～300 people	66(32.2)	17(19.8)	83(28.5)
	Over 301 people	139(67.8)	69(80.2)	208(71.5)

3.3 Research Variables

This research focuses on the importance of cloud computing security in three areas. The variables in the research are constructed on the basis of KISA ISMS. The KISA ISMS is the comprehensive system to operate and manage countermeasures for information security with respect to technical, managerial, and physical area [21].

Table 3. Research Variables and Operational Definition

Dep. Variable	Indep. Variable	Operational Definition
Importance of Managerial Security	Security policy	Establishment of Security policy and procedure that reflects CEO(CIO etc) intentions, regularly review and supplementation
	Security organizations	Organization of optimal size for the security mission, proper responsibility and authority setting
	Asset classification and control	Assessments, classification and cataloging of assets for the selective security level enforcement
	Personnel security	Management of current and former employees, Outsiders(e.g., Security training, Authorization)
	Security incident management	Incident reaction management in order to Proliferation of incidents and minimize the damage
	Security inspection	Regular or unexpected checks for security guidelines and procedure conducted without exception
Importance of Physical Security	Equipment/facility positioning	Safe positioning and locating from natural disasters(e.g., thunderbolt, earthquake, flood)
	Environmental control of facility	Preventing damage or failure due to environmental factors(e.g., temperature, humidity, atmosphere)
	Access monitoring/controlling	Monitoring/controlling illegal access to service -related facilities and equipment (e.g., CCTV)
	Utility support	Data backup and preparing alternative resources in case of power outage and communications failure, periodically check
	Import & export control of items	Control of unauthorized import and exports of goods(e.g., smartphone) within service facilities
Importance of Technical Security	Terminal Security	Removal potential security threats in the terminal (e.g., malicious code infections, terminal loss, personal information disclosure)
	Network Security	Removal potential security threats in the terminal (e.g., transferring data theft, DDoS)
	Platform Security	Removal potential security threats in the platform (e.g., operation system, hypervisor security)
	Storage Security	Removal potential security threats in the storage (e.g., access control, data encryption)
	Application Security	Removal potential security threats in the application(e.g., program and user certification, payment security)

* Research variables are selected based on Information Security Management System of Korea Internet and Security Agency

As presented in section 2.2, researches for security issues in Internet environment are conducted based on ISMS of ISO 27001 and KISA ISMS. Three representative researches such as Kim [2], Lee [17], and Kim [18] suggested the response technologies for security issues in the cloud computing environment based on ISMS. This research also focuses on the strategies for the security priority based on the three aspects of KISA ISMS. Therefore, variables are selected on the basis of three security areas in KISA ISMS and related researches as well and they are presented in **Table 3**. Kim [18] also summarized detailed items in the security architecture of the cloud computing based on KISA ISMS. For instance, he provided "entrance control" in physical security, "accident management" in managerial security, "application security" in technical security of service providers, and "the selection of the service providers" in technical security of service consumers. Therefore, the detailed variables are redefined in this research according to the items which are summarized in order to evaluate security issues of cloud computing in previous researches and KISA ISMS.

The KISA ISMS have also been widely used for the establishment of security strategies to public institutions such as government department and national institute as well as to private enterprises such as internet service providers, infrastructure providers, and service integration companies [21]. Since KISA ISMS is widely used for the security in Korea, the same variables are applied to the analysis of the security strategies in public institutions and private enterprises in this research. The dependent variables are measured on 5 point scales. The common independent variables for all analysis are gender, age, job tenure, and persons at work.

4. Analysis Results

4.1 The Awareness on Importance of Cloud Computing Managerial Security

With respect to managerial security, public institution workers recognize the importance of security inspections and private enterprise workers understand the significance of security policies (See **Table 4**). The importance of the security variables was highly represented: personnel security (4.44 and 4.13), security policy as 4.23 and 4.29, security group organization and operation (4.23 and 3.94), security accident management (4.15 and 4.22), security inspection (3.92 and 4.07), protection property classification and control (3.90 and 3.99) respectively on average. The analysis results show gender, age, job tenure, and number of employees are not statistically significant in the case of public institutions, but the age variable is statistically significant at the 5% significance level in private enterprises. In other words, young private enterprise workers recognize managerial security is significantly important. For the analysis results about detailed factors in managerial security, security inspection and security policy are significant in public institutions, while security policy, personnel security and security incident management have significant effects in private enterprises. Specially, in the case of public institutions, the coefficient of security inspection is statistically significant at 0.4533 and indicates that it is the most effective variable in the importance of cloud computing managerial security. The next coefficient of security policy is identified as the second most important variable (0.3909). Meanwhile, in the case of private enterprises, the coefficient (0.4624) of security policy is the most effective variable in security importance of cloud computing managerial security. Next, personnel security and security incident management is indicated to be effective in the awareness of managerial security importance.

In the case of public institutions, the odds ratio of security inspection is 1.5735, meaning that the importance of security inspection is 1.6 times higher regarding the awareness of odds in security importance than the awareness of managerial security importance. With the same method, security policy is 1.5, security groups and human security is 1.3, security incident management is 1.0, and capital security is about 0.9 times higher in odds. In the case of private enterprise, security policy's odds ratio is 1.5879. This means that the recognition for the importance of security policy is 1.6 times higher than the one for the non-importance of the policy in managerial security for cloud computing in the case of private companies. With the same method, personnel security was 1.4, security incident management 1.5, and running security organization and security inspection is 1.1 times higher in odds.

Table 4. Analysis result about awareness of the managerial security importance

	Public institutions workers				**Private enterprise workers**			
	LR chi2(7) = 32.39				LR chi2(7) = 59.36			
	Log likelihood = -66.244868				Log likelihood = -170.82183			
Independent variable	$\hat{\beta}$	exp($\hat{\beta}$)	t	P	$\hat{\beta}$	exp($\hat{\beta}$)	t	P
Security Policy	0.3909	1.4783	2	0.045	0.4624	1.5879	3.64	0
Security Organization	0.2534	1.2884	1.08	0.279	0.1315	1.1405	0.98	0.329
Asset classification and control	-0.0753	0.9274	-0.32	0.753	0.0599	1.0617	0.51	0.609
Personnel Security	0.2391	1.2701	1.17	0.244	0.3441	1.4107	3.06	0.002
Security Incident Management	0.0380	1.0387	0.16	0.876	0.3943	1.4834	2.9	0.004
Security Inspection	0.4533	1.5735	1.94	0.050	0.0577	1.0594	0.42	0.672
Gender	-0.2143	0.8071	-0.63	0.531	0.1577	1.1708	0.74	0.46
Age	0.0123	1.0124	0.39	0.693	-0.0349	0.9657	-2.05	0.041
Job tenure	0.0273	1.0277	1.03	0.305	0.0240	1.0243	1.08	0.281
Persons at work	0.1215	1.1292	1.11	0.265	0.0193	1.0195	0.28	0.776
cut1	4.9565				3.7723			
cut2	6.3284				5.4543			

Table 5 and **Fig. 1** show the results of the marginal effects change in the recognition of cloud computing importance in public institution and private enterprise workers. In the case of public institutions, when the gender changes from male to female, the proportion of cloud computing managerial security importance has an 8.4% increase. Also, managerial security is recognized as very important, as age increased, long time working, and increase in the size of the working place. On the other hand, as the age of private enterprise workers decreases, the proportion of being aware of the cloud computing's managerial security increases to 1.3%. Also, awareness of managerial security importance increases when the gender changed from female to male, long time working, and the increase of co-workers. In the case of public institution workers, as the subjective awareness in the importance of security inspection increased, the proportion of marginal effects is increased 17.9% and the proportion of security policy importance has a 15.5% increase. Besides this, security organization increases 10.0%, personnel security increases 9.5%, security incident management increases 1.3%, and capital security classification decreases 3.0%. So, public institution workers consider that managerial security is 18.0% higher in importance for one increase of security inspection, and the marginal effect of security inspection has the highest association with the importance of managerial security. In the case of private enterprise workers, as the subjective awareness in the importance of security policy increased, the proportion of marginal effects is increased 17.8%. With the same method, security incident management and personnel security are

increased 15.2% and 13.2%, respectfully. Security organization is increased 5.1%, capital security classification is 2.3%, and security inspection has a 2.2% increase, but they are not statistically significant. So, private enterprise workers consider that managerial security is 17.8% higher in importance for one increase of security policy, and its marginal effect has the highest association with the importance of managerial security.

Table 5. Marginal effect changes on the awareness of managerial security importance

	Public institution workers			**Private enterprise workers**		
	Prob(Y=3) normal	Prob(Y=4) important	Prob(Y=5) very important	Prob(Y=3) normal	Prob(Y=4) important	Prob(Y=5) very important
Security Policy	-0.0514	-0.1035	0.1549	-0.0682	-0.1096	0.1778
Security Organization	-0.0333	-0.0671	0.1004	-0.0194	-0.0312	0.0506
Asset classification and control	0.0099	0.0199	-0.0298	-0.0088	-0.0142	0.0230
Personnel Security	-0.0314	-0.0633	0.0947	-0.0507	-0.0816	0.1323
Security Incident Management	-0.0050	-0.0101	0.0150	-0.0581	-0.0935	0.1516
Security Inspection	-0.0596	-0.1200	0.1796	-0.0085	-0.0137	0.0222
Gender	0.0261	0.0580	-0.0841	-0.0247	-0.0351	0.0598
Age	-0.0016	-0.0033	0.0049	0.0051	0.0083	-0.0134
Job tenure	-0.0036	-0.0072	0.0108	-0.0035	-0.0057	0.0092
People at work	-0.0160	-0.0322	0.0481	-0.0028	-0.0046	0.0074

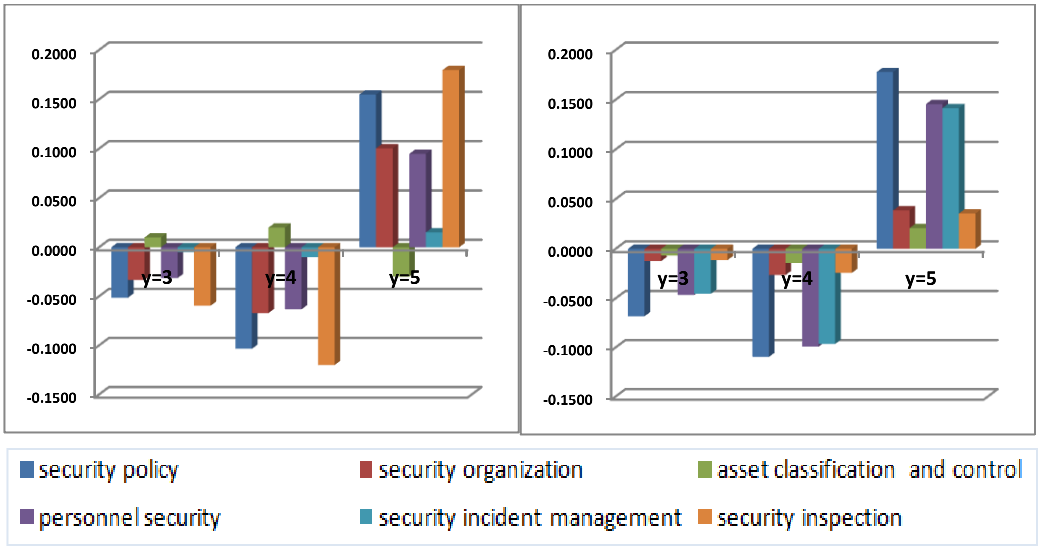

Fig. 1. Marginal effect changes on the awareness of managerial security importance (Public / Private)

4.2 The Awareness on Importance of Cloud Computing Physical Security

Of the components in physical security, public institution workers recognize the importance of access monitoring/controlling and private enterprise workers understand the significance of utility support (See, **Table 6**). The variables are generally highly recognized: access monitoring/controlling 4.27, 4.21, utility support 4.20, 4.06, equipment/facility positioning 3.90, 3.72, Environmental control of facility 3.80, 3.92, import & export control of items 3.79, 4.19 respectively on the average. The analysis results show gender, age, job tenure, and number of employees are not statistically significant in the case of public institutions, but the number of employees variable is statistically significant at the 10% significance level in private enterprises. In the case of public institutions, the coefficient of access monitoring/controlling is 0.6152 and it is the most effective variable in the importance of physical security in cloud computing. The coefficient of utility support is the most effective variable at 0.2463 in security importance of physical security. Next, personnel security and security incident management is indicated to be effective in the awareness of managerial security importance. The odds ratio of the two groups are as follows: access monitoring/controlling as 1.9 and 1.3, environmental control of facility as 1.5 and 1.2, utility support as equally 1.3, import & export control of items and equipment/facility positioning as 1.1.

Table 6. Analysis result about awareness of the physical security importance

	Public institutions workers				**Private enterprise workers**			
	LR chi2(7) = 40.68				LR chi2(7) = 31.53			
	Log likelihood = -63.96603				Log likelihood = -184.90354			
Independent variable	$\hat{\beta}$	exp($\hat{\beta}$)	t	P	$\hat{\beta}$	exp($\hat{\beta}$)	t	P
Equipment/facility positioning	0.1033	1.1088	0.51	0.609	0.1569	1.1699	1.51	0.131
Environmental control of facility	0.4252	1.5298	1.57	0.115	0.1910	1.2105	1.58	0.113
Access monitoring/controlling	0.6152	1.8501	2.66	0.008	0.2274	1.2553	1.99	0.047
Utility support	0.2710	1.3113	1.25	0.21	0.2463	1.2792	2.12	0.034
Import & export control of items	0.1270	1.1354	1.03	0.302	0.1330	1.1423	1.17	0.242
Gender	-0.0945	0.9098	-0.27	0.787	-0.0683	0.9339	-0.33	0.742
Age	0.0565	1.0581	1.62	0.106	0.0085	1.0086	0.51	0.613
Job tenure	0.0068	1.0068	0.23	0.817	-0.0176	0.9826	-0.78	0.433
Persons at work	-0.0036	0.9964	-0.03	0.972	0.1159	1.1229	1.79	0.073
cut1	6.8666				3.4187			
cut2	8.8665				5.1619			

The marginal effect results in the physical security are shown in **Table 7** and **Fig. 2**. In both groups, when the gender changes from male to female, the proportions of physical security importance are increased 3.3% and 2.0%, respectively. Also, awareness of physical security importance is increased when workers are older, but the marginal effects have opposite signs for job tenure and people at work values in each group. In the case of public institution workers, as the importance of access monitoring/controlling increased, the proportion of marginal effect on 'very important' of physical security has a 21.2% increase, while utility support increased, the proportion of marginal effect on physical security is increased 7.1% in the case of private enterprise workers. With the same method, the proportion of marginal effect on physical security increased, the variable of respectively environmental control of facility is 14.6% and 5.5%, the variable of import and export control of items has increases of 4.3% and 3.9%, and the equipment/facility positioning variable has a 3.6% and 4.6% respectively.

Table 7. Marginal effect changes on the awareness of physical security importance

	Public institution workers			**Private enterprise workers**		
	Prob(Y=3) normal	Prob(Y=4) important	Prob(Y=5) very important	Prob(Y=3) norrnal	Prob(Y=4) important	Prob(Y=5) very important
Equipment/Facility positioning	-0.0142	-0.0213	0.0356	-0.0401	-0.0054	0.0455
Environmental control of facility	-0.0586	-0.0878	0.1464	-0.0488	-0.0066	0.0554
Access monitoring/controlling	-0.0848	-0.1270	0.2119	-0.0581	-0.0079	0.0659
Utility support	-0.0374	-0.0560	0.0933	-0.0629	-0.0085	0.0714
Import & export control of items	-0.0175	-0.0262	0.0437	-0.0340	-0.0046	0.0386
Gender	0.0126	0.0203	-0.0329	0.0171	0.0030	-0.0201
Age	-0.0078	-0.0117	0.0195	-0.0022	-0.0003	0.0025
Job tenure	-0.0009	-0.0014	0.0023	0.0045	0.0006	-0.0051
People at work	0.0005	0.0007	-0.0012	-0.0296	-0.0040	0.0336

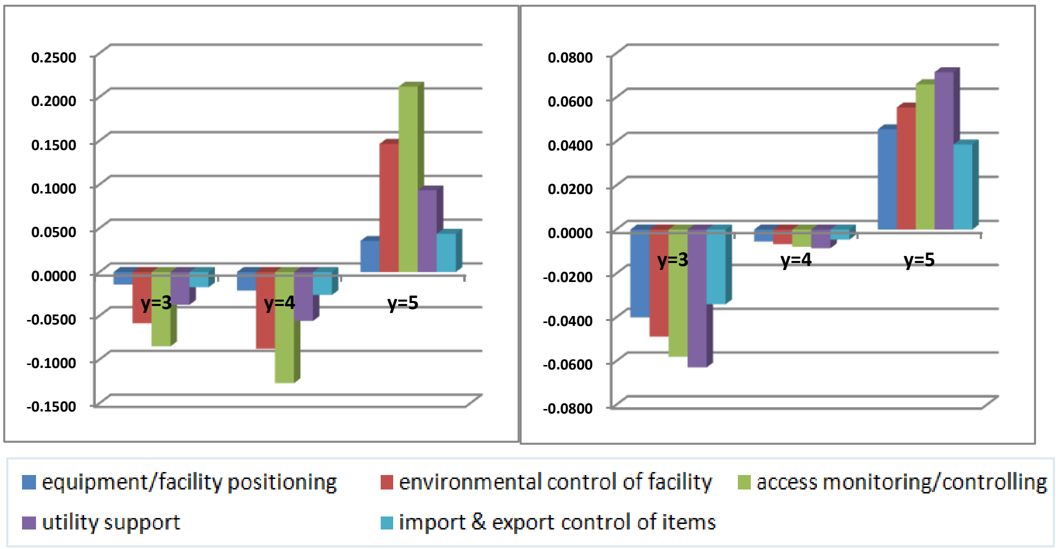

Fig. 2. Marginal effect changes on the awareness of physical security importance (Public / Private)

As a result, public institution workers consider that physical security is 21.2% higher in importance for one increase of monitoring/controlling, and its marginal effect has the highest association with the importance of managerial security. In the case of private enterprise, physical security has a 7.1% increase for the one increase of utility support.

4.3 The Awareness on Importance of Cloud Computing Technical Security

In the aspect of technical security, as the size of public institution gets smaller and the job tenure of private enterprise becomes longer, as the awareness of the importance in cloud computing increases (See **Table 8**). In the case of public institutions, the coefficient of storage security is 0.7597 and statistically significant. This indicates that the variable is the most effective variable in the awareness of the importance on technical security. The second most important variable is platform security and has 0.6325 as the coefficient. In the case of private enterprises, the coefficient of application security is 0.3691 and the most effective variable in the awareness of the importance on technical security.

In the case of public institution workers, the odds ratio of storage security is 2.1376, meaning that the importance of storage security is 2.1 times higher regarding the odds in security importance than the awareness of technical security importance. As for the results, platform security is 1.9, application security is 1.2, network security is 1.1 and terminal security is 0.7 times higher in odds. In the case of private enterprise workers, the importance of application security is 1.4 times higher than the non-importance of the policy in managerial security for cloud computing.

Table 8. Analysis result about awareness of the technical security importance

	Public institutions workers				**Private enterprise workers**			
	LR chi2(7) = 34.98				LR chi2(7) = 32.62			
	Log likelihood = -58.820841				Log likelihood = -155.67244			
Independent variable	$\hat{\beta}$	exp($\hat{\beta}$)	t	P	$\hat{\beta}$	exp($\hat{\beta}$)	t	P
Terminal security	-0.4031	0.6682	-1.84	0.066	0.1001	1.1053	0.71	0.475
Network security	0.1048	1.1105	0.36	0.715	0.1586	1.1718	1.12	0.264
Platform security	0.6325	1.8823	2.87	0.004	0.1828	1.2006	1.23	0.217
Storage security	0.7597	2.1376	2.7	0.007	0.2956	1.3439	2.04	0.042
Application security	0.1797	1.1968	0.91	0.362	0.3691	1.4465	2.4	0.016
Gender	-0.0469	0.9542	-0.13	0.897	0.0558	1.0574	0.25	0.8
Age	0.0003	1.0003	0.01	0.995	-0.0133	0.9868	-0.77	0.444
Job tenure	-0.0254	0.9749	-0.79	0.429	0.0501	1.0514	1.95	0.05
Persons at work	-0.2370	0.7890	-2.03	0.042	0.0304	1.0309	0.43	0.665
cut1	2.1091				2.8089			
cut2	3.9159				4.2120			

Table 9 and **Fig. 3** are the results of marginal effect changes in the recognition of technical importance in public institutions and private enterprises. In the case of public institutions, technical security is recognized very importantly, as the size of the group became smaller, workers are older, job tenure was shorter. Meanwhile, in the case of private enterprises, the proportion of recognizing technical security as very important increased, as job tenure was longer, the size of the group was bigger, workers are younger.

Table 9. Marginal effect changes on the awareness of technical security importance

	Public institutions workers			**Private enterprise workers**		
	Prob(Y=3) normal	Prob(Y=4) important	Prob(Y=5) very important	Prob(Y=3) normal	Prob(Y=4) important	Prob(Y=5) very important
Terminal security	0.0236	0.1354	-0.1590	-0.0090	-0.0289	0.0379
Network security	-0.0061	-0.0352	0.0413	-0.0142	-0.0458	0.0600
Platform security	-0.0370	-0.2124	0.2494	-0.0164	-0.0528	0.0692
Storage security	-0.0445	-0.2551	0.2996	-0.0266	-0.0853	0.1119
Application security	-0.0105	-0.0603	0.0709	-0.0332	-0.1066	0.1398
Gender	0.0027	0.0158	-0.0184	-0.0052	-0.0161	0.0212
Age	0.0000	-0.0001	0.0001	0.0012	0.0038	-0.0050
Job tenure	0.0015	0.0085	-0.0100	-0.0045	-0.0145	0.0190
People at work	0.0139	0.0796	-0.0935	-0.0027	-0.0088	0.0115

In the case of public institution workers, as the subjective awareness on the importance of storage security is increased, proportion of marginal effect on 'very important' of technical security has 30.0%, platform security has 24.9%, application security has 7.1%, network security has 4.1% increase respectively, but terminal security is decreased 15.9%. While in the case of private enterprises, as the subjective awareness on the importance of application security, storage security, platform security, network security, and terminal security rose, the proportion of marginal effect on technical security increased 14.0%, 11.2%, 6.9%, 6.0%, 3.8%, respectively. As a result, the marginal effect of storage security is most related to recognition of the importance of cloud computing technical security in public institutions, but the marginal effect of application security is most rated to that in private enterprises.

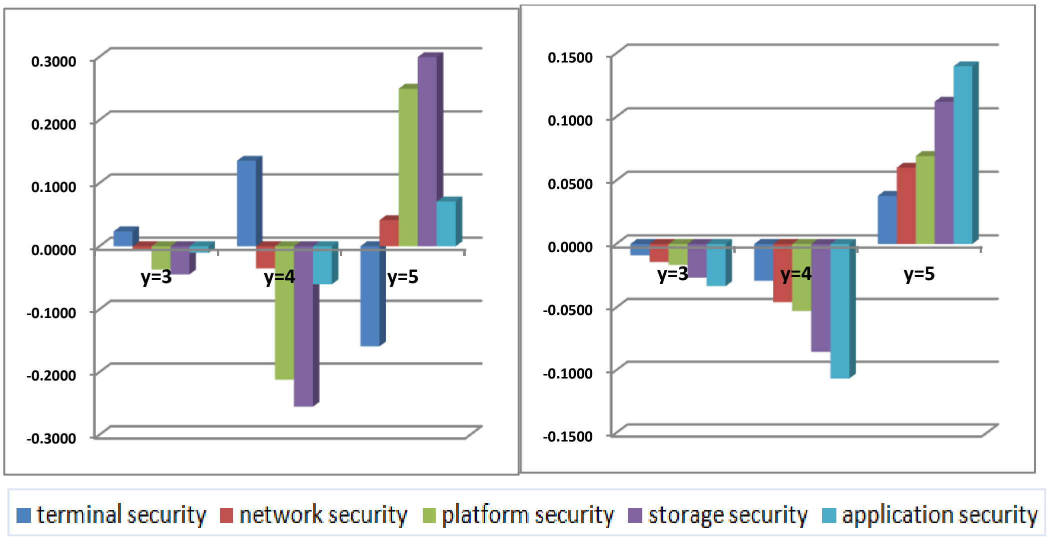

Fig. 3. Marginal effect changes on the awareness of technical security importance (Public / Private)

5. Conclusions and Discussions

5.1 Conclusions and Implications

Cloud computing has been introduced to improve efficiencies of business and group productivity in private enterprises and public institutions. Current studies for security issues in cloud computing were on focused on addressing technical problems. However, to help establish a security strategy for introducing cloud computing systems, it is necessary to analyze security priorities and countermeasures. Therefore, this research analyzed the differences in awareness for the security of cloud computing in private enterprises and public institutions by ordered probit model. As a result, private enterprise workers using cloud computing for work and public institution workers not using it showed a great difference in awareness.

The workers in public institutions recognized the importance of security inspection and security policy in the component of managerial security, but the employees in private enterprises put higher priorities on security policy, personnel security, and security incident management. This shows that the workers in public institutions recognize supervisions and controls of the primary action agency, and the aggressive activities of the agency contributes more to security establishment in introducing cloud computing services. On the other hand, private enterprise employees highly recognize security policy and threats from the outside or any related co-workers. This implies that public institutions have to pay more attention to the management of employees since the employees frequently join and resign at public institutions in Korea. Also, private enterprise employees consider security incident management more important compared to public institution workers. This seems to be caused by the economic damages from security incidents of the cloud computing services. Public institutions have to systematize the management process of security incidents that are directly connected to national security. The awareness difference between two groups about physical security structure is also analyzed. Public institutions workers rated high the importance of surveillance and control, while private enterprise employees put more priority on the importance of surveillance and control and utility support. The marginal effects of surveillance and control of public institutions workers have 21.2 % increase, while private enterprise employees have a change of 6.6%. This means that public institution workers highly consider surveillance and control to be more important than private enterprise employees. Private enterprise employees considered environmental and physical factors similarly, but the public institution workers considered only surveillance and control. Also, private enterprise employees highly rated the importance of utility support. This shows that they recognize the supply of electric power and the block of communication networks as significant factors for the cloud computing security.

Lastly, public institution workers highly valued the importance of platform and storage security in technical security area while recognizing that terminal security is not important. In contrast, private enterprise employees valued applications, storage, and terminal security as highly important. This shows that public institution workers perceive that technical security is established by security department rather than the efforts of individual user. More importantly, the public institution workers evaluated the technical security sector of cloud computing as the most important one according to previous researches [22][23]. However, they tend to avoid responsibility for the security by emphasizing the roles of security experts. Therefore, the public institutions have to pay more attention to the establishment of individual responsibilities for cloud computing security when they introduce the services. Additionally, it is necessary to educate employees on potential security threats and the possible damages to applications and terminals.

5.2 Discussions

In this research, we analyzed the recognition differences for cloud computing security in two different groups. The analysis conducted on the basis of security domain and subdomain in KISA ISMS. The analysis results shows that public institution workers, who do not have experience in cloud computing services, have significantly different awareness for security compared to private enterprise employees who use cloud computing services. Also, it is found that service users and nonusers have a recognition gap between each other, and suggests security strategies to public institutions and private enterprises that will introduce the cloud computing services. The level of technical security seems to reach a high standard by confronting diverse threats. However, since the physical and managerial security issues are able to be changed according to organizational culture and environment, security strategies have to be established by estimating the organizations and individuals. Thus, public institutions and private enterprises that will introduce cloud computing services must make efforts to establish effective security strategies to provide stable cloud services.

Currently, many public institutions and private enterprises are considering the introduction of cloud computing services for maximizing business performance that are constrained because of limited computing resources. Due to difficulties in time and budget for building high performance systems based on cloud computing services, the organization that wants to introduce the services needs to refer to the evaluation results for the status of existing services. The analysis results of this research offers a framework for establishing a system based on cloud computing services with minimum trials at the beginning stage. However, the research has data limitations in which public institution only provide 86 samples while private enterprise provided 206 samples. Also, this research only focuses on the recognitions IT employees in Korea. Since most service providers and consumers of cloud computing pay attention to security issues in the world, the scope of this research will be extended to not only the world popular providers of the services but also the domestic and global companies which use cloud computing services and want to introduce them for enhancing the company productivity.

References

[1] M. Armbrust, "A View of Cloud Computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50-58, 2010. Article (CrossRef Link)

[2] S. J. Kim, "Information Security Plan on Cloud Computing: Information Security Management System," *Management Consulting Review*, vol. 1, no. 2, pp. 194-208, 2010. http://www.dbpia.co.kr/Journal/ArticleDetail/1366259

[3] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang and A. Ghalsasi, "Cloud Computing – The Business Perspective," *Decision Support Systems*, vol. 51, no. 1, pp. 176-189, 2011. Article (CrossRef Link)

[4] S. Y. Shin, "Master Plan for Vitalization of Cloud Computing," *Local Information Magazine*, vol. 61, pp. 46-51, 2010. http://www.klid.or.kr/section/board/bbs_view.html?PID=localdata&seq=1195

[5] Korea Communications Commission and Korea Internet Security Agency, "Information Security guide for Cloud Services," *Korea Communications Commissions and Korea Internet Security Agency*, October, 2011. http://www.nipa.kr/know/trandInformationView.it?identifier=02-004-111020-000021&menuNo=26&page=5

[6] S. K. Eun, "Cloud Computing Security Technology Trends," *Review of Korea Institute of Information Security and Cryptology*, vol. 20, no. 2, pp. 27-31, 2010. http://ocean.kisti.re.kr/is/mv/showPDF_ocean.jsp?pYear=2010&koi=KISTI1.1003%2FJNL.JAKO201027463260075&sp=32&CN1=JAKO201027463260075&poid=kiisc&kojic=JBBHBD&sVnc=v20n2&sFree

[7] 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," in *Proc. of 2011 Korean Society for Internet Information Summer Conference*, vol. 12, no. 1, pp. 221-222, 2011.

[8] Korea Communications Commission Press, "KCC Open the Cloud Service Test Bed," *Korea Communications Commission*, November, 2010.

[9] F. Gens, R. Mahowald, R. L. Villars, D. Bradshaw, C. Morris, "Cloud Computing 2010 An IDC Update," *International Data Corporation*, 2010.

[10] J. Heiser and M. Nicolett, "Assessing the Security Risks of Cloud Computing," *Gartner*, 2008. http://www.gartner.com/DisplayDocument?id=685308

[11] S. Gorniak, D. Ikonomou, P. Saragiotis, P. Belimpasakis, B. Bencsath, M. Broda, L. Buttyan, G. Clemo, P. Kijewski, A. Merle, K. Mitrokotsa, A. Munro, O. Popov, C. W. Probst, L. Romano, C. Siaterlis, V. Siris, I. Verbauwhede, and C. Vishik, "Priorities for Research on Current and Emerging Network Trends," *European Network and Information Security Agency,* 2010.

[12] J. S. Ryu, "Cloud Computing as Green IT and Security Issues," *The Graduate School of Computer Information Communications*, Korea University, Aug.2010. http://naver.nanet.go.kr/SearchDetailView.do?cn=KDMT1201072878&sysid=nhn

[13] S. K. Eun, N. S. Cho, Y. H. Kim and D. S. Choi, "Cloud Computing Security Technology," *Electronics and Telecommunications Trends*, Electronics and Telecommunications Research Institute, vol. 24, no. 4, pp. 79-88, 2009. http://ettrends.etri.re.kr/PDFData/24-4_079_088.pdf

[14] Y. J. Rho, "A Study on the Private Information Technologies using Cloud Computing," *Department of Mechanical Engineering,* Korea University, 2010.

[15] C. S. Lim, "Cloud Computing Security Technology," *Review of Korea Institutes of Information Security and Cryptology*, vol. 19, no. 3, pp. 14-17, 2009. http://ocean.kisti.re.kr/is/mv/showPDF_ocean.jsp?pYear=2009&koi=KISTI1.1003%2FJNL.JAKO200922951807082&sp=14&CN1=JAKO200922951807082&poid=kiisc&kojic=JBBHBD&sVnc=v19n3&sFree

[16] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," December 2009. https://cloudsecurityalliance.org/research/security-guidance/

[17] 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. http://naver.nanet.go.kr/SearchDetailView.do?cn=KDMT1201130607&sysid=nhn

[18] 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 and Communication*, Sungkyunkwan University, 2011. http://www.riss.kr/search/detail/DetailView.do?p_mat_type=be54d9b8bc7cdb09&control_no=2de2b4752a6b263dffe0bdc3ef48d419&naverYN=Y

[19] K. E. Train, "Discrete Choice Methods with Simulation", *Cambridge University Press 2 edition*, USA, 2009. Article (CrossRef Link)

[20] W. E. Greene and D. A. Hensher, "Modeling Ordered Choices: A Primer and Recent Developments," *Social Science Research Network*, 2010. Article (CrossRef Link)

[21] Y. H. Cho, "Defect Management System Plan for ISMS Certification," *Dept. of Information Security, The Graduate School of Information and Communications*, Konkuk University, 2010. http://naver.nanet.go.kr/SearchDetailView.do?cn=KDMT1201130607&sysid=nhn

[22] J. S. Oh,, Y. B. Yoon, J. R. Seo and B. G. Lee, "The Difference of Awareness between Public institutions and Private Companies for Cloud Computing Security", *International Journal of Security and Its Applications*, Vol.6, No.3, pp.1-10, 2012.

http://www.sersc.org/journals/IJSIA/vol6_no3_2012/1.pdf

[23] Y. B. Yoon, J. S. Oh and B. G. Lee, "The Important Factors in Security for Introducing the Cloud Services", *Journal of Korean Society for Internet Information*, Vol.13, No.6, pp.21-28, 2012. Article (CrossRef Link).

Young Bae Yoon is a Korean air force officer. He received B.S. degree in Air Transportation at Korea Aerospace University in 2002 and M.I.S degree in Graduate School of Information at Yonsei University in 2013. His research interests are in the area of cloud services, information technology evaluation and security.

Junseok Oh is a research professor at Communications Policy Research Center in Yonsei University. He received B.E degree from Information Engineering at Hansung University in 2002 and M.S degree from Computer Science at Chungbuk National University in 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.

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.