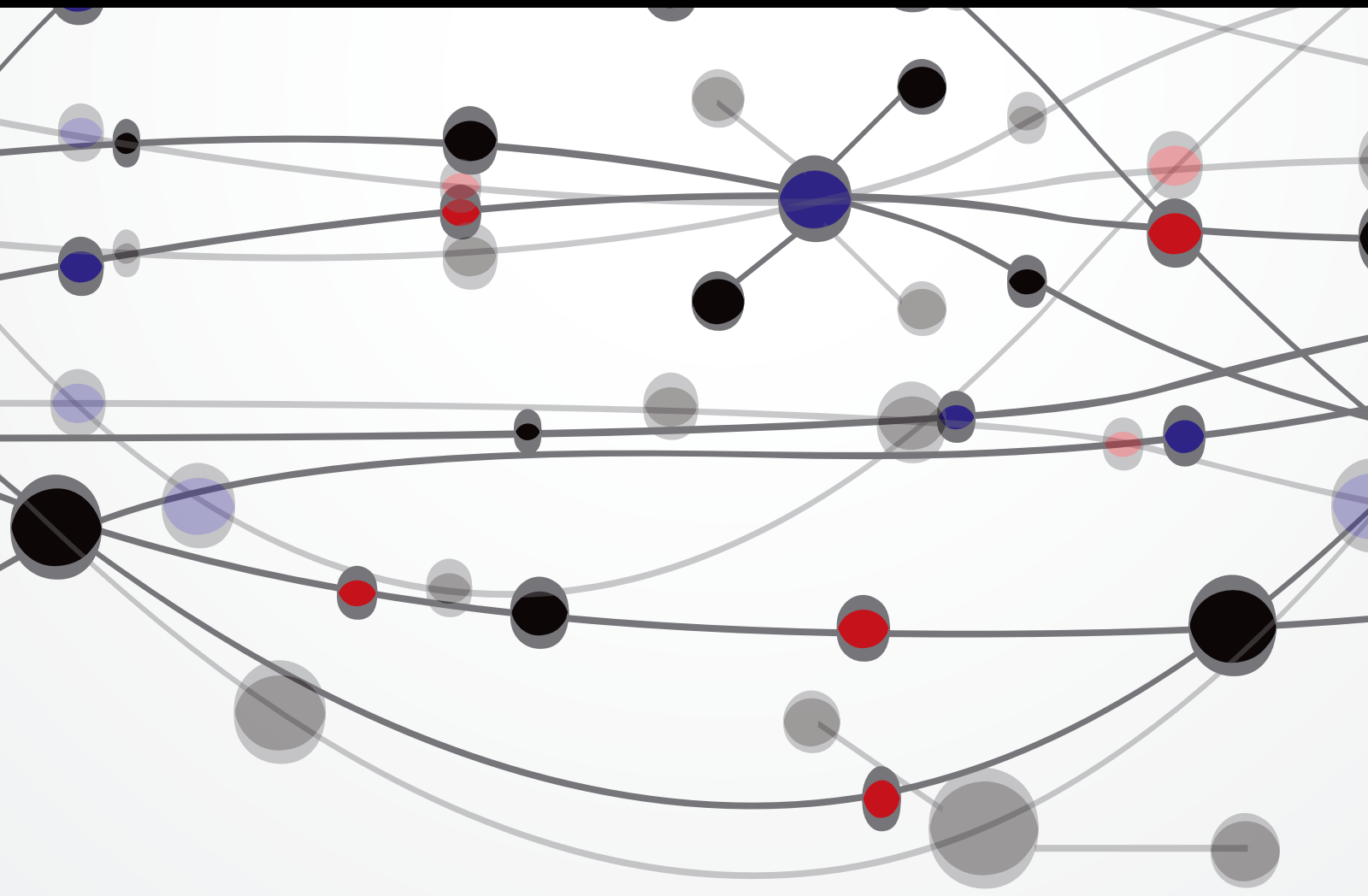
The Scientific World Journal

Strategic Management Advanced Service for Sustainable Computing Environment

Guest Editors: Sang-Soo Yeo, Qun Jin, Vincenzo Loia, and Hangbae Chang



Strategic Management Advanced Service for Sustainable Computing Environment

The Scientific World Journal

Strategic Management Advanced Service for Sustainable Computing Environment

Guest Editors: Sang-Soo Yeo, Qun Jin, Vincenzo Loia, and Hangbae Chang

Contents

Hindawi Publishing Corporation
The Scientific World Journal
Volume 2015, Article ID 715967, 2 pages
http://dx.doi.org/10.1155/2015/715967

Editorial

Strategic Management Advanced Service for Sustainable Computing Environment

Sang-Soo Yeo,[1] Qun Jin,[2] Vincenzo Loia,[3] and Hangbae Chang[4]

[1]*Division of Convergence Computer & Media, Mokwon University, Daejeon 302-729, Republic of Korea*
[2]*Department of Human Informatics and Cognitive Sciences, Waseda University, Tokorozawa 359-1192, Japan*
[3]*Department of Mathematics and Computer Science, University of Salerno, Fisciano, Salerno, Italy*
[4]*Department of Industrial Security, College of Business and Economics, Chung-Ang University, Seoul 156-756, Republic of Korea*

Correspondence should be addressed to Sang-Soo Yeo; sangsooyeo@gmail.com

Received 16 February 2015; Accepted 16 February 2015

Unquestionably, business and industrial information can be considered an extremely important asset to any organization. Some would even go as far as claiming that organization's information resources are the lifeblood of that organization. However, recently other competitors such as countries and enterprises are doing their best to have advanced technology of certain corporation. This business and industrial information leakage tend to halt the ordinary business process of enterprise, causing tremendous economical property loss as well as damage to the competitiveness of enterprise due to the leakage of technology which needs to be effort- and time-consuming.

Only security technology cannot directly protect against the underlying security incidents (business and industrial information leakage) that, in practice, lead to loss. Recent surveys suggest up to 60% of security breaches are related to human problem; yet few companies focus on human aspects in their security strategies. Hence to take preventive measures against security breaches, it is necessary to manage and converge three security areas (managerial, physical, and technical management) in the perspective of corporate and business security strategy.

The main motivation for this special issue is to bring together researchers and practitioners working on related fields in human centric security management and its services to present current research issues and advances. Papers on practical as well as on theoretical topics and problems are invited.

More specifically, the paper entitled "A Comprehensive Availability Modeling and Analysis of a Virtualized Servers System Using Stochastic Reward Nets" by T. A. Nguyen et al. proposed a virtualized servers system with multiple VMs via SRN. This paper encapsulated four VMs running on two VMMs into two hosts, and it also incorporated diverse failure modes and corresponding recovery behaviors regarding hardware and software aspects including host failure, SAN failure, aging-related failure, and Mandelbugs related failure in SRN models. The paper entitled "Software Authority Transition through Multiple Distributors" by K. Han and T. Shon discussed possible issues from using multiple OASs and proposed an improved PAS model that reduces management overheads without any additional entity, while still allowing users to obtain support from multiple OASs. This paper refined our model to support a temporary roaming situation, as well as a permanent OAS change. And it described the security of the proposed model. The paper entitled "The Study on Stage Financing Model of IT Project Investment" by S. Chen et al. applies the real option pricing model to measure the value brought by the stage financing strategy. The paper entitled "Advanced Approach to Information Security Management System Model for Industrial Control System" by S. Park and K. Lee presented two methodologies to prove that a new information security management system based on confidentiality, integrity, availability, and safety is required in the industrial control system. The paper entitled "An Integrative Behavioral Model of Information Security

Policy Compliance" by S. H. Kim et al. tried to find the factors of information security policy compliance and suggest the information security policy based upon the founded factors. The paper entitled "The Strategic Measures for the Industrial Security of Small and Medium Business" by C.-M. Lee presented that online security control services and technology deposit system are suggested for such measures. These measures could enhance to a certain extent the industrial security of SMB. The low security awareness and financial difficulties seem to be the main obstacles to equip the SMB with such measures. The paper entitled "AVQS: Attack Route-Based Vulnerability Quantification Scheme for Smart Grid" by J. Ko et al. proposed a novel AVQS to accurately measure the security level in a smart grid. The proposed approach includes NVS and end-to-end security functions. The paper entitled "The Need for Specific Penalties for Hacking in Criminal Law" by S. Oh and K. Lee analyzed the definitions and the penalties for hacking for each country and compared with the national law; then it made suggestions through more specific legislation. This paper expects it will reduce legal controversy and prevent excessive punishment. The paper entitled "Empirical Analysis of Retirement Pension and IFRS Adoption Effects on Accounting Information: Glance at IT Industry" by J. Kim reviewed new pension accounting with K-IFRS and provided empirical changes in liability for retirement allowances with adoption of K-IFRS. It will help to understand the effect of pension accounting on individual firm's financial report and the importance of public announcement of actuarial assumptions. The paper entitled "Security Techniques for Prevention of Rank Manipulation in Social Tagging Services including Robotic Domains" by O. Choi et al. proposed a detection method for tag-ranking manipulation to solve the problem of the existing methods which cannot guarantee the reliability of tagging. The paper entitled "Effects of Corporate Social Responsibility and Governance on Its Credit Ratings" by D. Kim and J. Kim showed nonfinancial information also may have effects on corporate credit rating. The investment on personal data protection could be an example of CSR/CGI activities which have positive effects on corporate credit ratings.

Eventually, we firmly believe that the accepted papers would be a meaningful contribution to researchers, students, and practitioners studying this field of strategic management advanced service for sustainable computing environment.

Acknowledgments

We would like to extend our sincere appreciation to all the authors for their priceless dedication and also to the referees for their support and hard work for reviewing the papers in a timely manner despite busyness.

Sang-Soo Yeo
Qun Jin
Vincenzo Loia
Hangbae Chang

Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 305452, 6 pages
http://dx.doi.org/10.1155/2014/305452

Research Article

Effects of Corporate Social Responsibility and Governance on Its Credit Ratings

Dong-young Kim[1] and JeongYeon Kim[2]

[1] *Gangdong College, Janghowon-eup, Icheon-si, Gyeonggi-do 467-900, Republic of Korea*
[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 19 August 2014; Accepted 16 September 2014; Published 27 October 2014

Academic Editor: Hangbae Chang

This study reviews the impact of corporate social responsibility (CSR) and corporate governance on its credit rating. The result of regression analysis to credit ratings with relevant primary independent variables shows that both factors have significant effects on it. As we have predicted, the signs of both regression coefficients have a positive sign (+) proving that corporates with excellent CSR and governance index (CGI) scores have higher credit ratings and vice versa. The results show nonfinancial information also may have effects on corporate credit rating. The investment on personal data protection could be an example of CSR/CGI activities which have positive effects on corporate credit ratings.

1. Introduction

Credit rating represents the credit rating agency's evaluation of qualitative and quantitative information on the credit worthiness of a company or government based on their ability to pay back the debt and the likelihood of default. Credit rating agencies disclose their evaluation results for investors to reflect them in their decision-making. Considering that it is not easy to evaluate all credit risks of corporate bond issuers, the evaluation results from credit rating agencies provide an investment guideline to market participants.

Even though agency may reflect additional nonpublic information in the evaluation, its credit rating is primarily based on the announced financial reports. It means that the reliability of accounting information is a critical factor to protect investors from credit risks. There were many efforts to improve the reliability of accounting information. After the experience of accounting frauds such as Enron case, US enacted the Sarbanes-Oxley Act to ensure the financial soundness of listed companies. Korean stock market also has experienced several accounting fraud cases, which were considered as the primary cause of "Korea Discount" phenomenon during last few decades and brought in many policies to verify corporates' accounting information including external audit requirements.

Although company's financial record is a primary factor to evaluate its credit rating, we can think of additional nonfinancial factors that have effects on company's credit rating. One of them is corporate social responsibility (CSR), a form of corporate self-regulation integrated into a business model. It embraces all business management activities beyond legal compliance based on ethics and morality of managers and stakeholders. In addition to the internal benefits of CSR activities such as better corporate image or sustainable management, CSR activities alleviate the risk of information asymmetry between investors by announcing reliable information. CSR activities also may reduce the company's ethical responsibility on its bankruptcy risks by providing investors with proper information on it.

Another example of nonfinancial information affecting the credit ratings is corporate governance. It refers to the mechanisms, processes, and relations by which corporations are controlled and directed. Corporate governance index (CGI) is the evaluation result of the company's internal environment and control system. Proper corporate governance enables reducing corporate's bankruptcy risks and providing useful, timely, and reliable information to the public.

In developed countries, CSR and corporate governance information are assumed as an important part of financial information because they enable investor to estimate

the sternness of company's internal control system and the accuracy of company's bankruptcy risk.

The purpose of this study is to verify if the evaluation on CSR and corporate governance is reflected into agencies' credit ratings in Korean money market and to review the correlations between them. This study can be differentiated from previous researches by the fact that we analyze effects on credit rating system of corporate aspects including both financial and nonfinancial information. In addition, the results verify that nonfinancial information such as CSR or corporate governance can be a proxy for credit rating based on the financial efficiency.

2. Theoretical Background

2.1. Credit Rating System. Credit ratings are usually attached to debt security such as a bond. Ratings are assigned by credit rating agencies using letter designations such as A, B, and C. Higher grades are intended to represent a lower probability of default. Related researches tried to identify corporate's components or elements which can affect its credit rating.

Standard & Poor's [1] published a report on how to evaluate corporate governance and governance practices. The report suggested 4 important factors on evaluating corporate governance: ownership structure, shareholder rights, financial transparency, and board structure. Individual characteristics of the factors enable effective decision-making by giving a control to managers' behavior and reducing the information asymmetry. The report also insisted identified factors can be used as a proxy of company's credit rating.

Moody's [2] reported that financial credit ratings and corporate governance are related to financial reporting quality, liquidity, and risk management. The expertise, vitality, and independency of board and audit committee can minimize the errors on the cash flow predictability and asset's measurement. Activities of board and audit committee are useful for the control and surveillance on management.

Bhojraj and Sengupta [3] analyzed the relationship between corporate governance and credit ratings. The results showed that companies with higher ratio of outside directors and institutional investment usually have higher credit ratings.

Dillenburg et al. [4] reported that credit rating agencies consider not only financial performance but also environmental, social, and ethical characteristics of corporate in their evaluation. Anderson et al. [5] analyzed the relationship between the agency costs and corporate governance. The independence of the board and audit committee results in higher credit rating and lower interest rates.

2.2. Corporate Social Responsibility. CSR-related studies have been done in the various fields of sociology, ethics, or economics. In the field of Business Administration, it was approached as a topic of human resource management and marketing instead of accounting field.

Carroll [6] had focused on ethical approaches on the relationship between business and society. He reviewed the corporates' social responsibility in terms of resolving social problems such as environmental improvement, community-support activities, and sustainable development.

Wood and Jones [7] reviewed the business activities with respect to the corporate responsibility to consumer, community, and other social issues. Creyer [8] insisted that the corporate stakeholders' behavior could be different according to the given expectations for ethical behavior. Ebner and Baumgatner [9] introduced the concept of sustainable development and reviewed the relationship between CSR activities and company's long-term growth. Kotler and Nancy [10] classified CSR activities into social contribution activities, consumer protection activities, and environmental protection activities. They reviewed the CSR effects based on each section.

International Standards Organization announced ISO 26000 as an international standard of corporate's social responsibility in November 1, 2010. It is the final output of efforts to integrate diverse aspects of organizations including ethics, management, and environment.

According to the research of Anderson and Cunningham [11], customers' conception on CSR is different according to his social status and demographic characteristics. Becker-Olsen et al. [12] found that customers reaction to CSR or purchase intention depends on the appropriateness between CSR activities and corporate's business area. Also the corporate's motivation of CSR-related activities, profits-oriented or community-support, affected the customers' evaluation. The analysis of Waddock and Graves [13] also supported the relationship between company's social performance and financial performance.

2.3. Corporate Governance. Governance structures identify the distribution of rights and responsibilities among different participants. It also includes the rules and procedures for making decisions in corporate affairs. There has been renewed interest in the corporate governance practices since the several stock market collapses during 2001-2002, most of which involved accounting fraud.

Cohen and Hanno [14] reviewed the effects of alignment on the management philosophy and governance control. In their analyzed preaudit planning, the auditor prefers to contract with the corporate having proper management philosophy and excellent governance structure. Asare et al. [15] showed that the audit fees are actually increased for companies with weak corporate governance structure by analyzing empirical data. Weak governance structure increases audit risk and audit fees are increasing according to it. Others [16, 17] reviewed the relationship between corporate governance and audit fees. They interpreted the risks of audit as higher probability of earning management, which can be a result of weak governance [16].

Kim [18] analyzed the impact of corporate governance on the credit rating. He used the evaluation method from S&P on corporate governance. The results showed that the institutional invest ratio, the quality of accruals, the timeliness of earnings, and the independence of board have positive (+) relations with corporate's credit rating.

3. Hypothesis

3.1. Hypothesis Development. If a company actively pursues corporate social responsibility, many researchers expect that

its business healthiness and fairness also improve. In addition, the advanced social services and excellent employees' satisfaction by contributing to economic development will lead the company to higher firm value in market. Also the mechanism of corporate governance protects the rights of shareholders and reduces the risk of bankruptcy by resolving the concerns of agency costs and asymmetric information.

The reported cases from other countries verify that CSR activities and corporate governance both should be considered to improve corporate's financial outcome. Many investors concern the risk of bankruptcy, which is related to financial reporting and internal control systems [19]. In Korea, investors also worry about issues of agency problems caused by separation of ownership and management. Logically, the CSR activities and corporate governance should play an important role in Korean capital market. Both of them improve overall efficiency of corporate by the alleviation of agency problem and the announcement of reliable financial information.

Many studies provide verification of their relationships. It would be clear that companies with excellent financial performance would have a higher credit rating. However, the relations between credit rating and nonfinancial information such as CSR and corporate governance are depending on market participants. Capital markets in developed countries are sensitive to the nonfinancial information in addition to the financial results.

The purpose of this study is to analyze the effects on credit rating system of nonfinancial information, CSR, and corporate governance, focusing on the Korean capital market. We set the following hypotheses on the effects of them on corporate credit ratings.

Hypothesis 1. CSR score has a significant positive (+) impact on the corporate's financial credit rating.

Hypothesis 2. Corporate governance score has a significant positive (+) impact on the corporate's financial credit rating.

3.2. Regression Model. To verify the effects of CSR and corporate governance on corporate credit rating, we first identify corporate's financial aspects having an effect on its credit rating evaluation. Previous researches suggested that financial variables having impacts on the credit rating are assets, inventory change, accounts receivable change, return over asset rate change, and debt ratio change. Adding a variable for CSR and corporate governance each, we can get (1) and (2) for regression analysis. Besides, industry dummy and dummy for year are added to identify their side effects:

$$\begin{aligned} \mathrm{CFR}_{i,t} &= \beta_0 + \beta_1 * \mathrm{CSR}_{i,t} + \beta_2 * \Delta\mathrm{ASST}_{i,t} \\ &\quad + \beta_3 * \Delta\mathrm{REC}_{i,t} + \beta_4 * \Delta\mathrm{INV}_{i,t} \\ &\quad + \beta_5 * \Delta\mathrm{ROA}_{i,t} + \beta_6 * \Delta\mathrm{DEBT}_{i,t} \\ &\quad + \Sigma\mathrm{ID}_i + \Sigma\mathrm{YR} + \varepsilon_{i,t}. \end{aligned} \tag{1}$$

$$\begin{aligned} \mathrm{CFR}_{i,t} &= \beta_0 + \beta_1 * \mathrm{CGI}_{i,t} + \beta_2 * \Delta\mathrm{ASST}_{i,t} \\ &\quad + \beta_3 * \Delta\mathrm{REC}_{i,t} + \beta_4 * \Delta\mathrm{INV}_{i,t} \\ &\quad + \beta_5 * \Delta\mathrm{ROA}_{i,t} + \beta_6 * \Delta\mathrm{DEBT}_{i,t} \\ &\quad + \Sigma\mathrm{ID}_i + \Sigma\mathrm{YR} + \varepsilon_{i,t}. \end{aligned} \tag{2}$$

(Cf)

$\mathrm{CFR}_{i,t}$: corporate i's financial credit rating at time t;

$\mathrm{CSR}_{i,t}$: corporate social responsibility index of corporate i at time t;

$\mathrm{CGI}_{i,t}$: corporate governance index of corporate i at time t;

$\Delta\mathrm{ASST}_{i,t}$: corporate i's changes of total assets, $(\mathrm{ASST}_{i,t} - \mathrm{ASST}_{i,t-1})/\mathrm{ASST}_{i,t-1}$;

$\Delta\mathrm{REC}_{i,t}$: corporate i's changes of account receivables, $(\mathrm{REC}_{i,t} - \mathrm{REC}_{i,t-1})/\mathrm{REC}_{i,t-1}$;

$\Delta\mathrm{INV}_{i,t}$: corporate i's changes of inventory assets, $(\mathrm{INV}_{i,t} - \mathrm{INV}_{i,t-1})/\mathrm{INV}_{i,t-1}$;

$\Delta\mathrm{ROA}_{i,t}$: corporate i's changes of return on assets, $(\mathrm{ROA}_{i,t} - \mathrm{ROA}_{i,t-1})/\mathrm{ROA}_{i,t-1}$;

$\Delta\mathrm{DEBT}_{i,t}$: corporate i's changes of debts, $(\mathrm{DEBT}_{i,t} - \mathrm{DEBT}_{i,t-1})/\mathrm{DEBT}_{i,t-1}$;

ID: dummy variable for company group;

YR: dummy variable for year;

$\varepsilon_{i,t}$: error.

As described before, we identified corporate aspects including both financial and nonfinancial information as independent variables affecting its credit rating, which can be a differentiation from other related researches. We can clearly identify the effects of nonfinancial information on corporate's credit ratings compared to that of financial information.

3.3. Data. For the data analysis, we use the credit rating scores published by NICE, a credit rating agency in Korea (http://www.nicerating.com/). NICE credit rating is the result of their integrated model of insolvency prediction and financial evaluation. It refines data categories based on the industry and the credibility intervals based on company assets and continuous holding period.

The financial rating is scored out of 100 points based on the financial statements of the company and additional nonfinancial items. Table 1 shows the metrics for credit rating. In data analysis, we use natural log of the total score to control heteroscedasticity of each item.

As a proxy of CSR evaluation, we used KEJI Index published by Citizen's Coalition for Economic Justice (CCEJ, http://www.ccej.or.kr/) in Korea. Table 2 shows their metrics for CSR.

As a proxy of corporate governance, we used the evaluated scores on it during 2007–2009 provided by "Corporate Governance Service" (http://www.cgs.or.kr/) established by the Ministry of Strategy and Finance in Korean Government. Table 3 shows their metrics for corporate governance.

Among the listed companies, we select candidates whose accounting period is January to December. Empirical data

Table 1: Criteria of credit rating.

Items	Variables	Assigned scores
Stability	Ratio of net worth to total capital	10
	Debt/sale	10
Liquidity	Sale/NCR (net capital ratio)	10
	Current ratio	10
Profitability	Ratio of net income to total capital	10
	Financial cost burden	10
Growth	Sales growth	5
	Total assets growth	5
Activity	Total assets turnover ratio	5
	Accounts receivable turnover ratio	5
Size	Total assets	7.5
	Sales	7.5
Nonfinancial	Corporate type	3
	Others	2
Total		100

Table 2: Evaluation item for CSR.

Items	Evaluation criteria
Healthiness	Shareholder composition, soundness of spending/investment and capital raise
Fairness	Fairness, transparency, relationship subcontract
Public contribution	Underprivileged protection, social welfare support
Consumer protection	Consumer rights protection, quality, advertising
Environmental protection	Environmental improvements result, violations, and pollution performance
Employee welfare	Industrial accidents, human resource investment, wage benefits, labor relations, equal employment
Economic development	Research and development efforts, financial performance, and economic contribution

set is the annual financial report during 2007–2009 from selected nonfinancial company. Among 612 companies, we could review financial reports for the period, and we selected 440 companies of which CSR and CGI data were available from the data providers. After removing 1% outliers, we had total 436 data for regression analysis. Table 4 indicates the distribution of data classified with industry and year.

4. Results

The descriptive statistics of the variables are shown in Table 5. The mean and the standard deviation of financial credit rating, CFR, are 68.128 and 11.415 each. CSR's minimum and maximum values are 0.000 and 74.350, while its average is 21.493. CGI's minimum and maximum values are 20 and 100, while its average is 41.589.

Table 3: Criteria for corporate governance.

Items	Description
Rights of shareholders	Introduction of the corporate governance charter and code of ethics Introduction of cumulative voting or written voting Introduction of staggered election
Board of directors	Outside directors and attendance ratio Outside directors' objections or suggested modifications Recommendation of outside directors
Disclosure	IR performance Disclosures frequency including voluntary, queries, and corrections Announcement of the board member's attendance and voting
Audit committee	Organization of the audit committee, the configuration, and operating Establishment of an internal crime reporter protection Recommendation of external auditors or consulting
Reward management	Dividend yield, share buyback Three-year average dividend payout ratio, interim dividend

Table 4: Data group categorised by industry.

Industry	2007	2008	2009	Total
Food/drug, textile, paper	31	30	34	95
Metal/nonmetal, chemistry	32	31	35	98
Electronics, machinery	43	45	43	131
Service	37	36	39	112
All	**143**	**142**	**151**	**436**

Table 5: Statistics of variables.

	Min.	Max.	Average	SD	Count
CFR	30	95	68.128	11.415	436
CSR	0	74.35	21.493	29.965	436
CGI	20	100	41.589	11.809	436
ΔASST	−0.89	0.869	0.006	0.172	436
ΔREC	−0.803	1.96	0.113	0.353	436
ΔINV	−0.945	1.986	−0.393	0.339	436
ΔROA	−6.928	7.502	−0.135	1.47	436
ΔDEBT	−0.467	0.954	0.025	0.184	436

Table 6 shows the correlation between the variables using Pearson correlation coefficients. Both CFR/CSR and CFR/CGI have positive (+) correlation at 1% significant level. Besides, CFR/ΔASST also shows positive correlation significant at the 1% level and CFR/ΔDEBT also shows negative (−) correlation significant at the 5% level.

Those results show credit rating values increases according to the company's asset increase or debt decrease. However, the rate changes of inventory, accounts receivable, and return

Table 6: Pearson correlation between variables.

	CFR	CSR	CGI	ΔASST	ΔREC	ΔINV	ΔROA	ΔDEBT
CFR	1							
CSR	0.060***	1						
CGI	0.180***	0.195***	1					
ΔASST	0.074***	−0.017	0.007	1				
ΔREC	−0.003	−0.023	0.069***	−0.008	1			
ΔINV	−0.009	−0.015	0.038	0.02	0.053	1		
ΔROA	0.016	0.036*	0.024	−0.004	0.016	0.012	1	
ΔDEBT	−0.007**	−0.012	−0.006	0.01	0.05	0.024	−0.014	1

*$P < 0.05$, **$P < 0.01$, and ***$P < 0.001$.

Table 7: Results of regression analysis with equations.

	Equation (1)	Equation (2)
CSR	0.294 (6.638***)	
CGI		0.093 (2.013**)
ΔASST	−0.013 (−0.228)	0.005 (0.118)
ΔREC	0.106 (2.285**)	0.097 (2.007**)
ΔINV	0.209 (4.594***)	0.230 (4.840***)
ΔROA	0.145 (3.265***)	0.161 (3.465***)
ΔDEBT	0.294 (−2.709***)	−0.123 (−2.550**)
ID	Included	Included
YR	Included	Included
F value	16.149***	8.722***
Adj R^2	0.176	0.098

Cf: $N = 436$; t-value in ( ).
*$P < 0.05$, **$P < 0.01$, and ***$P < 0.001$.

on asset do not have any significant correlation with corporate credit rating.

The results of regression analysis with (1) and (2) to verify the effects of CSR and corporate governance on credit rating are shown in Table 7. Result for (1) has 0.176 for adjusted R^2 and its F-value is significant. The coefficient of CSR has positive sign and is significant at 1% level, which means that company with higher evaluation on CSR has higher credit rating.

Result for (2) shows that adjusted R^2 is 0.098 and its F-value is also significant. The coefficient of CGI has positive sign and is significant at 5% level, which means that company with higher evaluation on CGI has higher credit rating.

5. Conclusion

This study verifies the relationship between credit rating and nonfinancial information such as CSR and corporate governance. CSR activities have effects of reducing agency costs by eliminating the information asymmetry between internal and external stakeholders. Companies can fundamentally improve their social responsibilities with public announcement of proper financial reports and investment risks. Corporate governance is a key element of the internal control system, which is also critical to provide timely and reliable corporate financial information for outside investors to accurately judge the bankruptcy risk of the company. Both of them help to reduce agency costs and minimize the unfavorable side effect of information asymmetry.

Traditionally, corporate's financial information and credit rating are intimately related. The suggested nonfinancial information has an effect on corporate credit rating individually, but integrated verification also considering the financial information is not provided for Korea market yet.

To prove our assumptions of nonfinancial information on the relationship, we provided empirical analysis with data from selected companies. The results of the analysis showed a significant correlation between credit rating and CSR and corporate governance. In the regression analysis between related variables, coefficients had positive (+) sign for both of them. Also the F-value of regression results was statistically significant at the 1% level. As we assumed, a company with higher evaluation on CSR and corporate governance has solid credit rating score. The effects of suggested nonfinancial information are positive on corporate credit rating regardless of the effects of financial information.

We interpret the analysis results as follows. Credit rating system in Korea market is mutualized as in other developed countries. The agents' index calculation methods are stabilized and we can predict the reaction of investors in stock markets according to the credit rating disclosure. The coherence between corresponding CSR/CGI variables and credit ratings has been increased during few decades and the results of data analysis between those variables prove their relationships.

The higher the credit rating has a corporate, the better the scores of corporate governance and corporate social responsibility are expected. Additional analysis for the refined metrics of CSR and corporate governance could provide investors with specific insights into the proxy of their market value. For the further research of CSR, we could consider wider nonfinancial area such as data security on personal information.

Disclosure

Dong-young Kim is the first author.

Conflict of Interests

The authors declare that they have no conflict of interests regarding the publication of this paper.

Acknowledgment

This research was supported by the MSIP (Ministry of Science, ICT & Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2014-H0301-14-1044) supervised by the NIPA (National ICT Industry Promotion Agency).

References

[1] S. A. Patel and G. Dallas, *Transparency and Disclosure: Overview of Methodology and Study Results—United States*, Standard & Poor's, 2002.

[2] Moody's, *Moody's Findings on Corporate Governance in the Uited States and Canada*, Moody's Investors Service, New York, NY, USA, 2004.

[3] S. Bhojraj and P. Sengupta, "Effect of corporate governance on bond ratings and yields : the role of institutional investors and outside directors," *Journal of Business*, vol. 76, no. 3, pp. 455–475, 2003.

[4] S. Dillenburg, T. Greene, and H. Erekson, "Approaching socially responsible Investment with a comprehensive ratings scheme: total social impact," *Journal of Business Ethics*, vol. 43, no. 3, pp. 167–177, 2003.

[5] R. C. Anderson, S. A. Mansi, and D. M. Reeb, "Board characteristics, accounting report integrity, and the cost of debt," *Journal of Accounting and Economics*, vol. 37, no. 3, pp. 315–342, 2004.

[6] A. Carroll, "A three-dimensional conceptual model of corporate performance," *The Academy of Management Review*, vol. 4, no. 4, pp. 497–505, 1991.

[7] D. J. Wood and R. E. Jones, "Stakeholder mismatching: a theoretical problem in empirical research on corporate social performance," *International Journal of Organizational Analysis*, vol. 3, no. 3, pp. 229–267, 1985.

[8] E. H. Creyer, "The influence of firm behavior on purchase intention: do consumers really care about business ethics?" *Journal of Consumer Marketing*, vol. 14, no. 6, pp. 421–432, 1997.

[9] D. Ebner and R. J. Baumgatner, "The relationship between sustainable development and corporate social responsibility," in *Proceedings of the Corporate Responsibility Research Conference*, pp. 4–5, 2006.

[10] p. Kotler and L. Nancy, *Corporate Social Responsibility: Doing the Most Good for Your company and Your Cause*, John Wiley & Sons, Hoboken, NJ, USA, 2005.

[11] W. T. Anderson Jr. and W. H. Cunningham, "The socially conscious consumer," *Journal of Marketing*, vol. 36, no. 3, pp. 23–31, 1972.

[12] K. L. Becker-Olsen, B. A. Cudmore, and R. P. Hill, "The impact of perceived corporate social responsibility on consumer behavior," *Journal of Business Research*, vol. 59, no. 1, pp. 46–53, 2006.

[13] S. A. Waddock and S. B. Graves, "The corporate social performance-financial performance link," *Strategic Management Journal*, vol. 18, no. 4, pp. 303–319, 1997.

[14] J. R. Cohen and D. M. Hanno, "Auditors' consideration of corporate governance and management control philosophy in preplanning and planning judgments," *Auditing*, vol. 19, no. 2, pp. 132–146, 2000.

[15] S. Asare, J. Cohen, and G. Trompeter, "The effect of management integrity and non-audit services on client acceptance & staffing decision," Working paper, University of Florida, 2002.

[16] J. C. Bedard and K. M. Johnstone, "Earnings manipulation risk, corporate governance risk, auditor' planning & pricing decisions," *Accounting Review*, vol. 79, no. 2, pp. 277–304, 2004.

[17] K. M. Johnstone and J. C. Bedard, "Risk management in client acceptance decisions," *The Accounting Review*, vol. 78, no. 4, pp. 1003–1025, 2003.

[18] B. Kim, "Corporate governance and firms credit ratings: based on S&P's (2002) corporate governance framework," *Accounting Information Review*, vol. 29, no. 1, pp. 261–288, 2011.

[19] W. Wallace, *A time Series Analysis of the Effect of Internal Audit Activities on External Fees*, Institute of Internal Auditors Research Foundation, Altamonte Spring, Fla, USA, 1984.

Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 165316, 18 pages
http://dx.doi.org/10.1155/2014/165316

Research Article

A Comprehensive Availability Modeling and Analysis of a Virtualized Servers System Using Stochastic Reward Nets

Tuan Anh Nguyen,[1] Dong Seong Kim,[2] and Jong Sou Park[1]

[1] *Department of Computer Engineering, Korea Aerospace University, 76 Hanggongdaehang-ro, Deogyang-gu, Goyang-si, Gyeonggi-do 412-791, Republic of Korea*
[2] *Department of Computer Science and Software Engineering, College of Engineering, University of Canterbury, Private 4800, Christchurch 8140, New Zealand*

Correspondence should be addressed to Tuan Anh Nguyen; anhnt2407@gmail.com

Received 8 May 2014; Accepted 2 July 2014; Published 5 August 2014

Academic Editor: Sang-Soo Yeo

It is important to assess availability of virtualized systems in IT business infrastructures. Previous work on availability modeling and analysis of the virtualized systems used a simplified configuration and assumption in which only one virtual machine (VM) runs on a virtual machine monitor (VMM) hosted on a physical server. In this paper, we show a comprehensive availability model using stochastic reward nets (SRN). The model takes into account (i) the detailed failures and recovery behaviors of multiple VMs, (ii) various other failure modes and corresponding recovery behaviors (e.g., hardware faults, failure and recovery due to Mandelbugs and aging-related bugs), and (iii) dependency between different subcomponents (e.g., between physical host failure and VMM, etc.) in a virtualized servers system. We also show numerical analysis on steady state availability, downtime in hours per year, transaction loss, and sensitivity analysis. This model provides a new finding on how to increase system availability by combining both software rejuvenations at VM and VMM in a wise manner.

1. Introduction

Computing systems with virtualization are rapidly gaining strong attention for computational sustainability by administrators of information resources in enterprises. Computational sustainability is a field to develop computational models, methods, and tools to help balance environmental, economic, and societal needs for a sustainable development [1]. Thus, virtualized computing systems, such as in software defined data center (SDDC) or infrastructure as a service (IaaS) in cloud computing, are core approach and promising solution to create a sustainable IT business infrastructure [1–3]. The IT business infrastructure with virtualization is capable to confront with variety of security concerns [4] as well as to avoid interruption of ordinary business processes [3, 5] and to assure high availability and continuity of information resources flowing within an organization [6]. In an IT business infrastructure, server virtualization is one of the essential parts of virtualization process along with storage virtualization, network virtualization, and workload management. Enterprises can save capital, floor space and energy via server virtualization and are able to improve business efficiencies due to resource utilization and autonomous management for heterogeneous workloads in data centers. The main idea behind server virtualization is to consolidate multiple workloads onto fewer physical servers (hereinafter, called host) with software based orchestration by creating multiple virtual servers (i.e., virtual machines (VM)) on a virtual machine monitor (VMM) in a physical host. In recent years, IT enterprises have also adopted server virtualization as the most appropriate approach in IaaS for cloud computing services to provide agile computing resources over the Internet. Cloud providers offer predescribed configuration of computing resources to cloud customer in accordance with service level based agreements (SLA) by assigning corresponding configuration of VM. Assuring high availability of cloud services over virtualization is of paramount importance. Thus, availability management and fault tolerance in such virtualized servers system are getting more concerned in both hardware and software aspects. High availability

(HA) solutions [6–8] and fault tolerant mechanisms [9–11] have been proposed to counteract with hardware or software faults in virtualized servers system. Nevertheless, the studies individually do not take into account various failure modes in a complete manner. Also, a small number of works studied availability of virtualized servers systems in a quantitative way. Thus, it is necessary to incorporate various hardware and software failure modes along with corresponding recovery behaviors and analyze the availability of such systems.

The main drawbacks of previous work are that most of virtualized systems are composed of only one VM running on one VMM in a physical server; see the papers [9, 10]. This architecture is commonly used in modeling and analysis of a virtualized server system in a number of studies, even though the proposed architecture in their hypothesis shows multiple VMs hosted on one VMM [11, 12]. Some studies [10, 13, 14] did take into account an additional physical host under active/cold standby or active/passive configurations [6], but only for assessing the effectiveness of live migration of a VM. Moreover, the previous work has not properly captured the behaviors of a virtualized system with multiple VMs running on multiple physical host servers. Only a few papers considered thoroughly the involvement of both hardware and software failure modes.

The main contributions of this paper are summarized as follows.

(i) Studied a virtualized servers system with two VMs running on one VMM in each host, which is the active/active HA configuration [6].

(ii) Incorporated various failure and recovery behaviors including hardware failure, software aging failure, and Mandelbug related failure.

(iii) Captured different types of hardware and software dependencies: (i) between a physical host and hosted VMM, (ii) between VMM and VMs, and (iii) between VMs and a storage area network (SAN).

(iv) Analyzed and found out (i) the use of a frequent rejuvenation on VM may lower steady state availability (SSA) of the virtualized systems whereas that of VMM rejuvenation may enhance the SSA; (ii) the frequent rejuvenation policy on VM is the main culprit of VM transaction loss; (iii) a proper combination of VM rejuvenation may enhance the SSA compared to that of VMM rejuvenation.

The rest of this paper is organized as follows. Related work is presented in Section 2. Section 3 introduces a virtualized servers system. Section 4 presents SRN models for the virtualized servers system. The numerical analysis and discussion are presented in Section 5. Finally, Section 6 concludes the paper.

2. Related Work

Server virtualization is now a mainstream technology offering a way to consolidate servers and enable autonomic management of heterogeneous workloads. Virtualized server systems may be composed of an overall architecture that is even more complex than that of traditional nonvirtualized server systems. According to virtualization concept, applications (hereafter, App) and operating system (OS) are encapsulated in a separate and completely isolated container called a virtual machine (VM), decoupled from the physical host by a hypervisor or virtual machine monitor (VMM) [13]. In virtualized server systems, a VM (i.e., virtual server) is a software implementation executing programs like a real server. Multiple VMs are designed to work simultaneously on one physical host regardless of different types of workloads. Therefore, instead of operating many servers at low utilization, virtualization squeezes more processing powers onto fewer servers running at higher level of total resource utilization. In previous literature [14], two types of server virtualization implementation have been presented: (i) hosted hypervisor running on a host operating system that provides virtualization services (e.g., Microsoft Virtual Server 2005 [15]); (ii) native or bare metal hypervisor running directly on system hardware (e.g., Microsoft Hyper-V [16], Citrix Xen [17], and VMWare ESX [18]). The native hypervisor implementation for server virtualization has been adopted in various studies on server systems [19–22] since this approach facilitates faster transactions with hardware devices [13]. Thus, this implementation approach is also adopted in this paper.

Software rejuvenation was first introduced by Huang et al. [23] as a promising solution to mitigate the adverse effects of software aging. The main idea behind software rejuvenation is to gracefully terminate and periodically or adaptively restart the software execution environment in order to clear aging status. Hence, the technique aims to postpone or prevent the occurrence of aging-related failures under specific policies. Many different policies have been proposed to implement software rejuvenation on different systems. A profound classification of software rejuvenation techniques has been presented in detail by Alonso et al. [24]. Accordingly, software rejuvenation approaches can be classified in two main groups: time-based and inspection-based strategies. A software system with time-based rejuvenation policy is periodically rejuvenated every time as a predefined time interval has elapsed [25]. The rejuvenation process is triggered by a clock counting time [26, 27]. The determination of optimal interval to achieve maximum availability and minimum downtime cost, however, is mostly performed through building and analyzing an analytical model [27–29], whereas inspection-based rejuvenation is triggered in the case if aging effects measured through observations of system state violate restrict criteria or particular conditions. The rejuvenation trigger epoch is decided by a variety of mechanisms including threshold-based methods using aging indicators [30–32]; prediction-based approaches: machine learning, statistical approaches, or structural models [33–36]; and mixed approaches using prediction methods to determine optimal threshold [37]. However, the implementation of inspection-based rejuvenation in a real environment could be troublesome for system administrator due to the growing complexity of the systems introduced by recent technologies (e.g., cloud computing) and heterogeneous environments (e.g., software defined data center) where the systems have

to interact with each other. Previous literature showed that time-based rejuvenation associated with a proper scheduling technique could be a suitable solution for these scenarios. For instance, Naksinehaboon et al. [38] proposed efficient rejuvenation scheduling techniques for operating system/kernel rejuvenation combination between different nodes in a high computing system (HPC). Machida et al. [39] has presented a combined scheduling technique for server virtualization in a virtual data center.

Server rejuvenation was first used by Machida et al. in [39, 40] as a term to imply software rejuvenation implementation on a server. In nonvirtualized server systems, server rejuvenation is performed in a reboot of operating system to clear aging-related bugs. It is reported in [32, 41, 42] that aging phenomena do manifest in an operating system and cause performance loss, significant resource exhaustion, and unexpected system failures. The detection and analyses in the studies, however, are complicated and mostly employed in an evaluation process of operating system rather than during software execution. In virtualized server systems, server rejuvenation refers to a combined-rejuvenation scheduling technique to perform rejuvenation processes on both VMM and VM subsystems within a server or among servers under predetermined policies [39, 40]. There are a number of studies on rejuvenation strategies which are applied on virtualized server systems. Thein et al. [9, 29] modeled and analyzed a virtualized single-server system with multiple VMs. The study showed that the use of virtualization technology associated with software rejuvenation techniques can improve system availability in virtualized systems versus in nonvirtualized systems. However, the software rejuvenation in the study was implemented only on VM subsystem regardless of VMM subsystem involvement. The technique therefore can clear aging states of VMs and applications, except VMM. Since a VMM is hosting software, it is not rebooted frequently in a long-run period. Thus, the VMM subsystem suffers aging phenomena more easily than other parts of the system do, and the VMM performance degradation due to accumulation of aging-related bugs can influence more severely on the hosted VM's operation. Researchers have been still putting their efforts in finding a proper approach for software rejuvenation implementation on a virtualized server system in consideration of both VMM and VM subsystems. To resolve this issue, three VMM rejuvenation techniques have been proposed in consideration of hosted VMs' behaviors in works [10, 40, 43], namely, cold-VM rejuvenation, warm-VM rejuvenation, and migrate-VM rejuvenation. In the warm-VM rejuvenation, all hosted VMs are shut down prior to VMM rejuvenation regardless of the VMs' operational status. After VMM rejuvenation, the VMs are booted in sequence, whereas the implementation of warm-VM rejuvenation is based on the mechanisms of on-memory suspension and resume of VM's operating status, respectively, before and after VMM rejuvenation. The VMs' executions are suspended and stored in a shared memory system before triggering VMM rejuvenation. After the completion of VMM rejuvenation, the VMM reloads VMs' memory images in sequence to restore the VMs' executions. Instead of shutting down or suspending VMs as in the cold-VM or the warm-VM rejuvenations, the VM-migrate rejuvenation offers a VM live-migration approach in which all running VMs are migrated to another host prior to VMM rejuvenation and are migrated back to the former host as soon as the VMM rejuvenation completes. Machida et al. [10, 40] applied the above VMM rejuvenation techniques on VMM subsystem along with time-based rejuvenation on VM subsystem in a typical servers system consisting of one primary host (providing services) and another secondary host (for live migration of VMs). The primary host enables one VM to run on a VMM whereas the secondary host runs a VMM in awaiting state for the sake of the VM live migration. This host, however, is not taken into consideration in modeling and analysis. In this paper, we studies an extended architecture of a virtualized system in which the system consists of two virtualized hosts, each host has two VMs running on one VMM. And we attempt to model and analyze the system with the active involvement of both hosts in providing services. To avoid the complexity in modeling, we do not apply the known-above VMM rejuvenation strategies, which are not our main focus (we attempt to model and analyze the virtualized system in a complete manner regarding both hardware and software aspects). Instead, our approach is to clear all VMs' operating states during VMM rejuvenation. The clean VMs are booted in sequence after the completion of the VMM rejuvenation.

Two main analysis approaches including measurement-based approach and analytic modeling approach are usually applied to study virtualized server systems with time-based rejuvenation. The former approach collects empirical data of system operation and applies statistical analysis to determine the epoch over which to perform rejuvenation [41, 44], whereas the latter approach analyzes the system based on a set of analytical models such as partial model, system model, or hierarchical model [27, 40, 45, 46]. The models aim to capture failure modes and recovery behaviors by defining system states and transitions. However, various assumptions on failure and repair time distributions of state transitions need to be incorporated in the models as input parameters. The system characteristics are analyzed through a variety of output metrics, for instance, steady state availability, loss probability, or downtime cost. Also, in a virtualized system with software rejuvenation, the optimal rejuvenation schedule is determined by optimization techniques under particular criteria which are to maximize availability or to minimize downtime cost. In previous literature, some analytical techniques have been used to model and analyze a virtualized server system with software rejuvenation. Thein and Park [29] presented a recursive availability model using CTMC to capture the behavior of a virtualized system with a large number of VMs but the model did not incorporate VMM rejuvenation. In work [45], Kim et al. attempted to incorporate in a hierarchical stochastic model based on fault tree and CTMC the details of different hardware failures (CPU, memory, power, etc.), software failures (VMs, VMM, and application) and corresponding recovery behaviors. The study took into consideration the system architecture of two hosts with one VM running on one VMM in each host. But the modeling did not cover completely dependent behaviors between hardware and software subsystems due to the state explosion issue in CTMC modeling in the case of complex

systems. Machida et al. [10, 40] presented comprehensive SRN availability models for VMM and VM in a server virtualized system with time-based rejuvenation. The models captured aging failure mode and applied time-based rejuvenation for both VMM and VM subsystems. Furthermore, the dependent behaviors between VMM and VM subsystems were taken into account in three cases of VMM rejuvenation techniques: cold-VM, warm-VM, and VM-migrate rejuvenations. In our work, we disregard VM live migration during VMM rejuvenation for simplicity. But we take into account in detail different hardware and software failure modes and recovery behaviors as well as dependent behaviors between subsystems. We attempt to analyze the impact of rejuvenation implementation on system availability of VM versus VMM subsystems in a typical virtualized system with multiple VMs.

3. A Virtualized Server System

3.1. System Architecture. The architecture of a typical virtualized servers system (VSS) with multiple VMs is depicted in Figure 1. The VSS consists of two physical servers (also called hosts, host1 and host2). Both hosts have an identical configuration. Each host has a VMM (which is also known as hypervisor) and each host runs two VMs on its VMM. Each VM subsystem is composed of an operating system (OS) and multiple identical applications (Apps) as wanted. In this paper, we disregard the involvement of OS, Apps, and workload, which has been studied in [47, 48]. The hosts share a storage area network (SAN) on which the VM images or VMM source code files are stored. We will be using this system to study availability of a virtualized system. The model can be further extended in the future, but our focus is to take into account the detailed behaviors of a virtualized system, in contrast to incorporating a large scale cloud system as in [49].

3.2. Failure Modes and Recovery Behaviors of the VSS. We take into account the following failure modes and corresponding recovery behaviors in SRN models to be presented in the next section.

(i) *Hardware failures* [45, 50] on hosts and SAN: both hosts are subject to hardware malfunctions due to hazardous faults on components (e.g., CPU, memory, disk, and cooler). Also, a SAN is likely exposed to hardware failures (e.g., failures of switches, disk array, tape, etc.). The hardware failures on hosts and SAN severely cause outage in operation of the subsystems. Once, the subsystems enter downtime state due to hardware failures, it is needed to summon a repairperson for hardware replacement or maintenance.

(ii) *Nonaging-related Mandelbugs failures* [51] on both VMMs and VMs subsystems: Both VMM and VM subsystems apparently confront with software faults which are broadly divided into Bohrbugs and Mandelbugs [52]. A subtype of Mandelbugs, nonaging-related Mandelbugs (NAM), whose causes are unknown and can go unnoticed after the deployment of VMM and VM subsystems on a virtualized system. Therefore, the VMM and VM subsystems are likely incurred nonaging failures under the occurrence of NAM. In this scenario, a summoned repairperson has to investigate and fix the bugs thoroughly.

(iii) *Software aging-related failures* [39, 53] on both VMMs and VMs subsystems: they are known as another subtype of Mandelbugs; software aging in long-run software systems like VMM and VM subsystems causes an increased failure rate and/or degraded performance due to accumulation of aging errors. The error condition brings a period of failure-probable state to bear on the VMM and VM subsystems in which the subsystems still run with degraded performance. If without external intervention, the subsystems inevitably undergo an aging-related failure [54]. Since then, a recovery process is conducted by a repairperson to remove aging causes and reconfigure the subsystems [55].

(iv) But we do not incorporate *Bohrbugs* [56] in the VMMs and VMs subsystems, which are able to be found and removed in software development and testing phases.

(v) *Dependencies* are also taken into account in detail.

(a) *Between host and VMM:*

(1) if a host goes into failure state, in consequence, the running VMM (in robust or failure-probable states) falls into downstate in which the VMM subsystem no longer provides virtualization. The VMM in downstate is restarted to robust state as soon as the host is recovered to healthy state;

(2) the VMM's operation, however, is suspended if the VMM currently resides in failure/rejuvenation states. After the failed host is repaired, a rollback and synchronization process (as adopting the active/active configuration [6]) is conducted to resume the VMM to the latest operational status which is logged and stored on SAN.

(b) *Between VMM and VM:*

(1) as the VMM enters either downstate or failure states, the hosted VM (in robust or failure-probable states) goes into downstate due to the consequence of its dependency on the hosting VMM. The VM in downstate is restarted to robust state when its VMM enters running states (either robust or failure-probable states);

(2) if a VM is currently in failure/rejuvenation states, instead of pushing the VM to downstate as usual, a temporary VM suspension is performed. The current state of the VM including the state of all applications and processes running on the VM is saved into VM image file and stored on SAN. As soon

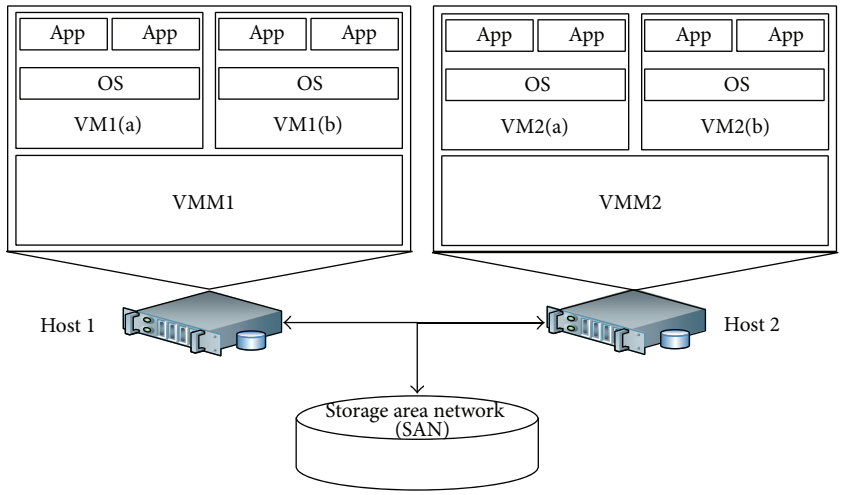


Figure 1: Architecture of a virtualized servers system.

as the hosting VMM enters running states (either robust or failure-probable states), the suspended VM is resumed by reloading the VM image file on SAN and it continues operating at its latest state;

(3) furthermore, as the VMM rejuvenation process is triggered, the current states of all hosted VMs are cleared and reset to the clean state in which the VMs are ready to boot right after the completion of the VMM rejuvenation [43]. This strategy is to clean the whole virtualized system (including both VMM and VM subsystems) after every interval of VMM rejuvenation.

(c) *Between VM and SAN:*

(1) a VMM (as a hypervisor program) is loaded onto host's internal memory to execute without interruption and for higher performance [43]. However, VM image files (large size) are stored on SAN. Thus, the current operational state of SAN decides the running state of VM;

(2) if the SAN fails, the VMs in running states (either robust or failure-probable states) go into downstate. A VM cannot restart unless the SAN is repaired;

(3) if the current state of a VM is not in running states, we assume that its operation is suspended temporarily and resumed after the completion of SAN recovery.

3.3. Assumptions. In order to capture proper behaviors of VSS with multiple VMs, we made some assumptions as follows.

(i) Distributions. In order to make the analytical model as close as possible to a practical system, it is necessary to assume the distribution types of time to failure and time to recovery. However, there is no consensus on distributions in every failure mode and corresponding recovery behavior. Thus, it is better to apply general distributions but not restrict to predetermined ones for wide applicability. There is a large number of papers [10, 27–29, 39, 40, 57–60] in previous work supporting the use of exponential distribution. In this paper, we assume that the exponential distribution is generally applied on all transition times of timed transitions in the models. However, we assume to apply a deterministic distribution on time to trigger rejuvenations for both VMM and VM subsystems since the rejuvenation intervals are fixed values.

(ii) Software Aging. Through previous experiments, software aging has been reported as a phenomenon resulting into two cases: (i) sudden crash/hang failure [39, 61], which leads to software unavailability; (ii) progressive performance degradation [62–64]. However in this paper, both effects are considered in a single model and captured by the state of failure-probable in which the system manifests its degraded performance or high probability of failure.

(iii) Unexpected Failure Events and Failover Mechanisms. Since our focus is on detailed behavior of a virtualized system with multiple VMs and hosts, we restrict ourselves to not incorporate live VM migration and other failover mechanisms for the virtualized system which have been studied as in [27, 40, 47]. Also, to simplify the modeling, we do not consider any unexpected and unpredicted failure events during VMM/VM suspension and resume operations. These mechanisms and failure events in a virtualized system with multiple VMs are promising topics for future work.

(iv) Monitoring Agents. In most of system architectures in previous work [27, 36, 59, 65], several terms such as software rejuvenation agent (SRA), rejuvenation manager (RM), or management server were used in system architecture description as common components to monitor aging phenomenon and proceed to rejuvenation accordingly. It is

supposed that our system does involve the above elements as a common management system to monitor and manage the operations of the virtualized system. However, since the above components are not taken into account in modeling as per previous studies, we therefore do not depict and describe the involvement of system management components for simplicity of system architecture presentation.

4. SRN Models of the VSS

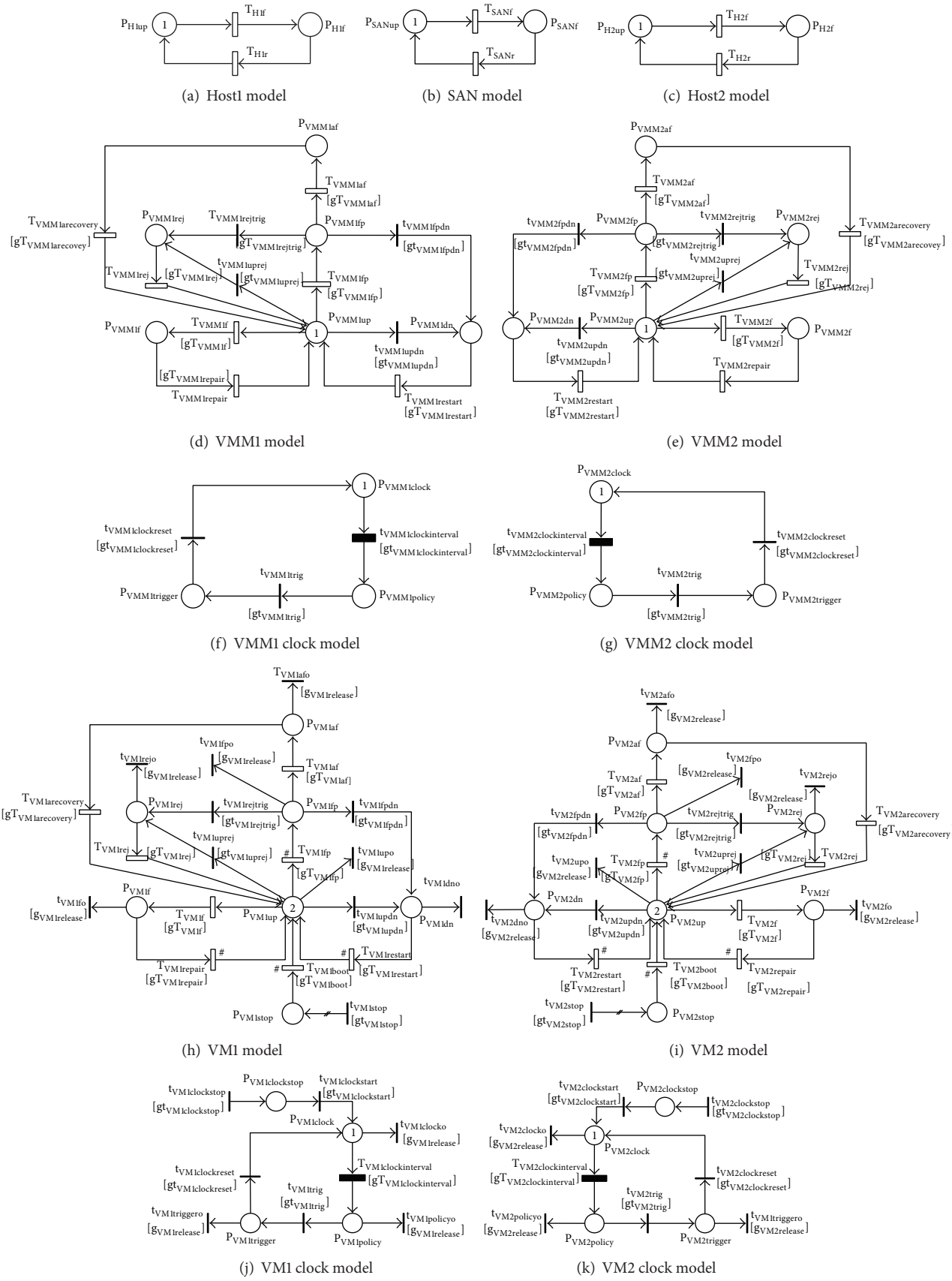
4.1. SRN Model of a Multiple-VMs Virtualized Server System. The entire SRN model of a VSS with multiple VMs is shown in Figure 2. The model is composed of partial SRN models of hosts, SAN, VMMs, and VMs derived from individual models in the next sections IV.B, IV.C, and IV.D. Figures 2(a)–2(k) depict, respectively, SRN models of host1, host2, SAN, VMM1, VMM2, VM1, and VM2. For the sake of time-based rejuvenation, each of VMM and VM models is correspondingly associated with a VMM clock or a VM clock. To actively control system behaviors and dependencies, a set of guard functions is attached to transitions in order to enable or disable the transitions under predetermined conditions. All guard function definitions in the system model can be consistently referred to the guard function definitions in the partial models (defined in Tables 1 and 2) with regard to the alteration of notations for the correspondingly attached transition and model. For example, we consider the guard function $gT_{VMMrestart}$ attached to the transition $T_{VMMrestart}$ in the VMM partial model. The notation of the above guard function in the VMM1 model (Figure 2(d)) is altered to $gT_{VMM1restart}$. This function is attached to $T_{VMM1restart}$, and its function definition is also altered accordingly. The above described alteration is applied consistently for all other guard functions, their definition, and notations in the system model.

4.2. Hosts and SAN Submodels. The failure and recovery behaviors of a host are represented as two places; up and failure in Figure 3(a). A host is in upstate represented by one token in P_{Hup}. Because of hardware malfunctions, failure transition T_{Hf} is fired; the token in P_{Hup} is taken and deposited in P_{Hf}; the host enters failure state. A failed host is repaired by summoning a repairperson and returns to upstate (P_{Hup}). The repair transition T_{Hr} is enabled; the token in P_{Hf} is taken and deposited in P_{Hup}.

Similarly, the failure and recovery behaviors of SAN are modeled as in Figure 3(b). The SAN is initially considered in upstate. As time goes by, the SAN fails due to hardware malfunctions, and its state becomes failure state (P_{SANf}). After recovery by summoning a repairperson, the SAN returns to upstate (P_{SANup}). When the SAN fails, T_{SANf} is fired; the token in P_{SANup} is taken and deposited in P_{SANf}. As the SAN is repaired (T_{SANr} is enabled), the token in sequence is taken from P_{SANf} and deposited in P_{SANup}.

4.3. VMM Models with Time-Based Rejuvenation. A VMM subsystem with time-based rejuvenation is modeled as shown in Figure 4. The model consists of two submodels: (a) VMM model and (b) VMM clock model. The VMM model (Figure 4(a)) captures different failure modes and recovery actions including aging-related failure and time-based rejuvenation policy, failures due to nonaging-related Mandelbugs (NAM) and repair, and dependency of the VMM on its underlying host. The VMM clock (Figure 4(b)) is used to trigger time-based rejuvenation. The VMM is initially in up and running state (depicted by one token in P_{VMMup}), in which the system is highly robust and works without errors. When a nonaging-related Mandelbug has appeared, the VMM goes into failure state (P_{VMMf}). The failure transition T_{VMMf} is fired; the token in P_{VMMup} is taken and deposited in P_{VMMf}. The repair is conducted by enabling $T_{VMMrepair}$, and then the token is taken from P_{VMMf} and deposited in P_{VMMup}. The repaired VMM returns to stable state (P_{VMMup}). Besides, as time goes on, the VMM in upstate undergoes the aging period [39]. This phenomenon is captured by transiting through T_{VMMfp} one token from P_{VMMup} to P_{VMMfp}. The VMM becomes failure-probable (the token in P_{VMMup} is taken and deposited in P_{VMMfp}). If the VMM rejuvenation process is not triggered, the VMM goes through an aging-related failure from failure-probable state. The token in P_{VMMfp} is taken and deposited in P_{VMMaf}. The recovery is captured by firing $T_{VMMarecovery}$. The token in P_{VMMaf} is taken out and deposited in P_{VMMup}. The VMM returns to the stable state P_{VMMup}. In the case that the point of time for rejuvenation has approached, regardless of the VMM status (either in the failure-probable state (P_{VMMfp}) or in the stable state (P_{VMMup})), time-based rejuvenation process of the VMM is triggered. This behavior is controlled by two guard functions $gt_{VMMrejtrig}$ and $gt_{VMMuprej}$. The immediate transitions $t_{VMMrejtrig}$ and $t_{VMMuprej}$ are enabled. The token in P_{VMMup} or P_{VMMfp} is taken and deposited in P_{VMMrej}. The VMM enters rejuvenation-ready state (P_{VMMrej}). Hereafter, the VMM is reset and undergoes a rejuvenation process. When this process completes, the transition T_{VMMrej} is enabled. The token in P_{VMMrej} is taken and deposited in the stable state (P_{VMMup}). We also take into account the dependency of the VMM on its underlying host. If the host enters failure state, the VMM in stable state (P_{VMMup}) or failure-probable state (P_{VMMfp}) goes instantly to downstate (P_{VMMdn}) through, respectively, either fired immediate transitions $t_{VMMupdn}$ or $t_{VMMfpdn}$. The token in P_{VMMup} or P_{VMMfp} is taken out and deposited in P_{VMMdn}. This token transition is controlled by the guard functions $gt_{VMMupdn}$ and $gt_{VMMfpdn}$. As soon as the host returns to upstate, the VMM restarts via enabling $T_{VMMrestart}$. The token in P_{VMMdn} is taken out and deposited in P_{VMMup}. However, if the VMM is in failure states (P_{VMMaf} and P_{VMMf}) or in rejuvenation-ready state (P_{VMMrej}) as the host enters downstate, the repair/maintenance operations of the VMM suspend temporarily. The operational status of the VMM stored on the shared storage system is fetched to roll back to the former state as soon as the host returns to upstate.

In order to carry out time-based rejuvenation, we use the VMM clock. To count the time progressing and to ensure precise intervals for rejuvenation, we employ a deterministic transition, $T_{VMMclockinterval}$, which takes the duration of $1/\tau_{VMM}$ to fire. In order to implement the models on software package SPNP [66], we use c_{VMM}-stage Erlang distribution to approximate the deterministic transition $T_{VMMclockinterval}$. The



(a) Host1 model (b) SAN model (c) Host2 model

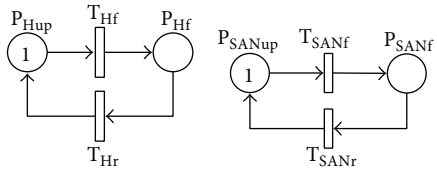
(d) VMM1 model (e) VMM2 model

(f) VMM1 clock model (g) VMM2 clock model

(h) VM1 model (i) VM2 model

(j) VM1 clock model (k) VM2 clock model

Figure 2: SRN models of a VSS with multiple virtual machines.



(a) Host model (b) SAN model

Figure 3: SRN models for host and SAN.

condition for counting time is that the VMM is in operation, or in other words, one token exists either in P_{VMMup} or P_{VMMfp}. At a specific interval, $T_{VMMclockinterval}$ is enabled; the token in $P_{VMMclock}$ is taken and deposited in $P_{VMMpolicy}$. At this moment, the VMM clock triggers the VMM rejuvenation process as long as $t_{VMMtrig}$ is enabled. Soon after the VMM enters rejuvenation-ready state P_{VMMrej}, the VMM clock is reset to counting state and starts a new routine. Thus, $t_{VMMclockreset}$ is enabled and the token in $P_{VMMtrigger}$ is taken and deposited in $P_{VMMclock}$.

The above dynamic behaviors of the VMM subsystem are controlled by a set of guard functions associated with respective transitions as listed in Table 1.

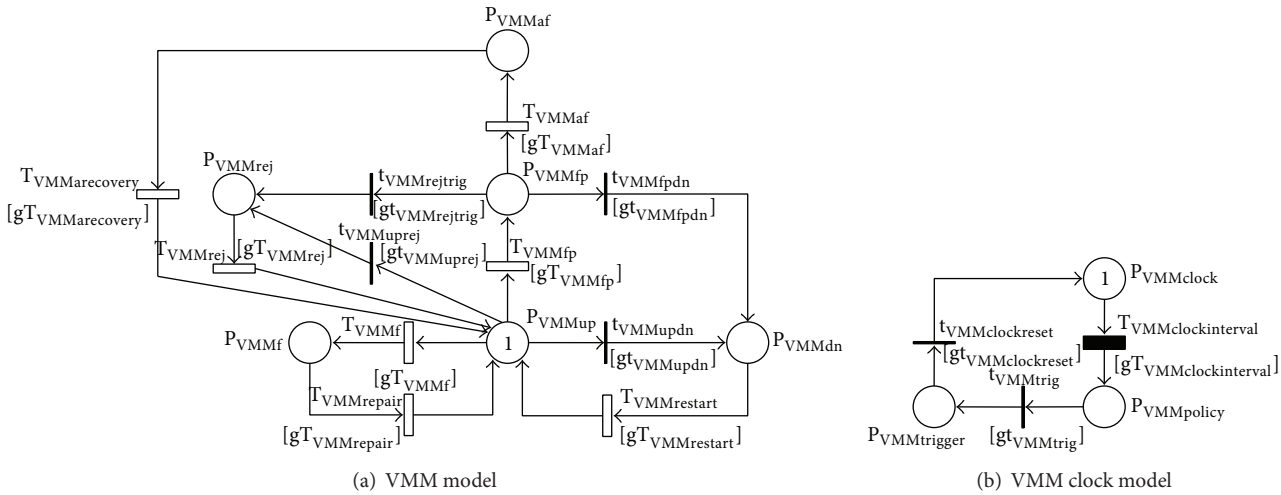
4.4. VM Models with Time-Based Rejuvenation. SRN models for VM and VM clock are shown in Figures 5(a) and 5(b), respectively. Initially, each VMM has two running VMs in robust state, which are represented by two tokens in P_{VMup}. The failure and recovery behaviors including the aging period, aging-related failure and recovery, nonaging-related Mandelbugs failure, and repair action are captured and described similarly to those in the VMM model (Figure 4(a)). We here describe the distinction of VM model. The dependency of VMs on VMM is captured in various cases of VMM failure modes. Moreover, the marking dependence between VMs and the dependence of VMs on SAN are also taken into account in this VM model.

The dependency between the running VM and its underlying VMM is captured in this model as follows. As long as the underlying VMM exists either in stable state (P_{VMup}) or in failure-probable state (P_{VMMfp}), the hosted VM can run uninterruptedly. If the VMM enters failure state or downstate, the hosted VM instantly goes to downstate (P_{VMdn}) regardless of its operational states (P_{VMup} or P_{VMfp}). The immediate transitions t_{VMupdn} and t_{VMfpdn} fire and the token either in P_{VMup} or in P_{VMfp} is taken out and deposited in P_{VMdn}. The failed VM can only restart after the underlying VMM returns to running states (P_{VMup}, P_{VMMfp}). However, if the VM is in failure states (P_{VMf}, P_{VMaf}) or rejuvenation-ready state (P_{VMrej}) as the VMM enters failure states or down state, the VM's operations are suspended. Its operational status is stored on shared storage system. After the VMM returns to running states, the former operational state of the VM is rolled back. We also incorporate the dependency between the VMM and the hosted VMs during VMM rejuvenation. When the VMM is under rejuvenation, the current states of VM and VM clock are cleaned and reconfigured to be ready to boot/start after the completion of the VMM rejuvenation. A set of immediate transitions (t_{VMupo}, t_{VMfpo}, t_{VMdno}, t_{VMafo}, t_{VMrejo}, t_{VMfo}) is fired to clear the current states of the VM system by removing all tokens in respective input places in VM model (see Figure 5(a)). Also, the immediate transitions $t_{VMclocko}$, $t_{VMpolicyo}$, $t_{VMtriggero}$ are used to remove tokens in their respective input places in VM clock model in order to clear the current states of the VM clock model (see Figure 5(b)). The VM clock is stopped by firing the transition $t_{VMclockstop}$ and depositing only one token in $P_{VMclockstop}$. To ensure that the two VMs are stopped and cleaned to their initial state, only two tokens at most can be deposited in P_{VMstop} through t_{VMstop}. Therefore, an input multiplicity arc is used to flexibly adjust the number of tokens deposited in P_{VMstop} upon the current number of tokens existing there. If there is no token in P_{VMstop}, the arc allows two tokens at most to be deposited in P_{VMstop}. If the number of tokens existing in P_{VMstop} is one, the arc enables to deposit only one token in P_{VMstop}. To implement this, a cardinality arc function $marc_{VMstop}$ is designed to control the number of tokens deposited in P_{VMstop} through the multiplicity arc. When the underlying VMM returns to stable state (P_{VMMup}) after rejuvenation and exists in running states (P_{VMMup} and P_{VMMfp}), it restarts each VM in sequence by enabling the transition T_{VMboot}. The tokens in P_{VMstop} are taken out one by one and deposited in P_{VMup}. A long with the completion of booting a VM, the VM clock also starts counting time as soon as $t_{VMclockstart}$ is fired and the token in $P_{VMclockstop}$ is taken and deposited in $P_{VMclock}$. Furthermore, there are some dependent cases in which two VMs all exist in the same state such as P_{VMdn}, P_{VMf}, P_{VMstop}, or P_{VMup} which, respectively, need to restart ($T_{VMrestart}$), to repair ($T_{VMrepair}$), to boot (T_{VMboot}), or are going to be failure-probable (T_{VMfp}). In these cases, all VMs compete to each other to enter a new state. For this reason, a dependency between VMs called marking dependence is necessary to be incorporated in the modeling since this dependency affects the rate of the transitions. A sign "#" is placed next to every output transition of the mentioned places to imply that a marking dependence is associated to related transitions (see Figure 5). The time to trigger VM rejuvenations is captured by using a deterministic transition, $T_{VMclockinterval}$, in VM clock model. The deterministic transition is fired after every interval of $1/\tau_{VM}$. We use c_{VM}-stage Erlang distribution for the deterministic transition $T_{VMclockinterval}$. The definition of guard functions is depicted as in Table 2.

5. Numerical Results and Discussions

We implemented the SRN models in stochastic Petri net package (SPNP) [66]. In order to study system characteristics in terms of business availability and continuity featured for computational sustainability in an IT business infrastructure, we analyzed the following metrics: steady-state availability (SSA), transaction loss, and sensitivity of the SSA with respect to clocks' interval. Table 3 summarizes the parameter default values, based on previous works [10, 45].

5.1. Steady-State Availability Analysis. We first computed the SSA of the VSS using the default parameters' value.



(a) VMM model (b) VMM clock model

Figure 4: SRN models for a VMM subsystem.

Table 1: Guard functions for the VMM submodel and VMM clock submodel.

Guard function name	Associated transition	Definition
$gT_{VMMrestart}$	$T_{VMMrestart}$	If ($\#P_{Hup} == 1$) 1 else 0
$gt_{VMMupdn}$	$t_{VMMupdn}$	If ($\#P_{Hf} == 1$) 1 else 0
gT_{VMMf}	T_{VMMf}	If ($\#P_{Hup} == 1$) 1 else 0
$gT_{VMMrepair}$	$T_{VMMrepair}$	If ($\#P_{Hup} == 1$) 1 else 0
gT_{VMMfp}	T_{VMMfp}	If ($\#P_{Hup} == 1$) 1 else 0
gT_{VMMaf}	T_{VMMaf}	If ($\#P_{Hup} == 1$) 1 else 0
$gT_{VMMarecovery}$	$T_{VMMarecovery}$	If ($\#P_{Hup} == 1$) 1 else 0
gT_{VMMfpd}	T_{VMMfpd}	If ($\#P_{Hf} == 1$) 1 else 0
$gT_{VMMinterval}$	$T_{VMMinterval}$	If ($\#P_{VMMup} == 1$ || $\#P_{VMMfp} == 1$) 1 else 0
$gt_{VMMtrig}$	$t_{VMMtrig}$	If ($\#P_{VMMup} == 1$ || $\#P_{VMMfp} == 1$) 1 else 0
$gT_{VMMclockinterval}$	$T_{VMMclockinterval}$	If ($\#P_{VMMup} == 1$|| $\#P_{VMMfp} == 1$) 1 else 0
$gt_{VMMclockback}$	$t_{VMMclockback}$	If ($\#P_{VMMaf} == 1$ || $\#P_{VMMf} == 1$ || $\#P_{VMMdn} == 1$) 1 else 0
$gT_{VMMrejtrig}$	$T_{VMMrejtrig}$	If ($\#P_{VMMtrigger} == 1$) 1 else 0
$gt_{VMMuprej}$	$t_{VMMuprej}$	If ($\#P_{VMMtrigger} == 1$) 1 else 0
$gt_{VMMclockreset}$	$t_{VMMclockreset}$	If ($\#P_{VMMrej} == 1$) 1 else 0
gT_{VMMrej}	T_{VMMrej}	If ($\#P_{Hup} == 1$) 1 else 0

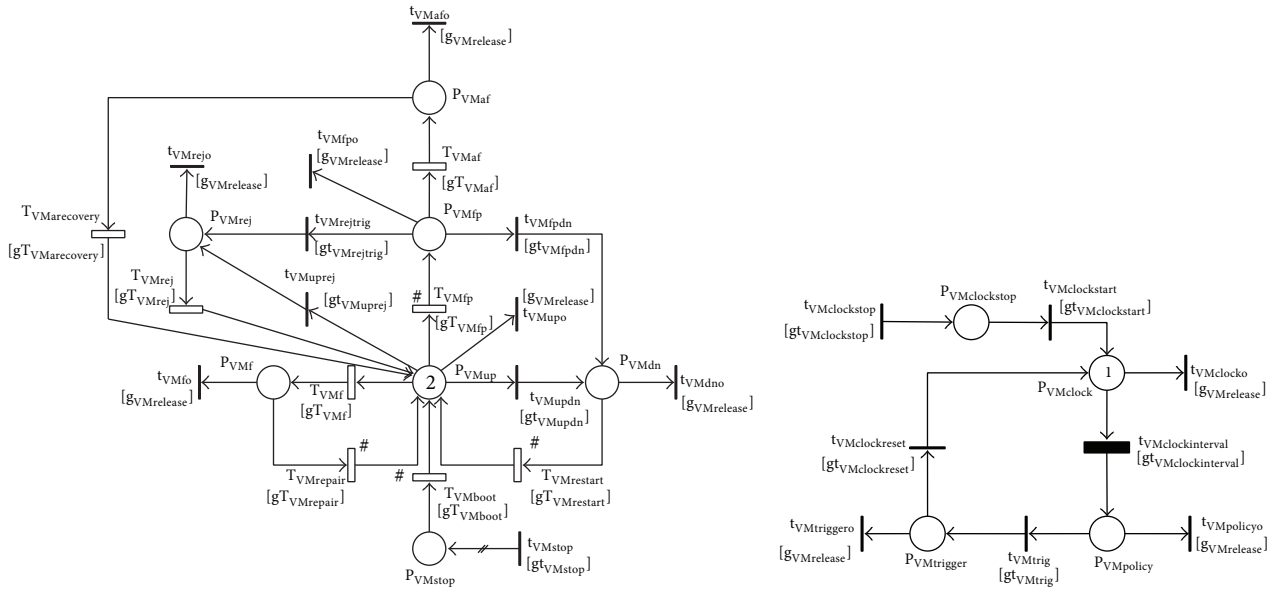
We conducted numerical experiments in seven case studies with regard to different rejuvenation combinations. The case studies are described along with notations in Table 4. The results are summarized as in Table 5.

The SSAs are abnormally not the highest as expected even though a combined-rejuvenation countermeasure is adopted simultaneously on both VMM and VM subsystems. This is because of the improper strategy of rejuvenation operations between VMM and VM subsystems. Furthermore, the presence of VMM rejuvenation has positive impact on system availability versus negative impact of the presence of VM rejuvenation strategy. This means, the presence of rejuvenation on VMM subsystems enables the system to gain SSA but inversely for the presence of rejuvenation on VM subsystems. This is derived by comparing SSAs in the cases with/without rejuvenation on VMM/VM subsystems. This phenomenon can be explained as the consequence of a frequent rejuvenation policy on VM subsystems in a system with multiple VMs. Also, it is because of inflexible and uncoordinated rejuvenation policies between both VMM and VM levels causing the side effect. Although this study reflects the abnormal role of rejuvenation policies on VMMs and VMs under given parameters in Table 3, we still recommend adopting rejuvenations at both VMM and VM levels thoroughly to avoid long-run system malfunctions because of software aging. The coordination of rejuvenation policies on each individual of VMMs and VMs requires more in-depth studies.

5.2. Transaction Loss. We use the following metrics to evaluate VMs subsystem downtime: total downtime in hours per year and mean time to failure equivalent (MTTFeq) as shown in Table 6. The total number of hours in a year of VMs subsystem downtime is about 72 hours, whereas the

Table 2: Guard functions for VM model and VM clock model.

Guard function	Transition	Definition
gT_{VMf}	T_{VMf}	If ($\#P_{VMMup} == 1$ || $\#P_{VMMfp} == 1$ && $\#P_{SANup} == 1$) 1 else 0
$gT_{VMrepair}$	$T_{VMrepair}$	If ($\#P_{VMMup} == 1$ || $\#P_{VMMfp} == 1$ && $\#P_{SANup} == 1$) 1 else 0
gt_{VMupd}	t_{VMupd}	If ($\#P_{VMMdn} == 1$ || $\#P_{VMMf} == 1$ || $\#P_{VMMaf} == 1$ || $\#P_{VMMrej} == 1$ || $\#P_{SANf} == 1$) 1 else 0
$gT_{VMrestart}$	$T_{VMrestart}$	If ($\#P_{VMMup} == 1$ || $\#P_{VMMfp} == 1$ && $\#P_{SANup} == 1$) 1 else 0
gT_{VMfp}	T_{VMfp}	If ($\#P_{VMMup} == 1$ || $\#P_{VMMfp} == 1$ && $\#P_{SANup} == 1$) 1 else 0
gT_{VMaf}	T_{VMaf}	If ($\#P_{VMMup} == 1$ || $\#P_{VMMfp} == 1$ && $\#P_{SANup} == 1$) 1 else 0
$gT_{VMarecovery}$	$T_{VMarecovery}$	If ($\#P_{VMMup} == 1$ || $\#P_{VMMfp} == 1$ && $\#P_{SANup} == 1$) 1 else 0
gT_{VMfpdn}	T_{VMfpdn}	If ($\#P_{VMMdn} == 1$ || $\#P_{VMMf} == 1$ || $\#P_{VMMaf} == 1$ || $\#P_{VMMrej} == 1$ || $\#P_{SANf} == 1$) 1 else 0
$gT_{VMinterval}$	$T_{VMinterval}$	If ($\#P_{VMup} == 1$ || $\#P_{VMup} == n_{VM}$ || $\#P_{VMfp} == 1$ || $\#P_{VMfp} == n_{VM}$) 1 else 0
$gt_{VMclockback}$	$t_{VMclockback}$	If ($\#P_{VMup} == 0$ && $\#P_{VMfp} == 0$) 1 else 0
$gt_{VMtrigger}$	$t_{VMtrigger}$	If ($\#P_{VMup} == 1$ || $\#P_{VMup} == n_{VM}$ || $\#P_{VMfp} == 1$ || $\#P_{VMfp} == n_{VM}$) 1 else 0
$gt_{VMclockreset}$	$t_{VMclockreset}$	If ($\#P_{VMrej} == 1$ || $\#P_{VMrej} == n_{VM}$) 1 else 0
$gT_{VMfprejtrig}$	$T_{VMfprejtrig}$	If ($\#P_{VMtrigger} == 1$) 1 else 0
$gt_{VMuprej}$	$t_{VMuprej}$	If ($\#P_{VMtrigger} == 1$) 1 else 0
gT_{VMrej}	T_{VMrej}	If ($\#P_{VMMup} == 1$ || $\#P_{VMMfp} == 1$ && $\#P_{SANup} == 1$) 1 else 0
gT_{VMboot}	T_{VMboot}	If ($\#P_{VMMrej} == 0$ && $\#P_{VMMup} == 1$ || $\#P_{VMMfp} == 1$) 1 else 0
gt_{VMstop}	t_{VMstop}	If ($\#P_{VMMrej} == 1$ && $\#P_{VMstop} < n_{VM}$) 1 else 0
$g_{VMrelease}$	t_{VMupo}, t_{VMfpo}, t_{VMafo}, t_{VMrejo}, t_{VMsdno}, t_{VMfo}, $t_{VMclocko}$, $t_{VMpolicyo}$, $t_{VMtriggero}$	If ($\#P_{VMMrej} == 1$) 1 else 0
$gt_{VMclockstart}$	$t_{VMclockstart}$	If ($\#P_{VMMrej} == 0$ && $\#P_{VMMup} == 1$ || $\#P_{VMMfp} == 1$ && $\#P_{VMclock} == 0$ && $\#P_{VMclockstop} == 1$) 1 else 0
$gt_{VMclockstop}$	$t_{VMclockstop}$	If ($\#P_{VMMrej} == 1$ && $\#P_{VMclockstop}! = 1$) 1 else 0
$marc_{VMstop}$	t_{VMstop}	If ($\#P_{VMstop} < n_{VM}$) (n_{VM} -$\#P_{VM1stop}$) else 0
$gT_{VMclockinterval}$	$T_{VMclockinterval}$	If ($\#P_{VMup} == 1$ || $\#P_{VMup} == n_{VM}$ || $\#P_{VMfp} == 1$ || $\#P_{VMfp} == n_{VM}$) 1 else 0
$gT_{VMMfpdn}$	$T_{VMMfpdn}$	If ($\#P_{Hf} == 1$) 1 else 0
gt_{VMupdn}	t_{VMupdn}	If ($\#P_{VMMdn} == 1$ || $\#P_{VMMf} == 1$ || $\#P_{VMMaf} == 1$ || $\#P_{VMMrej} == 1$ || $\#P_{SANf} == 1$) 1 else 0
gT_{VMd}	T_{VMd}	If ($\#P_{VMpolicy}! = c_{VM}$ && $\#P_{SANup} == 1$ && $\#P_{VMMup} == 1$ || $\#P_{VMMfp} == 1$) 1 else 0
gT_{VMdrej}	T_{VMdrej}	If ($\#P_{VMpolicy}! = c_{VM}$ && $\#P_{SANup} == 1$ && $\#P_{VMMup} == 1$ || $\#P_{VMMfp} == 1$) 1 else 0
gT_{VMd}	T_{VMd}	If ($\#P_{VMpolicy}! = c_{VM}$ && $\#P_{SANup} == 1$ && $\#P_{VMMup} == 1$ || $\#P_{VMMfp} == 1$) 1 else 0
gT_{VMdrej}	T_{VMdrej}	If ($\#P_{VMpolicy} == c_{VM}$ && $\#P_{SANup} == 1$ && $\#P_{VMMup} == 1$ || $\#P_{VMMfp} == 1$) 1 else 0



(a) VM model (b) VM clock model

Figure 5: SRN models of VM subsystem.

Table 3: Input parameter values used in the analysis.

Parameters	Description	Assigned transitions	Mean time/values
μ_{hr}	Host repair rate	T_{Hlr}, T_{H2r}	3 days
λ_{hf}	Host failure rate	T_{Hlf}, T_{H2f}	1 year
μ_{vmmr}	VMM restart rate from downstate	$T_{VMM1restart}$, $T_{VMM2restart}$	1 min
λ_{vmmf}	VMM nonaging failure rate	T_{VMM1f}, T_{VMM2f}	2654 hours
δ_{vmmr}	VMM repair rate	$T_{VMM1repair}$, $T_{VMM2repair}$	100 mins
β_{vmmfp}	VMM aging rate	T_{VMM1fp}, T_{VMM2fp}	1 month
λ_{vmmaf}	VMM aging failure rate	T_{VMM1af}, T_{VMM2af}	1 week
μ_{vmmar}	VMM recovery rate after aging failure	$T_{VMM1arecovery}$, $T_{VMM2arecovery}$	65 mins
τ_{vmm}	VMM clock interval	$T_{VMM1clockinterval}$, $T_{VMM1clockinterval}$	1 week
β_{vmmrej}	VMM rejuvenation rate	$T_{VMM1rej}$, $T_{VMM1rej}$	2 mins
λ_{sf}	SAN failure rate	T_{SANf}	1 year
μ_{sr}	SAN repair rate	$T_{SANrepair}$	3 days
λ_{vmf}	VM nonaging failure rate	T_{VM1f}, T_{VM2f}	2893 hours
δ_{vmr}	VM repair rate	$T_{VM1repair}$, $T_{VM2repair}$	30 mins
μ_{vmr}	VM restart rate	$T_{VM1restart}$, $T_{VM2restart}$	30 s
β_{vmfp}	VM aging rate	T_{VM1fp}, T_{VM2fp}	1 week
λ_{vmaf}	VM aging failure rate	T_{VM1af}, T_{VM2af}	3 days
μ_{vmar}	VM recovery rate after aging failure	$T_{VM1arecoveryt}$, $T_{VM2arecovery}$	35 mins
τ_{vmi}	VM clock interval	$T_{VM1clockinterval}$, $T_{VM2clockinterval}$	1 day
β_{vmrej}	VM rejuvenation rate	T_{VM1rej}, T_{VM2rej}	1 min
η_{vmb}	VM booting rate after VMM rejuvenation	$T_{VM1boot}$, $T_{VM2boot}$	30 s
c_{VMM}	Number of stages in c_{VMM}-stage Erlang distribution	x	2
c_{VM}	Number of stages in c_{VM}-stage Erlang distribution	x	2
n_{VM}	Number of VMs running on a VMM	x	2

Table 4: Description of case studies in steady state availability analysis.

Cases	Description
I	Rejuvenation is applied on all VMM and VM subsystems in both hosts.
II	Rejuvenation is not applied only on one of VMM subsystems in two hosts, but also on both VM subsystems in two hosts.
III	Rejuvenation is applied on both VMM subsystems in two hosts but not applied on only one of two VM subsystems.
IV	Rejuvenation is not applied on haft side of the system including VMM1 and VM1 subsystems but applied on VMM2 and VM2 subsystems.
V	Rejuvenation is not applied on both VMM subsystems in two hosts but applied on both VM subsystems.
VI	Rejuvenation is applied on both VMM subsystems in two hosts but not applied on both VM subsystems.
VII	Rejuvenation is not applied on VMM and VM subsystems in both hosts.

Table 5: SSAs of VSS under given parameter values in seven case studies.

Subsystem	I	II	III	IV	V	VI	VII
VM	0.991769547666	0.991766082049	0.991770317258	0.991766912872	0.991763344539	0.991771080172	0.99176419998
VMM	0.999912470996	0.999908948744	0.999912470996	0.999908948744	0.999905284754	0.999912470996	0.999905284754

Table 6: VMs subsystem downtime.

Output measures	Value (hours)
Total downtime per year	72.2205464
MTTFeq	218.379208

meantime between each failure of VMs subsystem is approximately at 218 hours. Furthermore, we took into consideration some main causes of transaction losses to compute expected number of transaction losses per year of VMs subsystem as in Table 7. We evaluate VMs transaction loss in three cases: (i) VSS with both VMM and VM rejuvenation; (ii) VSS without VM rejuvenation but with VMM rejuvenation; and (iii) VSS without VMM rejuvenation but with VM rejuvenation. Our analysis discussion is conducted as in the following major points.

(i) Under the default value of input parameters, the main culprit of VMs transaction losses is VM rejuvenation. The VM rejuvenation contributes the most of transaction losses which are relatively at 83.28% and 93.53% of total number of VM transaction losses, respectively, in the cases (i) and (iii) which are with and without VMM rejuvenation. The reason of the above side effect is that the frequent VM rejuvenation actions drastically reset the four VMs in either robust or aging states periodically at predetermined intervals regardless of operational efficiency and coordination. This is to imply the negative implications of improper VM rejuvenation actions in a virtualized system with multiple VMs.

(ii) However, if without VM rejuvenation, the aging-related failure on VMs subsystem occurs much more often. This is shown as follows. The ratio of transaction losses due to VM aging failure increases from about 2.05% up to 27.66% of total number of VM transaction losses, respectively, in the cases of with and without VM rejuvenation (cases (i) and (ii)). Accordingly, the number of VM transaction losses per year increases almost three times from about 33.8 up to 92.2 in respective cases, while the number and the ratio of transaction losses due to VM aging failure change slightly in the cases (i) and (iii) which are, respectively, with and without VMM rejuvenation. This again points out the negative impact of improper VM rejuvenation when the virtualized system hosts multiple VMs.

(iii) Apparently shown in Table 7, if without VMM rejuvenation (case (iii)), the number of VM transaction losses per year increases from about 38.9 in the case (i) (with VMM rejuvenation) up to 56.4 in the case (iii) (without VMM rejuvenation). This is clearly due to VMM aging failure. Without VMM rejuvenation, the VMMs likely undergo VMM aging-related failure, which extend the VMM downtime. Therefore, the number of VM transaction losses also increases as VMM rejuvenation is not applied. However, the presence of VMM rejuvenation also contributes a portion of VM transaction losses which is about 197 per year. The reason is due to the method used to deal with the hosted VMs during VMM rejuvenation. As VMM rejuvenation proceeds, the process not only rejuvenates VMM subsystem but also cleans VMs subsystem regardless of its current operational states. Without failover mechanisms, this policy causes VM transaction losses although VMs are in running states (robust or failure-probable states).

5.3. Sensitivity Analysis. The above SSA analysis and transaction loss analysis reveal complicated behaviors and characteristics of a virtualized system with multiple VMs. Hereby there is a critical need to analyze and seek for a proper combination of VMM and VM rejuvenations. In order to study particular affections of each combination of rejuvenations, we perform sensitivity analysis of system's SSA. Figure 6 shows the results of SSA analysis by varying rejuvenation clocks' interval

Table 7: Expected number of transaction loss per year of VMs subsystem.

Main causes	Case (i): with VMM and VM rejuvenation		Case (ii): without VM rejuvenation		Case (iii): without VMM rejuvenation	
VM nonaging failure	5.8	0.35%	5.4	1.62%	5.8	0.38%
VM aging failure	33.8	2.05%	92.2	27.66%	35.7	2.36%
VM rejuvenation	1373.9	83.28%	0	0.00%	1415.9	93.53%
VMM downtime	38.9	2.36%	38.9	11.67%	56.4	3.73%
VMM rejuvenation	196.9	11.94%	196.7	59.02%	0	0.00%
Total	1649.7	100.00%	333.3	100.00%	1513.9	100.00%

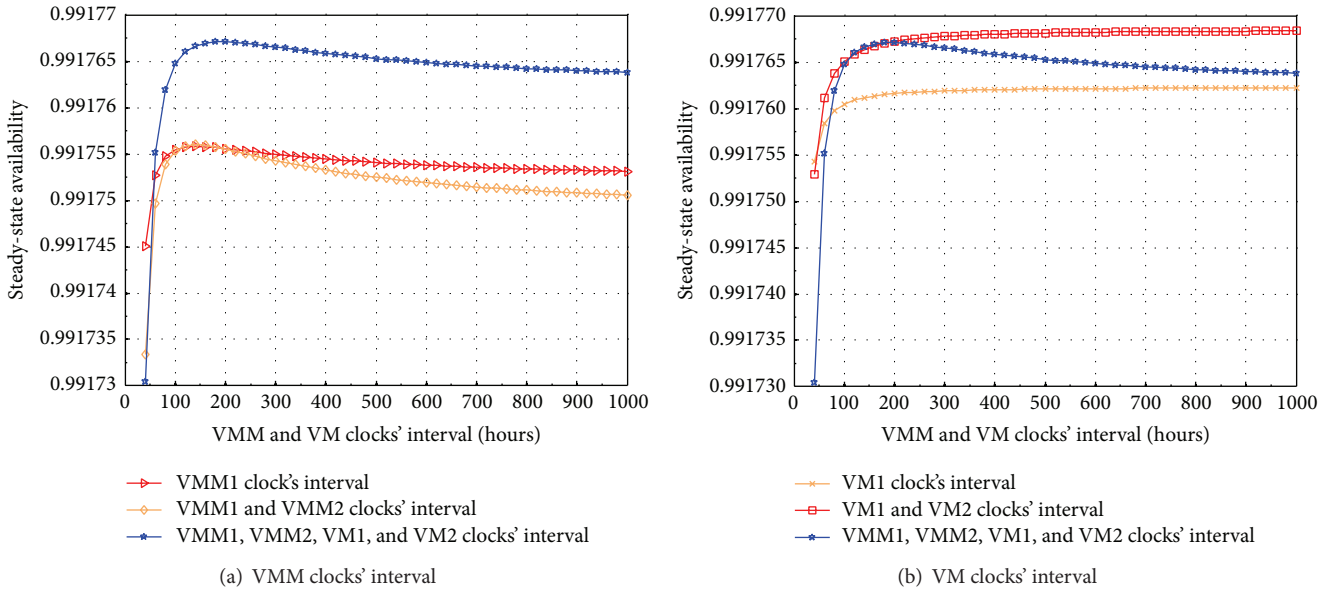
of VMM and VM subsystems. The sensitivity analysis is observed in 5 case studies with respect to the variation of (i) only VMM1 clock's interval; (ii) only VM1 clock's interval; (iii) both VMM1 and VMM2 clocks' interval; (iv) both VM1 and VM2 clocks' interval; and (v) all clocks' interval with the same duration. The interval values range in 0–1000 hours for experiment while other parameter values are fixed. It is apparent in the analysis results that there is a common variation tendency for all case studies. In the early period (0–200 hours), if we assign an increased value of clocks' interval, the SSA of system significantly increases. But after that, the more the value of clocks' interval increases, the more the SSA appears to drop. Figure 6(a) shows the SSA sensitivity with respect to the variation of VMM clocks' interval. It is very interesting that the rejuvenations on both VMM subsystems in two hosts (rhombus shaped line) with the same interval values are not an ideal solution compared to the rejuvenation only on one of the two VMMs (triangle shaped line). However, if the rejuvenations are conducted on both VMM subsystems and also together on both VM subsystems (star shaped line), the SSA is enhanced clearly. This pinpoints the role of rejuvenations with long intervals on VM subsystems in a system with multiple VMs. Figure 6(b) shows the SSA sensitivity with respect to the variation of VM clocks' interval. In this case, the rejuvenations on both VM subsystems (rectangle shaped line) enable the system to gain clearly higher SSA compared to the rejuvenation only on one of VM subsystems (cross shaped line) and even relatively higher compared to the rejuvenations on all VMMs, VMs subsystems (star shaped line). But it is not much different in early period of rejuvenation interval range (0–200 hours) in the comparison between the case of rejuvenations on both VMs and the case of rejuvenations on all VMMs and VMs.

We extend our sensitivity analysis of the SSA for VMM subsystem with respect to VMM and VM clocks' interval as showed in Figure 7. The sensitivity analysis is also performed in 5 case studies with the same settings as in the sensitivity analysis for VM subsystems. Comparing both sensitivity analyses showed in Figures 6 and 7, we find that the variation tendencies of the SSA in both analyses are similar to each other; however, the SSA values of VMM subsystem are always much higher compared to those of VM subsystem (the SSAs vary in the range of [0.999890–0.99915] for VMM subsystems and [0.991730–0.991770] for VM subsystems). Furthermore, the SSA sensitivity analysis of VMM subsystems in Figure 7 apparently reflects the dependency between VM subsystems and VMM subsystems in which the variations of VM clocks' interval do not affect the SSA of VMM subsystems. In Figure 7(a), the variations of VMM and VM clocks' interval in two cases, (iii) VMM1 and VMM2 clocks' interval (circle shaped line) and (v) all clocks' interval (star shaped line), bring about the same SSA analysis results of VMM subsystem (two lines overlap to each other). This points out that the involvement of the variation of VM clocks' interval does not affect the SSA of VMM subsystem. This phenomenon is reflected more clearly in Figure 7(b) in which the variations of VM clocks' interval in two cases, (ii) VM1 clock's interval (black circle shaped line) and (iv) VM1 and VM2 clocks' interval (rectangle shaped line), do not even change the SSA values of VMM subsystem (both lines horizontally overlap). Whereas in Figure 6, the variations of VMM clocks' interval do affect and the variations of VM clocks' interval strongly affect the SSA of VM subsystems. This argument reflects that the VM subsystems do depend on the VMM subsystems but the VMM subsystems do not depend on the VM subsystems. Nevertheless, the dependency of the VMM subsystems on the VM subsystems could be a fruitful topic for future extension. In Figure 7(a), we also find that the variations of both VMM clocks' interval in the case (iii), VMM1 and VMM2 clocks' interval, do enhance the SSA of VMM subsystems compared to those of only one VMM clock's interval in the case (i): VMM1 clock's interval.

Based on the above SSA sensitivity analyses for both VMM and VM subsystems with respect to corresponding VMM and VM clocks' interval, we recommend that system administrators should rejuvenate all VMM and VM subsystems with the value of intervals in the range [150–200] hours to gain high SSA.

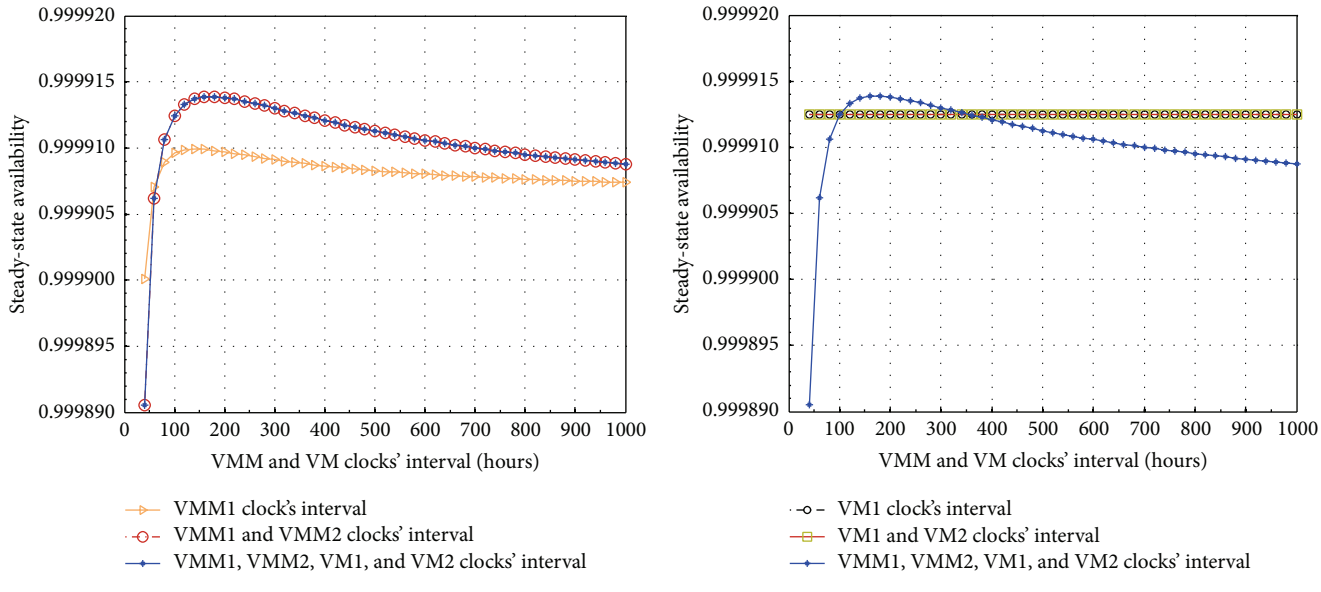
5.4. Limitation and Discussions. There are a number of research issues remaining open to improve as follows.

(i) In our system, the VMs' operational states are cleared and reset to clean state during VMM rejuvenation regardless of VMs' current status. This policy, however, drastically pushes a VM in running states (either robust state or failure-probable state) into downstate. Therefore, it could cause more VM transaction losses. Thus, a proper failover mechanism such as live VM migration can be considered as a mandatory measure in the virtualized system with multiple VMs



(a) VMM clocks' interval (b) VM clocks' interval

Figure 6: SSA sensitivity analysis of VM subsystem with respect to VMM and VM clocks' interval.



(a) VMM clocks' interval (b) VM clocks' interval

Figure 7: SSA sensitivity analysis of VMM subsystem with respect to VMM and VM clocks' interval.

to enhance significantly system availability. This idea still remains open for further extension of our work.

(ii) In our work, we neglected unexpected failure events during VMM/VM suspension or resume operations. But in reality, these operations could face a number of failure events regarding hardware and software aspects. Thus, there is still a need to light up this shadow corner in the empirical or analytical studies of virtualized system with multiple VMs.

(iii) In order to investigate detailed behaviors of time-based rejuvenation process on the virtualized system, in our modeling, we attempted to separate two VMMs and attach a VMM clock to trigger VMM rejuvenation process onto each VMM. But we did not separate two VMs on each VMM yet. Thus, the two VMs use the same VM clock to trigger VM rejuvenation process. However, in reality each VM could be equipped with its own clock so that each

VM could be monitored individually and rejuvenated separately in flexible rejuvenation strategies. This approach, nevertheless, need to be considered carefully regarding the types of stochastic model to avoid complicated and explosive modeling.

5.5. Future Research Avenue. Beyond the limitations and improvement opportunities in subsection D, we find a fruitful future research avenue for our work.

(i) Our work has done the sensitivity analysis of the SSA of both VMM and VM subsystems with respect to VMM and VM clocks' interval. Nevertheless, it is clear that a comprehensive sensitivity analysis can be performed with respect to many other parameters of the system. Thus, there is an open way to observe the VSS behaviors based on a set of parameters in order to gain higher interests.

(ii) In our work, we divide a very large and expected-to-build monolithic model into several submodels of every entity in the VSS system. We use SRN to construct individual submodels. By manipulating a set of guard functions attached to transitions, we make the SRN submodels interact to each other to capture the dependencies and complex behaviors within the whole system. Our focus is to develop a very detailed and comprehensive availability model rather than constructing a very large scale monolithic availability model. Thus, we attempt to observe the VSS as a unit in complex, actual systems with a large number of VSS nodes. From this point, we find an open future research avenue to scale up the complexity of the current system to a complex, actual systems composed of tens, hundreds of nodes. However, it is common to confront with the state-space explosion problem using Markovian models like the SRN as well as the difficulties of system model integration in large scale virtualized systems. To reduce the complexity of such large scale systems, we may follow the same approach in this paper. We can divide the overall model into submodels; with iteration over individual submodels we can obtain the overall solution for the whole system. Also, proper interactions between submodels need to be taken into consideration into the iterative overall solution. For further details, see [49, 67] for the works on the scalable availability SRN models and interacting Markov chain models of the real case study of infrastructure-as-a-service cloud (IaaS). This paper could be extended with similar approaches for future work.

(iii) The model in this study is based on the exponential distribution and Erlang distribution attached to transitions. However, in an actual virtualized system especially a system composed of both hardware and software components being modeled, many system behaviors do not conform to exponential distribution but nonexponential distribution, like hardware and software aging phenomena. Furthermore, the SRN model of the VSS in this paper is automatically converted to Markov reward model to be solved. A realistic virtualized system with many complex behaviors such as time-dependent rates, nonexponential distributions, and aging effects, however, cannot be modeled and captured by Markovian models but by non-Markovian models using discrete state-space methods. The methods allow to model and analytically evaluate any kind of dependability static and dynamic behaviors. Therefore, further work on incorporating nonexponential distribution and applying non-Markovian models for virtualized servers systems is an important endeavor. For more detail on nonexponential distribution, discrete state-space methods, and non-Markovian models in system dependability evaluation, see [68].

6. Conclusions

We have modeled and analyzed a virtualized servers system with multiple VMs via SRN. We encapsulated four VMs running on two VMMs into two hosts. We also incorporated diverse failure modes and corresponding recovery behaviors regarding hardware and software aspects including host failure, SAN failure, aging-related failure, and Mandelbugs related failure in SRN models. A variety of dependencies were taken into account in modeling as follows: (i) dependencies between a host and its hosted VMM, in turn between the VMM and its hosted VMs; (ii) interconnection dependency between SAN and VM subsystems; and (iii) marking dependency between VMs in a host. The SSA analysis showed that a frequent rejuvenation policy on VM may lower the SSA of the virtualized systems whereas that on VMM may enhance the system SSA. Based on the sensitivity analysis with respect to SSA, we showed that adopting a particular combination of rejuvenations on all VMM and VM subsystems in both hosts with the value of common interval in a specific range may help to increase system availability of the virtualized system.

Conflict of Interests

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

References

[1] C. P. Gomes, "Computational sustainability: computational methods for a sustainable environment, economy, and society," *The Bridge*, vol. 39, no. 4, pp. 5–13, 2010.

[2] J. Kaplan, W. Forrest, and N. Kindler, "Revolutionizing data center energy efficiency," Tech. Rep., McKinsey & Company, 2008.

[3] J. Schuneman, C. Matthys, M. Ferrier, S. E. Bach, and M. Cathcart, *Virtualization and the On Demand Business*, IBM Corp, Endicott, NY, USA, 2004.

[4] J. Sahoo, S. Mohapatra, and R. Lath, "Virtualization: a survey on concepts, taxonomy and associated security issues," in *Proceedings of the 2nd International Conference on Computer and Network Technology (ICCNT '10)*, pp. 222–226, Bangkok, Thailand, April 2010.

[5] R. Mikkilineni and G. Kankanhalli, "Using virtualization to prepare your data center for 'real-time assurance of business continuity," in *Proceedings of the 19th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE '10)*, pp. 76–81, Larissa, Greece, June 2010.

[6] S. Loveland, E. M. Dow, F. LeFevre, D. Beyer, and P. F. Chan, "Leveraging virtualization to optimize high-availability system configurations," *IBM Systems Journal*, vol. 47, no. 4, pp. 591–604, 2008.

[7] B. Cully, G. Lefebvre, D. Meyer, M. Feeley, N. Hutchinson, and A. Warfield, "Remus: high availability via asynchronous virtual machine replication," in *Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation (NSDI '08)*, pp. 161–174, 2008.

[8] E. M. Farr, R. E. Harper, L. F. Spainhower, and J. Xenidis, "A case for High Availability in a virtualized environment (HAVEN)," in *Proceedings of the 3rd International Conference on Availability, Security, and Reliability (ARES '08)*, pp. 675–682, Barcelona, Spain, March 2008.

[9] T. Thein, S. Chi, and J. S. Park, "Improving fault tolerance by virtualization and software rejuvenation," in *Proceedings of the 2nd Asia International Conference on Modelling and Simulation (AMS '08)*, pp. 855–860, May 2008.

[10] F. Machida, D. S. Kim, and K. S. Trivedi, "Modeling and analysis of software rejuvenation in a server virtualized system," in *Proceedings of the IEEE 2nd International Workshop on Software Aging and Rejuvenation*, pp. 1–6, 2010.

[11] L. Han and J. Xu, "Availability models for virtualized systems with rejuvenation," *Journal of Computer Information Systems*, vol. 20, pp. 8389–8396, 2013.

[12] A. Rezaei and M. Sharifi, "Rejuvenating high available virtualized systems," in *Proceedings of the 5th International Conference on Availability, Reliability, and Security (ARES '10)*, pp. 289–294, Kraków, Poland, February 2010.

[13] J. Daniels, "Server virtualization architecture and implementation," *Crossroads Magazine*, vol. 16, no. 1, pp. 8–12, 2009.

[14] R. Y. Ameen and A. Y. Hamo, "Survey of server virtualization," *International Journal of Computer Science and Information Security*, vol. 11, no. 3, pp. 65–74, 2013.

[15] R. Dittner, J. David Rule, K. Majors, M. ten Seldam, T. Grotenhuis, and G. Green, *Virtualization with Microsoft Virtual Server 2005*, Syngress Media, Rockland, Mass, USA, 1st edition, 2006.

[16] J. Kappel, A. Velte, and T. Velte, *Microsoft Virtualization with Hyper-V*, McGraw-Hill, New York, NY, USA, 1st edition, 2009.

[17] P. Barham, B. Dragovic, K. Fraser et al., "Xen and the art of virtualization," in *Proceedings of the 19th ACM Symposium on Operating Systems Principles (SOSP '03)*, pp. 164–177, usa, October 2003.

[18] A. Muller and S. Wilson, *Virtualization with VMware ESX Server*, Syngress Media, Rockland, Me, USA, 2005.

[19] F. Machida, D. S. Kim, J. S. Park, and K. S. Trivedi, "Toward optimal virtual machine placement and rejuvenation scheduling in a virtualized data center," in *Proceedings of the IEEE International Conference on Software Reliability Engineering Workshops (ISSRE Wksp '08)*, pp. 1–3, Seattle, Wash, USA, November 2008.

[20] B. Wei, C. Lin, and X. Kong, "Dependability modeling and analysis for the virtual data center of cloud computing," in *Proceedings of IEEE International Conference on High Performance Computing and Communications*, pp. 784–789, 2011.

[21] E. Arzuaga and D. R. Kaeli, "Quantifying load imbalance on virtualized enterprise servers," in *Proceedings of the 1st Joint WOSP/SIPEW International Conference on Performance Engineering (WOSP/SIPEW '10)*, pp. 235–242, January 2010.

[22] F. Machida, V. F. Nicola, and K. S. Trivedi, "Job completion time on a virtualized server with software rejuvenation," *ACM Journal on Emerging Technologies in Computing Systems*, vol. 10, no. 1, pp. 1–26, 2014.

[23] Y. Huang, C. Kintala, N. Kolettis, and N. D. Fulton, "Software rejuvenation: analysis, module and applications," in *Proceedings of the 25th International Symposium on Fault-Tolerant Computing (FTCS '95)*, pp. 381–390, June 1995.

[24] J. Alonso, R. Matias, E. Vicente, A. Maria, and K. S. Trivedi, "A comparative experimental study of software rejuvenation overhead," *Performance Evaluation*, vol. 70, no. 3, pp. 231–250, 2012.

[25] K. S. Trivedi, K. Vaidyanathan, and K. Goseva-Popstojanova, "Modeling and analysis of software aging and rejuvenation," in *Proceedings of the 33rd Annual Simulation Symposium (SS '00)*, pp. 270–279, Washington, DC, USA, April 2000.

[26] E. C. Andrade, F. MacHida, D. S. Kim, and K. S. Trivedi, "Modeling and analyzing server system with rejuvenation through SysML and stochastic reward nets," in *Proceedings of 6th International Conference on Availability, Reliability and Security*, pp. 161–168, August 2011.

[27] J. Xu, X. Li, Y. Zhong, and H. Zhang, "Availability modeling and analysis of a single-server virtualized system with rejuvenation," *Journal of Software*, vol. 9, no. 1, pp. 129–139, 2014.

[28] T. Thein, S. Do Chi, and J. S. Park, "Availability modeling and analysis on virtualized clustering with rejuvenation," *IJCSNS International Journal of Computer Science and Network Security*, vol. 8, no. 9, pp. 72–80, 2008.

[29] T. Thein and J. S. Park, "Availability analysis of application servers using software rejuvenation and virtualization," *Journal of Computer Science and Technology*, vol. 24, no. 2, pp. 339–346, 2009.

[30] J. Alonso, L. Silva, A. Andrzejak, P. Silva, and J. Torres, "High-available grid services through the use of virtualized clustering," in *Proceedings of the 8th IEEE/ACM International Conference on Grid Computing (GRID '07)*, pp. 34–41, Austin, Tex, USA, September 2007.

[31] L. M. Silva, J. Alonso, and J. Torres, "Using virtualization to improve software rejuvenation," *IEEE Transactions on Computers*, vol. 58, no. 11, pp. 1525–1538, 2009.

[32] D. Cotroneo, R. Natella, R. Pietrantuono, and S. Russo, "Software aging analysis of the linux operating system," in *Proceedings of the IEEE 21st International Symposium on Software Reliability Engineering (ISSRE '10)*, pp. 71–80, November 2010.

[33] R. Matias, P. F. Filho, R. M Jr., and P. J. F. Filho, "An experimental study on software aging and rejuvenation in web servers," in *Proceedings of the 30th Annual International Computer Software and Applications Conference (COMPSAC '06)*, vol. 1, pp. 189–196, 2006.

[34] A. Andrzejak and L. Silva, "Using machine learning for non-intrusive modeling and prediction of software aging," in *Proceedings of the IEEE Network Operations and Management Symposium (NOMS '08)*, pp. 25–32, Salvador, Brazil, April 2008.

[35] J. Alonso, J. Torres, J. L. Berral, and R. Gavaldà, "Adaptive on-line software aging prediction based on machine learning," in *Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN '10)*, pp. 507–516, Chicago, Ill, USA, July 2010.

[36] K. Vaidyanathan, R. E. Harper, S. W. Hunter, and K. S. Trivedi, "Analysis and implementation of software rejuvenation in cluster systems," *ACM SIGMETRICS Performance Evaluation Review*, vol. 29, no. 1, pp. 62–71, 2001.

[37] J. Araujo, R. Matos, V. Alves, and P. Maciel, "Software aging in the eucalyptus cloud computing infrastructure: characterization and rejuvenation," *ACM Journal on Emerging Technologies in Computing Systems*, vol. 10, no. 1, pp. 1–22, 2014.

[38] N. Naksinehaboon, N. Taerat, C. Leangsuksun, C. F. Chandler, and S. L. Scott, "Benefits of software rejuvenation on HPC systems," in *Proceedings of the International Symposium on Parallel and Distributed Processing with Applications (ISPA '10)*, pp. 499–506, September 2010.

[39] F. Machida, J. Xiang, K. Tadano, and Y. Maeno, "Combined server rejuvenation in a virtualized data center," in *Proceedings of the 9th IEEE International Conference on Ubiquitous Intelligence and Computing (UIC '12) and 9th IEEE International Conference on Autonomic and Trusted Computing (ATC '12)*, pp. 486–493, Fukuoka, Japan, September 2012.

[40] F. Machida, D. S. Kim, and K. S. Trivedi, "Modeling and analysis of software rejuvenation in a server virtualized system with live VM migration," *Performance Evaluation*, vol. 70, no. 3, pp. 212–230, 2013.

[41] S. Garg, A. van Moorsel, K. Vaidyanathan, and K. S. Trivedi, "Methodology for detection and estimation of software aging," in *Proceedings of the 9th International Symposium on Software Reliability Engineering (ISSRE '98)*, pp. 283–292, Paderborn, Germany, November 1998.

[42] K. Vaidyanathan and K. S. Trivedi, "Measurement-based model for estimation of resource exhaustion in operational software systems," in *Proceedings of the 10th International Symposium on Software Reliability Engineering (ISSRE '99)*, pp. 84–93, November 1999.

[43] K. Kourai and S. Chiba, "Fast software rejuvenation of virtual machine monitors," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 6, pp. 839–851, 2011.

[44] K. Vaidyanathan and K. S. Trivedi, "A comprehensive model for software rejuvenation," *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 2, pp. 124–137, 2005.

[45] D. S. Kim, F. Machida, and K. S. Trivedi, "Availability modeling and analysis of a virtualized system," in *Proceedings of the 15th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC '09)*, pp. 365–371, Shanghai, China, November 2009.

[46] R. D. S. Matos, P. R. M. MacIel, F. Machida, D. S. Kim, and K. S. Trivedi, "Sensitivity analysis of server virtualized system availability," *IEEE Transactions on Reliability*, vol. 61, no. 4, pp. 994–1006, 2012.

[47] Y. B. Y. Bao, X. S. X. Sun, and K. S. Trivedi, "A workload-based analysis of software aging, and rejuvenation," *IEEE Transactions on Reliability*, vol. 54, no. 3, pp. 541–548, 2005.

[48] D. Bruneo, S. Distefano, F. Longo, A. Puliafito, and M. Scarpa, "Workload-based software rejuvenation in cloud systems," *IEEE Transactions on Computers*, vol. 62, no. 6, pp. 1072–1085, 2013.

[49] F. Longo, R. Ghosh, V. K. Naik, and K. S. Trivedi, "A scalable availability model for Infrastructure-as-a-Service cloud," in *Proceedings of IEEE/IFIP 41st International Conference on Dependable Systems & Networks (DSN '11)*, pp. 335–346, June 2011.

[50] W. E. Smith, K. S. Trivedi, L. A. Tomek, and J. Ackaret, "Availability analysis of blade server systems," *IBM Systems Journal*, vol. 47, no. 4, pp. 621–640, 2008.

[51] M. Grottke, A. P. Nikora, and K. S. Trivedi, "An empirical investigation of fault types in space mission system software," in *Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN '10)*, pp. 447–456, Chicago, Ill, USA, June-July 2010.

[52] M. Grottke and K. S. Trivedi, "A classification of software faults," *The Journal of Reliability Engineering Association of Japan*, vol. 27, no. 7, pp. 425–438, 2005.

[53] L. Cui, B. Li, J. Li, J. Hardy, and L. Liu, "Software aging in virtualized environments: detection and prediction," in *Proceedings of the 18th IEEE International Conference on Parallel and Distributed Systems (ICPADS '12)*, pp. 718–719, Singapore, December 2012.

[54] M. Grottke, R. Matias, and K. S. Trivedi, "The fundamentals of software aging," in *Proceedings of IEEE International Conference on Software Reliability Engineering Workshops (ISSRE '08)*, pp. 1–6, 2008.

[55] X. Du, H. Lu, and Y. Rao, "Modeling and analyses of operational software system with rejuvenation and reconfiguration," in *Proceedings of International Conference on Computer Science and Information Technology*, vol. 255 of *Advances in Intelligent Systems and Computing*, pp. 799–807, 2014.

[56] M. Grottke and K. S. Trivedi, "Fighting bugs: remove, retry, replicate, and rejuvenate," *Computer*, vol. 40, no. 2, pp. 107–109, 2007.

[57] M. Steinder, I. Whalley, D. Carrera, I. Gaweda, and D. Chess, "Server virtualization in autonomic management of heterogeneous workloads," in *Proceedings of the 10th IFIP/IEEE International Symposium on Integrated Network Management (IM '07)*, pp. 139–148, May 2007.

[58] X. Zhang, C. Lin, and X. Kong, "Model-driven dependability analysis of virtualization systems," in *Proceedings of the 8th IEEE/ACIS International Conference on Computer and Information Science (ICIS '09)*, pp. 199–204, Shanghai, China, June 2009.

[59] S. Chi, J. S. Park, and T. Thandar, "Availability analysis and improvement of software rejuvenation using virtualization," *Economics and Applied Informatics*, no. 1, pp. 5–14, 2007.

[60] M. T. H. Myint and T. Thein, "Availability improvement in virtualized multiple servers with software rejuvenation and virtualization," in *Proceedings of the 4th IEEE International Conference on Secure Software Integration and Reliability Improvement (SSIRI '10)*, pp. 156–162, June 2010.

[61] M. Grottke, L. Li, K. Vaidyanathan, and K. S. Trivedi, "Analysis of software aging in a Web server," *IEEE Transactions on Reliability*, vol. 55, no. 3, pp. 411–420, 2006.

[62] G. Carrozza, D. Cotroneo, R. Natella, A. Pecchia, and S. Russo, "Memory leak analysis of mission-critical middleware," *Journal of Systems and Software*, vol. 83, no. 9, pp. 1556–1567, 2010.

[63] T. B. Ferreira, R. Matias, A. Macedo, and L. B. Araujo, "An experimental study on memory allocators in multicore and multithreaded applications," in *Proceedings of the 12th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT '11)*, pp. 92–98, Gwangju, Republic od Korea, October 2011.

[64] B. R. Mohan and G. Ram Mohana Reddy, "Software aging trend analysis of server virtualized system," in *Proceedings of International Conference on Information Networking (ICOIN '14)*, pp. 260–263, 2014.

[65] L. Silva, H. Madeira, and J. G. Silva, "Software aging and rejuvenation in a SOAP-based server," in *Proceedings of the 5th IEEE International Symposium on Network Computing and*

Applications (NCA '06), pp. 56–65, Cambridge, Mass, USA, July 2006.

[66] G. Ciardo, J. Muppala, and K. Trivedi, "SPNP: stochastic petri net package," in *Proceedings of the 3rd International Workshop on Petri Nets and Performance Models (PNPM '89)*, pp. 142–151, December 1989.

[67] R. Ghosh, K. S. Trivedi, V. K. Naik, and D. S. Kim, "End-to-end performability analysis for Infrastructure-as-a-Service cloud: an interacting stochastic models approach," in *Proceeding of the 16th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC '10)*, pp. 125–132, Tokyo, Japan, December 2010.

[68] S. Distefano and K. S. Trivedi, "Non-markovian state-space models in dependability evaluation," *Quality and Reliability Engineering International*, vol. 29, no. 2, pp. 225–239, 2013.

Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 713012, 6 pages
http://dx.doi.org/10.1155/2014/713012

Research Article

AVQS: Attack Route-Based Vulnerability Quantification Scheme for Smart Grid

Jongbin Ko,[1] Hyunwoo Lim,[2] Seokjun Lee,[2] and Taeshik Shon[2]

[1] *Information Security Technology Institute, SECUVE Inc., 801 Jnk Digital Tower, 111 Digital-ro 26gil, Guro-gu, Seoul 152-848, Republic of Korea*
[2] *Department of Computer Engineering, Ajou University, 206 Worldcup-ro, Yeongtong-gu, Suwon 443-749, Republic of Korea*

Correspondence should be addressed to Taeshik Shon; tsshon@ajou.ac.kr

Received 2 May 2014; Accepted 2 July 2014; Published 24 July 2014

Academic Editor: Sang-Soo Yeo

A smart grid is a large, consolidated electrical grid system that includes heterogeneous networks and systems. Based on the data, a smart grid system has a potential security threat in its network connectivity. To solve this problem, we develop and apply a novel scheme to measure the vulnerability in a smart grid domain. Vulnerability quantification can be the first step in security analysis because it can help prioritize the security problems. However, existing vulnerability quantification schemes are not suitable for smart grid because they do not consider network vulnerabilities. We propose a novel attack route-based vulnerability quantification scheme using a network vulnerability score and an end-to-end security score, depending on the specific smart grid network environment to calculate the vulnerability score for a particular attack route. To evaluate the proposed approach, we derive several attack scenarios from the advanced metering infrastructure domain. The experimental results of the proposed approach and the existing common vulnerability scoring system clearly show that we need to consider network connectivity for more optimized vulnerability quantification.

1. Introduction

Smart grid is spreading to our everyday life, with new services such as remote control and automated electrical demand and response. However, smart grid has a number of vulnerabilities in terms of cyber security. The security paradigms of previous electric grid were to isolate major electrical facilities from outside entry by logical and physical access restrictions. However, in a smart grid, all devices are mutually connected, and therefore they communicate with each other and also with the central control center. This provides a malicious attacker with an easy attack route to the smart grid control center. Thus, it is necessary to develop and implement a new security paradigm for considering network security.

The first consideration in this new smart grid security paradigm will be to accurately understand the security vulnerabilities and estimate the risk potential of the system. Vulnerability analysis studies have been conducted for supervisory control and data acquisition (SCADA) and power grid. However, these studies only review the vulnerability of the SCADA remote communication system [1] or conduct a vulnerability analysis for electrical engineering [2]. Vulnerability quantification is a powerful method of assessing the security reliability of a system. It objectively shows the overall safety of the system as a score rather than the abstract expressions as shown by some vulnerability analysis methods. The score helps the security administrator to monitor system vulnerability in order to maintain high security even during an attack.

However, applying a vulnerability quantification to smart grid is difficult because of the environmental differences between smart grid and legacy computer systems. A smart grid is a country-sized network composed of innumerable devices using various communication protocols. In addition, the devices have technical and functional differences from standard computers. Thus, applying a single-device vulnerability quantification scheme, such as the common vulnerability scoring system (CVSS), is not suitable for smart grid.

It is necessary to develop a novel vulnerability quantification scheme that is suitable to smart grid characteristics.

In this paper, we propose a novel attack route-based vulnerability quantification scheme (AVQS) that considers the network vulnerability score (NVS) and end-to-end security. We evaluate the proposed scheme by applying attack scenarios from advanced metering infrastructure (AMI) communication use cases.

In Section 2, we will present existing vulnerability quantification schemes and discuss their unsuitability for smart grids. In Section 3, the proposed approach for quantifying security vulnerability, AVQS, will be presented. We will also provide attack scenarios from AMI communication use cases, along with experimental results and analysis in Section 4. Finally, we will conclude the paper and discuss future work in Section 5.

2. Existing Vulnerability Quantification Schemes

2.1. Common Vulnerability Scoring System. The CVSS [3] was developed by a group of corporations, including CERT/CC, Cisco, DHS/MITRE, eBay, IBM, and Microsoft, to create a standardized, open vulnerability scoring framework. CVSS offers an objective and formal procedure to the vendors and users (e.g., security administrators) for evaluating the vulnerability of the target system.

CVSS has three metric groups—base, temporal, and environmental—that consist of several metrics such as the access vector, access complexity, authentication, confidentiality impact, integrity impact, exploitability, and target distribution.

(i) Base group represents the intrinsic and fundamental characteristics of vulnerabilities that are constant over time and user environments.

(ii) Temporal group represents the characteristics of vulnerabilities that change over time but not among user environments.

(iii) Environmental group represents the characteristics of vulnerabilities that are relevant and unique to a particular user environment.

CVSS uses the base group to define and communicate the fundamental characteristics of vulnerabilities. The temporal and environmental groups are selectively used to provide contextual information that more accurately reflects the risks particular to their unique environments.

When the base metrics are assigned values, the base equation is used to calculate a score ranging from 0 to 10 and create a vector, as illustrated in Figure 1. The vector facilitates the "open" nature of the framework. It is a text string that contains the values assigned to each metric, and it is used to communicate exactly the derivation of the score for each vulnerability. Therefore, the vector should always be displayed with the vulnerability score [4].

2.2. Limitations of CVSS on Smart Grids. CVSS gives a vulnerability score for each vulnerability of a target system. This method has the ability to manage each vulnerability individually, but it is not suitable for estimating the entire system's vulnerability. Further, CVSS cannot quantify the vulnerabilities when connections occur between devices inside the system. These limitations make it impossible for CVSS to accurately quantify the security vulnerability in network systems such as smart grid, which have various types of devices that are different from a general PC infrastructure network.

2.3. Limitations of Existing AVQSs. There are several vulnerability quantification schemes based on attack routes or attack trees for smart grids and supervisory control and data acquisition (SCADA) [5–8]. These schemes use attack route information (number of hops, number of paths to target, etc.) as the main element for vulnerability quantification. However, the output of these schemes is expressed in varying units, for example, days, grades, degrees, and so forth. The lack of unity and public confidence in the results makes the schemes unsuitable for smart grid.

3. AVQS for Smart Grid

In this section, we propose a novel AVQS for smart grids. The proposed scheme first calculates the CVSS scores of the nodes on the attack route. Then, it calculates the network vulnerability score, which considers the presence of network security functions (e.g., firewalls and intrusion-detection systems (IDS)), protocol types, and communication link types. Finally, it calculates the weighted average of the total scores, considering end-to-end security functions.

3.1. Definitions and Assumptions. When an attack occurs on one particular target node on the network, there can be several attack routes. An attack route consists of at least two nodes: sender and receiver. In the majority of cases, a network-based attack uses the vulnerabilities and weaknesses of the intermediate nodes on the attack route. Therefore, we define two types of connections on the attack route.

(i) Route is the end-to-end data communication connection from a sender to a receiver. It can have several intermediate nodes.

(ii) Section is the communication connection between two intermediate nodes on the attack route.

An attacker can use the vulnerabilities of each section to attack the route. In fact, the attacker can use local vulnerabilities for direct attacks, such as a root authority acquisition and insider attack. However, we only deal with network-based attacks, because CVSS can identify local vulnerabilities.

3.2. Building AVQS. Figure 2 presents a sample attack route. In Figure 2, we assume that the attack starts from node S (sender) to the target node R (receiver). Therefore, the attack route is S, A, B, and R. In this case, there are three sections, S to A, A to B, and B to R.

As mentioned above, our scheme considers the network environments of the section. We define it as the NVS, which

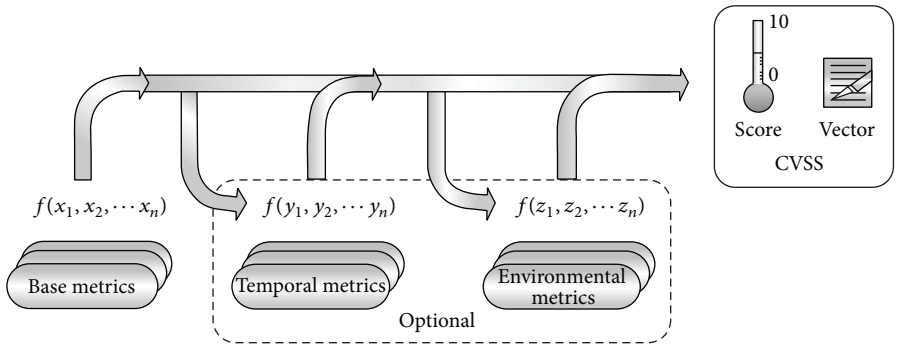


Figure 1: CVSS metrics and equations [3].

Table 1: Network vulnerability scores on the section.

Type			Score
Network security functions (a)	Present		0.13
	Not present		1.20
Communication link types (b)	Wired		0.13
	Wireless		0.67
Protocol types (c)	TCP/IP	With security	0.14
		Without security	0.4
	Electricity-specific protocols	With security	0.27
		Without security	0.53

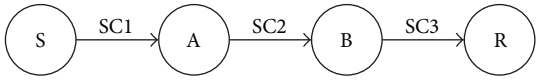


Figure 2: Sample attack route.

considers the security functions of the incoming section approaching a typical node on the attack route. In the case of Figure 2, the NVS of SC1 (Section 1) has a dependency on node A. Therefore, the AVQS score of node A is calculated by combining the CVSS of node A and the NVS of SC1:

$$\mathrm{AVQS}_i = \mathrm{CVSS}_i + \mathrm{NVS}_i \quad (\text{If } i \text{ is the first node of the attack route}, \mathrm{NVS}_i = 0). \tag{1}$$

NVS consists of three types, (a) network security functions, (b) communication link types, and (c) protocol types applied on the section. Equation (2) and Table 1 show the details of NVS:

$$\mathrm{NVS}_i = 0.2 \times \mathrm{CVSS}_i + S_i - 2.4 \quad (S = a + b + c). \tag{2}$$

The parameter constant values are defined to make vulnerability score range from 0 to 10 which is common range in CVSS. The difference between parameter constants represents the vulnerability level.

Network security functions (e.g., IDS and firewalls) have a high probability of detecting an attack through the network. Therefore, we assume that if network security functions are absent, the section has a high security-weakness score (lower is better). If one section has no network security functions, and the other sections are relatively secure (wired network and TCP/IP with security functions), it has a higher score than the rest.

The procedure for calculating NVS is as follows.

S_i is the sum of NVS scores (a), (b), and (c). The minimum value of S_i is 0.4 and the maximum value of S_i is 2.4. Thus, we regulate S_i from 0 to 2, as

$$S_i - 0.4. \tag{3}$$

As mentioned above, NVS_i has a dependency on node i because the security level of the section can be changed by CVSS_i itself. For example, when the calculated NVS_i has a low value (secure) and the CVSS_i has a high value (weak), it is difficult to determine the security degree. Thus, our scheme uses a floating variable to solve this problem:

$$\frac{10 - \mathrm{CVSS}_i}{5}. \tag{4}$$

By applying (4), NVS_i is changed properly according to CVSS_i from −2 to 2. For example, if CVSS_i is 0, the range of NVS_i is changed from −2 to 0. Further, if CVSS_i is 10, the range of NVS_i is changed from 0 to 2.

Therefore, the final NVS_i equation is presented as follows:

$$\mathrm{NVS}_i = S_i - 0.4 - \frac{10 - \mathrm{CVSS}_i}{5} = 0.2 \times \mathrm{CVSS}_i + S_i - 2.4 \quad (S = a + b + c). \tag{5}$$

Table 2: End-to-end security scores.

Type		Score
End-to-end security functions	Present	0.8
	Not present	1

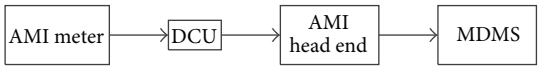


Figure 3: Communication flow of use case 1.

Then, we can calculate the AVQS score for node i using (1). After calculating AVQS scores for every node of the attack route, we can determine the overall AVQS score of the attack route:

$$\text{AVQS}_{\text{avg}} = \alpha \times \frac{\sum_{i=1}^{n} \text{AVQS}_i}{n}. \quad (6)$$

Here, α refers to end-to-end security functions, such as VPN, IPsec, and e2e encryption. These functions provide a secure communication channel from source to destination on the route. Therefore, α must be considered to determine an accurate vulnerability score of the attack route. However, some attackers can attack the target using specific techniques even when the function is applied. Therefore, our scheme applies the end-to-end security score to the final AVQS score. However, we make the influence of this score slight because it can be confusing. The end-to-end security scores of our scheme are shown in Table 2.

4. Experimental Results and Analysis

To verify the suitability of our scheme, we experimented with attack scenarios based on actual communication use cases of the AMI domain on smart grid.

4.1. Attack Scenarios. In order to quantify the vulnerability of the AMI group, we considered communication use cases of the AMI domain and attack scenarios that can actually occur in smart grid.

(i) Use Case 1. While communicating with the AMI meter, the meter data management system (MDMS) collects and stores the customers' electrical consumption information (see Figure 3).

(ii) Attack Scenario 1. In order to counterfeit and falsify the customers' electrical consumption information stored in the MDMS, we assume that the attacker trespasses through the data concentrator unit (DCU). In this case, the attacker can overcharge or undercharge the consumers (see Figure 4).

(iii) Use Case 2. This includes storing energy when electrical charges are low and using the energy when electrical charges are high (see Figure 5).

(iv) Attack Scenario 2. We assume that the attacker trespasses through the customer distributed energy resources-energy management system (DER-EMS) and illegally controls the energy services interface/customer energy management system (ESI/CEMS). In this case, the attacker can cause the DER and energy storage system (ESS) to malfunction. Owing to the attack, the consumer cannot charge the DER or spend electricity stored in the ESS (see Figure 6).

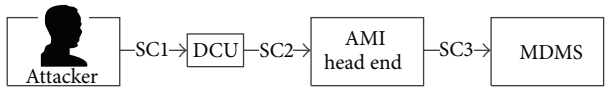


Figure 4: Attack route for Scenario 1.

Figure 5: Communication flow of use case 2.

4.2. Experimental Results. The CVSS values are calculated using NIST's "Common Vulnerability Scoring System Version 2 Calculator." Metric values and details can be found in NIST's criteria "A Complete Guide to the Common Vulnerability Scoring System Version 2.0." [1].

(i) Attack Scenario 1. Table 3 shows the calculated CVSS values of each node of the attack route for Attack Scenario 1. For the DCU, we only use the base and temporal metrics for calculation because the environmental metric of CVSS is an optional process.

Access Vector. All components consist of adjacent networks in a smart grid.

Access Complexity. Specialized access conditions or situations do not exist.

Authentication. Authentication is not required to access and exploit the vulnerability.

Confidentiality Impact. There is considerable information outflow, but the scope of the loss is constrained.

Integrity Impact. There is considerable information modification, but the scope of what the attacker can affect is limited.

Availability Impact. There is no impact to the availability of the system.

Exploitability. Even if the attacker is unskilled, he can easily attack vulnerabilities.

Remediation Level. There is an unofficial, nonvendor solution available.

Report Confidence. There is little confidence in the validity of the reports.

Table 3: CVSS per node of the attack route.

		DCU	AMI head end	MDMS
Base	Access vector	Adjacent network	Adjacent network	Adjacent network
	Access complexity	Low	Medium	High
	Authentication	None	Single instance	Multiple instances
	Confidentiality impact	Partial	Complete	Complete
	Integrity impact	Partial	Complete	Complete
	Availability impact	None	Partial	Complete
Temporal	Exploitability	High	Functional	Proof of concept
	Remediation level	Work around	Work around	Work around
	Report confidence	Unconfirmed	Confirmed	Confirmed
CVSS		**4.1**	**6.3**	**5.3**

Table 4: Network security scores and AVQS scores.

Type	SC1	SC2	SC3
Network security functions	Present	Not present	Present
Communication link type	Wired	Wired	Wired
Protocol type	Protocols for PLC without security	Protocols for PLC without security	TCP/IP with security
NVS	**−0.79**	**0.72**	**−0.95**
AVQS	**3.31**	**7.02**	**4.35**

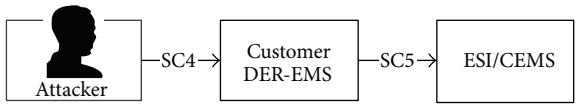


Figure 6: Attack route for Scenario 2.

Because of the presence of network security functions, communication link types, and protocol types, the NVS score is assigned as shown in Table 4. For example, there are no network security functions in Section "SC1." Further, Section "SC1" uses a wired network and a power-line communication (PLC) protocol without security.

The calculated NVS values of each section and the calculated AVQS values of each node are as follows. The NVS values are calculated by (5) and the AVQS and average AVQS values are calculated by (1) and (6), respectively.

(ii) Attack Scenario 2. We calculated CVSS, NVS, and AVQS in the same manner for Attack Scenario 2, as shown in Tables 5 and 6.

The comparison of the results of AVQS and the average CVSS shown in Table 7. In the case of Attack Scenario 1, we assume that end-to-end security is applied. By (6), the average AVQS is multiplied by 0.8. However, end-to-end security is not applied in Attack Scenario 2, and therefore, we multiply by 1. As a result, the average AVQS score is 3.91 in Attack Scenario 1 and 6.06 in Attack Scenario 2.

In the case of Attack Scenario 1, the difference of the two values is 1.32 because network security functions were applied to the route. This means that our model includes the network security feature characteristics and has accurate quantification. On the other hand, we can see that the final AVQS value is bigger than the average CVSS value in the case of Attack Scenario 2, because the network security functions were minimal. This shows that our proposed scheme can provide the proper vulnerability quantification results in two cases.

5. Conclusion

In this paper, we proposed a novel AVQS to accurately measure the security level in a smart grid. The proposed approach includes NVS and end-to-end security functions. To verify the proposed approach, we derived attack scenarios using a few use cases from AMI communications. The evaluation results showed an obvious difference between the proposed approach and the average CVSS. The difference between the two values indicates the importance of considering network security features. Thus, we can see that the proposed scheme is a more optimized approach than the previous one. In future work, various attack scenarios on the AMI and the rest of the domains like SA (substation automation), WAMS (wide area measurement system), and DER (distributed energy resources) should be considered.

Conflict of Interests

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

Table 5: CVSS per node of the attack route.

		Customer DER/EMS	ESI/CEMS
Base	Access vector	Adjacent network	Adjacent network
	Access complexity	Medium	High
	Authentication	Single instance	Multiple instances
	Confidentiality impact	Partial	Complete
	Integrity impact	Partial	Complete
	Availability impact	Complete	Complete
Temporal	Exploitability	Functional	Proof of concept
	Remediation level	Work around	Work around
	Report confidence	Confirmed	Confirmed
CVSS		**4.1**	**5.7**

Table 6: Network security scores and AVQS scores.

Type	SC4	SC5
Network security functions	Not present	Not present
Communication link type	Wired	Wired
Protocol type	Protocols for PLC without security	Protocols for PLC without security
NVS	**0.60**	**0.52**
AVQS	**6.3**	**5.82**

Table 7: Comparison of the experimental results.

	Attack Scenario 1	Attack Scenario 2
Average CVSS	5.23	5.50
Final AVQS	3.91	6.06

Acknowledgments

This work was supported by the Power Generation and Electricity Delivery Core Technology Program of Korea Institute of Energy Technology Evaluation and Planning (KETEP) granted financial resource from the Ministry of Trade, Industry and Energy, Republic of Korea (no. 20131020402090).

References

[1] K. HyungJun, "Security and vulnerability of SCADA systems over IP-based wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2012, Article ID 268478, 10 pages, 2012.

[2] F. Gutierrez, E. Barocio, F. Uribe, and P. Zuniga, "Vulnerability analysis of power grids using modified centrality measures," *Discrete Dynamics in Nature and Society*, vol. 2013, Article ID 135731, 11 pages, 2013.

[3] Z. Jianliang and M. Lee, "Will IEEE 802.15.4 make ubiquitous networking a reality?" *IEEE Communications Magazine*, vol. 42, no. 6, pp. 140–146, 2004.

[4] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *IEEE Security and Privacy*, vol. 4, no. 6, pp. 85–89, 2006.

[5] K. Jongbin, S. Lee, Y. Lim, S. Ju, and T. Shon, "A novel network modeling and evaluation approach for security vulnerability quantification in substation automation systems," *IEICE Transaction on Information and Systems*, vol. E96-D, no. 9, pp. 2021–2025, 2013.

[6] D. J. Leversage and E. James, "Estimating a system's mean time-to-compromise," *IEEE Security and Privacy*, vol. 6, no. 1, pp. 52–60, 2008.

[7] J. L. Bayuk and A. Mostashari, "Measuring cyber security in intelligent urban infrastructure systems," in *Proceedings of the 8th International Conference and Expo on Emerging Technologies for a Smarter World (CEWIT '11)*, pp. 1–6, New York, NY, USA, November 2011.

[8] P. A. S. Ralston, J. H. Graham, and J. L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," *ISA Transactions*, vol. 46, no. 4, pp. 583–594, 2007.

Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 321710, 6 pages
http://dx.doi.org/10.1155/2014/321710

Research Article

The Study on Stage Financing Model of IT Project Investment

Si-hua Chen,[1] Sheng-hua Xu,[1] Changhoon Lee,[2] Neal N. Xiong,[1] and Wei He[3]

[1] *Institute of Information Resource Management, School of Information Technology, Jiangxi University of Finance and Economics, No. 169, East Shuanggang Road, Changbei, Nanchang, Jiangxi 330013, China*
[2] *Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul 139-743, Republic of Korea*
[3] *School of Business and Administration, Jiangxi University of Finance and Economics, No. 169, East Shuanggang Road, Changbei, Nanchang, Jiangxi 330013, China*

Correspondence should be addressed to Neal N. Xiong; nxiong@coloradotech.edu

Received 3 May 2014; Accepted 13 July 2014; Published 23 July 2014

Academic Editor: Sang-Soo Yeo

Stage financing is the basic operation of venture capital investment. In investment, usually venture capitalists use different strategies to obtain the maximum returns. Due to its advantages to reduce the information asymmetry and agency cost, stage financing is widely used by venture capitalists. Although considerable attentions are devoted to stage financing, very little is known about the risk aversion strategies of IT projects. This paper mainly addresses the problem of risk aversion of venture capital investment in IT projects. Based on the analysis of characteristics of venture capital investment of IT projects, this paper introduces a real option pricing model to measure the value brought by the stage financing strategy and design a risk aversion model for IT projects. Because real option pricing method regards investment activity as contingent decision, it helps to make judgment on the management flexibility of IT projects and then make a more reasonable evaluation about the IT programs. Lastly by being applied to a real case, it further illustrates the effectiveness and feasibility of the model.

1. Introduction

For the private enterprises in early stage or expansion stage, if they have advantages in technologies, products, markets, or teams and possess the capability of fast growth, they may attract the attraction of venture capital. However, due to the enormous uncertainties faced by these enterprises, there are high risks for the venture capital to invest in these enterprises (we call them venture enterprises). Therefore, the investment to venture enterprises always takes the form of stage financing. That is, venture capital investors usually do not invest all to the venture enterprise at one time. They usually invest part of the capital of the enterprise at each development stage and remain the right to give up investment and to liquidate of any stage. The stage financing depends on the degree of information symmetry, the degree of satisfaction to the need of information, capital structure, and requirements of management incentive [1–4]. Stage financing is a kind of motivation method to venture enterprises [5–7]. There are two types of stage financing: milestone investment and round investment. For the first type, both sides set the goal of each stage and decide the total investment in the first contract to avoid negotiating again. In this way, venture capital investors can get high flexibility in advance. Once the venture entrepreneur cannot achieve the set goals (such as obtaining new patents, producing final products, or getting the foreseeable product market sales), venture capital investors have the right to give up the project. For round investment, it offers venture capital investors great flexibility afterwards. Usually they do not decide the total investment in the first contract. After each stage of investment, both sides need to negotiate about the investment of next stage. According to the theory of stage financing, scholars agree that stage financing can reduce risk of investment [8, 9], effectively motivate venture entrepreneurs [10], and reduce the commitment problem of renegotiation of venture entrepreneurs [11, 12].

2. Related Works

Stage financing depends on factors such as the extent of information symmetry, the extent of satisfaction to the need of information, capital structure of enterprises, and management incentives. Admati and Pfleiderer showed that entrepreneurs had typical investment preferences. As long as there is somebody willing to invest, the entrepreneurs will never give up the business he starts no matter how it is clear that the business will be a failure [13]. Before the investment, it is probable that the investors may not know the information of the business. Therefore, the full and one-off capital investment may bear high agent risk. According to traditional principal-agent theory, the asymmetry of information between the principal and the agent will result in the violation behaviors of the agent. In venture capital investment, due to the participation of risk capitalists, the asymmetry of information has been greatly reduced to large degree but this phenomenon still exists. Triant (2001) held the view that because information could not be effectively transferred to the investors, the discrimination ability of the investors on entrepreneurs and their investment project was weakened. Such kind of asymmetry of information not only increases the investment risk but also increases the financing cost of entrepreneurs [14]. The empirical study of Cumming and MacIntosh (2001) indicated that there was asymmetry of information in venture capital investment especially in early stage [15]. Adopting stage financing can reduce the extent of asymmetry of information. The extent of satisfaction to the need of information can influence stage financing from another perspective. Generally speaking, the higher the extent of satisfaction of information needs is, the less the stages of venture capital investment are. K. Smith and R. L. Smith (2000) pointed out that entrepreneurs knew better about the advantages of their technology while investors might know more about the economic values of project [16]. The information for investors to evaluate the investment opportunity is asymmetric and highly uncertain. By stage financing, the investors can obtain both internal and external information of enterprises at different stages and reduce investment risks. In addition, the capital structure of enterprises also influences stage financing. Gompers's study showed that when the ratio of intangible capital of risk enterprises is high, the agency cost and supervision cost are high and the stages of stage financing are more [17]. That is, the stages of stage financing are positively proportional to the ratio of intangible capital. A distinct feature of venture capital investment is management participation. By a series of institutions, an effective governance mechanism is formed which can promote the effective operation of risk enterprises and reduce management risks. Management incentives are the basic governance for risk enterprises. Cornelli and Yosha (1998), Gompers (1995), Sahlman (1990) pointed out the rights that investors could give up the investment liquidate at any stage are not only the pressures on the management of risk enterprises but also the incentives on the management. Therefore, stage financing is a kind of incentive method to risk enterprises [5, 18–25].

Stage financing is the basic strategy for venture capital investment. The process of stage financing is accompanied with stage evaluation. In fact, before each investment investors need to evaluate risk enterprises. It is recognized that the evaluation on risk enterprises consists of two perspectives: one is nonvalue evaluation on risk enterprises, that is, based on reasonable evaluation indicator system to make a comprehensive evaluation on the development capability of risk enterprises. Another is value evaluation, that is, to make an evaluation on the value of equity or value of risk enterprises [26–30]. From the perspective of investors, no matter what kind of form we take to evaluate at any stage, the final goal is to maximize the value of equity or value of enterprises.

The study on the risk of IT project investment becomes one hot topic in present MIS field. In the development of IT project, it is very important to effectively identify all the involved risk factors and offer effective risk management measures [31–35]. It is usually thought that there are two ways to control risks: decreasing the probability of risks or reducing the significant outcome brought by risk. In the present studies and practices, people usually prefer to curbing risk by the ways of reducing the production scale, continuing to do R&D or cancelling the project to achieve the goal of reducing risk probability [36–38].

However, the happening of some risks cannot be eliminated. From economy aspect, it is not worthwhile to eliminate some risks. Therefore, we should comprehensively consider the methods of avoiding or transferring risks. However, the present studies on risk management of IT projects are not enough. Originated from finance, the real option tool which is widely used in financial risk management provides powerful tool for it.

3. Stage Financing and Hypothesis

3.1. Different Development Stages of Enterprises and Stage Financing. Generally, the development of venture enterprises always experiences five phrases including the R&D stage, the initial stage, the early growth stage, the rapid growth stage, and the withdrawing stage. The investment stage of venture investment is consistent with the development stage of venture enterprises but sometimes there is also inconsistency. In each investment stage, the new internal and external information about the enterprise is released and they are the important proof for whether to continue to invest.

The investors adopt "wait and see" way and obtain the specific business performance indicators milestones, such as analyzing tests, product prototype, the first production, and the first marketing. "Milestones" can work as the benchmarks for investment stages. Through business process, the investors continuously look for milestones. On the basis, they will constantly evaluate the value of enterprises and decide whether to further invest or cooperate.

3.2. The Thought of Stage Financing of IT Project. In fact, the thought of stage financing of IT project has been adopted

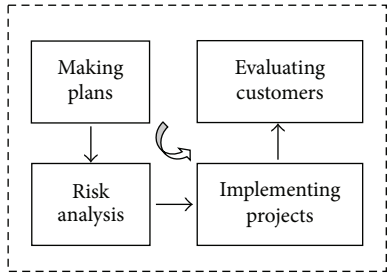


Figure 1: Multistage software development model.

in the development of software program. In software engineering, the BOEHM spiral model is in essence a multistage software development model. The spiral model combines the waterfall model and rapid prototype model. The model supposes that the development of software programs is a spiral rising process with several iterative cycles. In each stage the following activities are carried out as shown in Figure 1:

(1) making plans: defining the target of software and making plan, making clear the restrictive conditions of project development,

(2) risk analysis: analyzing and evaluating the scheme and considering how to recognize and eliminate risks,

(3) implementing projects: implementing software development and testing,

(4) evaluating customers: evaluating development work and proposing revision suggestions and making next plan.

First of all, each stage should define the goals of this stage, the scheme to achieve these goals, and the restrictive conditions. Then we analyze the development strategy of each scheme from the aspect of risk and try to exclude all kinds of potential risks. Sometimes it is even needed to construct prototype to finish. If some risks cannot be excluded, the scheme should stop immediately otherwise we need to start next development step. Lastly we need to evaluate the outcome of this stage and design for the next stage. With the successful application of the thought of stage financing of IT program to software project, more and more venture investment of IT program adopts the decision of multistage investment thought to reduce the risks and cost of investment to obtain more profits.

4. Real Option Pricing Model

Suppose there exists a new venture investment project. The factors influencing the value of the project include the quality of venture entrepreneur, market needs, and progress level of technology. To consider all the factors, this paper supposes that the value of venture investment project obeys the geometric Brownian movement in two continuous time slots:

$$dV = \alpha V dt + \sigma t V dW, \quad (1)$$

where V means value and t means time. α is the drift coefficient, which is decided by the quality of venture entrepreneur and the conditions of total market. σ is variance coefficient; dW is a standard Wiener process. To simplify it, this paper supposes that α is a constant. There are three investment times: T_1, and T_2, $0 < T_1 < T_2$. Suppose, at the time of $t = T_2$, the venture investment project needs the last venture investment M and then the venture investment organization can carry out the withdrawing mechanism and obtain the benefits. We further suppose that, at the time of $t = 0$, there is no capital for venture enterprise and it needs to get venture investment to support the rapid development of the enterprise within the period of $0 < t < T_2$.

This paper makes a comparison and we suppose that the two venture investment schemes are as follows:

(1) the stage financing: at the point of $t = 0$, the investment is I_1; at the point of $t = T_1$, the investment is K;

(2) the single stage of investment: at the point of $t = 0$, we invest I_2, $I_2 = I_1 + e - rT_1K$ (r is risk free interest rate).

Because it is hard for venture enterprises to get other capital except for venture investment, this paper believes that if venture investment organizations do not invest, the value of venture enterprises will be 0. The agency cost is the cost to reconciliate the different goals of them. For the venture investment organization, its goal is to maximize the benefits of the venture investment project. And the option value of it is the main part of the benefits of venture investment.

Because of the characteristics of option, the value of option, and the value of venture investment project is positive to the risk level of the investment period σ. Therefore, the venture investment organization hopes that the venture entrepreneur choose the higher risk level. However, for venture entrepreneur, his goal is to maximize the possibility of obtaining next venture investment. Therefore, to ensure to achieve the goal of each stage, generally he will adopt conservative operation behavior so that the risk level is low. The inconsistency of goals will produce the agency cost. This paper quantitatively describes the agency cost as the degree of risk of which the venture entrepreneur can choose the operation behavior, that is, the value of σ.

In the single investment stage, because there is no the benefit brought by the reduced agency cost of the stage financing, the risk level chosen by venture entrepreneur will be lower than the risk level chosen in the stage financing. To simplify it, this paper supposes that once the risk level of the investment period is set, it will be constant.

For the stage financing, at the point of $t = 0$, after we invest I_1, the venture investment organization will get a compound call option, that is, obtaining two rounds of

investment choices: when $t = T_1$, we invest K; when $t = T_2$, we invest M. Geske (1979) once induced the pricing model:

$$C_1 = VN\left(h_1 + \sigma_1\sqrt{\tau_1}, h_2 + \sigma_2\sqrt{\tau_2}, \sqrt{\frac{\tau_1}{\tau_2}}\right) - Me^{-r\tau_2}N\left(h_1, h_2, \sqrt{\frac{\tau_1}{\tau_2}}\right) - Me^{-r\tau_1}N\left(h_1\right), \tag{2}$$

where

$$h_1 = \frac{\ln\left(V/M\right) + \left(r - (1/2)\,{\sigma_1}^2\right)\tau_1}{\sigma_1\sqrt{\tau_1}}, \qquad h_2 = \frac{\ln\left(V/M\right) + \left(r - (1/2)\,{\sigma_2}^2\right)\tau_2}{\sigma_2\sqrt{\tau_2}}. \tag{3}$$

We can get the value of V from the formula:

$$VN\left(h_2 + \sigma_1\sqrt{\tau}\right) - Me^{-r\tau}N\left(h_2\right) - K = 0. \tag{4}$$

r is risk free interest rate:

$$\tau_1 = T_1 - t; \qquad \tau = T_2 - T_1; \qquad \tau_2 = T_2 - t = \tau_1 + \tau. \tag{5}$$

N is cumulative standard normal distribution function, $N(A, B, \rho)$ is bivariate cumulative standard normal distribution function, A and B are the upper limit of integral, and ρ is correlation coefficient. When $t = 0$, we can get

$$NV_1 = C_1 - I_1. \tag{6}$$

For single stage investment, at the point of $t = 0$, after investing I_2, we can get a simple call option. We can apply B-S model to calculate the value of the option:

$$C_2 = VN\left(d_1\right) - Me^{-r(T_2 - t)}N\left(d_2\right), \qquad d_1 = \frac{\ln\left(V/M\right) + \left(r + (1/2)\,{\sigma_1}^2\right)\left(T_1 - t\right)}{\sigma_1\sqrt{\left(\left(T_1 - t\right)\right)}}, \qquad d_2 = \frac{\ln\left(V/M\right) + \left(r + (1/2)\,{\sigma_2}^2\right)\left(T_2 - t\right)}{\sigma_2\sqrt{\left(\left(T_2 - t\right)\right)}}. \tag{7}$$

r is risk free interest rate; $N(\cdot)$ is cumulative standard normal distribution function. Then at the point of $t = 0$, we can get

$$NV_2 = C_2 - I_2. \tag{8}$$

We compare the effect produced from stage financing with the single stage investment, that is, the odds between the net value of stage financing and the net value of single stage investment ($NV_1 - NV_2$). To further explore the contribution of stage financing, by using the difference analysis method, we define the difference of investment value due to different risk level at the same investment stage as risk effect; we define the effect produced by delaying some initial investment capital K to invest at the time of $t = T_1$ as delay effect. The sum of delay effect and risk effect should be equal to the total effect of stage financing. The real option pricing method regards investment activity as contingent decision. Therefore, it can make judgment on the value of the management flexibility of the project and then make a more reasonable evaluation about the IT program.

5. The Real Option Analysis of Risk Aversion Strategy of Multistage

An enterprise is considering to develop a ERP system to integrate the internal business process of the enterprise. Once being established, the system will support the daily activities of the enterprise such as purchasing, selling, and production. The system is planned to be finished within 3 years and is estimated to be invested 250 thousand dollars. If it is successfully implemented, it will bring 300 thousand dollars profits. First, we adopt NPV (net value) method to evaluate the economic benefits of the project. We suppose the risk free interest rate is 12%. The expected earnings are 34 884 dollars.

When adopting NPV method, in fact they regard that the investment to the project is one-off. However, with the real option thought, we can apply stage financing strategy to avoid the risks of the project. For example, the storage management subsystem is an important part of ERP system. It is highly connected with the purchasing, selling, and logistics of the enterprise. Therefore, the decision maker can divide the ERP system into 2 phrases to develop. At the first stage, we can develop the storage management system. After the system is successfully implemented, the development team can go into the second stage to finish the development of other parts of the whole ERP system.

To simplify it, we suppose that the time of the first stage is one year. The development fees for storage management system are 50 thousand dollars. The time of the second stage is two years and the development cost is 200 thousand dollars. The following thing is to adopt the real option pricing method to evaluate the revised development strategy of the project to test the economic benefits of the strategy. The development cost of storage management system ($k = 50$ thousand dollars) can be regarded as a European call option of the investment of the second stage. The expected earnings of the option are $V = 300$ thousand dollars; the implementing cost of the option is $M = 200$ thousand dollars. Then we can apply Black-Scholes pricing model to calculate the option value C_0:

$$C_0 = VN\left(d_1\right) - Me^{-rT}N\left(d_2\right), \tag{9}$$

where

$$d_1 = \frac{\ln\left(V/M\right) + \left(1 + (1/2)\,\sigma^2\right)T}{\sigma\sqrt{T}}, \qquad d_2 = d_1 - \sigma\sqrt{T}. \tag{10}$$

σ is the variance of expected earnings and we set it as 50%; r is the risk free interest rate; $N(\cdot)$ stands for cumulative normal distribution function. Taking the values of these parameters to the formula, we can get the option price: $C_0 = 162\,559$

dollars. Considering the development cost of the first stage, according to multistage strategy the earnings to develop the ERP project are 118 213 dollars. In another word, the multistage development strategy will bring 118 213 − 34 884 = 83 329 dollars extra earnings. At the same time, this project can also be regarded as a two-stage IT investment project. When the enterprise invests in the first stage, it also gets the investment option of the second stage. The compound option pricing formula proposed by [39] can precisely evaluate the compound option. So here this paper will use this compound option pricing formula to estimate the value of the project again. The pricing formula is as follows:

$$C_1 = VN\left(h_1 + \sigma_1\sqrt{\tau_1}, h_2 + \sigma_2\sqrt{\tau_2}, \sqrt{\frac{\tau_1}{\tau_2}}\right) - Me^{-r\tau_2}N\left(h_1, h_2, \sqrt{\frac{\tau_1}{\tau_2}}\right) - Me^{-r\tau_1}N\left(h_1\right), \tag{11}$$

where

$$h_1 = \frac{\ln\left(V/\overline{V}\right) + \left(r - (1/2)\,{\sigma_1}^2\right)\tau_1}{\sigma_1\sqrt{\tau_1}}, \qquad h_2 = \frac{\ln\left(V/\overline{M}\right) + \left(r - (1/2)\,{\sigma_2}^2\right)\tau_2}{\sigma_2\sqrt{\tau_2}}. \tag{12}$$

From formula $VN(h_2 + \sigma_1\sqrt{\tau}) - Me^{-r\tau}N(h_2) - K = 0$, we can get the value of V. Making $V = 300000$ dollars, $K = 50000$ dollars, $M = 200000$ dollars, $T_1 = 1$ year, $T_2 = 3$ years, $r = 12\%$, $\sigma = 50\%$, we can get the value of compound option $C_0 = 134\,659$ dollars. Comparing the value of compound option with net present value, the value of option of the project increases 134 659 − 34 884 = 99 775 dollars.

6. Conclusions

The IT projects always have high risks. The benefits of projects are influenced by many uncertain factors. Some studies pointed out that the traditional NPV method may underestimate the value of project in uncertain environment. Sometimes the value may be underestimated about half of it. Dividing the development of ERP system into 2 stages is in fact providing a waiting option for decision makers. If the development of first stage is successful and can achieve good effect, then we can continue to develop other parts of ERP system. On the contrary, if the development of first stage fails or there appear some disadvantageous factors, the decision makers may delay the development of the second stage or even cancel the whole project to avoid larger loss.

The wrong need analysis or unclear need definition is one of the most common risks in the development of IT projects. Because there is high correlation between storage management system and other parts of ERP system, the development of first stage will help development staff to understand the business process of the enterprise and better understand and design customers' needs so as to better reduce the need risks of the second stage and increase the success probability of the project.

For some IT projects such as big ERP projects, they are generally highly complex. In particular, when it adopts new technology or has lots of interactions with external systems, the development task is more difficult. The strategy of stage financing is equal to first making experiment on small scale which provides the learning opportunity for development staff to get familiar with new technologies. It also can reveal the potential problems and then help to make corresponding measures, such as developing some assisting tools to reduce the complexity risks of the project.

This paper applies the real option pricing model to measure the value brought by the stage financing strategy. But there are still some limitations. First of all, the factors which influence investment such as management participation and incentives have not been included in this model. Secondly, this paper only considers the value of equity and has not considered the application of other financial tools such as convertible bonds, preferred stock to stage financing. All these problems still wait to be explored in future research.

Conflict of Interests

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

Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grant nos. 71361013, 71261009, 71273122, and 71163014; China Postdoctoral Science Foundation under Grant no. 2013M541867; The Education Department of Jiangxi Province Science and Technology Research Projects under Grant no. 11728; and Jiangxi Province Science Foundation of China under Grants no. 20122BAB211022.

References

[1] Z. L. Liu and W. X. Xu, "Decision-making on stage financing," *Chinese Journal of Management Science*, vol. 10, no. 2, pp. 1–5, 2002.

[2] X. Liu, "The real option value of the multi-period venture investment," *Chinese Journal of Management Science*, vol. 13, no. 3, pp. 26–31, 2005.

[3] X. U. Xian Ping, "International comparison of the mode of venture investment," *Management World*, vol. 8, no. 2, pp. 63–68, 2001.

[4] X. Xu, "The risk evaluation and control of risk investment," *Chinese Journal of Management Science*, vol. 9, no. 4, pp. 75–80, 2001.

[5] W. A. Sahlman, "The structure and governance of venture-capital organizations," *Journal of Financial Economics*, vol. 27, no. 2, pp. 473–521, 1990.

[6] P. Gompers and J. Lerner, "An analysis of compensation in the U.S. venture capital partnership," *Journal of Financial Economics*, vol. 51, no. 1, pp. 3–44, 1999.

[7] S. Wang and H. Zhou, "Staged financing in venture capital: moral hazard and risks," *Journal of Corporate Finance*, vol. 10, no. 1, pp. 131–155, 2004.

[8] T. Hellmann, *Financial Structure and Control in Venture Capital*, Graduate School of Business, Stanford University, Stanford, Calif, USA, 1994.

[9] Y. Li, "Duration analysis of venture capital staging: a real options perspective," *Journal of Business Venturing*, vol. 23, no. 5, pp. 497–512, 2008.

[10] P. A. Gompers, "Optimal investment, monitoring, and the staging of venture capital," *Journal of Finance*, vol. 50, no. 5, pp. 1481–1488, 1995.

[11] D. V. Neher, "Staged financing: an agency perspective," *Review of Economic Studies*, vol. 66, no. 2, pp. 255–274, 1999.

[12] H. Christian and F. Rieder, "What drives venture capital syndication?" *Applied Economics*, vol. 42, no. 8, pp. 1476–4282, 2010.

[13] A. R. Admati and P. C. Pfleiderer, "Robust financial contracting and the role of venture capitalists," *Journal of Finance*, vol. 49, no. 2, pp. 371–402, 1994.

[14] G. G. Triants, "Financial contract design in the world of venture capital," *Chicago Law Review*, vol. 68, 2001.

[15] D. J. Cumming and J. G. MacIntosh, "Venture capital investment duration in Canada and the United States," *Journal of Multinational Financial Management*, vol. 11, no. 4-5, pp. 445–463, 2001.

[16] J. K. Smith and R. L. Smith, *Entrepreneurial Finance*, John Wiley & Sons, 2000.

[17] P. Gompers, "Optimal investment, monitoring, and the staging of venture capital," *Journal of Finance*, vol. 50, no. 5, pp. 1461–1489, 1995.

[18] F. Cornelli and O. Yosha, "Stage financing and the role of convertible delt," Working Paper Series, London Business School and Tel Aviv University, 1998.

[19] L. Yuexin, W. Gang, X. Haoqing et al., "A decision-making model on stage financing for smart transmission grid investment based on technology readiness," *Energy Procedia*, vol. 14, pp. 681–688, 2012.

[20] E. Rasmussen and R. Sørheim, "Obtaining early-stage financing for technology entrepreneurship: reassessing the demand-side perspective," *Venture Capital*, vol. 14, no. 2-3, pp. 77–89, 2012.

[21] X. Tian, "The causes and consequences of venture capital stage financing," *Journal of Financial Economics*, vol. 101, no. 1, pp. 132–159, 2011.

[22] C. M. Boyer, "Early stage financing of clean technology industries: does private equity backing matter?" *Journal of Private Equity*, vol. 14, no. 4, pp. 73–78, 2011.

[23] R. Inderst and H. M. Mueller, "Early-stage financing and firm growth in new industries," *Journal of Financial Economics*, vol. 93, no. 2, pp. 276–291, 2009.

[24] S. Nouira, M. Klofsten, and D. Lindholm, "The logic of the entrepreneur: implications of the entrepreneur's perception of early-stage financing," *The International Journal of Entrepreneurship and Innovation*, vol. 6, no. 2, pp. 85–96, 2005.

[25] E. Bauer and H. Burghof, "The economics of state subsidies in early stage financing," *International Journal of the Economics of Business*, vol. 14, no. 3, pp. 433–457, 2007.

[26] D. Valliere, "Quality signals in early-stage venture capital markets," *International Journal of Entrepreneurial Venturing*, vol. 4, no. 3, pp. 199–213, 2012.

[27] H. Berglund, "Early stage venture capital investing: comparing California and Scandinavia," *Venture Capital*, vol. 13, no. 2, pp. 119–145, 2011.

[28] S.-H. Chen, "Empirical research on knowledge integration improving innovation ability of IT enterprise—based on structural equation model," *Information*, vol. 14, no. 3, pp. 753–758, 2011.

[29] H. Wei, "China's technology innovation strategy from technology transfer perspective," *Information*, vol. 15, no. 11, pp. 4841–4846, 2012.

[30] D. Engel and M. Keilbach, "Firm-level implications of early stage venture capital investment: an empirical investigation," *Journal of Empirical Finance*, vol. 14, no. 2, pp. 150–167, 2007.

[31] J.-E. Guo, W.-J. Yan, and G.-X. Zhang, "Stage investment cost and adding investment triggers in venture capital," *Systems Engineering—Theory and Practice*, vol. 28, no. 8, pp. 38–43, 2008.

[32] S.-H. Chen, "A novel culture algorithm and it's application in knowledge integration," *Information*, vol. 15, no. 11, pp. 4847–4854, 2012.

[33] H. van Auken, "A model of community-based venture capital formation to fund early-stage technology-based firms," *Journal of Small Business Management*, vol. 40, no. 4, pp. 287–301, 2002.

[34] R. Gerrard, M. Guillén, J. P. Nielsen, and A. M. Pérez- Marín, "Long-run savings and investment strategy optimization," *The Scientific World Journal*, vol. 2014, Article ID 510531, 13 pages, 2014.

[35] J. Xu and C. Feng, "Multimode resource-constrained multiple project scheduling problem under fuzzy random environment and its application to a large scale hydropower construction project," *The Scientific World Journal*, vol. 2014, Article ID 463692, 20 pages, 2014.

[36] Z. Jin-Long and C. Tao, "Hedging risks in software projects though staging strategy: real options analyses," *Journal of Wuhan University of Technology*, vol. 29, no. 3, pp. 84–87, 2007.

[37] E. H. Wang and M.-T. Wang, "Prioritizing the investment of research and development in the construction industry using strategic mapping technique," *Information*, vol. 14, no. 8, pp. 2685–2700, 2011.

[38] H. Wei, "An inventory controlled supply chain model based on improved BP neural network," *Discrete Dynamics in Nature and Society*, vol. 2013, Article ID 537675, 7 pages, 2013.

[39] R. Geske, "The valuation of compound options," *Journal of Financial Economics*, vol. 7, no. 1, pp. 63–81, 1979.

Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 348305, 13 pages
http://dx.doi.org/10.1155/2014/348305

Research Article

Advanced Approach to Information Security Management System Model for Industrial Control System

Sanghyun Park and Kyungho Lee

Center for Information Security Technologies (CIST), Korea University, Seoul 136-713, Republic of Korea

Correspondence should be addressed to Kyungho Lee; kevinlee@korea.ac.kr

Received 13 April 2014; Accepted 6 June 2014; Published 21 July 2014

Academic Editor: Sang-Soo Yeo

Organizations make use of important information in day-to-day business. Protecting sensitive information is imperative and must be managed. Companies in many parts of the world protect sensitive information using the international standard known as the information security management system (ISMS). ISO 27000 series is the international standard ISMS used to protect confidentiality, integrity, and availability of sensitive information. While an ISMS based on ISO 27000 series has no particular flaws for general information systems, it is unfit to manage sensitive information for industrial control systems (ICSs) because the first priority of industrial control is safety of the system. Therefore, a new information security management system based on confidentiality, integrity, and availability as well as safety is required for ICSs. This new ISMS must be mutually exclusive of an ICS. This paper provides a new paradigm of ISMS for ICSs, which will be shown to be more suitable than the existing ISMS.

1. Introduction

In general information systems, almost all security groups use the international information security management system (ISMS) standard which is ISO 27000 series. ISO 27000 series focuses on protection of confidentiality, integrity, and availability of information [1–3]. This ISMS is appropriate for general information systems, where the main threats are dynamic and variable, like malicious hacking.

However, industrial control systems (ICSs) are different from general information systems. While protection from dynamic, variable threats is important on an ICS, safety is most crucial in industrial control [4–6].

When national infrastructures, like nuclear power plants, deploy an ICS, the ICS is evaluated on the basis of safety [7]. In the field, safety is evaluated by IEC 61508 and IEC 61511. IEC 61508 is the international standard for Functional Safety of Electrical-Electronic-Programmable Electronic Safety-Related Systems and IEC 61511 is the technical standard that defines practices in the engineering of systems that ensures safety of an industrial process (see Figure 1).

ISMS is based on confidentiality, integrity, and availability, and the security needs of ICS are not mutually exclusive because the nature of such businesses is different from general information systems. ICS is of significance in the control of national infrastructures. These systems have unquestionable value, and they must be safe [7, 8]. For this reason, ICSs require safety first, rather than other ISMS based attributes. In the field, process owners for ICSs in fact follow the safety standards IEC 61508 and IEC 61511.

In short, it should be configured to a new ISMS based on views of confidentiality, integrity, and availability, as well as safety (see Figure 2).

The ISMS is framework which has presented three views which are confidentiality, integrity, and availability to protect information [1]. However, this paper casts doubt on sufficiency for the three views of existing ISMS to protect assets from internal and external threats and vulnerabilities in ICS.

In case of ICS, social impact due to threats and vulnerabilities like hacking, natural disaster, and internal problems for system cannot compare with general information systems and has great damage that brings out severe economic and social dislocation [4, 5, 8]. Thus, safety becomes the main keyword in ICS.

The requirements of IEC 61511 are based on safety, whereas the requirements and controls of ISO 27001 and

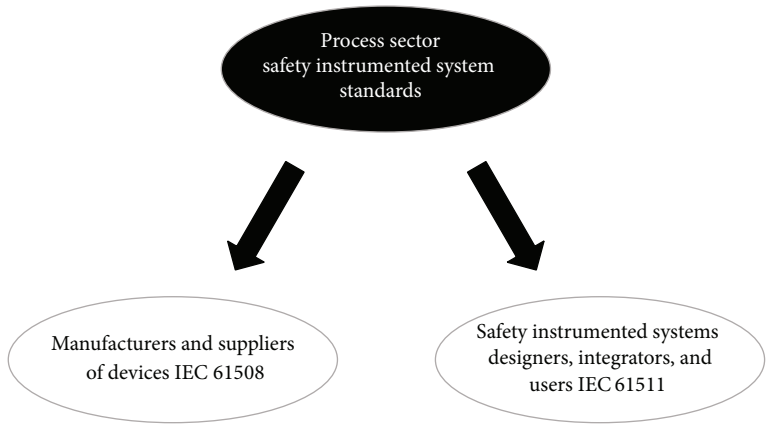


Figure 1: Relationship between IEC 61508 and IEC 61511.

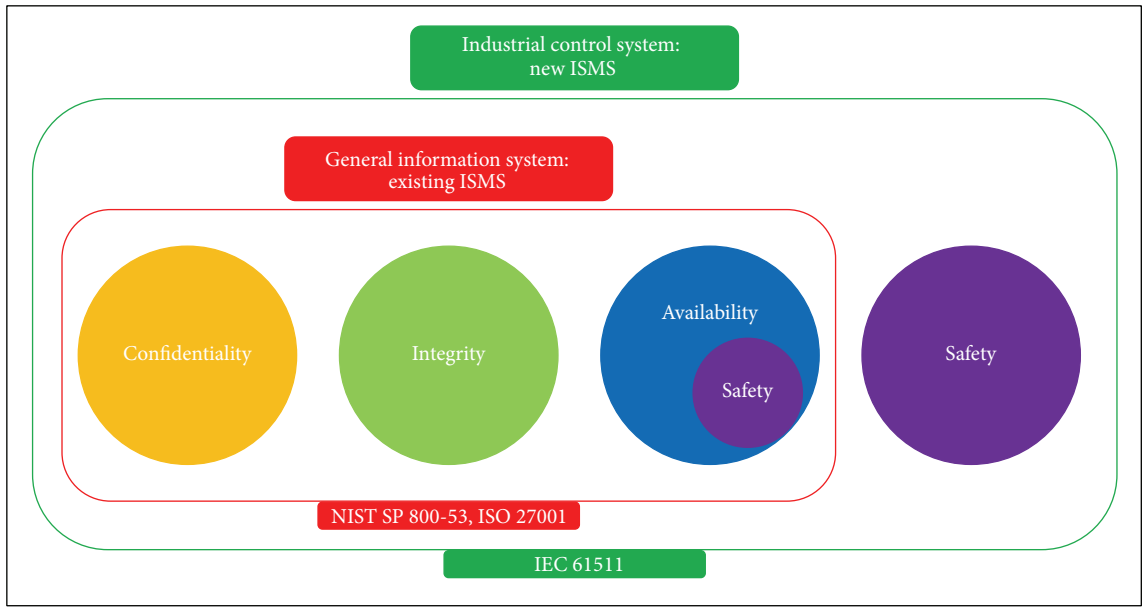


Figure 2: The goal of new information security management system for industrial control system.

NIST SP 800-53 are based on confidentiality, integrity, and availability [7]. When it comes to the safety in ISO 27001 and NIST SP 800-53, it is just a part of availability, so the safety of IEC 61511 is different from the safety of NIST SP 800-53 and ISO 27001.

As a result, this paper suggests that safety presented IEC 61511 should be considered as a part of new ISMS with confidentiality, integrity, and availability. The reason is that information in ICSs could be exposed, leaked, or tweaked if internal safety for system is not guaranteed for unexpected environmental changes like fluctuation of temperature and humidity in ICSs and absence of safety from external threats and vulnerabilities like hacking and natural disaster have a great ripple effect socioeconomically [8, 9].

Therefore, safety should be acknowledged as essential value in ISMS of equal level with confidentiality, integrity, and availability in ICS.

In order to prove this point, we will compare and analyze security controls or requirements of three international standards, namely, ISO 27001, NIST SP 800-53, and IEC 61511. If the safety requirements of IEC 61511, which is followed by people in the ICS field, barely match the security controls that include 21 requirements of ISO 27001, or the security controls of NIST SP 800-53, the ISMS for ICSs, in its present form, is faulty and ineffective [1, 10, 11].

This paper will also compare and analyze common security controls of NIST SP 800-53 that were successfully carried out by the South Korea energy group (thermal, gas, nuclear, combined cycle, electricity, and power exchange) using safety requirements of IEC 61511. The reason for using common security controls to compare with requirements of IEC 61511 is that common security controls are sufficient for every ICS, regardless of the specific application. For these reasons, comparing common security controls and safety

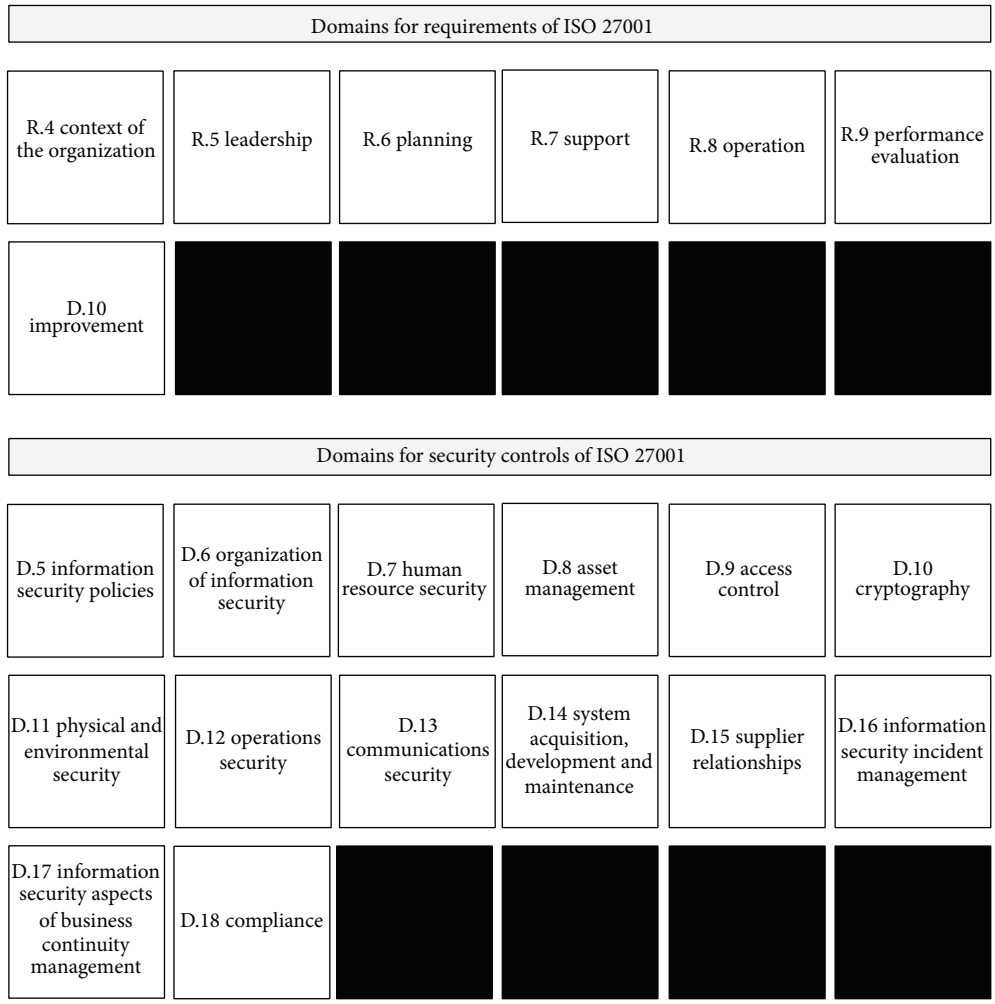


Figure 3: Domains for security controls and requirements of ISO 27001.

requirements of IEC 61511 is essential to further generalize this for every ICS. If the result of matching is the same with the above result of comparison for safety requirements of IEC 61511, security controls of ISO 27001, and security controls of NIST Special Publication 800-53, this analysis can also prove that the ISMS is presently faulty and ineffective in a general ICS environment. In other words, the ISMS that focuses on confidentiality, integrity, and availability of information based on ISO 27000 series is unfit to manage sensitive information on an ICS.

2. Introduction of Control Sets for ISO 27001, NIST SP 800-53, and IEC 61511

2.1. Domains for Security Controls and Requirements of ISO 27001. ISO 27001 is a document published by ISO and IEC on information technology-security techniques-information security management system-requirements. This document specifies the requirements and security controls for establishing, implementing, maintaining, and continually improving an ISMS within the context of the organization. The security controls presented by ISO 27001 are composed of 34 subdomains in 14 domains. The total number of security controls, which includes 21 requirements, is 140 pieces. The domains for security controls and requirements of ISO 27001 are presented in Figure 3 [1].

2.2. Domains for Security Controls of NIST SP 800-53. The NIST Special Publication 800-53 is a document published by NIST for Recommended Security Controls in Federal Information Systems and Organizations. This document especially recommends security controls for ICSs. The recommended security controls are composed of 90 subdomains in 17 domains. The total number of controls is 186 pieces. The domains for recommended security controls are shown in Figure 4 [10].

2.3. Domains for Safety Requirements of IEC 61511. IEC 61511 is a technical standard used in the engineering of systems, and it ensures the safety of an industrial process.

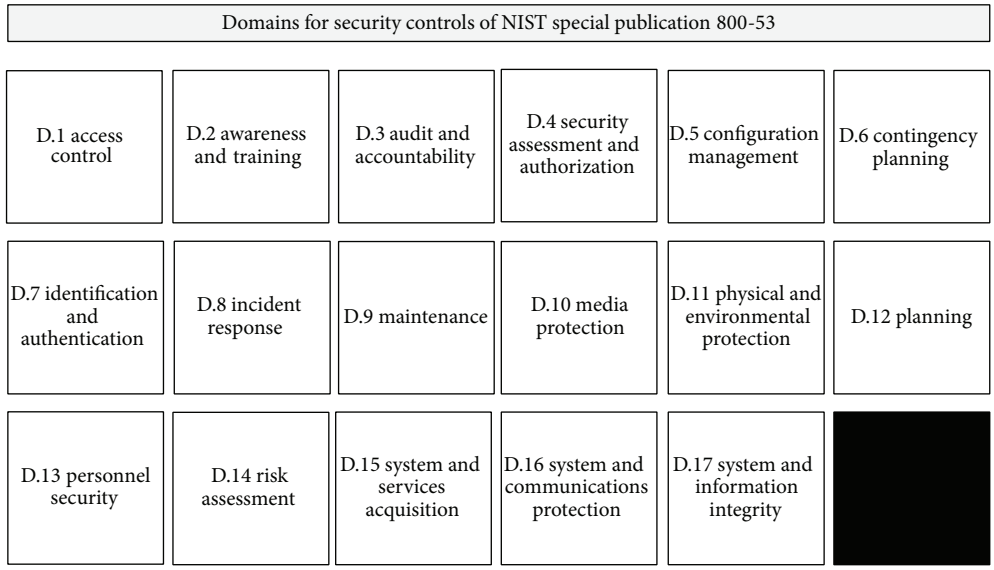


Figure 4: Domains for security controls of NIST SP 800-53.

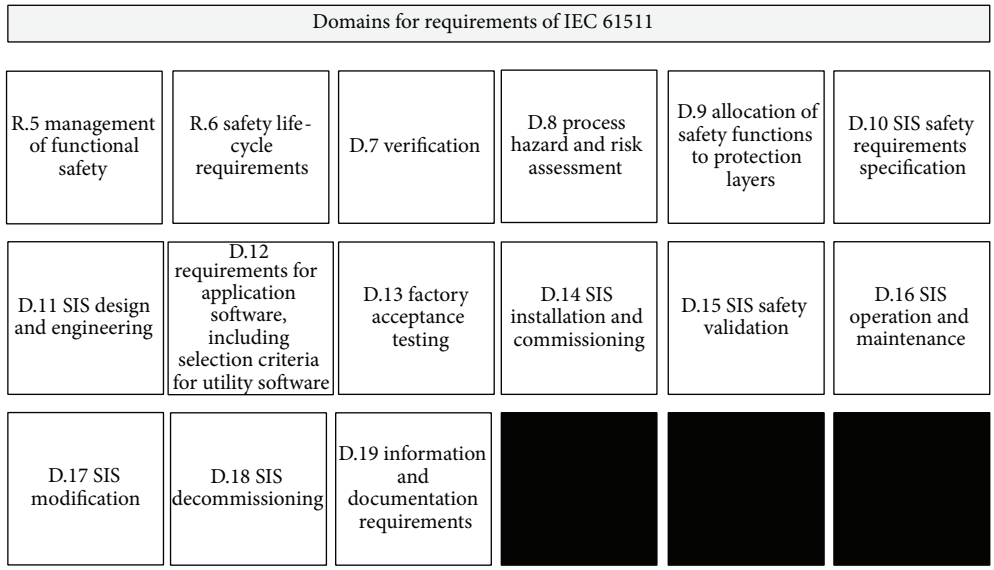


Figure 5: Domains for safety requirements of IEC 61511.

IEC 61511 consists of 3 chapters. The first chapter is called "framework, definitions, system, hardware and software requirements"; the second chapter is called "guidelines for the application of IEC 61511-1"; and the third chapter is called "guidance for the determination of the required safety integrity levels." The safety requirements of IEC 61511 are divided into five safety parts and the safety parts consist of development, allocation, design, installation, commissioning, validation, operation, modification, and decommissioning for an ICS. The safety requirements of IEC 61511 are composed of 15 domains and the total number of controls is 215 pieces. The domain for requirements and overall framework of IEC 61511 are shown in Figures 5 and 6 [7].

3. Matching Analysis for Security Controls and Requirements of International Standards

Each part of IEC 61511 has several requirements that include the security controls of NIST SP 800-53 or the security controls of ISO 27001.

In order to prove this point, we compare and analyze the security controls/requirements of three international standards, namely ISO 27001, NIST SP 800-53, and IEC 61511, below.

3.1. Preparation of Matching Analysis for Security Controls and Requirements of International Standards. We present a comparative security controls list for IEC 61511, ISO 27001,

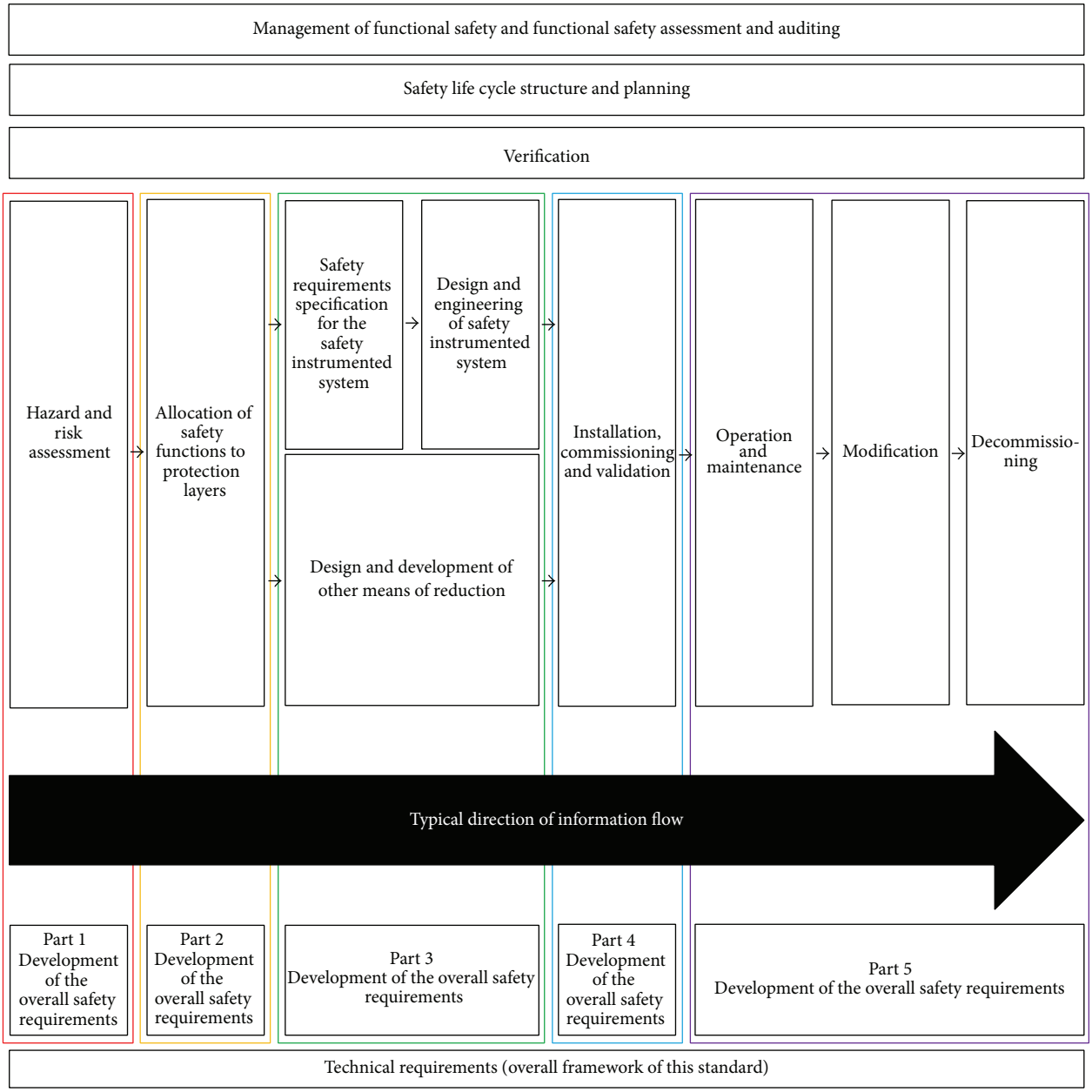


Figure 6: Overall framework of IEC 61511.

and NIST SP 800-53. The example for list up is presented in Table 1 [1, 7].

3.2. Result of Matching Analysis for Security Controls and Requirements of International Standards. In order to find out whether security controls for international standards match, we compare the requirements of IEC 61511 with security controls of NIST SP 800-53 and security controls of ISO 27001.

There are two results based on this comparison. Firstly, the percentage of matching security controls of ISO 27001 with safety requirements of IEC 61511 is 15%. Specifically, the total number of security controls for ISO 27001 is 140 pieces and 21 pieces of these matched with safety requirements of IEC 61511.

Secondly, the percentage of matching security controls for NIST SP 800-53 with safety requirements of IEC 61511 is 16.49%. Specifically, the total number of security controls of NIST SP 800-53 is 194 pieces and 34 pieces of these matched with safety requirements of IEC 61511.

In short, the percentage of matching requirements of IEC 61511, with both security controls of NIST SP 800-53 and security controls of ISO 27001, is quite low. These results mean that ISMS based on ISO 27001 or NIST SP 800-53 is insufficient for a real industrial control system's environment

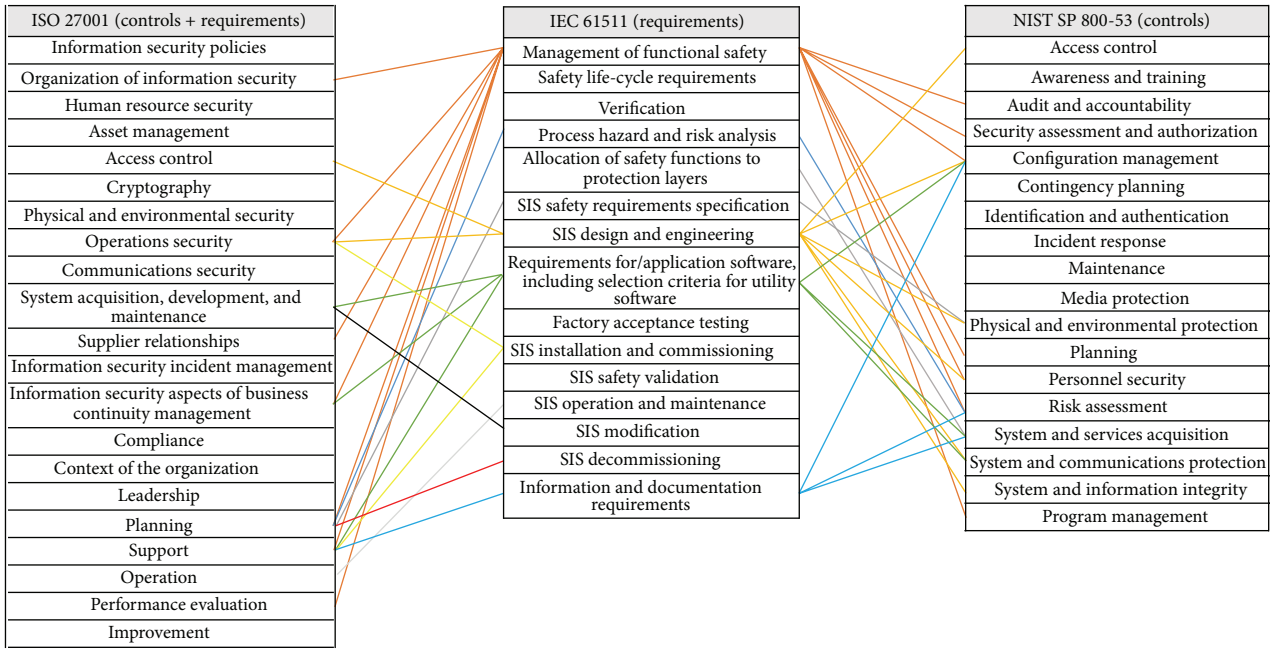


Figure 7: The matching for domains of international standards.

Table 1: The example of security controls list up for international standard.

Domain number	IEC 61511	Domain number	ISO 27001
5.2.2.1	Persons, departments, organizations, or other units which are responsible for carrying out and reviewing each of the safety life-cycle phases shall be identified and be informed of the responsibilities assigned to them (including, where relevant, licensing authorities or safety regulatory bodies).	A.6.1.1	All information security responsibilities shall be defined and allocated.

because the ISMS does not reflect specificity for the nature of ICS. The specificity is safety, which is a core value on the IEC 61511 (see Table 2 and Figure 7).

3.3. Extracting Items from IEC 61511 to Append New ISMS. The extracting items from IEC 61511 to append new ISMS are selected by certain conditions as follows. The first step is to choose nonmatching requirements of all for IEC 61511 with requirements and controls for NIST SP 800-53 and ISO 27001. The next step is to choose general requirements in each ICS life-cycle types of the nonmatching requirements for IEC 61511 with requirements and controls of NIST SP 800-53 and ISO 27001 and the general requirements are the extracting items. The reason to select general requirements of nonmatching requirements is to maintain a level of requirements and controls with ISO 27001 and NIST SP 800-53 and assure safety for new ISMS [12, 13].

The recommended extracting items of safety from IEC 61511 to develop new ISMS are shown in Table 3.

This paper presents that the safety has two meanings broadly. The first meaning is safety against external factors like hacking and natural disaster; another is safety against internal factors like internal failure for system.

The requirements of IEC 61511 and the requirements of ISO 27001 and NIST SP 800-53 do not present direct requirements against internal and external threats and vulnerabilities to hinder safety in ICS. Instead, requirements of IEC 61511 present safety requirements in each ICS life-cycle types that guarantee safety from the internal and external threats and vulnerabilities, and the safety requirements aim to improve safety for ICS that is core to manage well risk from the internal and external threats and vulnerabilities.

4. Matching Analysis for Common Security Controls of NIST SP 800-53 in South Korea Energy Industry and Safety Requirements of IEC 61511

Each part of IEC 61511 has several requirements that include the security controls of NIST SP 800-53. In this section, we will not compare and analyze whole security controls of international standards, but instead we will compare and analyze common security controls of NIST SP 800-53 that were successfully carried out by the South Korea energy group (thermal, gas, nuclear, combined cycle, electricity, and

Table 2: The matching analysis for requirements or security controls of international standards.

	Comparison targets	
	ISO 27001	NIST SP 800-53
The total number of security controls and requirements	140 (requirements: 21, security controls: 114)	194
The total number of matching security controls for comparison target with safety requirements of IEC 61511	21	32
The percentage of matching security controls for comparison target with safety requirements of IEC 61511	15%	16.49%

Table 3: The example of recommended extracting items from IEC 61511.

	Recommended extracting items
IEC 61511	The safety requirements shall be derived from the allocation of safety instrumented functions and from those requirements identified during safety planning.
	The need for a factory acceptance testing should be specified during the design phase of a project.
	Installation and commissioning planning shall define all activities required for installation and commissioning.
	The planning shall provide the following: (i) the installation and commissioning activities; (ii) the procedures, measures, and techniques to be used for installation and commissioning; (iii) when these activities shall take place; (iv) the persons, departments, and organizations responsible for these activities.
	Installation and commissioning planning may be integrated in the overall project planning where appropriate.
	The validation of the safety instrumented system and its associated safety instrumented functions shall be carried out in accordance with the safety instrumented system validation planning.
	⋮
	Discrepancies between expected behaviour and actual behaviour of the SIS shall be analysed and, where necessary, modifications made such that the required safety is maintained. This shall include monitoring the following: (i) the actions taken following a demand on the system; (ii) the failures of equipment forming part of the SIS established during routine testing or actual demand; (iii) the cause of the demands; (iv) the cause of false trips.
	The procedures shall include a clear method of identifying and requesting the work to be done and the hazards which may be affected (modification and decommissioning).
	Modification shall be performed with qualified personnel who have been properly trained. All affected and appropriate personnel should be notified of the change and trained with regard to the change.

power exchange) with safety requirements of IEC 61511. This is because entire security controls of NIST SP 800-53 do not apply to the South Korea energy group.

In order to find out the common security controls from the entire security controls of NIST SP 800-53, we constructed evaluation frame that has security controls of NIST SP 800-53. We asked the South Korea energy group, that is, power exchange, electricity, gas, combined cycle, nuclear, and thermal groups, to fill out a questionnaire [10, 11, 14] (see Table 4).

4.1. The Data Gathering to Find Out Common Security Controls of NIST SP 800-53 in South Korea Energy Industry. In order to gather data, we drew up an evaluation sheet for the security controls based on the NIST Special Publication 800-53 that includes security guidance and recommends security controls for ICSs [15–18].

The evaluation sheet is shown in Figure 8.

Answers for each item are classified as yes, no, partial, and N/A. Developers, operators of energy management system, and process owners filled up the questionnaire.

4.2. The Result for Common Security Controls of NIST SP 800-53 in South Korea Energy Industry. We compared and analyzed the current security controls status for the South Korea energy group (thermal, gas, nuclear, combined cycle, electricity, and power exchange) and then collected a common security controls mean, that is, controls for every South Korea group to carry out successfully. The common security controls are as show in Table 5.

4.3. Results of Matching Analysis for Common Security Controls of NIST SP 800-53 in South Korea Energy Groups and Requirements IEC 61511. The safety requirements of IEC

Table 4: The domain and subdomain of NIST SP 800-53 for an ICS.

Domain	Subdomain
D.1 Access Control	D.1.2 Account Management
	D.1.3 Access Enforcement
	D.1.5 Separation of Duties
	D.1.6 Least Privilege
	D.1.7 Unsuccessful Login Attempts
	D.1.8 System Use Notification
	D.1.10 Concurrent Session Control
	D.1.11 Session Lock
	D.1.17 Remote Access
	D.1.18 Wireless Access
	D.1.19 Access Control for Mobile Devices
	D.1.22 Publicly Accessible Content
D.2 Awareness and Training	D.2.2 Security Awareness
	D.2.3 Security Training
D.3 Audit and Accountability	D.3.2 Auditable Events
	D.3.3 Response to Audit Processing Failures
	D.3.4 Audit Reduction and Report Generation
	D.3.5 Audit Generation
D.4 Security Assessment and Authorization	D.4.2 Security Assessments
	D.4.7 Continuous Monitoring
D.5 Configuration Management	D.5.3 Configuration Change Control
	D.5.4 Security Impact Analysis
	D.5.5 Access Restrictions for Change
	D.5.6 Configuration setting
	D.5.7 Least Functionality
D.6 Contingency Planning	D.6.2 Contingency Plan
	D.6.4 Contingency Plan Testing and Exercises
	D.6.10 Information System Recovery and Reconstitution
D.7 Identification and Authentication	D.7.2 Identification and Authentication (Organizational Users)
	D.7.3 Device Identification and Authentication
	D.7.4 Identifier Management
	D.7.5 Authenticator Management
	D.7.7 Cryptographic Module Authentication
D.8 Incident Response	D.8.6 Incident Reporting
D.9 Maintenance	D.9.4 Non-Local Maintenance
D.10 Media Protection	D.10.5 Media Transport
D.11 Physical and Environmental Protection	D.11.3 Physical Access Control
D.12 Planning	D.12.2 System Security Plan
D.14 Risk Assessment	D.14.2 System Categorization
	D.14.3 Risk Assessment
	D.14.5 Vulnerability Scanning
D.15 System and Services Acquisition	D.15.4 Acquisitions
	D.15.8 Security Engineering Principles
D.16 System and Communications Protection	D.16.2 Application Partitioning
	D.16.3 Security Function Isolation
	D.16.7 Boundary Protection
	D.16.8 Transmission Integrity
	D.16.9 Transmission Confidentiality
	D.16.10 Network Disconnect
	D.16.12 Cryptographic Key Establishment and Management
	D.16.13 Use of Cryptography
	D.16.14 Public Access Protections
	D.16.15 Collaborative Computing Devices
	D.16.19 Voice Over Internet Protocol
	D.16.20 Secure Name/Address Resolution Service (Authoritative Source)
	D.16.21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)
	D.16.22 Architecture and Provisioning for Name/Address Resolution Service
	D.16.23 Session Authenticity
D.17 System and Information Integrity	D.17.2 Flaw Remediation
	D.17.3 Malicious Code Protection
	D.17.4 Information System Monitoring
	D.17.6 Security Functionality Verification
	D.17.7 Software and Information Integrity
	D.17.8 Spam Protection

61511 match common security controls of NIST SP 800-53. In fact, it may be more difficult to match the safety requirements of IEC 61511 with common security controls of NIST SP 800-53 due to the nature of the standard. The standard generalizes requirements, while the value for common security controls of NIST SP 800-53 compare well enough with the safety requirements of IEC 61511 (see Table 6).

It is difficult to match common security controls of NIST SP 800-53 with safety requirements of IEC 61511 perfectly; however, the safety requirements of IEC 61511 match with common security controls. In other words, it is not hard to include safety as an ICS attribute.

Table 5: The List of Common Security Controls in South Korea Energy Industry for NIST SP 800-53.

Number	Main domain name	Subdomain name	Code of security control	Security control
1	Access control	Account management	AC-2	The organization manages information system accounts, including identifying account types.
2		Separation of duties	AC-5	The organization implements separation of duties through assigned information system access authorizations.
3		Least privilege	AC-6	The organization employs the concept of least privilege, allowing only authorized accesses for users which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
4	Media protection	Media access	MP-2	The organization restricts access to [Assignment: organization-defined types of digital and non-digital media] to [Assignment: organization-defined list of authorized individuals] using [Assignment: organization-defined security measures].
5		Media marking	MP-3.a	The organization marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.
6			MP-3.b	The organization exempts [Assignment: organization-defined list of removable media types] from marking as long as the exempted items remain within [Assignment: organization-defined controlled areas].
7		Media storage	MP-4.a	The organization physically controls and securely stores [Assignment: organization-defined types of digital and non-digital media] within [Assignment: organization-defined controlled areas] using [Assignment: organization-defined security measures].
8			MP-4.b	The organization protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
9		Media transport	MP-5.a	The organization protects and controls [Assignment: organization-defined types of digital and non-digital media] during transport outside of controlled areas using [Assignment: organization-defined security measures].
10			MP-5.c	The organization restricts the activities associated with transport of such media to authorized personnel.

Table 5: Continued.

Number	Main domain name	Subdomain name	Code of security control	Security control
11	Physical and environmental protection	Physical access authorizations	PE-2	The organization develops and keeps a current list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible).
12		Monitoring physical access	PE-6.a	The organization monitors physical access to the information system to identify and respond to physical security incidents.
13			PE-6.b	The organization reviews physical access logs [Assignment: organization-defined frequency].
14		Visitor control	PE-7	The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides, other than areas designated as publicly accessible.
15		Emergency shutoff	PE-10	The organization provides the capability of shutting off power to the information system, or individual system components, in emergency situations.
16		Emergency lighting	PE-12	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.
17		Fire protection	PE-13	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.
18		Temperature and humidity controls	PE-14	The organization maintains temperature and humidity levels within the facility where the information system resides at [Assignment: organization-defined acceptable levels].
19		Water damage protection	PE-15	The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.
20		Location of information system Components	PE-18	The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.
21	System and communications protection	Denial of service protection	SC-5	The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list].
22		Boundary protection	SC-7.a	The information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.
23			SC-7.b	The information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Table 6: Comparison for common security controls of NIST SP 800-53 and safety requirements of IEC 61511.

Number	Main domain name	Code of security control for common security controls in South Korea Energy Industry	Safety requirements of IEC 61511
1	Access control	AC-2	⟨**R.11.7.2.4**⟩ Enabling and disabling the read-write access shall be carried out only by a configuration or programming process using the maintenance/engineering interface with appropriate documentation and security measures.
2		AC-5	
3		AC-6	
4	Media protection	MP-2	—
5		MP-3.a	
6		MP-3.b	
7		MP-4.a	
8		MP-4.b	
9		MP-5.a	
10		MP-5.c	
11	Physical and environmental protection	PE-2	⟨**D.11.2.11**⟩ For subsystems that on loss of power do not fail to the safe state, all of the following requirements shall be met and action taken according to 11.3: (i) loss of circuit integrity is detected (for example, end-of-line monitoring); (ii) power supply integrity is ensured using supplemental power supply (for example, battery back-up and uninterruptible power supplies); (iii) loss of power to the subsystem is detected.
12		PE-6.a	
13		PE-6.b	
14		PE-7	
15		PE-10	
16		PE-12	
17		PE-13	
18		PE-14	
19		PE-15	
20		PE-18	
21	System and communications protection	SC-5	⟨**D.11.7.3.3**⟩ The communication interface shall be sufficiently robust to withstand electromagnetic interference including power surges without causing a dangerous failure of the SIF.
22		SC-7.a	
23		SC-7.b	

The point of this paper is that the safety emphasized on IEC 61511 can reflect information security management system for ICS.

5. Conclusions

This paper presented two methodologies to prove that a new information security management system based on confidentiality, integrity, availability, and safety is required on the industrial control system.

The first methodology was analysis of matching security controls with international standards. From the first methodology, it was seen that the percentage of matching between the requirements of IEC 61511, the security controls of NIST SP 800-53, and the security controls of ISO 27001 is very low. These results mean that ISMS based on ISO 27001 or NIST SP 800-53 is insufficient to make for real ICSs because the ISMS does not reflect specificity of the nature of ICSs (see Figure 9).

The second methodology involved analysis of matching of the common security controls of NIST SP 800-53 that were successfully carried out by the South Korea energy group (thermal, gas, nuclear, combined cycle, electricity, and power exchange) with the safety requirements of IEC 61511. These results showed that it is difficult to match common security controls of NIST SP 800-53 in South Korea with safety requirements of IEC 61511 perfectly. However, the safety requirements of IEC 61511 match reasonably well with common security controls. In other words, it is not hard for safety to be included in an industrial control system.

The ICS is different from a general information system and an ISMS based on confidentiality, integrity, and availability never achieves mutually exclusive security policy for an ICS.

Just as integrity is significant for finance and confidentiality is significant for manufacturing, safety is significant for ICSs [3, 5, 6]. This paper proves that safety is very significant for ICSs, and safety should be included in an ISMS based on confidentiality, integrity, and availability of information.

In brief, a new ISMS based on confidentiality, integrity, and availability as well as safety is required in ICSs. This new information security management system is mutually exclusive to the nature of industrial control system.

We expect that the performance of information security for ICSs will be improved through our work.

Domain	Contents
D.1	Access control
D.1.2	Access control account management
Description of controls	◑ The control system that can not manage the account (e.g., remote terminal) is required to adopt a suitable alternative control.

Details code	Questions	Answer area						
		Control status (√)				Answer basis	Evidence	Location of evidence
		Yes	N/A	No	Partial			
D.1.2.2	Using, form (individuals, groups, and guests) for each account information has been identified in specific?	√				Identification is based on the command center information	The command center information security rules	The command center information security rules Article 8. Access control System number 43. User account management
		Cycle						
		Once a year						
		Opinion						

Figure 8: Example of an evaluation sheet.

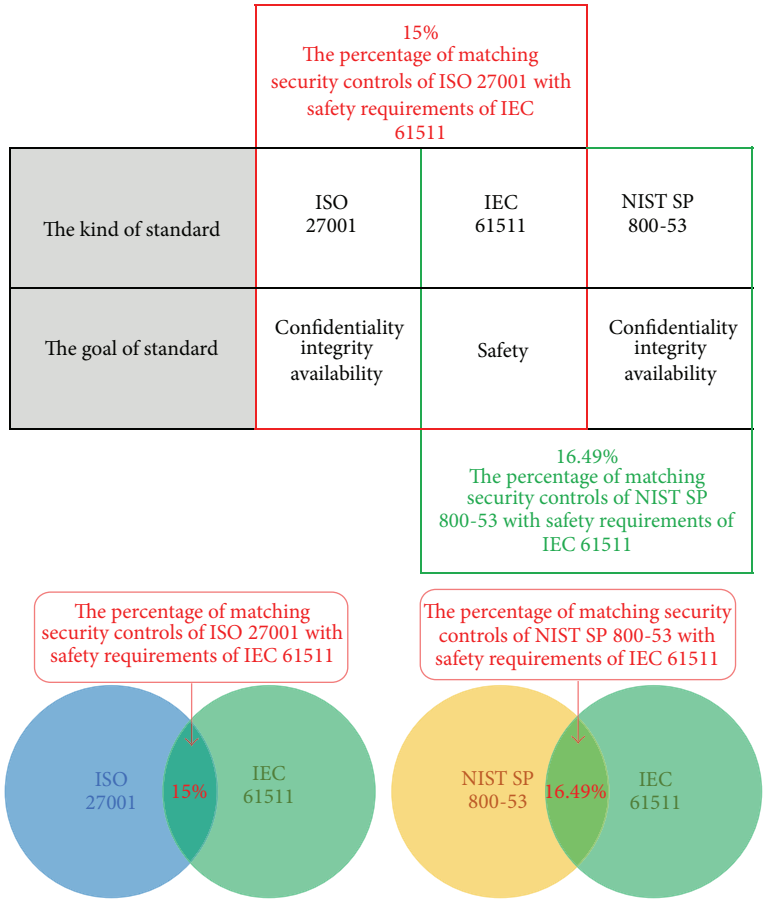


Figure 9: Comparative analysis for controls of international standards.

Conflict of Interests

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

Acknowledgment

This work was supported by a grant from Korea University.

References

[1] International Organization for Standardization, ISO 27001, 2013.

[2] K. Beckers, "Goal-based establishment of an information security management system compliant to ISO 27001," *Theory and Practice of Computer*, vol. 8327, pp. 102–113, 2014.

[3] E. Humphreys, "Information security management standards: compliance, governance and risk management," *Information Security Technical Report*, vol. 13, no. 4, pp. 247–255, 2008.

[4] X. Xu, "Global and initiative safety mechanism in industrial control system," *International Journal of Computational Science and Engineering*, vol. 9, no. 1-2, pp. 139–146, 2014.

[5] R. D. Larkin, J. Lopez Jr., J. W. Butts, and M. R. Grimaila, "Evaluation of security solutions in the SCADA environment," *ACM SIGMIS Database*, vol. 45, no. 1, pp. 38–53, 2014.

[6] I. N. Fovino, "SCADA system cyber security," in *Secure Smart Embedded Devices, Platforms and Applications*, pp. 451–471, Springer, 2014.

[7] International Electrotechnical Commission, IEC 61511-1, 2003.

[8] J. Weiss, "Industrial Control System (ICS) cyber security for water and wastewater systems," *Securing Water and Wastewater Systems*, vol. 2, pp. 87–105, 2014.

[9] T. Lu, "Cyberphysical security for industrial control systems based on wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 438350, 17 pages, 2014.

[10] National Institute of Standards and Technology, NIST Special Publication 800-53, 2009.

[11] "National Institute of Standards and Technology," NIST Special Publication 800-82, 2011.

[12] I. H. Al-Mayahi and S. P. Mansoor, "Information security policy development," *Journal of Advanced Management Science*, vol. 2, no. 2, pp. 135–139, 2014.

[13] F. Parra, "A nomological network analysis of research on information security management systems," in *Proceedings of the 47th Hawaii International Conference on System Sciences (HICSS '14)*, pp. 4336–4345, January 2014.

[14] J. Mun, "Security controls based on K-ISMS in cloud computing service," in *Advanced in Computer Science and Its Applications*, vol. 297, pp. 391–404, Springer, 2014.

[15] International Organization for Standardization, ISO 27004, 2009.

[16] National Institute of Standards and Technology, NIST Special Publication 800-55, 2007.

[17] R. Bojanc and B. Jerman-Blažič, "An economic modelling approach to information security risk management," *International Journal of Information Management*, vol. 28, no. 5, pp. 413–422, 2008.

[18] K. Farn, S. Lin, and A. R. Fung, "A study on information security management system evaluation—assets, threat and vulnerability," *Computer Standards & Interfaces*, vol. 26, no. 6, pp. 501–513, 2004.

Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 295789, 6 pages
http://dx.doi.org/10.1155/2014/295789

Research Article

Software Authority Transition through Multiple Distributors

Kyusunk Han[1] and Taeshik Shon[2]

[1] *University of Michigan, 500 S. State Street, Ann Arbor, MI 48109, USA*
[2] *Department of Information Computer Engineering, Ajou University, San 5, Woncheon-dong, Yeongtong-gu, Suwon 443-749, Republic of Korea*

Correspondence should be addressed to Taeshik Shon; tsshon@ajou.ac.kr

Received 4 June 2014; Accepted 2 July 2014; Published 20 July 2014

Academic Editor: Sang-Soo Yeo

The rapid growth in the use of smartphones and tablets has changed the software distribution ecosystem. The trend today is to purchase software through application stores rather than from traditional offline markets. Smartphone and tablet users can install applications easily by purchasing from the online store deployed in their device. Several systems, such as Android or PC-based OS units, allow users to install software from multiple sources. Such openness, however, can promote serious threats, including malware and illegal usage. In order to prevent such threats, several stores use online authentication techniques. These methods can, however, also present a problem whereby even licensed users cannot use their purchased application. In this paper, we discuss these issues and provide an authentication method that will make purchased applications available to the registered user at all times.

1. Introduction

In recent years, software distribution models have changed rapidly. Apple's *iOS Appstore* and *iTunes* made a significant change to the ecosystem of software and content distribution.

The convenience of these systems inspired other competitors and solutions. For mobile devices, for example, Google launched *Google Play* for their Android OS, and Amazon have developed their own *Amazon Appstore*. The success of these endeavors has influenced the PC-based OS software ecosystem. Microsoft has recently released *Windows Store* for Windows 8, and Apple has released *Mac Appstore*.

Whereas Apple's iOS only allows access to their built-in store, most distributors allow users other options. For example, the Android system allows access to Google's built-in store service as well as other mobile carriers' store services, even including those manually installed by the user. While users can purchase apps from the Windows and Mac appstores, they can also purchase them from other distributors or developers as well.

Although such market services provide significant convenience to users, they have introduced several issues. With the traditional software purchase environment, users could obtain product support regardless of where they purchased their applications. Users who purchase an application from a specific online appstore, however, cannot get support if they cancel or lose their connection to the store. Moreover, if an app requires an online authentication process to verify a valid license, the user will not even be able to launch the app.

In this paper, we discuss the software authorization issue and propose an extended "purchase authentication service" (PAS) model [1] that ensures users are authorized to access applications even if they change their status. Our extended PAS avoids the use of an independent system, which can cause overheads. We demonstrate two scenarios: (1) users are using a roaming service and (2) users permanently change their contact details.

We present an overview of the online application store model in Section 2. In Section 3, we discuss problems with application authorization. We then propose, in Section 4, an authentication protocol that allows a user to obtain authorization from multiple vendors. We then analyze the security of the model in Section 5 and conclude this paper in Section 6.

2. Online Application Store

Commercial consumer software was traditionally distributed as a package through offline markets. Users purchased an

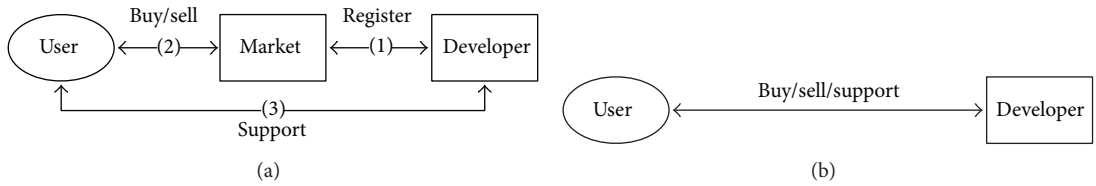


Figure 1: Traditional distribution—(a) individual markets; (b) direct from developers.

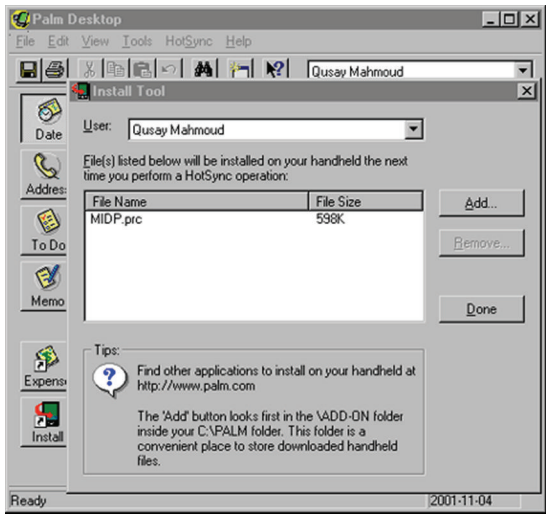


Figure 2: Application management in Palm OS. Legacy devices needed to connect to a PC to install mobile applications.

application from either (a) individual markets or (b) developers directly, as shown in Figure 1. When digital download services were introduced, users could still purchase from either source and receive support for that application by directly contacting the developer.

Conventional markets, however, must address the following two issues: *license management* and *software installation*. For license management, users purchasing from a web-market could download the application directly from the specific website. For authorization, users received license codes through emails or receipts. Users had to keep or request new license codes from distributors when they were required to reinstall the app.

The mobile handset market, in addition to the PC market, also provided digital download services. For example, legacy mobile devices, such as those based on *Palm OS* and *Windows CE*, widely used until the late 2000s, enabled users to install any application they chose to their devices.

The installation process, however, was not convenient. Figure 2 shows an example of installing an application on a *Palm OS*-based device. To install an application, users had to manage a desktop application that synchronized with the mobile device.

Although later Wi-Fi-enabled devices could download and install applications without desktop tools, the purchase and authorization process remained the same as shown in Figure 1. Users still managed their license codes themselves.

2.1. Online Application Stores. Online application stores (OASs) provide users with easier license and application code management. When a user purchases an app from an OAS, it requires only one click to install, reinstall, or update the app. In fact, the market share of *Palm OS*, *Windows CE*, and even *Symbian OS* quickly decreased once Apple launched the *Appstore* for *iPhone*. OASs are not only used with mobile devices. PC environments, including Windows and Mac OS X, and software distributors such as Amazon are rapidly deploying market services, as shown in Figure 3.

Multiple OASs are often preinstalled or installed by users on their devices and systems. By connecting to an OAS, a user can easily purchase applications. When a user needs support, they can easily get updates from their application provider, as shown in Figure 4.

2.2. Types of OAS User Registration. We separate OASs into the three groups discussed in [1]: OAS from OS holder (Type 1), OAS from Content distributor (Type 2), and OAS from mobile carriers (Type 3).

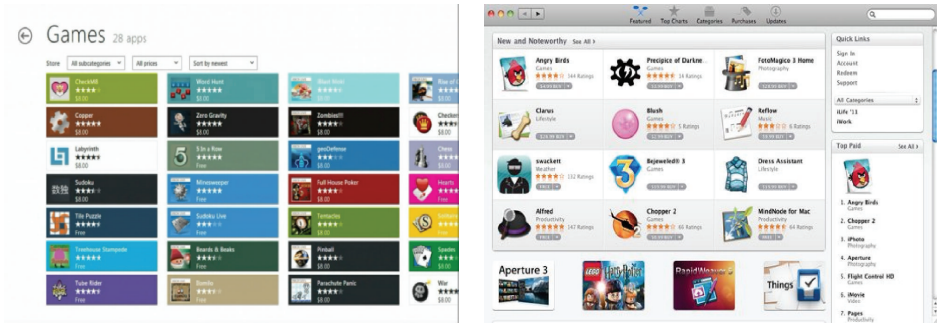
(i) Type 1: the store application is preinstalled on the device. Users register their accounts with the service. To purchase applications, users must also register their billing information. Depending on the billing information or location information, the store can provide localized services. Microsoft's *Windows Store*, Apple's *Appstore*, the Ubuntu *Software Center*, and *Google Play* are examples.

(ii) Type 2: users manually install the store application on their device. Users register their accounts. To purchase applications, users must also register their billing information. Stores authenticate users with the billing information. *Amazon Appstore* and *Steam Online* are examples.

(iii) Type 3: mobile carriers/manufacturers preinstall their own OASs on the device. Mobile users are already registered through their carrier subscription information. The store verifies the information from the USIM in the device. Only subscribed devices can use the service. Users must be connected to the cellular network.

3. Application Management from Multiple OASs

In this section, we discuss issues with application management from multiple OASs and extend the PAS introduced in [1] to overcome such issues.



(a) (b)

Figure 3: (a) Windows marketplace (b) Mac Appstore.

Figure 4: Online application distribution.

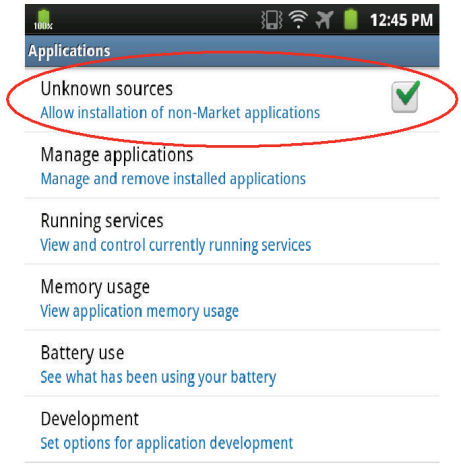


Figure 5: Android OS allows unauthorized applications.

3.1. Application Management from Multiple OASs

3.1.1. Software License Check Problem. Software piracy has long been a serious security problem. Many proposals [2–4] have attempted to prevent this problem by the use of a software license confirmation. They focus on the verification of the validity of the software license from the original source.

For example, the Android system enables anyone to develop and distribute Android software. It uses the Android application package file (APK) format to distribute and install applications and middleware to the device. Although the Android system initially demands that all applications be signed by the application developer to ensure the trust of the applications, installing unauthorized applications manually is also allowed, as shown in Figure 5. This openness permits the illegal distribution of cracked applications and malware (Graham Cluley, "Android malware poses as Angry Birds Space game," NakedSecurity, SophosLab April 12, 2012) to the Android system [5].

Therefore, many researchers have focused on prevention mechanisms against such threats [6–9], including online authentication. Such authentication systems, however, can decrease the availability of applications.

While many vendors do deploy online authentication systems, Type 3 distributors generally use an authentication process via a wireless network. For example, Korean local distributors, including *SKT T-store* and *KT Olleh market*, commonly utilize users' subscribed information in the USIM over the cellular network. When a user launches an application, they must be connected to the network. Those who are not connected to the network via a cellular connection fail to be authenticated.

3.1.2. Software Support without Original OAS. In the traditional application distribution environment shown in Figure 1, stores only provide applications to users. Users then contact the developers directly for support. Although this is not a very convenient process, once a user has purchased an application, they can obtain continued support from the developer.

In contrast, in the current distribution process shown in Figure 4, OASs not only sell applications but also provide support to users. Although such a mechanism brings huge convenience to users, they must maintain their connection to the store to receive this support. A user who cannot contact the store will fail to get further support and must purchase the same application again, from a different store that he can contact. This generally occurs for Types 2 and 3 cases, where the OAS only provides service for the localized domain.

3.1.3. OAS Management Problem. OAS users can purchase software from multiple OASs, as shown in Section 2.2. This can cause problems with verifying the license. Although allowing multiple OASs in a device allows users to choose their preferred service, any OAS that a user contacts can manage the software. Whereas legacy distribution systems allow users to get software support, regardless of where the application was purchased, OAS users can only get support from the OAS from whom they made their purchase.

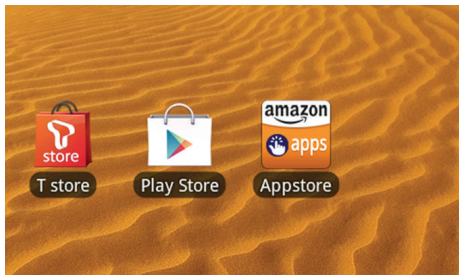


Figure 6: An example of various OASs in one mobile device: *SKT T-store* (Type 3), *Google Play store* (Type 1), and *Amazon Appstore* (Type 2).

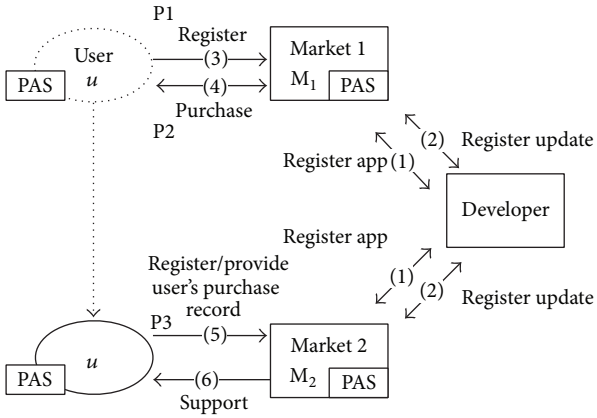


Figure 7: System model.

Therefore, OAS users who purchase apps from multiple OASs must manage multiple OAS systems in the device, as shown in Figure 6. This increases the management overhead, especially to mobile device users.

3.2. PAS Model. In order to resolve the issues discussed above, we propose a PAS model. This enables users who have already purchased applications to receive support when they change their status or cannot reach the original OAS, temporarily or permanently [1]. We define the PAS as a trusted entity that stores users' purchase records. We have limited the functionality of the PAS model to the mobile environment.

4. Improved PAS Model

Maintaining an additional trusted entity for the PAS could increase the management overhead. In this paper, therefore, we extend the model by adding a PKI feature and modify the PAS as a part of this service. This does not require an additional entity, and hence there are no additional management issues. When a user purchases an application from OAS_1, OAS_1 stores the user's purchase record. At a later time, if a user loses contact with OAS_1, he can obtain support from OAS_2 by providing this proof of purchase. We assume that a user is always registered with at least one service.

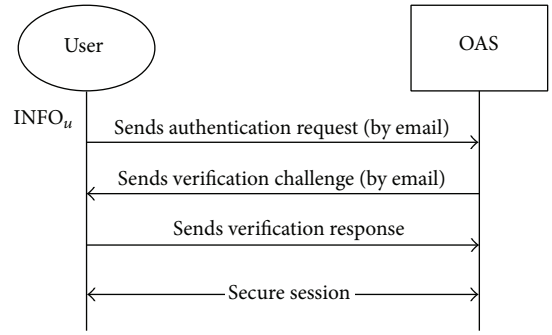


Figure 8: Checking *UAddr* by email verification.

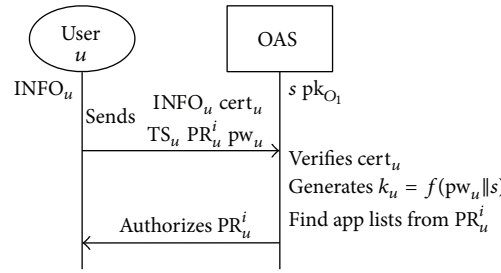


Figure 9: P1: Registration phase.

4.1. Improved System Model. We assume the following system model, illustrated in Figure 7. A developer provides applications to the OASs. A user, U, purchases applications from the OASs. The OASs share their public keys, pk_j, $0 \le j \le n$, where n is the ID of the OAS. Stores (OAS_1 and OAS_2) have a secure association. OASs also share the seed secret, s. Developers always register (1) and update (2) their applications. U must first register himself to an OAS, say, OAS_1. (3) After successful registration, U may purchase multiple applications from OAS_1. (4) OAS_1 stores U's information using the PAS. When U has a status change, he may request to update his registration to a newly connected store, OAS_2 (5). OAS_2 provides services after validating U (6).

4.2. P1: Initial User Registration Phase. The user registration process is initiated when a user first registers with a specific store. Let a user, U, register with store OAS_1.

When U requests their registration to OAS_1, OAS_1 establishes a secure channel with U. We assume that email is used to establish the secure channel, as is used by many Internet services. Figure 8 shows an example of this process.

The Registration phase, P1 in Figure 7, registers U to OAS_1 as shown in Figure 9. $\mathrm{INFO}_{\mathcal{U}}$ denotes the user purchase record stored by the OAS. When a user requests support from OAS_1, the store verifies $\mathrm{INFO}_{\mathcal{U}}$. $\mathrm{INFO}_{\mathcal{U}}$ includes the elements in Table 1.

When U and OAS_1 establish a secure channel, U selects and sends PWD to OAS_1. OAS_1 gathers $\mathrm{INFO}_{\mathcal{U}}$ and generates $\mathrm{cert}_{\mathcal{U}}$ as follows:

$$\mathrm{cert}_{\mathcal{U}} = \mathrm{sign}_{sk_{O_1}} \left\{ h\left(\mathrm{Addr}_{\mathcal{U}}^{P}\right) \| h\left(\mathrm{pw}_{\mathcal{U}}\right) \| \cdots (\mathrm{opt}) \cdots \| h\left(\mathrm{TS}\right) \| h\left(\mathrm{PR}_{\mathcal{U}}\right) \right\}, \quad (1)$$

Table 1: $INFO_{\mathcal{U}}$ elements.

Element	Description
$Addr^{P}_{\mathcal{U}}$	User's primary contact information (e.g., email address)
$Addr^{S}_{\mathcal{U}}$	User's supplementary information (e.g., phone number; optional)
$PN_{\mathcal{U}}$	Device information (optional)
$CN_{\mathcal{U}}$	Country code (optional)
$CR_{\mathcal{U}}$	Carrier code (Type 3)
TS	Timestamp
$pw_{\mathcal{U}}$	Passcode for the registration
$PR_{\mathcal{U}}$	Purchase record of U

where sk_{O_1} is a private key of OAS_1 and $sign_k\{m\}$ denotes a signature of m signed by k. $PR_{\mathcal{U}} = enc_{k_{\mathcal{U}}}\{App_i\}$, where i is the purchased app ID and $k_{\mathcal{U}} = f(pw_{\mathcal{U}}||s)$, where $f(m)$ is a key generation function with input m and s is the seed secret of the OASs. opt denotes optional information for deployment.

OAS_1 then sends TS, $PR_{\mathcal{U}}$, and $cert_{\mathcal{U}}$ to U. U stores $cert_{\mathcal{U}}$, $PR_{\mathcal{U}}$, and TS.

4.3. P2: Purchase Phase. The purchase phase, P2 in Figure 7, is invoked when U purchases applications from OAS_1.

When U purchases App_i from OAS_1, OAS_1 updates $PR_{\mathcal{U}}$. In the first step, OAS_1 decrypts $PR_{\mathcal{U}}$ with $k_{\mathcal{U}}$ and adds APP_i to the application list. If s is updated to s^{new}, OAS_1 generates a new $k^{new}_{\mathcal{U}} = f(pw_{\mathcal{U}}||s^{new})$. Then, $PR^{new}_{\mathcal{U}}$ is generated by encrypting the updated application list using $k^{new}_{\mathcal{U}}$.

Finally, OAS_1 sends $PR^{new}_{\mathcal{U}}$ to U, where it is also stored.

4.4. P3: Purchase Authentication Phase. The purchase authentication phase, P3 in Figure 7, is invoked when U contacts a new OAS, one from whom he did not purchase the application. We consider the case where U requests support from OAS_2. We assume that U registers himself with OAS_2, using the user registration phase, or temporarily contacts OAS_2 and then requests support for an application already purchased from OAS_1.

4.4.1. Step 1: Check User's Registration Information. To verify U's purchase record, OAS_2 checks U's registration information $Addr_{\mathcal{U}}$, as shown in Figure 8. Through a secure channel, U requests the purchase authentication from OAS_1 and sends $INFO_{\mathcal{U}}$ with $pw_{\mathcal{U}}$, $cert_{\mathcal{U}}$, $TS_{\mathcal{U}}$, and $PR_{\mathcal{U}}$ to OAS_2. OAS_2 then verifies $cert_{\mathcal{U}}$ with OAS_1's public key pk_{O_1}. After verifying U's registration information, OAS_2 generates $k_{\mathcal{U}}$ with $pw_{\mathcal{U}}$ and s. OAS_2 then decrypts U's purchase record, $PR_{\mathcal{U}}$, with $k_{\mathcal{U}}$.

4.4.2. Step 2: User Authorization. The processes are slightly different depending on the user's status. In this paper, we show two cases: U temporarily uses a roaming service and U permanently changes his OAS.

Case A: *U Temporarily Uses a Roaming Service*. When U connects to OAS_2 as a roaming service, OAS_2 grants temporary authorization to U. U still has his original $PR_{\mathcal{U}}$, $INFO_{\mathcal{U}}$, and $Cert_{\mathcal{U}}$, and OAS_2 does not send a new certificate. OAS_2 has access to the billing information of U and can request payment. The authorization remains valid for a specific time period; for example, OAS_2 can authorize U for one day.

Case B: U Permanently Changes His OAS. When U permanently changes from OAS_1 to OAS_2, $Cert_{\mathcal{U}}$ from OAS_1 is revoked and OAS_2 issues a new $Cert^{new}_{\mathcal{U}}$ to U. $INFO_{\mathcal{U}}$ is updated. For example, U may have a new $Addr^{S}_{\mathcal{U}}$. If the user keeps his old email, $Addr^{P}_{\mathcal{U}}$ does not change. If the user connects using the same device, $PN_{\mathcal{U}}$ remains unchanged. $TS_{\mathcal{U}}$ is updated. U receives $INFO^{new}_{\mathcal{U}}$, $Cert_{\mathcal{U}}$ and stores them with $PR_{\mathcal{U}}$. OAS_2 also stores the information. By this process, OAS_2 can bill U.

5. Security Analysis

In this section, we show that the security of the design satisfies standard security requirements and also show that the design is secure against possible attack. We assume OAS_i, where i is the ID of the OAS, can be trusted. Performance is not an issue in this paper and depends upon the actual deployment case.

5.1. Security Requirements. The following are the security requirements for the PAS model.

(i) Nonrepudiation: the user should not be able to claim that his records are invalid.

(ii) Authentication: the distributor must be able to validate the user's request.

(iii) Privacy: the distributor can only know the user's information after the user is approved.

The handling of malicious applications in the store is not the focus of this paper.

5.2. Nonrepudiation. $pw_{\mathcal{U}}$ is chosen by U, and U does not know the k_U generated from $pw_{\mathcal{U}}$. Since OAS_2 can request information about $PR_{\mathcal{U}}$ only when U requests a service, repudiation from U can be prevented.

5.3. Authentication. $Cert_{\mathcal{U}}$ enables OAS_i to check the validity of U. Since only a valid OAS_i can generate a $Cert_{\mathcal{U}}$, using the private key sk_{O_i}, a malicious user or other attacker cannot forge or abuse it.

5.4. Privacy. Without $pw_{\mathcal{U}}$, OAS_i cannot access the application list in $PR_{\mathcal{U}}$. OAS_i can only generate the $k_{\mathcal{U}}$ that decrypts $PR_{\mathcal{U}}$ to see the application list when U sends $pw_{\mathcal{U}}$.

U can replace $pw_{\mathcal{U}}$ at any time. Although a specific OAS_i can see the application list if a user chooses to use a temporary roaming service, it will not be aware of any future changes to $pw_{\mathcal{U}}$.

Only hashed user information from Table 1 is stored in $Cert_{\mathcal{U}}$. Thus, an unapproved OAS_i cannot know the information before U provides them with access.

5.5. Security against Possible Attack Scenarios. We assume that a malicious user Eve, E, could try to obtain support from a market without any purchase record. E could try the following scenarios.

5.5.1. Fraudulent User Tries to Get Authorization Illegally. E impersonates U. In this case, where the attacker impersonates a legal user, E would require $\text{INFO}_{\mathcal{U}}$, including $\text{Addr}_{\mathcal{U}}$, to impersonate U in OAS_1 or OAS_2.

E would not, however, be able to enter $\text{Addr}_{\mathcal{U}}$ during the PAS registration phase described in Section 4.4.1. Securing U's email account is not the focus of this paper.

Even when E compromises U's device and extracts $\text{INFO}_{\mathcal{U}}$ and $\text{Cert}_{\mathcal{U}}$, E still does not know the password $\text{pw}_{\mathcal{U}}$. Deploying the PAS model, OAS_i can limit the number of password attempts. For example, if several invalid password entries are attempted, OAS_i can temporarily place U's account on hold. In such a case, U would have to contact the service by phone or physical mail. We do not show the details of this process in this paper.

5.5.2. Forged Purchase Record. The malicious user E could forge his own purchase record $\text{PR}_{\mathscr{E}}$. In this case, E would have to be able to modify $\text{PR}_{\mathscr{E}}$ in the PAS. For this to succeed, E would have to know s in order to generate $k_{\mathscr{E}}$ and then generate $\text{Cert}_{\mathscr{E}}$. This is impossible without knowing sk_{OAS_i}.

6. Conclusion

With OASs becoming the main channel of software distribution, software license authentication issues present a potential problem when using multiple OASs. We have discussed possible issues from using multiple OASs and proposed an improved PAS model that reduces management overheads without any additional entity, while still allowing users to obtain support from multiple OASs. We refined our model to support a temporary roaming situation, as well as a permanent OAS change. We described the security of the proposed model.

Our design shows not only the technical availability of ongoing benefits to users, but also a possible business model for OASs.

Conflict of Interests

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

Acknowledgments

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science, and Technology (no. 2012R1A1A1010667).

References

[1] K. Han and T. Shon, "Authentication of mobile applications through various local distributors," *Multimedia Tools and Applications*, 2013.

[2] K. Fukushima, S. Kiyomoto, and Y. Miyake, "Software protection combined with tamper-proof device," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E95.A, no. 1, pp. 213–222, 2012.

[3] G. Horvat, D. Sostaric, and D. Zagar, "Multi-agent based software licensing model for embedded systems," in *Agent and Multi-Agent Systems. Technologies and Applications*, G. Jezic, M. Kusek, N.-T. Nguyen, R. Howlett, and L. Jain, Eds., vol. 7327 of *Lecture Notes in Computer Science*, pp. 648–657, Springer, Berlin, Germany, 2012.

[4] W. Liu, "Software protection with encryption and verification," in *Software Engineering and Knowledge Engineering: Theory and Practice*, Y. Wu, Ed., vol. 115 of *Advances in Intelligent and Soft Computing*, pp. 131–138, Springer, Berlin, Germany, 2012.

[5] M. Backes, S. Gerling, and P. von Styp-Rekowsky, "A novel attack against android phones," http://arxiv.org/abs/1106.4184.

[6] P. Albano, A. Castiglione, G. Cattaneo, and A. de Santis, "A novel anti-forensics technique for the android OS," in *Proceedings of the 6th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA '11)*, pp. 380–385, October 2011.

[7] F. di Cerbo, A. Girardello, F. Michahelles, and S. Voronkova, "Detection of malicious applications on android OS," in *Proceedings of the 4th International Conference on Computational Forensics (IWCF '10)*, pp. 138–149, Springer, Berlin, Heidelberg, 2011.

[8] W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri, "A study of android application security," in *Proceedings of the 20th USENIX Conference on Security (SEC '11)*, p. 21, USENIX Association, Berkeley, Calif, USA, 2011.

[9] W. Zhou, Y. Zhou, X. Jiang, and P. Ning, "Detecting repackaged smartphone applications in third-party android marketplaces," in *Proceedings of the 2nd ACM Conference on Data and Application Security and Privacy (CODASPY '12)*, pp. 317–326, ACM, San Antonio, Tex, USA, 2012.

Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 832638, 10 pages
http://dx.doi.org/10.1155/2014/832638

Research Article

Security Techniques for Prevention of Rank Manipulation in Social Tagging Services including Robotic Domains

Okkyung Choi,[1] Hanyoung Jung,[2] and Seungbin Moon[1]

[1] *Department of Computer Engineering, Sejong University, Seoul 143-747, Republic of Korea*
[2] *Department of Knowledge Information Engineering, Graduate School of Ajou University, Suwon 443-749, Republic of Korea*

Correspondence should be addressed to Seungbin Moon; sbmoon@sejong.ac.kr

Received 14 March 2014; Accepted 11 May 2014; Published 9 July 2014

Academic Editor: Sang-Soo Yeo

With smartphone distribution becoming common and robotic applications on the rise, social tagging services for various applications including robotic domains have advanced significantly. Though social tagging plays an important role when users are finding the exact information through web search, reliability and semantic relation between web contents and tags are not considered. Spams are making ill use of this aspect and put irrelevant tags deliberately on contents and induce users to advertise contents when they click items of search results. Therefore, this study proposes a detection method for tag-ranking manipulation to solve the problem of the existing methods which cannot guarantee the reliability of tagging. Similarity is measured for ranking the grade of registered tag on the contents, and weighted values of each tag are measured by means of synonym relevance, frequency, and semantic distances between tags. Lastly, experimental evaluation results are provided and its efficiency and accuracy are verified through them.

1. Introduction

As social networking services are becoming common and robotic technology has advanced, the number of social tagging services for various applications including robotic domainsis also rising. A tagging service allows a user to enter a description of the contents of a resource using a simple term or an annotation. Social tagging, also referred to as collaborative tagging, has a flat structure unlike the taxonomy which has a systematic structure by specialists in a specific domain and can be also called a collection of tagging data formed in an open environment.

The term tagging refers to the action of entering a keyword or a tag, namely, a search label that can represent contents. It contains a keyword so that a site administrator can easily classify the contents into categories by subject. Tagging can also be used for a link to blogs or webpages. As the tags are classified and arranged based on subjects or categories, general users can use the tags to gain access to corresponding content [1]. Though tagging plays an important role when users are finding the exact information through web search, reliability of semantic relation between web contents and tags is not considered. Spams are making ill use of this aspect and put irrelevant tags deliberately on contents such as photos, videos, and blogs and induce users to advertise contents when users click items of search results. As the number of users utilizing social media services is increasing, many researches have proposed the methods focusing on social recommendation services with collaborative tagging [2–8]. In common collaborative tagging systems such as http://Delicious.com, http://Twitter.com, http://Facebook.com, and https://www.Flickr.com, users freely assign keywords or tags to annotate the contents, such as movies and pictures for sharing purposes. But, traditional collaborative tagging systems do not consider the semantics of tags [2], so ambiguous tags can be used for representing contents. To solve the problem of lack of relationship between tags, Kim et al. [2] proposed a semantic collaborative filtering method for enhancing the quality of recommendations and Kleinberg [3] addressed the central issue of the distillation of broad search topics through the discovery of "authoritative" information sources on the topic and developed HITS (hypertext induced topics search) algorithm. The HITS algorithm made use

of authorities and hubs to serve the efficient and accurate ranking [3]. Wang et al. [9] introduced a framework for the personalization of social media systems and Hotho et al. [8] presented FolkRank, which is the leading one among social tagging service algorithms to solve the problem of the existing method of PageRank. As stated so far, user-entered tagging information can be utilized to draw out more accurate search results, because it is capable of depicting and summarizing the webpage contents in more detailed and precise manners than extracted keywords.

Though some social tagging services were proposed in past researches, problematic points can be summarized as follows. First, traditional collaborative tagging systems allow anyone to freely post information. Therefore, they can lead to unnecessary and unwanted tags that are completely irrelevant to the contents of a webpage. Second, a growing number of malicious websites take advantage of such loopholes and post tags that do not match up with the contents of a webpage in order to increase search engine ranking. Third, the graph-based previous work does not take into consideration the synonym relevance, frequency, and semantic distances between tags.

Thus, the purpose of this study is to enable effective ranking services by analyzing the algorithms from previous studies and by developing a new method for blocking out unsuitable tagging methods to prevent the use of personalized social ranking services as for rank manipulation. To address the discussed issues, ranking measurement algorithm is proposed to rank the grade of registered tag on the contents, and weighted values of each tag are measured by means of synonym relevance,, frequency, and semantic distances between tags. In addition, it is designed along with step-by-step designing method for efficient accurate search and composition and its efficiency and accuracy are verified by comparison with the existing systems.

The rest of this paper is organized as follows. Several related works are compared in the next section. In Section 3, the design of the suggested method is described, along with the principles of its modules and advanced algorithm. In Section 4, we describe experimental results to verify efficiency and validity of our research. Conclusions are provided in Section 5.

2. Related Work

2.1. Social Tagging Systems. Social tagging is the practice of allowing any user to freely annotate the content of a webpage with arbitrary keywords [2, 3]. Social media sites with social tagging have become tremendously popular in recent years. Social tagging changes people's life patterns and also gives a rich distribution of information. Therefore, recommender systems that are based on social tagging have become an active and growing topic of studies. These studies can be divided into three areas: tag suggestions, social searches, and social recommendations [2].

Kim et al. [2] proposed a semantic collaborative filtering method for enhancing the quality of recommendations that are derived from user-generated tags. In addition, they explore several advantages of semantic tagging as a means for avoiding ambiguity, synonymy, and semantic interoperability, which are notable challenges in information filtering. The proposed approach uses social tagging to find semantically similar users and subsequently discovers semantically relevant items for each user.

In collaborative tagging systems such as http://Delicious.com and https://www.Flickr.com, users assign keywords or tags to their uploaded resources such as bookmarks and pictures for sharing purposes. The collection of resources and tags generated by a user is called a personomy and the collection of all personomies constitutes a folksonomy. The most significant purpose of a folksonomy is to help users to find useful resources or experts on specific topics in an efficient way [4].

Wang et al. [9] introduced a framework for the personalization of social media systems. Their study consists of three tasks that would benefit from personalization: collaborative tagging, collaborative browsing, and collaborative searching. They propose a ranking model for each task that integrates the individual user's tagging history in the recommendation of tags and content in order to align its suggestions with the individual user's preferences. They use two real datasets to demonstrate all three tasks. The personalized ranking should take into account both the user's own preferences and the opinions of others.

2.2. Graph-Based Ranking Algorithm. For the web, where documents are linked to each other with hyperlinks, methods such as PageRank and HITS have been developed for calculating a criticality score by analyzing the link structure between the documents using large-size web graphs. According to Google's PageRank method that was developed in 1998, the more a webpage is referred to by other webpages, the higher the criticality score is [4]. Existing search engines determine searching ranks based on keywords, but Google gives searching ranks based on the number of pages that are referred for each webpage. It has the advantage of bringing more accurate search results and a higher quantity of search results as compared to other search engines. Therefore, it is the most used search engine in schools and research centers, because its searching rank decision method differentiates it from other search engines. However, it has some disadvantages in that it sometimes returns broken links or information that has nothing to do with the user's intentions. Furthermore, Google's PageRank method can result in a "Google Bomb." The composite score that determines an overall rank in Google is calculated by summing the PageRank score, which gives higher scores to webpages that have more linkage, and the content score, which gives higher scores based on the criticality of the text. However, this method has a weakness. The criticality of a webpage can be purposely elevated by a malicious program, such as Link Farms, that uses spam pages in order to raise the searching rank of a specific page.

Kleinberg [3] addressed the central issue of the distillation of broad search topics through the discovery of "authoritative" information sources on these topics. They proposed and tested an algorithmic formulation of the notion of authority

that is based on the relationship between a set of relevant authoritative pages and the set of "hub pages" that join them together in the link structure. Their formulation is associated with the eigenvectors of certain matrices associated with the link graph. These associations in turn motivate additional heuristics for link-based analysis.

In Noll and Meinel's study [11], social annotation via the so-called collaborative tagging is the process by which many users add metadata to shared content in the form of unstructured keywords. In their paper, they analyzed large sets of real-world data in order to explore and study social annotation and tagging with regard to their usefulness for web document classification. They were interested in finding out which kinds of documents are annotated more by end users than others, how users tend to annotate these documents, and, in particular, how these user-generated folksonomies are compared with the top-down taxonomies that are maintained by classification experts for the same sets of documents. They described what could be deduced from the results for further research and development in the areas of document classification and information retrieval.

FolkRank, which was presented by Hotho et al. [8], is the leading ranking algorithm among social tagging service algorithms. This ranking algorithm, in general, conducts a structural analysis of the graph (network) link/connection. PageRank basically measures the importance of a webpage using a probability-based method that is based on an analysis of the connection of hyperlinks [4, 7, 8]. FolkRank also added additional functionality to the existing PageRank method by means of a ranking algorithm that analyzes the relation between links to a folksonomy in a graph-based approach but failed to present ranking results in a more detailed and accurate manner by analyzing the mere relationship between users, tags, and resources. Another disadvantage is that users may intentionally write tags and expose advertisements for wrongful purposes. So, it is necessary to precisely extract a keyword representing the actual document.

3. Proposed Method

Collaborative tagging systems help voluntary users allocate tags freely to a great number of resources that are available on websites. Folksonomies are sets of resources that are collected and tagged by different users and classified in a bottom-up manner. A folksonomy is comprised of the users, resources, tags, and tag allocation relationships between them [4]. The HITS algorithm made use of authorities and hubs to give ranking scores where authority scores increase as they are linked more by the webpages of major websites, with herb scores higher when linked more by the webpages of other major websites [5]. The Google PageRank algorithm and Kleinberg's HITS algorithm adopt a method of determining the ranking based on the number of pages referred for each webpage and the number of hyperlinks. This method is not suitable for resource-based social network services such as Facebook or Twitter.

Li et al. [6] gave a comparative analysis of the tags created by users on a webpage that was bookmarked on "delicious" and the keywords that were extracted automatically from the contents of identical webpage. Their analysis showed that user-generated tags are sufficient for describing the contents of webpages. In addition, they conducted an experimental analysis that concluded that tags provide a description and summary of the contents that are based on a human perspective, rather than only a set of extracted keywords [6, 7]. But, the problem is that a lot of noisy data are also introduced as the tags and they are freely entered by users without any restrictions.

This paper, therefore, aims to propose research methods and solutions for the issues indicated above. First, an analysis will be conducted on the types of ranking manipulation in social tagging services. This will be followed by suggestions for improved methods for detecting ranking manipulation that are suitable for the present environment for social tagging services. Second, an improved ranking algorithm will be proposed to provide more accurate and reliable information. Features of a ranking method will be investigated through the analysis of the existing algorithm for social tagging services.

3.1. Proposed Method. The most important reason to use tags is their inherent simplicity. By inputting a few words, users can assemble a large collection of tags in a minimal amount of time. Social tagging is also flexible in a way that is not limited by situation or purpose. However, there are some spammers who utilize tagging services for antisocial behavior. Since spammers can influence tagging systems and post spam using scripts, they attack again when their spam is eliminated. Even when spam protection techniques are used, spammers find another way to attack. Therefore, it is difficult to prevent spam completely.

Smith [10] suggested several methods for fighting spammers. The first one is to prevent automatic tagging by checking whether the tagging is being executed by a human or a bot. CAPCHA (Completely Automated Public Turing Test for Telling Computer and Humans Apart) is an automatic tagging protection technique that can protect tagging from simple spam texts. The second one is to differentiate user rights so that systems can block the access of a user who enters spam tags. This method cannot prevent spam tagging completely, but it can minimize its impact. The third one is a method for deleting or putting a special mark on a relevant tag when another user reports that the relevant tag is inappropriate.

The methods include an automatic tagging protection function so that some inappropriate tagging can be blocked, but there is a problem. Synonyms or similar words cannot be recognized. Since they do not include any analysis on similar tags or relations between tags, there is an advantage that tags even substantially significant can be excluded. For example, as for a specific resource, "folksonomy" is recognized as a correct tagging but "collaborative tagging" is recognized as a wrong one. Such an error is caused by the absence of analysis on tags for synonyms or similar words. Therefore, this study analyzes synonyms or similar-word tags in order to enable more reliable and efficient social tagging service registration and browsing. Figure 1 is overall proposed method. The left

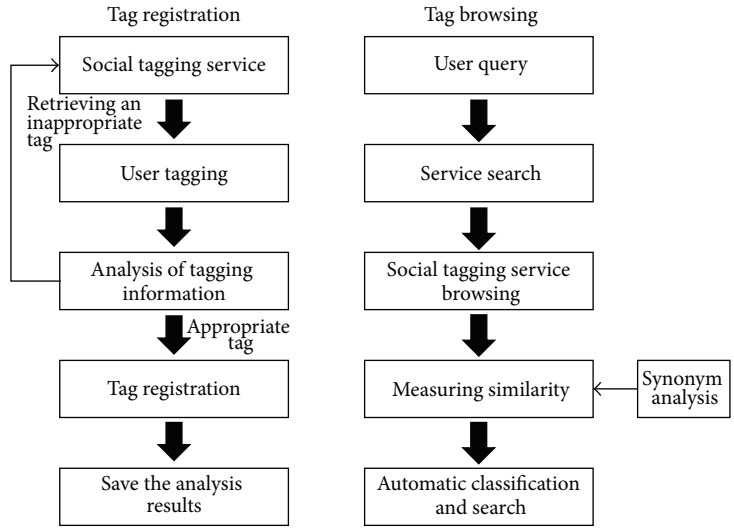


Figure 1: Overall proposed method.

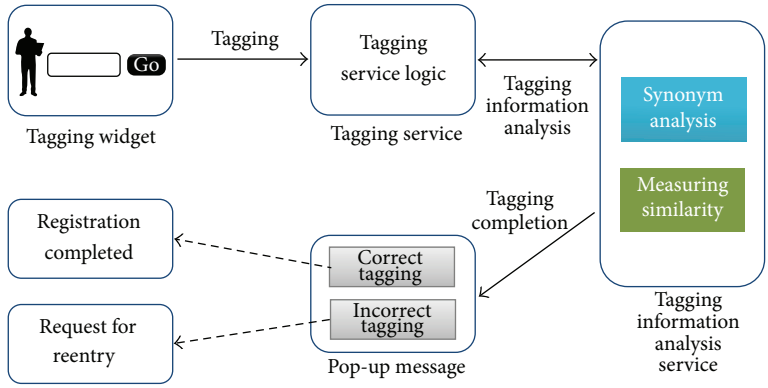


Figure 2: Process of tag registration.

side of Figure 1 shows the process of registering tags using social tagging service and the right side of Figure 1 shows the process of searching the reliable and exact social tagging service when a user queries a tag.

More detailed process is shown in Figure 2.

Figure 2 shows the tag registration flow and its phased process is as follows.

(1) The user inputs a tag.

(2) The input tag goes through the tagging service phase and then it continues to the synonym analysis and similarity measuring process using the tagging information analysis service.

(3) The tagged information is judged whether it was a correct or a wrong tag through tagging information analysis service and returns the result.

(4) If it is a correct tag, it is registered in the social tagging service with a message that says [Registration completed], but if not, it requests the user to retry.

The previous works are about finding the social tagging services which only have the tags that are simply registered, but this study is different given the following points. First, if a user makes a query in order to find a social tagging service, it analyzes the words from top to bottom in a web page and extracts the words similar to the tag that the user entered. Lastly, based on established Ontology, the extracted words and user's queries are analyzed in order to compare the relevance and similarity between them. It then measures the level of similarity. As a result, they are automatically classified according to the level of similarity and then return the results which have the highest similarity to the user. Therefore, search results based on automatic classification can be more reliable and accurate.

3.2. Advanced Semantic Tagging Algorithm. The key to advanced semantic tagging algorithm lies in how precisely the quality of resources and an individual's interest are reflected in the result. The weighting method that is proposed in this study is based on users, resources, tags, and relations, where different return values are given for the same content if users have different interests.

Equation (1) represents an advanced semantic tagging algorithm for automatically classifying and authorizing the ranking of social network documents using semantic metadata. This algorithm consists of the cosine similarity of the existing vector model and the reflected value proportional to the added weight (k_j) proposed in Definition 1 [12–14]. Consider

$$\operatorname{sim}\left(d_j q\right) = k_j \times \frac{\vec{d}_j \cdot \vec{q}}{\left|\vec{d}_j\right| \times |\vec{q}|}. \tag{1}$$

This unit describes the reflected value proportional to the added-weight for application to the ranking measurement algorithm. The reflected value of weight (k_j) for the automatic classification and ranking is as follows. Definition 1 is the reflected value of weight (k_j) based on R_j, a variable measuring the synonym relation between each tag (j) of social tagging information; D_j, a variable measuring the connection relation between each tag; U_j, a variable measuring the connection relation between users and tags; and Re_j, a variable reflecting the importance of resources.

Definition 1. Consider

$$k_j = \frac{R_j}{D_j} \times U_j \times \mathrm{Re}_j, \tag{2}$$

where R_j is a variable measuring the synonym relation between each tag, D_j is a variable measuring the connection relation between each tag, U_j is a variable measuring the connection relation between users and tags, and Re_j is a variable reflecting the importance of resources.

Definition 2 is a *semantic relevance value* (R_j) based on f_{ij}, a variable measuring the number of tags (j) generated in content (i) and S_r, a variable measuring the similarity (synonym relation) between each tag.

Definition 2. Consider

$$R_j = \frac{f_{ij}}{T_j} \times S_j, \tag{3}$$

where f_{ij} is a variable measuring the frequency of tags (j) registered in contents (i), T_j is a variable measuring the total number of tags (j), and S_j is a variable measuring the similarity (synonym relation) between each tag. Consider

$$S_j = \frac{1}{\sum_{i=1}^{n} (S_r)}, \quad \left(0 < (S_r) \le 1\right), \tag{4}$$

where f_{ij} is a variable measuring the frequency of tags (j) registered in contents (i) and T_j is a variable measuring the total number of tags (j). If the tag "amazon" was registered 7 times in contents (i), similarity "0.7" is measured for variable S_j; if the tag "tablet" is registered twice in contents (i), similarity "0.2" is measured for variable S_j. If the frequency of the tag is "0", then the value "0.001" is measured for variable S_j; if the frequency of the tag is over "10", then the value "1.0" is measured for variable S_j.

Definition 3 is the relation between each tag; that is, a variable D_j defines the proximity depending on a distance. A variable (D_j) measuring the relation between each tag determines the weight with the use of the proximity (H_p) between each of the parallel nodes and the proximity (V_p) between each of the vertical nodes in the structures of each content.

Definition 3. Consider

$$D_j = \sum_{i=1}^{n} \left(H_p \times V_p\right), \tag{5}$$

where H_p is the horizontal proximity between each tag and V_p is the vertical proximity between each tag.

The semantic distance variable D_j uses the proximity between each horizontal node (H_p) and the proximity between each vertical node (V_p) of each of the contents' structures.

3.3. System Architecture. Figure 3 is the system architecture of the suggested algorithm. The evaluation was conducted in a passive and automatic manner, analyzed by an administrator, and applied to the system using the algorithm.

When a user posts information on the bulletin board, it is saved in the "Contents" table of the storage system. The extraction agent retrieves the tags from the "Contents" table and shows the tags to the user. When a user clicks the Save button after selecting tags, the user's tagging registration is completed and the tags are stored in the "Tagging" table. A thesaurus classification method is used to compare the synonym relevance of each registered tag and to obtain a weighted value for each tag by measuring the similarity between the contents and the tags. A weighted value for each tag is stored in the "Ranking List" table in the Tag DB. The weighted values of the stored tags are used to classify normal tags and spam tags. The spam tags are deleted based on the results from the "Ranking List."

3.4. System Flowchart. Figure 4 is a flowchart of the suggested method. It is a detection process based on a user's tag registration and suggestion of contents.

The phased process is as follows.

(1) The user posts information on the bulletin board.

(2) In the logic phase of the tagging service, the program selects the tags that are automatically extracted from the existing contents of the webpage.

(3) The user can select tags from the tag lists that have been extracted automatically or the user can register a tag by typing it in.

(4) Once the new tag has been entered, the tag goes through the tagging service phase. This phase includes synonym analysis and the similarity measurement process using the tagging information analysis service.

(5) After the application of the algorithm using synonym analysis and the similarity measurement process,

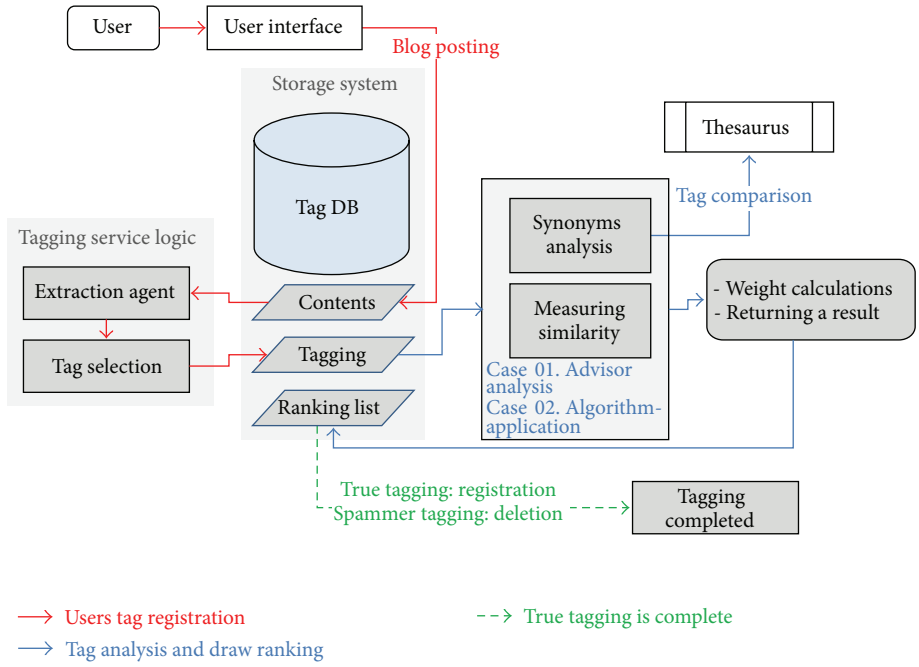


Figure 3: System architecture.

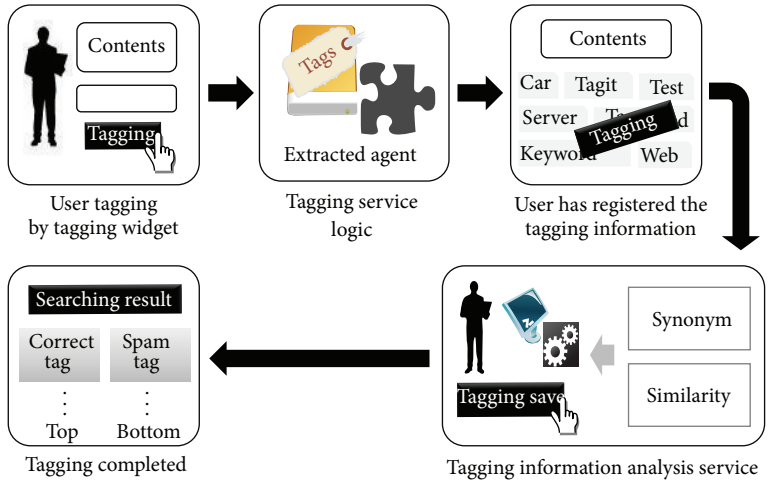


Figure 4: System flowchart.

valid and invalid tags can be distinguished from one another.

(6) If the new tag is a valid tag, the tag is registered in the social tagging service and the following message is displayed: [Registration Completed]. However, if the new tag is invalid, the program asks the user to attempt the registration process again.

4. System Implementation

4.1. Implementation Environment. The program was developed using HTML, PHP5, Javascript, and Ajax based on the CentOS operating system and the Apache Web Server. The database uses MySQL. The implementation environment of server is as shown in Table 1.

Table 1: Implementation environment.

Classification	Environment
Operation system	CentOS 6.3
Web server	Apache Web Server (2.2.9)
Database	MySQL
Language	PHP5, HTML, Javascript, and Ajax

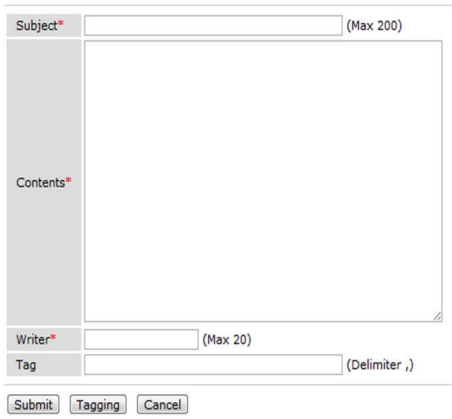


Figure 5: User input screen.

Figure 6: User input screen (tags that are extracted automatically are shown in this screen).

4.2. Implementation Results

4.2.1. User Screen. Figure 5 is a user input screen for entering written words in a message board and typing in tags. As shown in Figure 5, after entering information, the user clicks the [Tagging] button and extraction tags related to the topic are displayed as shown in Figure 6. When the user clicks the tag related to his/her topic, it is registered. As for common message boards, when the user clicks the "Submit" button, the information in the written message is transmitted to the server and saved in the MySQL database.

Figure 6 shows the automatically extracted tags that can be used as tags when the user clicks the "Tagging" button. The user can choose a tag that is related to the existing subject and contents of the webpage. Tags can also be entered manually by the user.

When the user clicks the "Submit" button, the user's tags are saved in the database and they can be displayed in the Bulletin list as shown in Figure 7.

Figure 8 shows a bulletin list that was created by a user. The user's postings are saved on the website. The user can see the content by just clicking on the title of a list. If the user wants to search based on a specific keyword, the meaning

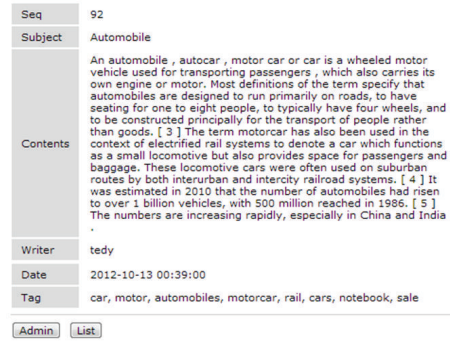


Figure 7: User input screen (tags are completed in the bulletin board).

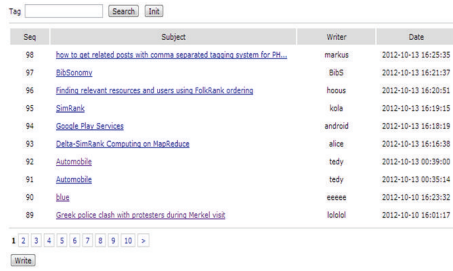


Figure 8: Bulletin list written by a user.

of a search keyword that is used within the domain can be defined accurately by an ontology server. Additionally, based on the constructed ontology, similar words are searched for and interpreted [15]. In this way, the user can see the exact results that he/she is searching for.

4.2.2. Administrator Screen. The administrator can identify the weighted value of the tags that were written by the user. The administrator can delete a tag by making judgments regarding valid tagging and spammer tagging based on the result of the weighted value shown in Figure 9.

5. Performance Evaluation

In this study, an experiment was conducted for four weeks after credible statistics were secured from preoperations. It was conducted with 18 graduate students who had been attending the University for several weeks and who had enough knowledge about how to use the system.

For the analysis of the performance of the proposed system, real data was taken and used for comparison. To evaluate the degree of similarity between the tag and the measuring methods of synonym analysis, this study used actual dataset contents that were suggested beforehand in the blog. This study was executed using Android-based platforms such as Nexus S and Galaxy S3. The evaluation test was conducted in two ways to prevent the experiment from ranking in manipulation on social tagging. One test method was to measure the simple frequency of blog contents and registered tags and the other was to measure tag similarity

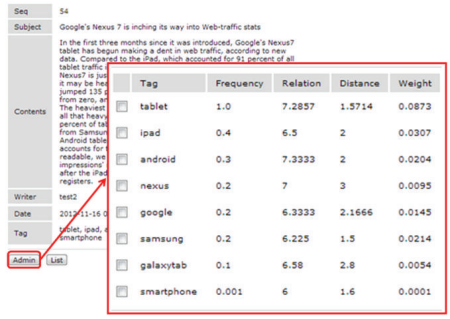


Figure 9: Administrator screen.

Subject	The Mini: A Smaller iPad
Contents	Apple's new iPad Mini, unveiled Oct. 23, is smaller and lighter than its predecessor. Its screen is 7.9 diagonal inches, making its surface area significantly smaller than the current 9.7-inch iPad. It weighs about two-thirds of a pound. The company is selling the lowest priced Mini for $330, about $130 more than similarly sized tablets from competitors. The introduction of a smaller iPad is a bit of a shift for the company. In a call with investors, Mr. Jobs once said 7-inch tablets from competitors like Samsung and Research In Motion were "tweeners" that were too big to compete with a smartphone and too small to compete with an iPad. The new iPad Mini is slightly larger than 7 inches, but can still fall into that category. But with all the action in the technology market, smaller tablets have become impossible to ignore. Google, Apple's fiercest competitor, recently released its 7-inch Nexus 7 tablet for $200. Google, Apple's fiercest competitor, had recently released its 7-inch Nexus7 tablet for $200. And Amazon recently introduced seven new Kindles, including a 7-inch tablet for $160 and an 8.9-inch tablet for $300. Barnes and Noble's Nook tablet, which starts at $200, has also sold well. Combined, the three companies have sold about 15 million of these smaller, cheaper tablets, according to estimates by Forrester.

Figure 10: Resource of a test object.

and perform synonym analysis. Through these methods, judgments were made about whether a tag was valid or invalid. Tagging refers to methods for assigning one or several tags to one piece of content.

5.1. Comparison with Existing Studies and Suggested Method. For this experiment, we posted the contents related to title "The Mini: A Smaller iPad" on the bulletin board. Tags were registered by using the automatic tag extraction system in the blog site. Figure 10 shows what was written about the Apple "iPad Mini," which was released in 2012. Consider

$$\mathrm{Rel}\left(t_j, d_j\right) = \frac{\mathrm{TagCount}\left(t_j, d_j\right)}{\mathrm{TotCount}\left(d_j\right)}. \quad (6)$$

A comparison test was performed to compare the proposed method and the previous work [5]. The tag relevance measuring formula (6) is equivalent to Im's formula.

TagCount denotes the number of times tag(t_j) is assigned to contents (d_j). TotCount(d_j) denotes the total number of tags assigned to the contents d_j.

The content theme that was used for this experiment was Google Nexus 7, which is noted for Internet service, smartphone, and the notebook OS. A total of nine tags were posted, such as "Tablet," "iPad," "Android," "Google," "Nexus," "Samsung," "smartphone," "Galaxy Tab," and "Galaxy Note." Among these, the "Tablet," "Android," "Google," and "Nexus" tags were directly related to the theme of Figure 10. The rest had low correlations. The main contents of Figure 10

Subject	Apple's iPadmini
Contents	Apple's iPadmini is expected to cash in on the apparent demand driven by Amazon and Google for smaller tablets with seven-inch screens. But finance chief Peter Oppenheimer said in a conference call that the "mini" has "substantially lower" profit margins than Apple's overall margins. Well I guess this will be the next problem for Apple. Apparently people are selling their "old" iPad's like hotcakes (read a quote as 2nd hand sales went up 700% the day after the mini was announced). If people really prefer the smaller version, the sales of the larger iPads will drop, and Apple's profitmargin will drop accordingly

Figure 11: Contents for the "Apple iPad Mini" theme.

are related to the "Nexus 7" tablet PC. In addition, the "iPad" and "Galaxy Tab" tags were registered because they are classified as tablet PCs. Table 2 shows that the frequency of the "Nexus" tag, which is related to the theme, and the "Samsung" tag, which has a low correlation with the theme, were given the same measurement values on two occasions. The measurement value of the tag relation in Im's study is the same as the Rel-method row in Figure 10.

When judging only by measuring the values from the existing method and suggested method, the degree of similarity of the two tags—"nexus" and "Samsung"—can be considered to be the same. However, the "Nexus" tag refers to a tablet PC that was released by Google and it should be considered as having high similarity with the Google-related tag. Methods that measure the relationship between the tag and the contents based simply on frequency have a problem due to the limitations in measuring the relevance between contents and tags.

On the other hand, the comparative result of the suggested method shows a weighted value of "0.0778" for the "Nexus" tag and a weighted value of "0.0579" for the "Samsung" tag. This proves that simple frequency measuring methods such as Im are not effective for distinguishing tags having little or no relation to the details of the contents. However, the method proposed in this study, which measures the synonym relevance and the synonym similarity distance, gives better judgments about the relevance of tags and contents.

5.2. Weighted Value Comparison between Correct Tagging and Entirely Incorrect Tagging. In paragraphs 2 and 3, for the performance testing of the suggested method, the experiment was conducted partially for valid tagging and invalid tagging of the contents.

Figure 11 shows the contents that were written for the "Apple iPad Mini" theme. Apple is also noted for the Apple tablet product. Five tags, which were related to theme, were entered as shown in Table 3.

To compare the weighted values for valid tags and invalid tags, Table 4 shows tags of well-known overseas wear such as "Nike," Gucci," and "Levis." The synonym analysis and similarity distance for each tag show different relation row based on brand names.

Figure 12 is a comparison chart of weighted values between valid and invalid tags. True_tag refers to an attempt to enter a valid tag and Untrue_tag refers to an attempt to do the opposite. It shows a maximum weighted value of "0.6" in the case of valid tagging and the highest weighted value for

Table 2: Comparison with an existing study and the proposed method.

Tag Number	Tag	Frequency	[10]	Proposed weight (K_j)
1	Tablet	10	1.1111	0.5152
2	iPad	4	0.4444	0.1444
3	Android	3	0.3333	0.1222
4	**Nexus**	**2**	**0.2222**	**0.0778**
5	Google	2	0.2222	0.0650
6	**Samsung**	**2**	**0.2222**	**0.0579**
7	Galaxy Tab	1	0.1111	0.0261
8	Smartphone	0	0.0000	0.0042
9	Galaxy Note	0	0.0000	0.0050

Table 3: Results for valid tags on the "Apple iPad Mini" theme.

Tag Number	Tag	Frequency (R_{ij})	Total_tag (T_i)	Relation (S_j)	Distance (D_j)	Weight (K_j)
1	amazon	0.1	5	2.5	2.5	0.125
2	google	0.1	5	3	2.5	0.015
3	seven-inch	0.1	5	3.75	2.5	0.1875
4	ipadmini	0.1	5	8	1.5	0.24
5	apple	0.4	5	3.5	2.25	0.6

Table 4: Results for invalid tags on the "Apple iPad Mini" theme.

Tag Number	Tag	Frequency (R_{ij})	Total_tag (T_i)	Relation (S_j)	Distance (D_j)	Weight (K_j)
1	nike	0.001	5	4	2.5	0.0028
2	gucci	0.001	5	3.75	3	0.0026
3	levis	0.001	5	4	2.3333	0.0032
4	Versace	0.001	5	3.75	3	0.00262
5	Umbro	0.001	5	4	3.5	0.0028

the Untrue_tag values is "levis", which was "0.0032". When the two tagging methods are compared, the weighted value shows a great difference.

5.3. Experimental Results and Analysis. This section deals with the question of how to differentiate the method used in basic research by complementing the following features. Table 5 shows a qualitative comparison between the proposed method and other methods.

FolkRank, which was presented by Hotho et al. [8] with complementary additions to the existing PageRank method, is the leading algorithm among social tagging service algorithms that analyze the link relations for folksonomy using the graph-based approach. However, because it does not take the weight of the words included in a sentence or the weight of synonyms and their relevance into consideration, this ranking method fails to present ranking results in a detailed and accurate manner, by analyzing the relationship between users, tags, and resources. Another problem is that the user may intentionally write tags and expose advertisements for wrongful purposes. Therefore, it is necessary to extract precise keywords that represent the actual document and measure the similarity between document keywords and the tags in an exact way.

As a result, the measure of similarity based on the ranking measurement algorithm serves as an upgrade to the existing vector model and the FolkRank method. The proposed method showed improved outcomes as compared to the existing FolkRank method and the vector model. However, it is not possible to verify its efficiency and accuracy completely as criteria for standardized assessments have not been suggested.

Table 5: Comparison between FolkRank and the suggested method.

Variables	FolkRank	Our method
Ontologies	Not used	Used
Graph-based approach algorithm	Used	Used
Weight of the words	Not used	Used
Weight of synonyms and its relevance	Not used	Used
Prevention of manipulation	Medium	High
Efficiency of ranking	Medium	High

6. Conclusion

With the popularization of Internet services and the rapid development in robotic applications, social web users have been overwhelmed and participated in many social media services that use collaborative tagging [15–18]. Collaborative tagging allows users to annotate the user-generated content and enables effective retrieval of uncategorized data [7]. Social tagging services allow Internet users to share web resources and they function as a foundation for ranking the collection of all resources and tags that have been created by users. Now that such social tagging services allow an

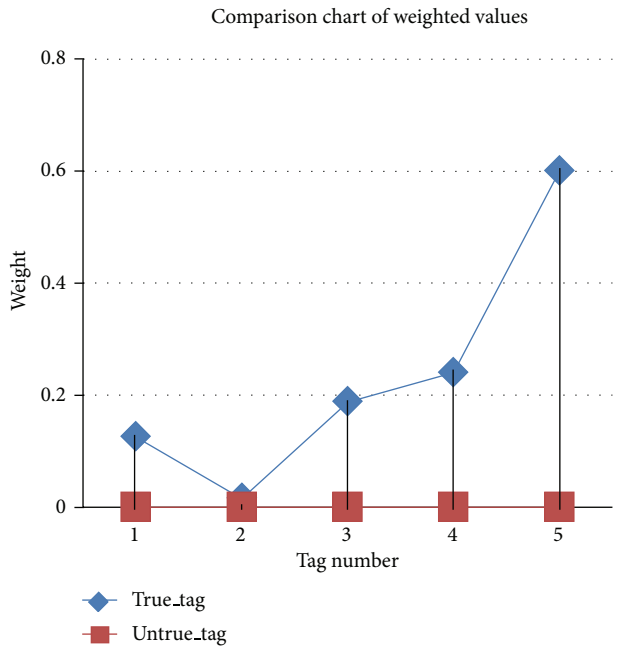


Figure 12: Comparison chart between "correct tagging" and "100% incorrect tagging."

enormous amount of information to be accumulated by many users in a short period of time and a growing number of users are intentionally abusing these services in an illegal manner in order to distort the ranking of specific resources.

As a result, users often have difficulties finding social media services that are matched to their needs [14]. While there exist some useful tags, useless and unwanted tags are also present in great numbers. This study found a solution that enables efficient and accurate ranking. In addition, refined social tags enable an analysis and classifications of effective social tagging services as they can go beyond merely classifying and managing contents to play a role as an important medium in information filtering. In the future, if the proposed method is utilized in the robotic applications, the efficient and accurate social tagging services using robotic recognitions can be realized.

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 Technology Innovation Programme of the Knowledge Economy (no. 10041659) funded by the Ministry of Trade, Industry and Energy (MOTIE, Korea).

References

[1] "New Technology Terms," Telecommunications Technology Association, 2006, http://www.tta.or.kr.

[2] H. Kim, A. Roczniak, P. Lévy, and A. El Saddik, "Social media filtering based on collaborative tagging in semantic space," *Multimedia Tools and Applications*, vol. 56, no. 1, pp. 63–89, 2012.

[3] J. M. Kleinberg, "Authoritative sources in a hyperlinked environment," *Journal of the ACM*, vol. 46, no. 5, pp. 604–632, 1999.

[4] H. Park and S. Rho, "A folksonomy ranking framework: a semantic graph-based approach," *Asia Pacific Journal of Information Systems*, vol. 21, no. 2, pp. 89–116, 2011.

[5] S. A. Golder and B. A. Huberman, "Usage patterns of collaborative tagging systems," *Journal of Information Science*, vol. 32, no. 2, pp. 198–208, 2006.

[6] X. Li, L. Guo, and Y. Zhao, "Tag-based social interest discovery," in *Proceedings of the 17th International Conference on World Wide Web (WWW '08)*, pp. 675–684, April 2008.

[7] http://foaf.tistory.com/24.

[8] A. Hotho, R. Jäschke, C. Schmitz, and G. Stumme, "Folkrank: a ranking algorithm for folksonomies," in *Proceedings of the Workshop-Woche on Lernen, Wissen und Adaptivitat (LWA '06)*, pp. 111–114, October 2006.

[9] J. Wang, M. Clements, J. Yang, A. P. de Vries, and M. J. T. Reinders, "Personalization of tagging systems," *Information Processing and Management*, vol. 46, no. 1, pp. 58–70, 2010.

[10] G. Smith, *Tagging: People-Powered Metadata for the Social Web*, Acorn, 2011.

[11] M. G. Noll and C. Meinel, "Exploring social annotations for web document classification," in *Proceedings of the Annual ACM Symposium on Applied Computing (SAC '08)*, pp. 2315–2320, Fortaleza, Brazil, March 2008.

[12] O. Choi, S. Yoon, M. Oh, and S. Han, "Semantic web Search Model for information retrieval of the semantic data," in *Proceedings of the 2nd HSI Conference*, pp. 588–593, June 2003.

[13] O. Choi, S. H. Moon, S. Han, and A. Abraham, "Intelligent Web Services System based on matchmaking algorithm," *WSEAS Transactions on Circuits and Systems*, vol. 5, no. 8, pp. 1166–1172, 2006.

[14] Y. Lim, K. Lee, H. Kim, J. Ahn, and H. Kim, "Improving tag search based on user activeness scores," *Journal of KIISE : Computer Systems and Theory*, vol. 17, no. 3, 2011.

[15] H. Kim, M. Rawashdeh, A. Alghamdi, and A. El Saddik, "Folksonomy-based personalized search and ranking in social media services," *Information Systems*, vol. 37, no. 1, pp. 61–76, 2012.

[16] O. Choi, H. Jung, B. G. Lee, H. Kim, B. Jung, and S. Moon, "A semantic-based robot expression services for prevention of rank manipulation," in *Proceedings of the KSII 8th Asia Pacific International Conference on Information Science and Technology (APIC-IST '13)*, 2013.

[17] H.-Y. Jeong and S.-S. Yeo, "The quality model for e-learning system with multimedia contents: a pairwise comparison approach," in *Multimedia Tools and Applications*, Springer, New York, NY, USA, 2013.

[18] O. Choi, I. Jeon, S.-W. Yoo, and S. Moon, "An extended DCT domain watermarking for robot vision against geometric image attacks," *Journal of Applied Mathematics*, vol. 2013, Article ID 632043, 8 pages, 2013.

Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 736738, 6 pages
http://dx.doi.org/10.1155/2014/736738

Review Article

The Need for Specific Penalties for Hacking in Criminal Law

Sangkyo Oh and Kyungho Lee

Center for Information Security Technologies (CIST), Korea University, Seoul 136-701, Republic of Korea

Correspondence should be addressed to Kyungho Lee; kevinlee@korea.ac.kr

Received 13 April 2014; Accepted 29 May 2014; Published 16 June 2014

Academic Editor: Sang-Soo Yeo

In spite of the fact that hacking is a widely used term, it is still not legally established. Moreover, the definition of the concept of hacking has been deployed in a wide variety of ways in national literature. This ambiguity has led to various side effects. Recently in the United States, reforms collectively known as Aaron's Law were proposed as intended amendments to the Computer Fraud and Abuse Act (CFAA). Most experts expect that this change will put the brakes on the CFAA as a severe punishment policy, and result in a drop in controversial court decisions. In this study, we analyze the definitions and the penalties for hacking for each country and compare them with the national law and then make suggestions through more specific legislation. We expect it will reduce legal controversy and prevent excessive punishment.

1. Introduction

Hacking [1, 2] began as a way to find computer network security vulnerabilities in order to solve these problems and prevent malicious actions. The term "hacking" was used for the first time in the late 1950s in the minutes of a meeting of the Tech Model Railroad Club at the Massachusetts Institute of Technology (MIT). The original meaning of "hack" is just to feel pleasure in the work process itself. However, this meaning was gradually turned into a bad one through its constant association with computer criminals [3–5]. In other words, some hackers began to profit from the information that was pulled out of someone else's computer by breaking into it. Hackers also spread malicious programs through a computer network in order to destroy data. Some prefer to differentiate hackers—people who do not use a system illegally but expose holes within systems—from crackers—people who destruct systems. In general, however, distinguishing between hackers and crackers is meaningless to criminals.

Recently, Aaron Swartz who was the founder of Reddit and Demand Progress committed suicide. In early 2011, he hacked JSTOR, the paid journal database, using MIT's network. Federal prosecutors charged him with the maximum penalty of $1 million in fines, 35 years in prison, and asset forfeiture.

The Computer Fraud and Abuse Act (CFAA) [6–8] has been widely abused by prosecutors to hamper security research, to stifle innovation, and to lock people who have caused little or no economic harm away for years (Figure 1). The CFAA was originally intended to cover the offence of hacking in relation to defense and bank computers, but it has been expanded in order to cover every virtual computer on the Internet to mete out disproportionate penalties for virtual crimes [9].

In USA, reforms collectively known as Aaron's Law [10] intended as amendments to the CFAA have been proposed. The major proposed revisions to the CFAA are related to the use of the provisions "exceeds authorized access" and "access without authorization." Punishment will be administered only if one or more technical or physical measures are intentionally bypassed. Furthermore, in terms of the penalty, the person will be punished only if the information obtained by hacking into a computer is valued over $5000. This change will put the brakes on the CFAA as a severe punishment policy, bring clarity, and reduce legal controversy in court decisions.

According to the legal provisions of South Korea, hacking means an act that unauthorized or authorized people use to abuse their authority to break into an information network by using an information processing device such as a computer. In other words, the current "Promotion of Information

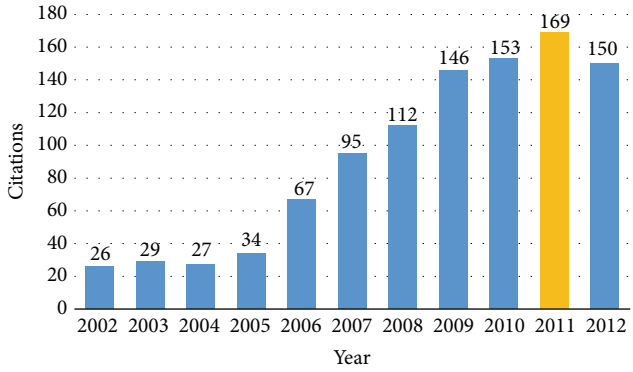


Figure 1: Computer Fraud and Abuse Act (CFAA) in the courts [9].

and Communications Network Utilization and Information Protection Act" is the same as the CFAA in USA just before its revision. Any person that violates this could be sentenced to less than three years' imprisonment or a fine of 30 million won or less. However, as in the case of Aaron Swartz, it has the potential to lead to an excessive application of legal principles.

As a result, this study analyzes the international justice and punishment for hackers, then compares them with the "Promotion of Information and Communications Network Utilization and Information Protection Act" through specific legislation related to judicial interpretation, and attempts to reduce legal controversy. Subsequently, we propose measures to prevent excessive punishment.

2. Penalties of Countries

In this study, we deal with the meaning of cybercrime [11] related to provisions of the law and analyze the principles common to the laws and penalties. We will use comparative law methods in a narrow sense. Two or more social systems and legal systems of the country will be compared. In addition, we will perform a comparative analysis of the contents of several laws for legislation or amendments.

Countries are selected by a specific rule based on the data collection possibility unity for analysis and effectiveness. Target countries are the USA, Germany, and China. USA recognizes cybersecurity as the national security dimensions of cybersecurity awareness. In the German legal system cybersecurity legislation has traditionally had the most profound influence on us [12]. Recently, there was a discussion about cybersecurity in China.

We will find the better way forward to amend the Promotion of Information and Communications Network Utilization and Information Protection Act by comparing it to the laws of each country.

2.1. Penalties of Germany. Information network for "electronic residential intrusion" penalties in Article 202(a) of the German Penal Code is provided. Information network intrusions method means to access protected information without the permission of the constituent elements or to allow a third party to access to information. The privacy protection provisions have penalty functions, so that no matter what is the information content of the object that has been breached, the act itself will be regarded as a crime. The penalty would not need to be a result of the breaches.

There is no restriction on how the system is used to bypass the security holes, even if access to the information you enter in a position to recognize the crime is established. If a person finds out a system password using trojans and phishing techniques, even if he is the owner of the corporation, it is considered a crime because it was done without the approval of the owner.

Constituent elements of the "access" mean the content of information that can be recognized. Thus, using the login information to access the network does not constitute a crime, so you are not subject to criminal penalties. However, direct access means that the information is recognizable. So, another way to find out the information is not appropriate.

2.2. Penalties of the USA. Computer hackers in the USA go to jail for 10 years for a first offence, and a recidivist gets up to 20 years in prison. In addition, any attempt to cause damage to computers will result in serious problems. Even if there is no explicit damage, the attempt to cause damage to computer would be punished by the legislative provisions. The scale of damage is estimated by the sum of the overall damage in one year. In particular, defense or national security cases can be punished without proof.

Causing damage through the use of computer malware, programs, information dissemination, and unauthorized computer intrusion have resulted in legislative provisions being introduced in the federal Criminal Code criminalizing. Distributed denial of service (DDoS) attacks also punished by federal Criminal Code and imposed penalties for cybercrime, such as hacking and viruses. The cybercrime sentencing standard has been tightened. If the cybercrime committed was intentional, it could result in up to 20 years in prison. Moreover, if damage to human life was caused, it could lead to life imprisonment.

The Cyber Security Enhancement legislation in 2002 (Cyber Security Enhancement Act of 2002) has introduced privacy protection, computer crime sentencing detail, and guide for enhanced penalties. Specifically, the guidelines were modified to consider the seriousness of the sentencing under Article 225 of the Computer Fraud and Abuse Act (Computer Fraud and Abuse Act, CFAA). Besides, a cyberattacker who intentionally or inadvertently violates the law and causes serious injury may go to jail for up to 20 years. In addition, intentionally or negligently causing death may be punished by life imprisonment.

2.3. Penalties of China. Cybercrimes are not regulated by one single special law in China. Rather, they are covered by a scope of laws and regulations with a comprehensive nature, such as Ordinance for Security Protection of Computer Information System, Criminal Law Articles 285–287, Decision Regarding the Maintenance of Internet Security, and Provisions on Administrative Punishment concerning the Management of Public Security [13].

Table 1: Comparing each country's criminal law.

	Korea	Germany	USA	China
Legislation	Network Act, 48	Criminal Law, 202(a)	CFAA (18 U.S.C 1030)	Criminal Law, 285
Criterion for punishment	Access abusing their authority	Access without authorization	Exceeds authorized access	Intrusion actions
Penalty (imprisonment)	3 years	3 years	Over 10 years	3–7 years
Feature	In distributed laws	In Criminal Law	Severe punishment	Punish acts of indirect

In 2009, the Amendment to the Criminal Law of China (VII), which was deliberated at the 7th meeting of the Standing Committee of the Eleventh National People's Congress, was passed. Subsequently, China added "hacker" to the Criminal Code in order to be able to legally punish hacking. According to Article 285 of the existing criminal law in China, on the violation of state regulation and intrusion of national affairs, defense, construction, science, and technology, the area of unlawful breaching of computer information systems was punishable with less than three years of imprisonment.

However, under the existing laws, law enforcement agencies faced many challenges to be able to arrest "hackers." They illegally intrude into someone else's account, computer system, and steal information such as passwords. There is also large-scale illegal control of another person's computer. Thus, they make a critical impact on network security. To ensure the correction of the insufficient legal grounds, the Criminal Code Amendment (7) Law was passed, while a second clause and third clause were added to Article 285 of the Criminal Code.

In addition, in 2011 the Supreme People's Court prepared for a trial to punish the people who unlawfully breached the network to obtain information or plant malware by "interpretation of the law for computer information criminal case." The Supreme People's Procuratorate pointed out that the illegal market for the buying and selling of materials and tools for hacking was growing and it was regarded as a criminal offence. Previously, this was punishable with only three years in prison. A relatively light punishment was imposed. However, after this trial, it was held that acts such as providing software to hackers are grave criminal offences. Perhaps this "indirect" law is subject to the Criminal Code and it will allow those who commit this offence to be jailed for up to ten years.

3. Comparison of Criminal Laws

In this case, Republic of Korea court will be able to make a decision according to the "Promotion of Information and Communications Network Utilization and Protection Act." Thus, violators would be punished by either a fine of up to 30 million won or a maximum prison sentence of three years [14, 15].

In addition, the United States court will be able to make a decision according to the copyright laws. At this time, a sentence of less than three years' imprisonment or a fine of 30 million won or less is applied.

Under German law, criminals are punished under Article 202a of the Criminal Code. They are sent to jail for less than three years. Also, pursuant to Article 109 of the Copyright Act, the punishment becomes less than three years in prison. On the other hand, China court can make an order to stop using it and may request damage compensation.

Punishment after the structuring of German cybersecurity legislation enables the integration of management. In the case of Korea, cybersecurity criminal penalties for infringement of the Information and Communication Network Utilization and Information Protection Act, the Criminal Code, E-Trade Promotion, Information Infrastructure Protection Act, Communications Privacy Act, and other laws and regulations are decentralized. It leads to problems with understanding penalties, and it makes it difficult to evaluate the laws.

In addition, the German cybersecurity legislation on cybersecurity violations and possible penalties are lumped together. Therefore, it is easy to understand the information. This leads to an effective general prevention of cybercrime. Furthermore, in terms of equality of penalties for legal regulations, it seems to be more preferable than distributed case. Laws and regulations are varied; the purpose of each and the operating policies are different. As a result, it is difficult to secure equity through consistency as a legal basis. It will be useful that law enforcement agencies who enforce the law (prosecutors and courts) interpret and apply the law with regard to the penalties in the Criminal Code.

In the case of Germany, the regulations do not disperse. Therefore, it is possible to punish without exception. But, in the case of Korea, there is no provision for punishment. We shall refer to the German legislative system. Penalties for and violations of cybersecurity provisions should be both included in the Criminal Code. This gap should be complementary. In this respect, the German postpunishment cybersecurity legislation is very useful to us. The main direction of the maintenance of the laws and regulations should be on the basic law. Furthermore, the provisions of other laws that are passed are too specialized or simplified, and common details should be defined in the basic laws.

Cybercrime in the USA began in the mid-1980s. The laws on cybercrime were made and developed through the interactions. However, the extent of the actual low level of criminal penalties was, in the 2000s, caused by the awareness of the seriousness of the damage that can arise and the strict punishment that can be imposed for such an offence. USA is constantly expanding the range of penalties depending on

Table 2: The punishment criteria of hacking in Korea.

Action	Legal	Penalty	Intentional
Intrusion	No	Imprison/monetary	Yes/no

the gravity of the crime; however, its stringent sentencing of Aaron Swartz led to unfortunate side effects such as his suicide. This result is a good lesson for us on criminal law (Table 1).

4. Case Studies

The Ministry of Information and Communication announced amendments to the "Promotion of Information and Communication Network Utilization and Information Protection Act" as part of its follow-up measures to the "1.25 Internet Security Incident," and to expand the scope of the penalty for cybercrime. Just an attempt at hacking or introduction of a virus can result in a criminal penalty with a maximum sentence of five years in prison or a fine of 50 million won.

4.1. Port Scan. A port scan [16] is a subject of punishment in Korea because it is regarded as an attempt to attack. Strictly speaking, a port scan is a vulnerability inspection skill rather than a hacking attack. But sometimes hackers misuse such a skill to find out the host's weak point, and hackers try attacks based on this information (Figure 2).

This kind of hacking is considered a "trial of intrusion" rather than "intrusion." However, it is an action "beyond the limits of authority" allowed and can be admitted as starting to execute an attack. Therefore, it can be punishable under Article 48 of the "Promotion of Information and Communication Network Utilization and Information Protection Act."

But as mentioned earlier, focusing on "intrusion," we can have other constructions of law. "Intrusion" means that the agent does not follow the normal certification procedure for utilizing the resource of information network system or uses an abnormal method to get authorization for entering information network system. When the resources of the information network system can be used arbitrarily, the resulting state is defined as completion of intrusion. Therefore, port scanning by hackers is defined not as the action of intrusion into an information network system but as the action of preparation for attempting to break into a targeted web server. We should regard the installing of a program for intrusion, when security vulnerability is discovered after port scanning, as the onset point of the execution of a hacking.

In addition, just executing a port scan does not damage the system. Actually, one can tell when a port scan is done on purpose by the periodicity or the specific port range of the object of port scanning. The malicious packets are usually filtered through a FW (firewall) or IDS (intrusion detection system).

4.2. Collecting Email Addresses. Similarly, there is an act concerning the collection of e-mail addresses. To punish this kind of preliminary act for spam mail sending is unreasonable and prior criminalization because it is unclear whether spam mail sending is a crime that warrants sentencing. We do not criminalize unwanted postal mail or leaflets that are delivered to a receiver in the real world. In this situation, the criminalization of spam mail is an unreasonable action. Moreover, there is no legal provisions to punish the collection of e-mail addresses what is not using some program or technical device [17].

4.3. iPhone Jail Breaking. It belongs to a hack that manipulates the kernel of operating system in hardware such as iPhone for using more than the originally programmed functions. It is a real interesting mix of professionals looking at this. But it is not violating copyright laws. Moreover, it is considered as having no intention to cybercrime. This pseudohacking is ruled out of subject to criminal prosecution [18].

4.4. Attempted DDoS Attack. DDoS attacker is punished by the law regarding the promotion of information and communication network use and protection of information Articles 48 and 71. But this law cannot punish an attempted crime. So DDoS Attacker will not be punished if there are no breakdowns in network. Moreover, the scope of attempted DDoS attack will be expanded by technological development [19].

5. Punishment Criteria

Determination of punishment means that decision punitive measures about convicted person [20]. At this time, determination of punishment should ensure predictability and controllability by the provisions.

Therefore, we need to adjust the scope of punishment for hacking as shown in Tables 2 and 3. As stated in Table 3, we should be able to punish legally with more detailed criteria.

At first, we divide the subject of punishment into two groups, with intention or without intention (inspection, just an attempt, etc.). We do not suggest concrete sentences but we need to apply different standards according to the scale of damage arising from the use of a malicious program.

6. Conclusions

Most cyberhackings are perpetrated by hackers to show off or satisfy themselves. Therefore, enhancing punishment is not the best way to prevent hacking. It is more important that they are educated about the damage caused by cyberhacking rather than punishing them. This will fundamentally solve the legal problem of preventing hacking attempts.

As we mentioned above, in USA, the penalties for cybercrime can be more than 20 years' imprisonment, but the definition of hacking is still not clear. Of course, penalties for hacking are also unclear due to the rapid development of technology. On the other hand, the domestic law for hackers provides a variety of penalties, and it is also not clear. This difference comes from the interpretation. Even if

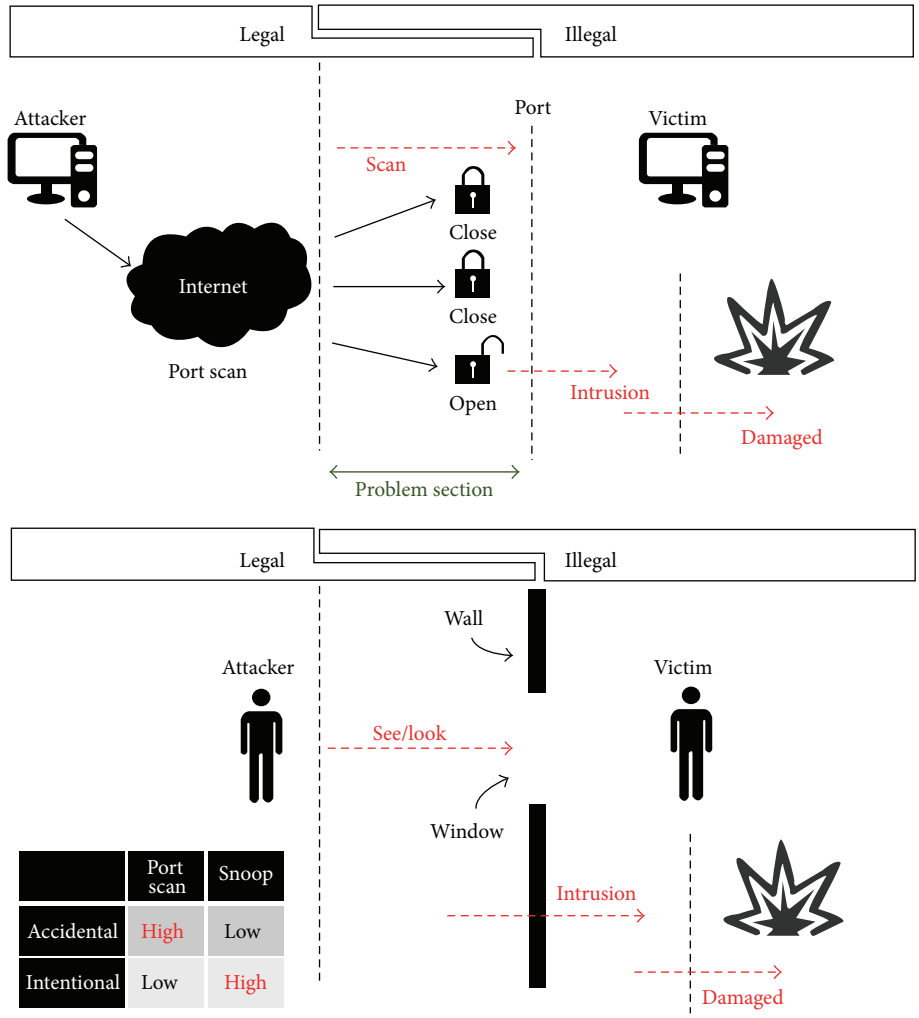


Figure 2: Legal comparison between port scan and snoop.

Table 3: The improved punishment criteria for hacking.

Action	Legal	Penalty	Intentional
Find out vulnerabilities	Yes	Fine	No
Attempted access	No	Monetary	Yes
Install malicious program	No	Imprisonment/monetary	Yes
Damage less than 50 million won by installing a malicious program	No	Imprisonment/monetary	Yes
Damage more than 50 million won by installing a malicious program	No	Imprisonment and monetary	Yes

the user simply breaks a contract, unreasonable punishment is likely to be administered. Thus, it is necessary to define rules more clearly and specifically. Taking into consideration the relative uniformity, and the specific provisions of the criminal law in Germany, we must modify the "Promotion of Information and Communications Network Utilization and Information Protection Act" and other regulations. By doing this, legal controversy and excessive punishment will be reduced.

Additionally, reasonable adjustment of statutory punishment is needed in the future. At present, statutory punishment is distinguished from sentencing in current Korean court [21]. Sentencing level converged on the lowest limit of statutory punishment.

Conflict of Interests

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

Acknowledgment

This work was supported by Korea University Grant.

References

[1] R. K. B. Jain, "Hacking-ethical or criminal: a legal quandary," *The IUP Journal of Information Technology*, pp. 49–56, 2008.

[2] A. Dudley, J. Braman, and G. Vincenti, *Investigating Cyber Law and Cyber Ethics*, Information Science Reference, Hershey, Pa, USA, 2011.

[3] G. Cybenko, A. Giani, C. Heckman, and P. Thompson, "Cognitive hacking: technological and legal issues," in *Proceedings of the Law and Technology Conference*, 2002.

[4] A. Chandler, "The changing definition and image of hackers in popular discourse," *International Journal of the Sociology of Law*, vol. 24, no. 2, pp. 229–251, 1996.

[5] Y. Choi, "Present information crimes and systematic countermeasures," *Korea Institute of Criminology*, vol. 1997, no. 1, pp. 13–236, 1997.

[6] 2014, http://en.wikipedia .org/wiki/Computer_Fraud_and_Abuse_Act.

[7] R. C. Kain, "Federal computer fraud and abuse act: employee hacking legal in California and Virginia, but illegal in Miami, Dallas, Chicago, and Boston," *The Florida Bar Journal*, vol. 87, no. 1, 2013.

[8] T. E. Booms, "Hacking into federal court: employee authorization under the computer fraud and abuse act," *Vanderbilt Journal of Entertainment and Technology Law*, vol. 13, 2011.

[9] Korea Internet and Security Agency, "Internet legislation trend," *Internet Legislation Trend*, vol. 70, 2013.

[10] D. Searls, "How "Aaron's law" is good for business," *Harvard Business Review*, 2013, http://blogs.hbr.org/2013/02/how-aarons-law-is-good-for-bus/.

[11] H. Jahankhani and A. Al-Nemrat, "Examination of cyber-criminal behaviour," *International Journal of Information Science and Management*, pp. 41–48, 2010.

[12] Korea Internet and Security Agency, "A Study on Solutions for the Advancement of Security Legislation," Korea Communications Commission, December 2011.

[13] B. Liang and H. Lu, "Internet development, censorship, and cyber crimes in China," *Journal of Contemporary Criminal Justice*, vol. 26, no. 1, pp. 103–120, 2010.

[14] S. Yang, "Cyber crime trends and criminal liability," Internet & Security Focus, September 2013.

[15] H. Choi, "Loopholes in criminal law to new types of hacking attacks," *Criminal Policy Research*, vol. 18, no. 4, 2007.

[16] 2014, http://en.wikipedia.org/wiki/Portscan.

[17] S.-R. Kim, "Zur Strafbarkeit von Phishing," *IT & Law Review*, vol. 4, 2010.

[18] L. W. Sang, "Die Vorfeldkriminalisierung des Hackens und das seine Eintritt in die Alltagssphare," *Anam Law Review*, vol. 28, p. 294, 2009.

[19] L. W. Sang, "A study on discussion of the attempted hacking penal measure," *Korean Journal of Comparative Criminal Law*, vol. 13, 2011.

[20] S. Jeong, "A study on reasonable sentencing in structural aspects," *Chungnam Law Review*, vol. 24, no. 2, 2013.

[21] S. Lee, "A study on the improvement of discretionary mitigation statute in new sentencing system," *Inha Law Review*, vol. 16, no. 3, 2013.

Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 809219, 6 pages
http://dx.doi.org/10.1155/2014/809219

Research Article

Empirical Analysis of Retirement Pension and IFRS Adoption Effects on Accounting Information: Glance at IT Industry

JeongYeon Kim

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 30 March 2014; Accepted 16 May 2014; Published 9 June 2014

Academic Editor: Hangbae Chang

This study reviews new pension accounting with K-IFRS and provides empirical changes in liability for retirement allowances with adoption of K-IFRS. It will help to understand the effect of pension accounting on individual firm's financial report and the importance of public announcement of actuarial assumptions. Firms that adopted K-IFRS had various changes in retirement liability compared to the previous financial report not based on K-IFRS. Their actuarial assumptions for pension accounting should be announced, but only few of them were published. Data analysis shows that the small differences of the actuarial assumption may result in a big change of retirement related liability. Firms within IT industry also have similar behaviors, which means that additional financial regulations for pension accounting are recommended.

1. Introduction

Many developed countries have introduced several types of pension scheme for wage earners to diminish expected economic difficulties after their retirement. Occupational pension scheme, which is introduced recently in Korea, organizes 3-tier social security program with national pension and individual pension service. It can be differentiated from others by the fact that the responsibility of retirement pension payment is on related company.

Historically, the issue of retirement allowance from the workers' view point is the reliability of payment [1]. Government tries to guarantee retired employees the payment of predefined retirement allowances, but there are many overriding legal considerations for the bankrupted companies' obligations. Besides, new pension scheme as a retirement allowance raises other questions from the firm's accounting view point on how to describe pension related liabilities in firm's financial reports. Pension is a kind of future payment and its exact amount is not predictable.

To improve above issues, Korean government introduced important changes in retirement allowance policy and related accounting standards. First, Korean government required that all listed companies entrust predefined retirement allowances to selected financial organizations. The responsibility of retirement allowance is still on each company, but new policy ensures the minimum payment of it with the reserved money. Second, Korean government required that all listed companies provide workers with several pension schemes as a retirement allowance and report related liability based on K-IFRS in their financial reports.

There are many researches on the effectiveness of new retirement allowance policy checking if the policy actually helps retired workers to get their retirement allowance timely or if the external funds are properly operated by the financial organizations for payments. In addition to them, there are arguments about the effects of new pension scheme on individual financial reports. Logically, it may give no effects on the business results of firms. New policy just requires that companies transit internal reserves for retirement allowance into an external organization.

However, new financial standards with pension accounting make remarkable changes in liability estimation method for retirement allowances. New financial standards, K-IFRS, take a principle-based approach without guidelines for operational details and allow firm's alternation within given principles. Pension accounting needs complicated projection process for the expected liability with several actuarial

assumptions. The guideline for the required variables for the assumptions such as life expectancy or average wage increase is provided, but there are no specific regulations yet in Korea.

Researchers reported that some firms try to increase or decrease their short-term earnings by changing required money for retirement allowance or by changing the actuarial assumptions to estimate pension related liability [2–4]. In that context, new estimation method for retirement related liability could be an interesting observation or checkpoint for the transparency of accounting information in Korea. Generally speaking, the adoption of IFRS is supposed to improve the principal qualitative characteristics of accounting information in relevance, reliability, understandability, and comparability [5, 6].

To review the changes in firm's liability for retirement allowance, we select listed companies in Korean stock market, which adopted K-IFRS early in 2009 or 2010. We compare their liability for retirement allowance in financial reports after activation of new policy. Also we check related public announcements from the companies if they had provided proper explanations for their actuarial assumptions to estimate the liability. With the comparisons, we try to identify suspicious companies where the changes in financial report are hardly explained with the public announcements.

The paper proceeds as follows: we review theories on pension accounting and the previous researches on K-IFRS's adoption. This leads to the different expectations for the effects of new pension policy with K-IFRS. Following that, we review reported estimation results on retirement related liability and data analysis.

2. Theoretical Background

In 2005, Korean government introduced occupational pension schemes as a retirement allowance by making a law called "Employee Retirement Benefit Security Act." After having grace periods for the new policy, Korean government requires that all listed companies actually implement it from 2012. At the same time, new financial standards called K-IFRS are activated.

2.1. K-IFRS Adoption with Pension Accounting. K-IFRS provides two different basic pension schemes based on how to decide on the total benefit of retirement and who will operate the reserved fund. Defined-contribution (DC) plan is a type of retirement plan in which the employer, employee, or both make contributions to the account for worker's retirement allowance on a regular basis. Only employer's contributions to the account are guaranteed, not the employee's future benefits. Defined-benefit (DB) pension is a type of pension plan in which an employer promises a specified monthly benefit on retirement predetermined by a formula based on the employee's earning history, tenure of service, and age rather than depending directly on individual investment returns. A DB plan is "defined" in the sense that the benefit formula is defined and known in advance, while a DC plan is defined in the sense that the formula for computing the employer's and employee's contributions is defined and known in advance.

For accounting information, DC plan is simple. Firms provide calculated contribution to individuals and report them as retirement allowances. The money in individual accounts should be operated by retirees and the decision on investment risk and investment rewards is placed on each individual. Also all obligations of additional financial report for the operations of the committed fund are on external financial organization. Therefore, firm or employer does not have any other responsibilities for retirement allowance and operational report for the committed fund.

In contrast, DB plan is complicated to get accounting information for the future liability. Firms should commit legally required money to external financial organization based on their estimation for the total pension related liability. Government announced that the required ratio of external severances will be increased gradually, but it is 60% of the reported liability as before the policy changes. Each firm can reserve more money to get additional tax benefit. However, the decision for the additional money amount to reserve is up to the individual firm and related information is guided to be properly announced.

2.2. Issues for Future Liability Estimation. Traditionally, DB plan has been popular for retirees because they can expect certain amount of allowance after their retirement. However, during last few decades, DC plan has gained momentum and popularity. By changing DB plan to DC plan, individual firms can typically save a significant amount of money because the benefits afforded by DC plans are typically lower than what is offered by DB plans. However, it may be also criticized as the primary responsibility for preparing for retirement has been removed from employers and placed on employees.

Accounting information of DB plan starts from the estimation of the employee's pension benefit. IFRS suggests projected benefit obligation (PBO) as a standard estimation method to estimate more realistic future liability, which considers all pension benefits for both vested and nonvested employees based on their future compensation [7]. From the estimated future liability, PBO gets the present value of it with a conservative discount factor. Despite its conservative approach to real pension liability, PBO is being criticized for its inaccuracy [8]. Many actuarial assumptions such as life expectancy or compensation increase rate of work as the source of inaccuracy. Also the complexities associated with estimating DB plan liabilities make it difficult to foresee the required current budget for retirement benefit expenditures [1].

The second issue is related to the accounting flexibility for company's DB plan assets and liabilities. For example, FASB 87 in the U.S. allows the off-balance sheet accounting of pension assets and liability amounts. It means that the estimated liability with PBO and employer's contributions are not recorded as a liability or as an asset on the company's balance sheet. Instead, their netted amounts are reported on the company's balance sheet [9]. It makes firm's financial report cannot deliver proper information on actual financial condition of the firm, which may lead investors to erroneous conclusions. Korea had similar issues until the activation of

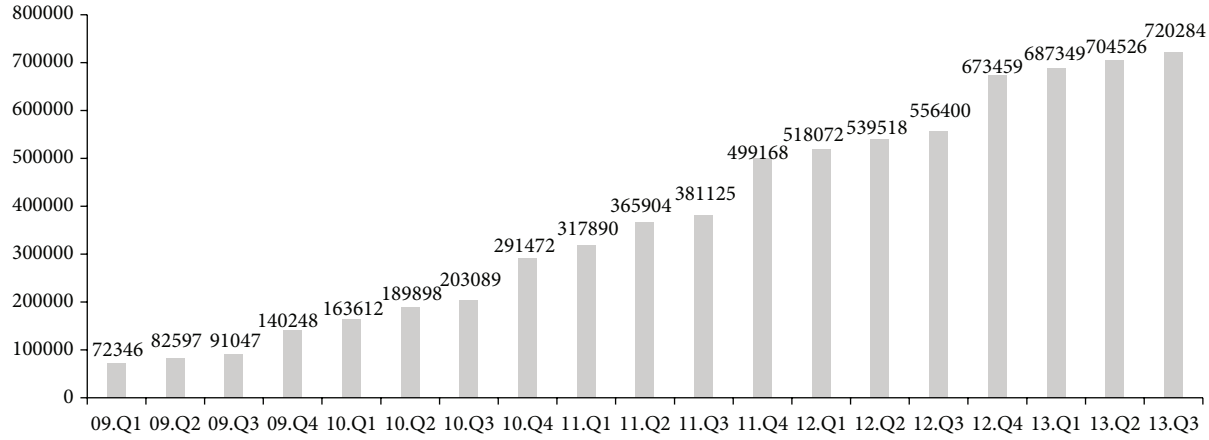


Figure 1: Total amount of external reserves for retirement allowances.

new financial standards. However, recently adopted K-IFRS is not a perfect solution for the issue either. K-IFRS provides the principles for pension accounting and also permits individual firm's arbitrary operations within the principles. If auditing organization does not provide proper guidelines on actuarial assumptions for PBO or other details of pension accounting, we will have other accounting flexibility issues even with new financial standards [10].

2.3. Benefits via Tax Concessions versus Manipulated Accounting Information. Occupational pension schemes for worker's retirement have been encouraged via tax concessions in many countries. Korean government also admits tax benefits for whole amount of external reserves committed to financial organization as retirement allowance, while internal reserves for retirement allowance have a certain limitation for tax benefits. The more money a firm commits to external financial organizations, the more tax benefits it gets.

Researches show that firms with good business results have a tendency to increase the reserves for retirement allowance to get more tax benefits [3, 11]. Some results show that it can be a preceding index for good business results. In contrast, firms expecting a bad business result decrease it to keep earnings as much as possible. Because minor changes in accrual assumption can result in big differences in firm's liability estimation, it is possible that firms can adjust the liability with announcements. Currently proper guidelines for the announcement of change of accrual assumptions are suggested but they are not mandatory.

One example of inappropriate use is recently announced for national pension liability in Korea. Korean Ministry of Strategy and Finance announced that the Korean government needs additional fund for government employees' pension. Government had estimated the liability with fixed life expectancy as the result of 2006 and assumed that current employees with insufficient conditions will not be a subject of pension schemes even in future. With the correction of unrealistic assumptions, government announced that new liability in 2013 was increased by 25 billion dollars compared to previous estimation result.

3. Expectations versus Actual Results with Pension Accounting

With the legislation of "Employee Retirement Benefit Security Act" in 2005, there were many optimistic forecasts on the size of external reserves for retirement allowance. In 2007, in early stage of the gray period, experts had an expectation that the total reserves will reach up to 80.7 billion dollars for 5 million accounts until 2015. We can see that the actual statistics of the retirement allowance are actually similar to the expectations. Korea has 4.6 million accounts for pension plans, which is 45.6% of whole wage earners in Korea. The external reserves reach 65.5 billion dollars at 2013 Q3. Figure 1 shows the changes of external reserves for retirement allowances with KRW units.

As we expected, DB plan is the most popular pension plan. 65.1% of the total accounts are for DB plan, while accounts for DC plan are 32.9%, and IRP (Individual Retirement Plans) have 2.0% of the total accounts at 2013 Q3. The firm counts for each pension plan show that 31.6% of total firms provide DB plan only while 52.5% of total firms provide DC plan only. 2.4% of total firms provide both DB and DC plans to their workers and 13.6% of total firms provide IRP.

However, the adoption rate and the preference of pension plan can be different considering firm size. As we can see in Figure 2 and Table 1, almost all firms having more than 500 waged workers already adopted pension plan (98.6%) and 49.36% of them provide DB plan only.

3.1. Expected Changes in Liability. With the adoption of new financial standards and new retirement policy, there are many different opinions on the change of estimated liability. Simple induction with PBO method leads to the conclusion that it will increase the liability because PBO considers the final wage as bases for liability estimation. Although the estimation is converted to present value with a discount factor, the increase rate of wage is expected to be greater than the inflation rate.

Cho and Rho [12] compared liability based on previous financial standards and K-IFRS with PBO. According to the

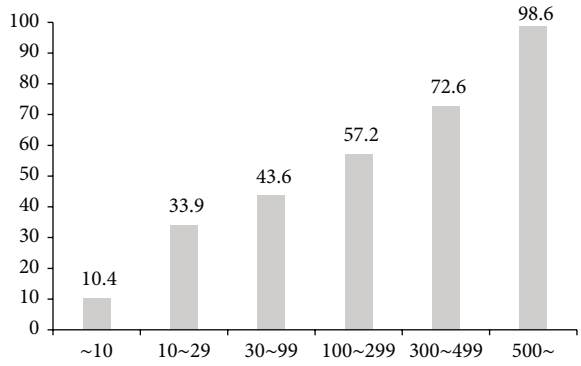


Figure 2: Ratio of firms with pension plan considering its size.

Table 1: Pension plan considering firm size.

Size	DB	DB/DC	DC	IRP	Firm count
~9	24.97%	1.04%	51.26%	22.73%	140,689
10~29	37.56%	2.54%	59.90%		62,732
30~99	47.15%	4.94%	47.91%		23,542
100~299	54.81%	10.96%	34.22%		6,367
300~499	57.13%	18.59%	24.28%		1,038
500~	49.36%	32.81%	17.83%		1,335

study, the estimated liability for retirement allowance with PBO will be slightly smaller than the liability with previous financial standard. The firms having actuarial assumptions of higher wage increase rates and lower inflation rates will have estimations with increased liability. It shows that the result of liability estimation depends on individual firm's arbitrary actuarial assumptions and proper regulations are required to prevent manipulating accounting information for pension accounting [2, 8, 13].

For IT industry with higher rate of payroll costs and R&D costs, the firms may prefer DC plan or try to estimate decreased liability.

3.2. Financial Report Analysis for Pension Plan. This study chooses the K-IFRS adopted financial reports of 2009 and 2010 for firms listed in Korea stock markets. They provided both financial reports under previous financial reports and K-IFRS, which easily can be compared for the changes in pension related liability caused by PBO. The counts of firms to be compared are 14 from the results of 2009 and 46 from the results of 2010. Table 2 shows the count of financial reports categorized by its type and year.

We also review their announcement for pension adoption and their actuarial assumptions for their liability estimations. 25 firms from selected 60 had adopted occupational pension plan as retirement benefits and provided financial information K-IFRS requires during the period. DB plan was the most popular plan and 19 firms out of 25 selected it as their pension plan. Table 3 shows the distribution of firm's pension plans and related liability changes.

For the changes of liability for retirement allowance, 15 firms out of 25 reported that it is decreased compared to other financial reports based on previous financial standards, while 9 firms reported that it is increased. One firm already had external reserves for whole amount of the liability and reported no changes for it.

Table 2: Financial report counts with early K-IFRS adoption.

Year	Financial report type	Firm count
2009	Consolidated	11
	Individual	3
2010	Consolidated	39
	Individual	7

Table 3: Pension plan for firms with early K-IFRS adoption.

Type	Classification	Firm count
Pension plan	DB	19
	DC	3
	DB/DC	3
Changes of liability for retirement allowance	Increase	9
	No change	1
	Decrease	15

Figure 3 is presenting the change ratio of liability for retirement allowance with K-IFRS. A firm that adopted DC plan and had no external reserves shows 100% decrease of liability. Another firm that already had 100% external reserves for retirement allowances shows no change of liability. Most of their changes are under 20% and match previous expectations.

However, some firms have represented a sharp change above 30% of liability. To track the reasons of individual change, we have to review their actuarial assumptions and previous internal reserves, which should be able to get the information through public announcement.

Reviewing the public announcement related to pension plan and related liability estimation, we just found only 4 disclosures of 3 firms having specific explanation on their assumption. Although K-IFRS recommends public announcements for all pension related information, firms do not have any motivation or obligation for it. Most firms simply described their discount factor to get present value of future pension liability as the market interest rate of government bonds or corporate bonds instead of providing specific number. It shows that current pension accounting guidelines under K-IFRS are not the proper answer to flexible accounting issues [2].

Table 4 summarizes the actuarial assumptions and changes of liability for the cases with public announcements. Each case has significant differences in wage increase rate and discount factor, which are the most influential variables in liability estimation.

Case 1 with relatively higher wage increase rate and lower discount factor resulted in the increase of estimated liability. On the contrary, case 2 with relatively lower wage increase rate and higher discount factor resulted in the decrease of estimated liability. This comparison shows the effect of actuarial assumptions on liability estimation. The issue is that

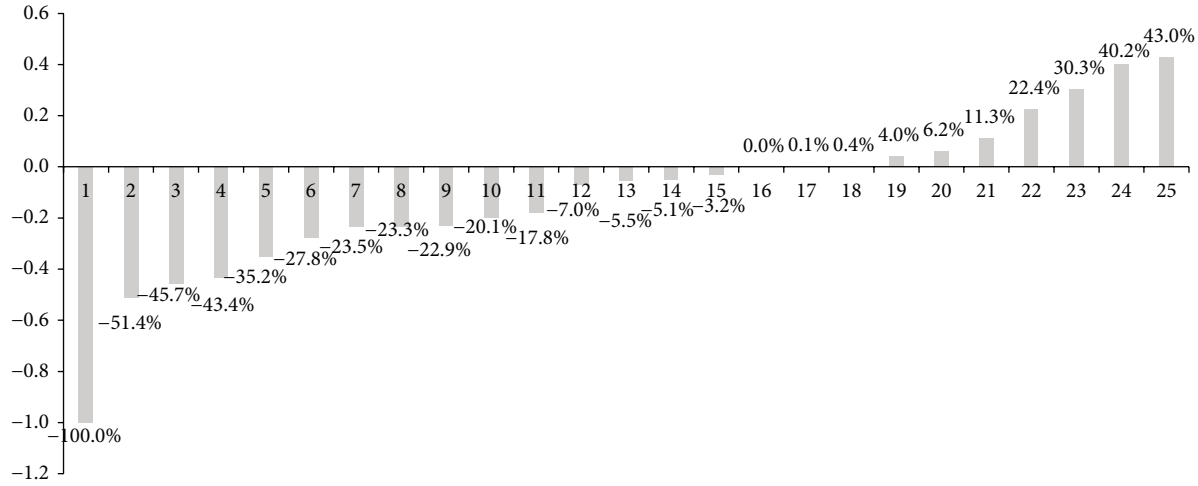


Figure 3: Changed liability for retirement allowance with K-IFRS adoption.

Table 4: Important actuarial assumptions from public disclosure.

Assumption	Case 1	Case 2	Case 3	Case 4
Discount factor	4.95%	7.37%	6.55%	5.39%
Inflation rate		2.50%	2.50%	
Interest rate	3.50%	5.85%	5.85%	4.48%
Wage increase rate	6.15%	3.79%	3.68%	Standard* + 3.33%
Change of liability	22.38%	−51.36%	N/A	6.21%

*Standard wage increase announced by Korea Insurance Development Institute.

investor cannot judge if the assumptions are appropriate or not.

4. Discussion

In this case study, we review the differences of liability for retirement allowance before and after adoption of K-IFRS and pension plan. With the comparison of financial reports for same year company data, we showed that the difference was not recognizable only if the PBO liability estimation is based on reasonable actuarial assumptions. However, some companies used quite different discount factor or wage increase rate and it resulted in big differences in their pension related liability estimation. According to previous research, it can be abused for earning management. Therefore, additional regulations should be added including requirements of proper public announcement for the information.

We hope that future research will continue along the lines of this study by addressing its limitation. This study measured the differences of liability estimation based on individual firm's announcements. Developing more cases with firm internal financial information and developing proper regulations to compare exact financial status of firms especially for liability of retirement allowances could be followed.

Conflict of Interests

The author declares that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government (NRF-2013S1A5A8024133).

References

[1] J. R. Francis and S. A. Reiter, "Determinants of corporate pension funding strategy," *Journal of Accounting and Economics*, vol. 9, no. 1, pp. 35–59, 1987.

[2] D. Bergstresser, M. Desai, and J. Rauh, "Earnings manipulation, pension assumptions, and managerial investment decisions," *The Quarterly Journal of Economics*, vol. 121, no. 1, pp. 157–195, 2006.

[3] M. R. Sankar and K. R. Subramanyam, "Reporting discretion and private information communication through earnings," *Journal of Accounting Research*, vol. 39, no. 2, pp. 365–386, 2001.

[4] H. Stolowy and G. Breton, "Accounts manipulation: a literature review and proposed conceptual framework," *Review of Accounting and Finance*, vol. 3, no. 1, pp. 5–92, 2004.

[5] C. W. Kang, "Influences of the introduction of IFRS upon transparency of financial accounting and the corporate tax," *Korea International Accounting Review*, vol. 35, pp. 1–26, 2011.

[6] S. W. Lim and W. C. Lee, "The effects of the IFRS adoption on financial statements changes," *Korea International Accounting Review*, vol. 34, pp. 293–312, 2010.

[7] M. E. Barth, W. H. Beaver, and W. R. Landsman, "The market valuation implications of net periodic pension cost components," *Journal of Accounting and Economics*, vol. 15, no. 1, pp. 27–62, 1992.

[8] M. E. Barth, "Relative measurement errors among alternative pension asset and liability measures," *The Accounting Review*, vol. 66, no. 3, pp. 433–463, 1991.

[9] A. I. Blankley and E. P. Swanson, "A longitudinal study of SFAS 87 pension rate assumptions," *Accounting Horizons*, vol. 9, pp. 1–21, 1995.

[10] G. Pownall and K. Schipper, "Implications of accounting research for the SEC's consideration of International Accounting Standards for U.S. securities offerings," *Accounting Horizons*, vol. 13, no. 3, pp. 259–280, 1999.

[11] M. Stone, "A financing explanation for overfunded pension plan terminations," *Journal of Accounting Research*, vol. 25, no. 2, pp. 317–326, 1987.

[12] K. J. Cho and J. S. Rho, "A study on the issues and improvement of Korean international financial reporting standards," *Korea International Accounting Review*, vol. 32, pp. 89–310, 2010.

[13] S. S. Yoon, "A study on the earnings management vehicles," *Korean Accounting Review*, vol. 29, pp. 33–59, 2004.

Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 463870, 12 pages
http://dx.doi.org/10.1155/2014/463870

Research Article

An Integrative Behavioral Model of Information Security Policy Compliance

Sang Hoon Kim,[1] Kyung Hoon Yang,[2] and Sunyoung Park[3]

[1] *Department of Business Administration, Kwangwoon University, 26 Kwangwoon-gil, Nowon-gu, Seoul 139-701, Republic of Korea*
[2] *College of Business School, University of Wisconsin-La Crosse, 1725 State Street, La Crosse, WI 54601, USA*
[3] *Namyang R&D Center, Hyundai Motor Company, 772-1 Jangdeok-dong, Hwaseong-Si, Gyeonggi-do 445-706, Republic of Korea*

Correspondence should be addressed to Kyung Hoon Yang; kyang@uwlax.edu

Received 25 February 2014; Accepted 23 April 2014; Published 28 May 2014

Academic Editor: Hangbae Chang

The authors found the behavioral factors that influence the organization members' compliance with the information security policy in organizations on the basis of neutralization theory, Theory of planned behavior, and protection motivation theory. Depending on the theory of planned behavior, members' attitudes towards compliance, as well as normative belief and self-efficacy, were believed to determine the intention to comply with the information security policy. Neutralization theory, a prominent theory in criminology, could be expected to provide the explanation for information system security policy violations. Based on the protection motivation theory, it was inferred that the expected efficacy could have an impact on intentions of compliance. By the above logical reasoning, the integrative behavioral model and eight hypotheses could be derived. Data were collected by conducting a survey; 194 out of 207 questionnaires were available. The test of the causal model was conducted by PLS. The reliability, validity, and model fit were found to be statistically significant. The results of the hypotheses tests showed that seven of the eight hypotheses were acceptable. The theoretical implications of this study are as follows: (1) the study is expected to play a role of the baseline for future research about organization members' compliance with the information security policy, (2) the study attempted an interdisciplinary approach by combining psychology and information system security research, and (3) the study suggested concrete operational definitions of influencing factors for information security policy compliance through a comprehensive theoretical review. Also, the study has some practical implications. First, it can provide the guideline to support the successful execution of the strategic establishment for the implement of information system security policies in organizations. Second, it proves that the need of education and training programs suppressing members' neutralization intention to violate information security policy should be emphasized.

1. Introduction

These days, many corporations are beginning to recognize that technology-based solutions alone cannot reduce security risks; therefore, they are beginning to emphasize the managerial factors of security as well as technological and physical ones. As managerial issues have become important, the members' compliance with the information security policy in organizations emerges as a core issue of the managerial issues [1, 2]. Even though organizations provide and support the policy and education, in order for the policies and education to be effective, each member should comply with the actual security guidance and observance of the policy.

In the paper, the authors researched to find the factors for organization members to comply with the information security policy. For that purpose, a model which was based upon the related theories was suggested and validated. The theoretical implications of this study are as follows: the study is expected to play a role of the baseline for future research about organization members' compliance with the information security policy, the study attempted an interdisciplinary approach by combining psychology and information system security research, and the study suggested concrete operational definitions of influencing factors for information security policy compliance through a comprehensive theoretical review. The derived results could be

applied to build the strategy and the future research issues will be discussed as well.

2. Literature Review

2.1. Compliance with the Information Security Policy. Many security experts use technical terminologies such as error, malfunction, breach, or failure when they explain security problems. That means that security problems are traditionally considered to be technology problems and more advanced algorithms or technologies are suggested to solve security problems. As a consequence, the more advanced security-threating technologies emerge, the more experts try to develop further advanced security technologies to nullify the new threating technologies. It is a cycle where continually arising security threats create the necessity for more advanced security techniques. This can be a waste of time and effort and, furthermore, it cannot be an ultimate solution to security. Therefore, to disconnect this endless circulation, a different approach, one that is managerially as well as technically efficient, should be considered. As managerial aspects are emphasized, members' compliance with the information security policy becomes a hot issue. Bulgurcu et al. [3] mentioned that the main stream of research of human perspective of information security is to find the factors that connect the end users' behaviors and members' compliance with the information security policy in organizations. Mistakes, errors, inappropriate usage, and ignorance of the members make the information security system of the organization dangerous [4]. Therefore, it has been recognized that appropriate knowledge and activities are the most important factors for the information systems security in the organizations. For that purpose, the most important factor is the members' compliance with the information security policy in organizations.

2.2. Theory. To build the model, instead of one main theory, four theories are used: planned action theory, rational choice theory, neutralization theory, and protection motivation theory. Even though the four theories were developed independently, all four explain the behavior of the users and all of them are harmonious in explaining security policy compliance. The research model was built based upon the four theories mentioned above.

2.2.1. Planned Action Theory and Theory of Planned Behavior. Traditionally, attitude has been considered a major variable in explaining the actions of human in social psychology. However, many scholars have insisted that other factors besides attitude should be also considered to explain the relationship among attitude, intentions of action, and action. One of the theories is the theory of reasoned action (TRA) which was suggested by Fishbein and Ajzen [5]. However, this theory's validity and the limits of the applications have been criticized. This theory assumes that each individual can control one's actions, but in the real world, there are many cases where an individual cannot control his or her actions [6]. Even though they may have a positive attitude and subjective norms, an individual cannot carry the action when they do not have opportunities and resources. Therefore, action control factors should be added to TRA to cover the limits. The extended theory is the theory of planned behavior (TPB) which was suggested by Azjen [7]. According to the theory of planned behavior, an individual will perceive the fact that they can control the actions only when they have a positive attitude and subjective norms towards the actions as well as opportunities and resources of the actions, and they will begin to have an intention of action only when they perceive the fact that they can control it.

2.2.2. Rational Choice Theory. Bulgurcu et al. [3] had researched the topic of members' compliance with the information security policy in organizations on the basis of the rational choice theory and perception of information security. The rational choice theory insists that an individual makes a decision by comparing the costs and benefits of one's decision making. The rational choice depends on the perceptions of the individual.

2.2.3. Neutralization Theory. Many researchers have suggested sanctions to security policy violators such as penalties and punishments based on the control theory [8–11]. Although control theory could explain the reason for security policy violations, the explanation of these theories is limited, because the potential factors of security policy violence are not clearly identified and these theories cannot be used to prevent violence.

Siponen and Vance [12] insisted that the fear of punishment cannot explain the policy violence actions because members also know and apply the theory to their actions. The Neutralization theory was first suggested by Piquero et al. [13] to explain crimes in criminology. The theory insists that both those that obey the rules and those that violate them respect the norms and values of the community. In spite of this, the actual reason that some people violate the rules, according to the neutralization theory, is that they somehow justify themselves [14]. Rogers and Buffalo [15] insisted that the neutralization theory is the theory that explains how people nullify the existing norms of society by justifying the violation of the norm. Sykes and Matza [14] suggested the five types of the neutralization techniques that justify the offenders. The first is the denial of responsibility with which the violator denies responsibility [14, 15]. The second is the denial of injury. Here, they insist that what they did was the best way to minimize injury to the organization. The third is the way in which it appeals to the higher loyalties of the organization. It means that the offenders admitted that they were wrong; however, they insist that their actions were performed in order to protect or support organizations such as their family, friends, or company. The fourth is the condemnation of the condemners. This means that the violators countercondemn the people who condemn the violators and neutralize their activities. The fifth is the denial of wrongdoing to the victim. They believe the victims deserved to be punished. This mentality is usually used to justify attacks on members of minority groups, such as homosexuals [16].

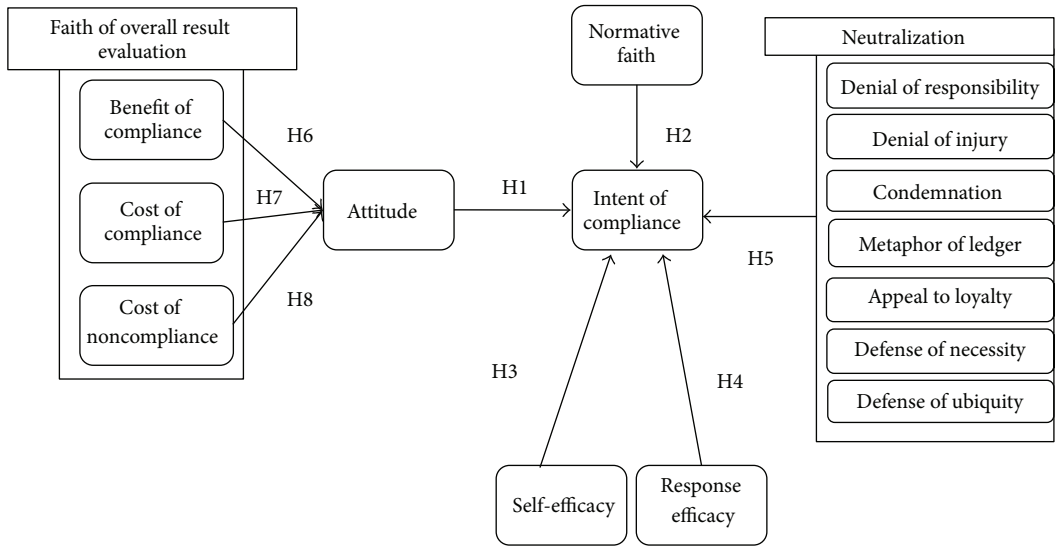


Figure 1: Research Model.

Siponen and Vance [12] studied the relationship between the neutralization theory and the violation of information security policy in organizations. In their research, they deleted "the denial of injury" which was suggested by Sykes and Matza [14] and added "the metaphor of the ledger" which was suggested by Klockars [17] and "the defense of necessity" which was suggested by Minor [18]. The basic idea of the metaphor of the ledger is that individuals think that any good deeds they have performed should outweigh a few harmful actions [13, 17]. In the defense of necessity point of view, violators believe that it is unnecessary to feel guilty as rule violations are sometimes unavoidable in life [18].

Cressey [19] introduced "the defense of ubiquity" and it was further developed by Coleman [20]. The main idea of this concept is that violators justify their activities by insisting that almost everybody commits those kinds of violations of norms. Therefore, there is no need to feel guilty.

2.2.4. Protection Motivation Theory. The protection motivation theory explains how individuals change their attitudes and actions when facing danger. This theory was developed by Rogers [21]. The theory, mainly developed in the field of psychology, tries to find the factors that affect the intentions of activity based upon "fear appeal." According to the theory, when an individual is exposed to a message of danger, protection motivations that stimulate the actions are made. This theory assumes that there are three factors in fear appeal: the severity which measures the extent of the threat, the exposure which measures the possibility of being exposed to the threats, and the response efficacy which measures how to treat the threats efficiently. Later, Rogers [22] added self-efficacy to the list.

Johnston and Warkentin [23] studied the relationship between security activity and the fear appeal and derived the research model based upon the protection motivation theory. They also added "the social effects" and "the intentions of action" which were used in technology adoption. Furthermore, they assumed that severity and danger sensitivity affected efficacy and efficacy directly affected intentions of behavior.

3. Research Model and Hypotheses

The research assumed that the attitudes, the norms, and the self-efficacy of members affected the intentions of information security policy compliance based upon the theory of reasoned action and the neutralization theory. Also based upon the research of Ajzen [7] and Bulgurcu et al. [3], the authors assumed that the belief towards information security policy compliance affected the attitude of information security policy compliance. Also, the authors assumed that the response efficacy affected the intentions of information security policy compliance based upon the protection motivation theory. Based upon the previous research and the above assumptions, the integrated behavioral research model, as described in Figure 1, was suggested.

Three independent variables, the attitude, the subjective norm, and the perceived control of actions, have been derived upon the theory of reasoned action to measure the intentions of action. In the research, the meanings of the variables are modified without loss of generality. A variable "attitude" means the attitude towards the security policy compliance, and "normative belief" means the normative belief of security policy compliance. Also, Ajzen [7] found that the "perceived action control" of the theory of reasoned action derived from the concept "self-efficacy," with the meaning of these two concepts (perceived action control and self-efficacy) being similar. In the research, based upon the research of Ajzen [7], the concept of self-efficacy towards security policy compliance implies the concept of perceived action control.

Based upon the theory of reasoned action, the following three hypotheses are set up.

Hypothesis 1. The more positive the attitude of the members of the organization towards information security policy

compliance, the higher the intention of information security policy compliance.

Hypothesis 2. The stronger the normative belief of the members of the organization towards information security policy compliance, the higher the intention of information security policy compliance.

Hypothesis 3. The stronger the self-efficacy of the members of the organization towards information security policy compliance, the higher the intention of information security policy compliance.

"Response efficacy" means the degree of individual belief that the recommended plans of action to the threats are effective [21, 24]. According to the protection motivation theory, response efficacy has positive effects in the decrease of threats by adopting the recommended plans of action. By applying the above theory to the research, the information security policy can be considered as the recommended plan of action to the threats. Therefore the degree of belief that the information security policy will be effective towards information security can be considered as a response efficacy. The higher the degree of which the members of the organization believe that the information security policy to information security is effective, the higher the intentions of information security policy compliance. Based upon the above inference, Hypothesis 4 is set up.

Hypothesis 4. The stronger the response efficacy of the members of the organization towards information security policy compliance, the higher the intention of information security policy compliance.

According to previous research, people have the intention to present themselves in an amicable image [25, 26]. Therefore, when a member of the organization commits a wrongdoing, he or she tries to justify their action and uphold their image. The neutralization theory explains how the members of an organization excuse and justify their unjustified behaviors. The neutralization theory was used in the research to explain how the members of an organization justify the violation of information security policy.

There are critics that say that the neutralization theory was developed to explain crimes such as felonies or misdemeanors and that applying this theory to the violation of information security policy is not appropriate. However, even though the violation of the information security policy is not a crime, both are violations of the social norms. Akers and Sellers [27] insisted that a violation can be applied to social norms as well as crimes. Based upon previous research [27], Siponen and Vance [12] applied the neutralization theory to the information security policy.

In the research, the neutralization theory is analyzed by the second-order construct, which consists of several subfactors. The reason of the second-order construct is that the neutralization theory consists of several dimensions, and that should be represented in the modeling [28]. Furthermore, the basic factors are already found in the previous research [12]. Hypothesis 5 is derived based upon the above reasoning.

Hypothesis 5. The higher the neutralization levels of the members of the organization, the lower the degree of information security policy compliance of the members of the organization.

According to previous research, the individual attitude towards the action is related to the individual belief towards the results of the action [5, 7]. Also, according to the rational choice theory, the individual considers the cost and benefits of the action and decides which has a larger net benefit. In the research, variables "attitude" and "belief" are brought from the rational choice theory. It means that the member will consider the cost and benefit and will decide whether he will violate the norm. For the belief of the overall evaluations, three variables are considered: benefit of compliance, cost of compliance, and cost of noncompliance. The attitude of the members would be more favorable towards the information security policy compliance when the benefit of compliance is bigger than the cost of compliance or the net benefit of the noncompliance. This assumption is in accord with previous research that insists there is a positive relationship between policy compliance and the judgment made by the cost benefit analysis of policy compliance [29]. Furthermore, Price Waterhouse Coopers [30] had similar results where there was a negative relationship between the intentions of the policy compliance and the cost of the policy compliance. Based upon previous research, the following hypotheses are derived.

Hypothesis 6. The higher the degree of the perception of benefit by the organization members towards information security policy compliance, the higher the intention of information security policy compliance.

Hypothesis 7. The higher the degree of the perception of cost by the organization members towards information security policy compliance, the lower the intention of information security policy compliance.

Hypothesis 8. The higher the degree of the perception of cost by the organization members towards information security policy noncompliance, the higher the intention of information security policy compliance.

4. Construction of Variables and Measurement

4.1. Construction of Variables. The majority of the variables used in the research came from previous research and some of them have been modified for the purpose of this research. An advantage of using variables from previous research is that the variables have already been verified. The variables are summarized in Table 1. Based upon these definitions, Likert scale-based measure indices were made.

4.2. Data Collection and Analysis. The authors surveyed the information systems users in the organizations that have information security policies. They reviewed a long list of companies that were then randomly selected. The surveyors visited the companies and explained the purposes of the

Table 1: Definition of variables.

Variables	Definition	Items	Related research
Intentions of compliance	The degree of intentions which protects the information and resources of the organization from potential threats by the compliance of information security policy	IN1~3	Bulgurcu et al. [3]
Normative belief	The degree of perceptive social pressure of neighbors such as the supervisor, colleague, and manager when they comply with the policy	NB1~3	Bulgurcu et al. [3]
Neutralization	The degree of logic which nullifies the existing norm of society that is related to the compliance of information security policy by justifying the violation of the norm.		
Neutralization theory			
Denial of responsibility	The degree that the violator denies responsibility of the compliance violation of the information security policy	DR1~3	Sykes and Matza [14] Siponen and Vance [12] S. J. Lee and M. J. Lee [16]
Denial of injury	The degree that what they did was the best way to minimize the injury of the compliance violation of the information security policy.	DI1~3	
Appeal to higher loyalties	The degree that they believe there was no other way to protect their groups except through the compliance violation of the information security policy.	AL1~3	
Condemnation of condemners	The degree that the violators condemn the condemners to neutralize the compliance violation of the information security policy.	CC1~3	
Metaphor of the ledger	The degree of belief that the compliance violation of information security policy would be accepted because of the many good deeds that they have done in the past.	ML1~3	
Defense of necessity	The degree that there is no need to feel guilty for the compliance violation of the information security policy because the violation was unavoidable.	DN1~3	
Defense of ubiquity	The degree that the violators justify the compliance violation of the information security policy by insisting that almost everybody violates policies.	DU1	
Attitude	The degree to which compliance of information security policy affects the evaluation positively	AT1~4	Bulgurcu et al. [3]
Benefit of compliance	The degree of the perception of benefit by the members of the organization towards information security policy compliance	BE1~4	Bulgurcu et al. [3]
Cost of compliance	The degree of the perception of cost by the members of the organization towards information security policy compliance	CO1~3	Bulgurcu et al. [3]
Cost of noncompliance	The degree of the perception of cost by the members of the organization towards information security policy noncompliance	NC1~4	Bulgurcu et al. [3]
Self-efficacy	The degree of the individual's confidence that they have enough techniques, knowledge, and ability on the information security policy	SE1~3	Bulgurcu et al. [3]
Response efficacy	The degree of belief that the information security policy can handle the threats efficiently	RE1~3	Johnston and Warkentin [23]

research. Eventually 32 companies from 10 industries were randomly selected. Two or three people from each rank, as well as the line worker, middle manager, and top manager in each company, answered the questionnaires. The distribution of the response of rank is 26 top managers (13.4%), 85 middle managers (43.8%), 68 line workers (35.1%), and 15 no responses (7.7%). The distribution of age is 75 in their 20's (38.7%), 61 in their 30's (31.4%), 39 in their 40's (20.1%), 14 in their 50's (7.2%), and 5 no responses (2.6%).

To measure the "neutralization," the scenario method was used. Based upon the Siponen and Vance [12] research, the scenario cases were prepared. Three scenarios were prepared and a scenario was randomly selected. The selected scenario was included in the questionnaires. After reading the scenario on the violation of the information security compliance that had happened in other companies or had a possibility of happening, the respondents answered the questionnaires. The reason that a scenario method was used is because if

Table 2: Demographic characteristics of the respondents.

Classification		Frequency	Percentage (%)
Gender	Male	127	65.5
	Female	67	34.5
Age	20~29	75	38.7
	30~39	61	31.4
	40~49	39	20.1
	50~59	14	7.2
	No response	5	2.6
Education	High school graduate	23	11.9
	Undergraduate	144	74.2
	Graduate school	27	13.9
Number of employees	<100	73	37.6
	100~1,000	61	31.4
	1,000~10,000	32	16.5
	>10,000	8	4.1
	No response	20	10.3
Annual sales volume	<$10 M	49	25.3
	$10 M~$100 M	33	17.0
	$100 M~$1000 M	28	14.4
	$1000 M~$1 B	20	10.3
	>1 B	2	1.0
	No response	62	32
Category of business	Manufacturing	33	17
	Construction	12	6.2
	Communication	30	15.5
	Transportation	1	0.5
	Distribution	12	6.2
	Service	55	28.4
	Finance	30	15.5
	And so forth	21	10.8
Rank	Line worker	68	36.4
	Middle manager	57	30.5
	General Manager	28	15.0
	CEO	26	13.9
	And so forth	8	4.3
	No response	7	3.6
Department	Planning/Administration	39	20.1
	Personnel/Education	14	7.2
	R&D	22	11.3
	Marketing	37	19.1
	Computer/Information	55	28.4
	And so forth	23	11.9
	No response	4	2.1

the questions were asked directly, then the respondents might not be willing to answer the questionnaires frankly or might answer according to perceived social norms when asked about ethical issues such as violations against the information security compliance. The advantage of the scenario method is that the respondents can answer without any guilt or fear of exposing oneself because the scenario method assumes that the case is not real or has happened to someone else [31].

A total of 207 questionnaires were collected and 13 were excluded due to insincere or incomplete answers and 194 questionnaires were used. The survey took approximately three months. The descriptive explanation is summarized in Table 2.

5. Hypotheses Test and Analysis of Results

For the test of reliability and validity of variables, the structural equation modeling (SEM) was used. The software SPSS 18.0 was used for the data analysis. The PLS method was used for the reliability, validity, and hypotheses tests. PLS is known to be suitable in analyzing relatively small size data. Furthermore, LISEL is not as accurate when two level

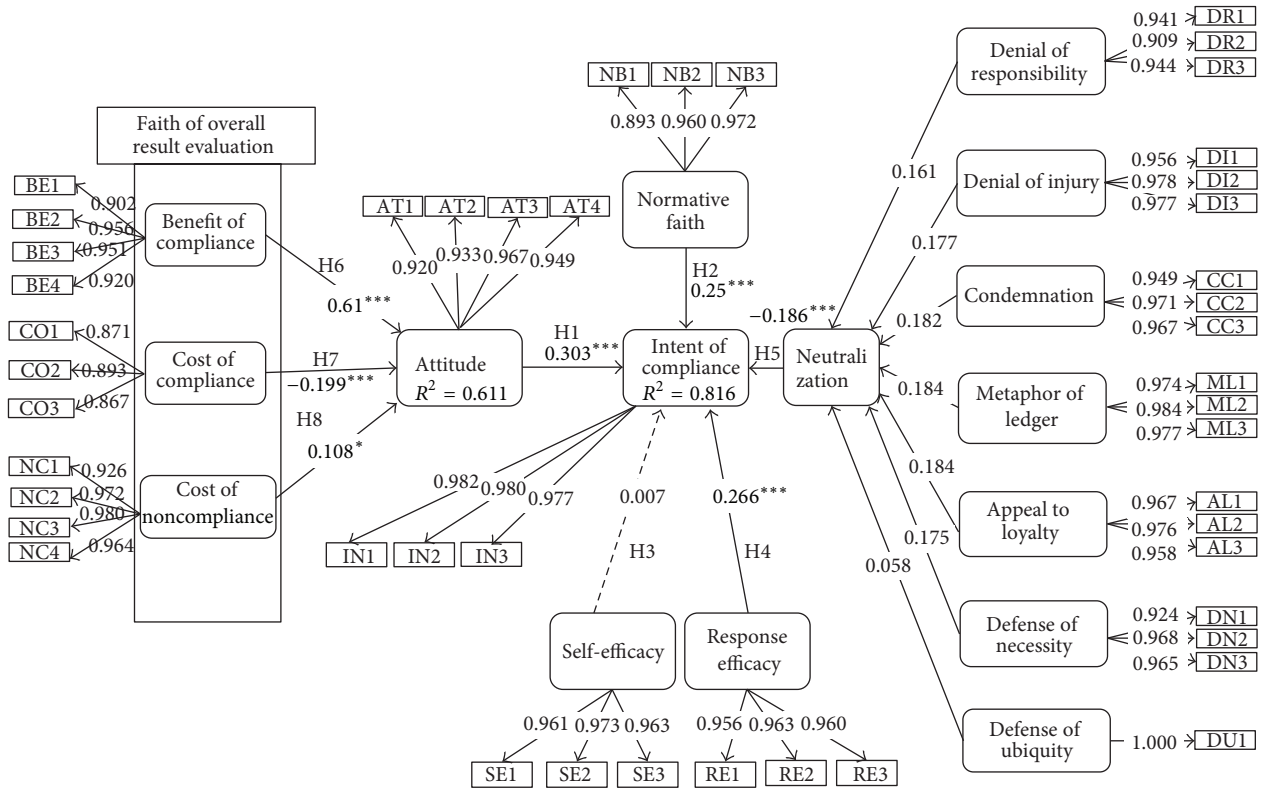


Figure 2

analyses are used, such as the neutralization of this research [32]. By considering the above factors, "SmartPLSver. 2.0. M3" was adopted.

5.1. Reliability and Validity of Variables

5.1.1. Reliability Test. According to previous research [32], when the composite reliability (CSRI) is above 0.7 and the average variance extracted (AVE) is above 0.5, the variables are considered to be internally consistent. In the research, the AVE of every variable is above 0.73, the CSRI is above 0.95, and Cronbach's alpha is also above 0.93. Therefore, the data are considered to be reliable.

5.1.2. Validity Test. It is recommended that the value of factor loading should be above 0.7 and the value of factor loading should be greater than that of the cross loading in order to have a convergent validity [33, 34]. In this research, every condition is satisfied and the result is summarized in Tables 3 and 4. To measure the discriminant validity, the values of factor loading are compared to the values of cross loading and it was found that the former is greater than the latter.

The second condition for the discriminant validity is that the square root of the values of the average variance extracted (AVE) should be bigger than the correlation coefficient. In this research, this condition is also satisfied. Therefore, the discriminant validity is satisfied.

5.2. The Fitness Test of the Model. Since the objective of PLS analysis is to maximize the variance explained, and assumptions regarding the distribution are not set up in PLS analysis, the fitness test among the explained variance of endogenous variables is preferred rather than the goodness-of-fit measures in covariance structure analysis. Therefore the forecasting fitness and the goodness-of-fit should be considered. For the forecasting fitness, R^2 is used. The range of high (above 0.26), middle (between 0.13 and 0.26), and low (above 0.02 and below 0.13) is used for classification [32]. However, R^2 is not good for a convenient measure. Therefore the value of the redundancy value of the Stone-Geisser Q2 test is more popularly used [35]. If the value of redundancy is greater than 0, it is interpreted to be forecasting fitted. Goodness-of-fit is calculated by the square root of value which is obtained by multiplying the average of R^2 and the average of communality [36]. The value of the degree of fitness should be greater than 0.1 and classified as higher (above 0.36), middle (0.25~0.36), and lower (0.1~0.25). The result is summarized in Table 5. In Table 5, R^2 of compliance intentions is 81.6% and that of attitude is 61.1%; the values of redundancy are positive numbers. The goodness-of-fit measure of the model is 0.857, which is significant. Overall, the model passes the goodness-of-fit measures test.

5.3. Results of the Hypotheses Test and Discussion. The bootstrap method was used to evaluate the path coefficient because PLS cannot show the significance of the path coefficient and the confidence level. The results are summarized in Figure 2.

Table 3: Factor loading and cross loading.

Variables	Appeal to higher loyalties (AL)	Attitude (AT)	Benefit of compliance (BE)	Condemnation of condemners (CC)	Cost of compliance (CO)	Denial of injury (DI)	Defense of necessity (DN)	Denial of responsibility (DR)
AL1	**0.967**	−0.591	−0.431	0.823	0.528	0.756	0.818	0.725
AL2	**0.976**	−0.596	−0.429	0.812	0.508	0.747	0.826	0.729
AL3	**0.958**	−0.571	−0.394	0.804	0.547	0.724	0.842	0.712
AT1	−0.641	**0.920**	0.640	−0.593	−0.493	−0.645	−0.604	−0.656
AT2	−0.499	**0.933**	0.737	−0.467	−0.415	−0.523	−0.457	−0.576
AT3	−0.574	**0.957**	0.714	−0.491	−0.499	−0.580	−0.540	−0.620
AT4	−0.560	**0.949**	0.747	−0.527	−0.456	−0.553	−0.523	−0.614
BE1	−0.484	0.734	**0.902**	−0.457	−0.422	−0.581	−0.450	−0.552
BE2	−0.433	0.723	**0.956**	−0.396	−0.410	−0.538	−0.427	−0.569
BE3	−0.345	0.680	**0.951**	−0.305	−0.393	−0.460	−0.354	−0.486
BE4	−0.343	0.671	**0.920**	−0.311	−0.401	−0.435	−0.367	−0.463
CC1	0.773	−0.488	−0.347	**0.949**	0.476	0.739	0.740	0.699
CC2	0.841	−0.551	−0.404	**0.971**	0.536	0.749	0.818	0.705
CC3	0.812	−0.556	−0.391	**0.967**	0.536	0.716	0.785	0.721
CO1	0.596	−0.515	−0.441	0.556	**0.871**	0.498	0.601	0.572
CO2	0.421	−0.408	−0.362	0.413	**0.893**	0.333	0.444	0.424
CO3	0.373	−0.351	−0.320	0.412	**0.867**	0.292	0.392	0.383
DI1	0.701	−0.553	−0.495	0.700	0.371	**0.956**	0.707	0.704
DI2	0.757	−0.599	−0.532	0.757	0.448	**0.978**	0.724	0.721
DI3	0.775	−0.631	−0.551	0.763	0.467	**0.977**	0.737	0.742
DN1	0.763	−0.515	−0.362	0.724	0.506	0.669	**0.924**	0.624
DN2	0.835	−0.536	−0.416	0.784	0.544	0.723	**0.968**	0.683
DN3	0.848	−0.564	−0.448	0.810	0.555	0.734	**0.965**	0.701
DR1	0.711	−0.678	−0.580	0.672	0.513	0.714	0.685	**0.941**
DR2	0.665	−0.523	−0.451	0.655	0.502	0.612	0.611	**0.909**
DR3	0.710	−0.628	−0.519	0.728	0.492	0.748	0.669	**0.944**

Table 4: Factor loading and cross loading.

Variables	Defense of ubiquity (DU)	Intentions of compliance (IN)	Metaphor of the ledger (ML)	Normative belief (NB)	Cost of noncompliance (NC)	Response efficacy (RE)	Self-efficacy (SE)
DU1	**1.000**	−0.551	0.722	−0.468	−0.291	−0.482	−0.351
IN1	−0.541	**0.982**	−0.677	0.811	0.488	0.794	0.579
IN2	−0.543	**0.980**	−0.668	0.788	0.496	0.789	0.582
IN3	−0.536	**0.977**	−0.669	0.829	0.511	0.798	0.583
ML1	0.704	−0.666	**0.974**	−0.602	−0.323	−0.578	−0.355
ML2	0.708	−0.679	**0.984**	−0.616	−0.361	−0.597	−0.380
ML3	0.708	−0.666	**0.977**	−0.587	−0.345	−0.589	−0.337
NB1	−0.409	0.685	−0.499	**0.893**	0.473	0.642	0.524
NB2	−0.455	0.824	−0.616	**0.960**	0.506	0.738	0.582
NB3	−0.458	0.817	−0.613	**0.972**	0.524	0.746	0.604
NC1	−0.237	0.431	−0.291	0.433	**0.926**	0.405	0.312
NC2	−0.323	0.527	−0.368	0.536	**0.972**	0.478	0.361
NC3	−0.298	0.514	−0.358	0.529	**0.980**	0.464	0.365
NC4	−0.255	0.475	−0.323	0.534	**0.964**	0.453	0.353
RE1	−0.467	0.763	−0.571	0.713	0.465	**0.956**	0.638
RE2	−0.443	0.748	−0.535	0.693	0.412	**0.963**	0.628
RE3	−0.477	0.818	−0.619	0.763	0.474	**0.960**	0.624
SE1	−0.340	0.558	−0.330	0.578	0.382	0.613	**0.961**
SE2	−0.333	0.581	−0.352	0.601	0.319	0.650	**0.973**
SE3	−0.344	0.579	−0.376	0.577	0.353	0.637	**0.963**

Table 5: Goodness-of-fit measure of the model.

	R^2	Communality	Redundancy
Normative belief (NB)		0.888	
Response efficacy (RE)		0.921	
Cost of noncompliance (NC)		0.923	
Condemnation of condemners (CC)		0.926	
Self-efficacy (SE)		0.932	
Cost of compliance (CO)		0.770	
Intentions of compliance (IN)	0.816	0.960	0.336
Benefit of compliance (BE)		0.870	
Neutralization*	1	0.735	0.221
Denial of responsibility (DR)		0.868	
Appeal to higher loyalties (AL)		0.935	
Attitude (AT)	0.611	0.884	0.084
Defense of ubiquity (DU)		1	
Denial of injury (DI)		0.942	
Defense of necessity (DN)		0.907	
Metaphor of the ledger (ML)		0.957	
Average	0.809	0.901	0.214
Fitness of the model		0.857	

*Neutralization is a second-order construct.

Hypothesis 1. The path coefficient of Hypothesis 1 is 0.303 and the t value is 3.895; therefore, this hypothesis is supported. This means that the theory of reasoned action is confirmed to be appropriate in explaining the attitude towards the information security as previous research insisted. Therefore, we can say that the more positive the attitude of the members of the organization towards information security policy compliance, the higher the intention of information security policy compliance. Based upon this research result, policy makers should make a policy which can more positively develop the attitude of the members of the organization towards information security policy compliance.

Hypothesis 2. Hypothesis 2 is supported. The path coefficient of Hypothesis 2 is 0.25 and the t value is 3.136. The result says that when the members of the organization comply with

the information security policy, they consider not only their internal factors but also their external environment as well as social factors. The environmental and social factors in the organization include the supervisors, colleagues, and top managers. Therefore, the relationship with them will affect the intentions of the information security police compliance.

Hypothesis 3. The path coefficient of Hypothesis 3 is 0.007 and the t value is 0.128 which means that there is no statistical significance between the two variables. Hence this hypothesis is rejected. Based on the research, there is no relationship between self-efficacy of the members of the organization towards information security policy compliance and the intention of information security policy compliance. This can be interpreted as the higher self-efficacy of the members of the organization towards information security policy compliance not affecting the intentions of information security policy compliance of the members of the organization. This result is different from previous results [7] and further research is required.

Hypothesis 4. The path coefficient of Hypothesis 4 is 0.266 and the t value is 4.385, so this hypothesis is supported. This result means that the more the members of an organization consider the information security policy to be effective, the more their intentions of compliance will increase. Therefore, it is important to make the members of an organization believe that the information security policy is effective.

Hypothesis 5. Hypothesis 5 is supported because the path coefficient is −0.186 and the t value is 4.552. The results can be interpreted as the members of the organization try to justify the violation of information security policy compliance through the seven types of neutralization techniques mentioned in the research. The one thing to emphasize is that all of seven types of neutralization techniques are found to be significant and all of them should be considered.

Hypothesis 6. The path coefficient and t value are 9.181 and 0.61, respectively, and this hypothesis is supported. The result says that the benefit of compliance is higher than the cost of benefit or cost of noncompliance. It means that the benefit of compliance has a higher influence than the cost of benefit or cost of noncompliance to the information security policy compliance. The benefit of compliance can include financial benefits, reputations, and positive factors for promotions, satisfaction, and pride. Therefore, policy makers should consider these factors to increase the benefit of compliance to make the members comply with the information security policy.

Hypothesis 7. Hypothesis 7 is supported because the path coefficient and the t value are 3.699 and −0.199, respectively. The results say that the more the members of the organization recognize the cost of compliance, the more the members of the organization do not comply with the information security policy. The cost of compliance can include annoyances, time effort and so on. Therefore, policy maker should consider these factors in decreasing the cost of compliance to make the members comply with the information security policy.

Hypothesis 8. The path coefficient and t value are 0.108 and 1.716, respectively, and the hypothesis is supported. The results say that the more the members of the organization recognize the cost of noncompliance, the more the members of the organization comply with the information security policy. The cost of noncompliance can include guilt, bad reputations, and disadvantages of promotion. Therefore, policy makers should consider these factors in increasing the cost of noncompliance to make the members comply with the information security policy.

6. Conclusion and Limits

6.1. Contribution. In the research, the authors try to find the factors of information security policy compliance and suggest the information security policy based upon the founded factors. For those purposes, the authors reviewed the previous research and the related literature. They reviewed the concept of information security and security policy. After that, based upon the literature review, they derived the factors which affect the intentions of policy compliance. In detail, they derived attitude, normal belief, and self-efficacy based upon the theory of reasoned action, seven factors from the neutralization theory, and response efficacy from the protection motivation theory. Based upon the mentioned theory, they set up the model and hypotheses, analyze, and found the seven out of eight hypotheses to be supported.

6.2. Limitations. This paper also has the following limitations. The first is the application of multiple theories. By using multiple theories, coordination can be an issue. However, the authors tried to find the common factors of the theory for the one subject. The second is the collection of data. Because the authors collected the companies that have security, it is possible that the data collection is biased. Lastly, there are factors other than the behavioral effects affecting the security. Those factors should also be considered in future research.

In spite of the above limits, the research has the following theoretical implications. First, the authors found the factors based upon the several previous theories, and they expect that these founded factors could be used as the factors towards the intentions of information security policy compliance for future research. Second, they adopted several theories from several arenas such as neutralization theory in criminology and combined them with the theories in the information systems field. Third, they defined the construction of the factors which were obtained through literature. These variable constructions would be used for future research in the area of information security policy.

6.3. Implications. The practical implications of this research are as follows. First, the result of the research can be used as the guideline for the practitioners. Second, the research shows that there is a positive relationship between the members' belief of security policy effectiveness and policy compliance. Therefore this research would provide the theoretical foundations for the cost and benefit of the policy compliance. Therefore, the more the members trust security policy, the more the members comply with the policy. As

such, this finding can be used as the foundation of security policy education. Third, the research found that neutralization weakens the intentions of the policy compliance, and, therefore, the organization needs some training programs or education which oppresses neutralization. Fourth, the research found that response efficacy affects the intentions of policy compliance but self-efficacy does not. It implies that the education program which enlightens members that the security policy is actually effective to the organization security is better than the reinforcement of techniques of the members to security.

Conflict of Interests

The authors declare that they have no conflict of interests regarding the publication of this paper.

Acknowledgment

The present research has been conducted by the Research Grant of Kwangwoon University in 2013.

References

[1] S. R. Boss, L. J. Kirsch, I. Angermeier, R. A. Shingler, and R. W. Boss, "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security," *European Journal of Information Systems*, vol. 18, no. 2, pp. 151–164, 2009.

[2] M. Siponen, S. Pahnila, and A. Mahmood, "Employees' adherence to information security policies: An Empirical Study," in *New Approaches for Security, Privacy and Trust in Complex Environments*, H. Venter, M. Eloff, L. Labuschagne, J. Eloff, and R. von Solms, Eds., Springer, Boston, Mass, USA, 2007.

[3] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly: Management Information Systems*, vol. 34, no. 3, pp. 523–548, 2010.

[4] M. Durgin, *Understanding the Importance of and Implementing Internal Security Measures*, SANS Institute Reading Room, 2007.

[5] M. Fishbein and I. Ajzen, *Belief, Attitude, Intention, and Behavior: An Introduciton to Theory and Research*, Addison-Wesley, Reading, UK, 1975.

[6] K. L. Johnston and K. M. White, "Binge-drinking: a test of the role of group norms in the theory of planned behaviour," *Psychology and Health*, vol. 18, no. 1, pp. 63–77, 2003.

[7] I. Ajzen, "The theory of planned behavior," *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp. 179–211, 1991.

[8] M. Theoharidou, S. Kokolakis, M. Karyda, and E. Kiountouzis, "The insider threat to information systems and the effectiveness of ISO17799," *Computers and Security*, vol. 24, no. 6, pp. 472–484, 2005.

[9] J. T. Scholtz, "Enforcement policy and corporate misconduct: the changing perspective of deterrence theory," *Law and Contemporary Problems*, vol. 60, pp. 253–268, 1997.

[10] D. W. Straub and W. D. Nance, "Discovering and disciplining computer abuse in organizations: A Field Study," *MIS Quarterly*, vol. 14, pp. 45–60, 1990.

[11] J. A. Hoffer and D. W. Straub, "The 9 to 5 underground: are you policing computer crimes?" *Sloan Management Review*, vol. 30, pp. 35–43, 1989.

[12] M. Siponen and A. Vance, "Neutralization: new insights into the problem of employee information systems security policy violations," *MIS Quarterly: Management Information Systems*, vol. 34, no. 3, pp. 487–502, 2010.

[13] N. L. Piquero, S. G. Tibbetts, and M. B. Blankenship, "Examining the role of differential association and techniques of neutralization in explaining corporate crime," *Deviant Behavior*, vol. 26, no. 2, pp. 159–188, 2005.

[14] G. Sykes and D. Matza, "Techniques of neutralization: a theory of delinquency," *American Sociological Review*, vol. 22, no. 6, pp. 664–670, 1957.

[15] J. W. Rogers and M. D. Buffalo, "Neutralization techniques: toward a simplified measurement scale," *Pacific Sociological Review*, vol. 17, no. 3, pp. 313–331, 1974.

[16] S. J. Lee and M. J. Lee, "An Exploratory Study on the Information Security Culture Indicator," *Informatization Policy*, vol. 15, no. 3, pp. 100–119, 2008.

[17] C. B. Klockars, *The Professional Fence*, Free Press, New York, NY, USA, 1974.

[18] W. W. Minor, "Techniques of neutralization: a reconceptualization and empirical examination," *Journal of Research in Crime and Delinquency*, vol. 18, no. 2, pp. 295–318, 1981.

[19] D. R. Cressey, *Other People's Money: A Study in the Social Psychology of Embezzlement*, Free Press, Glencoe, Ill, USA, 1953.

[20] J. W. Coleman, "Toward an integrated theory of whitte-collar crime," *American Journal of Sociology*, vol. 93, pp. 406–439, 1987.

[21] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," *Journal of Psychology*, vol. 91, pp. 93–114, 1975.

[22] R. W. Rogers, "Cognitive and psychological process in fear appeals and attitude change: a revised theory of protection motivation," in *Social Psychology*, J. Cacioppo and R. Petty, Eds., Guilford, New York, NY, USA, 1983.

[23] A. C. Johnston and M. Warkentin, "Fear appeals and information s ecurity behaviors: An Empirical Study," *MIS Quarterly: Management Information Systems*, vol. 34, no. 3, pp. 549–566, 2010.

[24] K. Witte, "Putting the fear back into fear appeals: the extended parallel process model," *Communication Monographs*, vol. 59, pp. 329–349, 1992.

[25] J. Greenberg, "The cognitive geometry of employee theft: negotiating "the line" between taking and stealing," in *Dysfunctional Behavior in Organizations: Nonviolent Behaviors in Organizations. Part B*, R. Griffin, A. O'Leary-Kelly, and J. Collins, Eds., JAI Press, Stamford, Conn, USA, 1998.

[26] S. L. Robinson and M. S. Kraatz, "Constructing the reality of normative behavior: the use of neutralization strategies by organizational deviants," in *Dysfunctional Behavior in Organizations: Violent & Deviant Behavior. Part A*, R. Griffin, A. O'Leary-Kelly, and J. Collins, Eds., JAI Press, Stamford, Conn, USA, 1998.

[27] R. L. Akers and C. S. Sellers, *Criminological Theories: Introduction, Evaluation, and Application*, Roxbury Press, Los Angeles, Calif, USA, 4th edition, 2004.

[28] S. Petter, D. Straub, and A. Rai, "Specifying formative constructs in information systems research," *MIS Quarterly: Management Information Systems*, vol. 31, no. 4, pp. 623–656, 2007.

[29] T. R. Tyler and S. L. Blader, "Can businesses effectively regulate employee conduct? The antecedents of rule following in work

settings," *Academy of Management Journal*, vol. 48, no. 6, pp. 1143–1158, 2005.

[30] Price Waterhouse Coopers, *Employee Behavior Key to Improving Information Security*, New Survey Finds, 2008.

[31] L. K. Trevino, "Experimental approaches to studying ethical-unethical behavior in organizations," *Business Ethics Quarterly*, vol. 2, no. 2, pp. 121–136, 1992.

[32] W. W. Chin, "Issues and opinion on structural equation modeling," *MIS Quarterly: Management Information Systems*, vol. 22, no. 1, pp. 7–16, 1998.

[33] D. Gefen and D. W. Straub, "A practical guide to factorial validity using PLS-Graph: tutorial and annotated example," *Communications of the Association for Information Systems*, vol. 16, no. 5, pp. 91–109, 2005.

[34] M. Srite and E. Karahanna, "The role of espoused national cultural values in technology acceptance," *MIS Quarterly: Management Information Systems*, vol. 30, no. 3, pp. 679–704, 2006.

[35] J. Cohen, *Statistical Power Analysis for the Behavioral Sciences*, Lawrence Erlbaum, 2nd edition, 1988.

[36] M. Tenenhaus, V. E. Vinzi, Y. M. Chatelin, and C. Lauro, "PLS path modeling," *Computational Statistics & Data Analysis*, vol. 48, no. 1, pp. 159–205, 2005.

Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 614201, 4 pages
http://dx.doi.org/10.1155/2014/614201

Research Article

The Strategic Measures for the Industrial Security of Small and Medium Business

Chang-Moo Lee

Department of Police Administration (Criminal Justice), Hannam University, Daejeon 306-791, Republic of Korea

Correspondence should be addressed to Chang-Moo Lee; jbalanced@gmail.com

Received 28 March 2014; Accepted 8 April 2014; Published 11 May 2014

Academic Editor: Hangbae Chang

The competitiveness of companies increasingly depends upon whether they possess the cutting-edge or core technology. The technology should be protected from industrial espionage or leakage. A special attention needs to be given to SMB (small and medium business), furthermore, because SMB occupies most of the companies but has serious problems in terms of industrial security. The technology leakages of SMB would account for more than 2/3 of total leakages during last five years. The purpose of this study is, therefore, to analyze the problems of SMB in terms of industrial security and suggest the strategic solutions for SMB in South Korea. The low security awareness and financial difficulties, however, make it difficult for SMB to build the effective security management system which would protect the company from industrial espionage and leakage of its technology. The growing dependence of SMB on network such as internet, in addition, puts the SMB at risk of leaking its technology through hacking or similar ways. It requires new measures to confront and control such a risk. Online security control services and technology deposit system are suggested for such measures.

1. Introduction

The development of technology entails the possibility of leakage [1]. South Korea has shown rapid growth in technology during the past 20 years, particularly in IT sector. The remarkable development in technology increased, however, a risk of technology leakage. The leakage of industrial technology presupposes, therefore, high technology and marketability [2–4]. South Korea did not possess high technology to be leaked in 1960s and 1970s when main industries were shoes and textiles.

Since the 1980s, however, South Korea has rapidly been developing in such industries as telecommunication, automobile, ship-building, and electronics. Many companies in these industries have possessed their own cutting-edge technology. The companies with world-class technology have achieved dominant positions in the world market. The Swiss International Institute for Management Development (IMD) evaluated South Korea's technological competitiveness 11th in the world in 2013 [5].

The growing portion of the PCT (patent cooperation treaty) applications would also refer to the technological power which subsequently increases the possibility of technology leakage. South Korea ranked fifth in terms of PCT filing. South Korea filed 11,848 PCT applications in 2012, representing an increase of 13.4% on 2011. This corresponds to 6.1% of all PCT applications filed in the world ([6, Pages 24–27]).

Samsung acquired 4,676 patents in the United States in 2013, the second highest in the world, after IBM (IFI claims patent services, 2014). In addition, ETRI (Electronics and Telecommunications Research Institute) of South Korea was reported to register patents the most in the world in a comprehensive evaluation conducted for research institutes, universities, and government agencies, followed by MIT and Stanford University in the United States [7].

Thus, South Korea has been described as an emerging economic powerhouse with high technologies in many industries. Since such technologies have astronomical economic value, many foreign and domestic companies seem to have a strong interest in the technologies, which might drive them to commit illegal activities such as industrial espionage.

In addition, lots of technology leakage occurs among the small and medium business (SMB) because SMB occupies

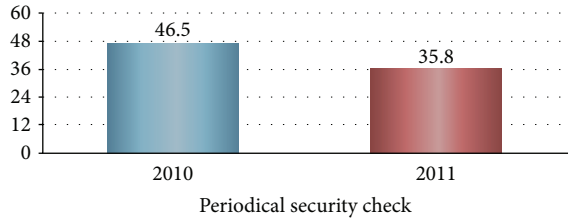


Figure 1: Periodical security check of SMB (%). Source: KISA, information security survey, 2012.

Table 1: The recent damage trends of technology leakage of SMB (2008~2012).

Year	Percentage of technology leakage	Average amount of damage per case (US $)	Number of samples
2008	15.3%	901,000	1,500
2009	14.7%	1,020,000	1,500
2010	13.2%	1,490,000	1,350
2011	12.5%	1,580,000	1,475
2012	12.1%	1,570,000	1,501

Sources: small and medium business administration, *A Report on Technology Leakage of SMB*, 2013.

most of the companies and lacks in the investment of security. The technology leakages of SMB would account for more than 2/3 of total leakages during last five years [8]. Some stronger and strategic measures should be designed for the industrial security of SMB. The purpose of this study is, therefore, to analyze the problems of SMB in terms of industrial security and suggest the strategic solutions for SMB.

2. The Problems of the Industrial Security of SMB

Even though the technology leakage of SMB tends to decrease from 15.3% of the companies surveyed in 2008 to 12.1% in 2012, the average loss has been increasing from US $ 901,000 in 2008 to US $ 1,570,000 in 2012, which seemed to result from the leakage of high value technology. Moreover, 37% of SMB suffered from industrial technology leakage more than twice, which shows the loosened security measures of SMB.

On the other hand, the level of security investment of SMB is only 55% of large companies in terms of security products and services. The security expenditures of SMB occupy 11.7% of security products and 19.3% of security services, while most of companies consist of SMB; see Table 2. It shows that the security of SMB remains at a poor stage, which needs to be improved with investing more attention and resources upon security system.

The SMB's problem of security is also shown in the evaluation of security capability. SMB recorded only 58 points while large companies and R&D institutes had 89 and 88 points each in the level of security capability in 2013. The distribution of level clearly indicates the seriousness of the problem, as shown in Table 3. There was no SMB evaluated as excellent, whereas 59.4% of large companies and 45.5% of R&D institutes were evaluated as excellent. More than half of SMB were evaluated as dangerous in the level of security capability.

The sources of the industrial technology leakage show that the leakage of SMB is usually committed by retired employees. The leakage by retired employees is 74.6%, as indicated in Table 5, while it is 9.2% by current employees, 15.1% by vendor, and 15.1% by rival company. The leakage by retired employees continues to increase from 62.4% in 2008 to 74.6% in 2011, while the leakage by current employees tends to decrease from 23.6% in 2008 to 9.2% in 2011. Another significant change comes from rival company. The proportion of rival company increased from 7.9% in 2008 to 15.1% in 2011, in terms of the sources of technology leakage.

As shown in Table 5, the loosened security management (52.7%) was suggested as the major cause of SMB industrial technology leakage, followed by lack of security awareness (46.4%) and individual profit pursuit (30.3%). Complaint on company's treatment (22.4%) and financial difficulty of security investment (22.4%) were listed to be the following major causes of SMB technology leakage; see Table 4.

According to the industrial security management survey report by the small and medium business administration in 2012, in addition, SMB regarded preventing leakage threat from inside as the primary goal for the protection of industrial technology. It was shown that 71.5% of SMB surveyed selected the security efforts against inside threat as the most important one among security measures to be performed. Security awareness (36.5%) and the prevention of key personnel turnover (26.1%) were chosen to be the next important measures for industrial security. Other measures also included building supervision system of security management (21.5%) and acquiring security personnel and equipment (20.8%).

3. The Strategic Measures for the Industrial Security of SMB

3.1. Providing Online Security Control for SMB. Business work process continues to rely on online network such as internet. It is also inevitable that cutting-edge technology and competitive trade secrets should be stored to computer. The risk of leakage through online network has, therefore, been growing [9]. Most of large companies are likely to employ online security monitoring services for 24 hours a day, 365 days. The high cost of online monitoring services, however,

Table 2: Security expenditures (%).

	Government agencies	Financial institutions	Large companies	Small and medium businesses	Others	Total
Security products	33.4	19.4	**21.3**	**11.7**	14.1	100.0
Security services	28.1	12.9	**32.9**	**19.3**	6.8	100.0
Total	32.6	18.5	**23.0**	**12.8**	13.2	100.0

Source: small and medium business administration, *The Survey Report of the Small and Medium Business Administration on Industrial Security,* 2012 [10].

Table 3: Level of security capability (points, %).

	Points	Distribution of level				
		Excellent	Good	Ordinary	Weak	Dangerous
Large companies	89	59.4%	25.0%	15.6%	0.0%	0.0%
Small and medium businesses	**58**	**0.0%**	**17.3%**	**15.4%**	**15.4%**	**51.9%**
R and D institutes	88	45.5%	36.4%	18.2%	0.0%	0.0%

Source: KAIT, industrial technology security issue, 2013, vol. 9.

Table 4: Sources of SMB industrial technology leakage (multiple responses, %).

	Retired employees	Current employees	Vendor	Rival company	Others
2008	62.4	23.6	21.0	7.9	5.7
2009	67.0	19	20.4	12.2	3.6
2010	74.5	8.5	10.6	12.8	4.3
2011	74.6	9.2	15.1	15.1	3.2

Source: small and medium business administration, *The Survey Report of the Small and Medium Business Administration on Industrial Security,* 2012 [10].

makes it difficult for SMB to use the services, although SMB needs the services. The percentage of SMB experiencing damages from the intrusion of network system was 10.5% of the companies that responded to the Survey of Information Security by Korea Internet and Security Agency (KISA) in 2012. It was shown, in addition, that 63.6% of SMB did not spend any expenditure on information security. Only 1.4% of the SMB surveyed was revealed to have invested more than 10% of the expenditures for informatization to protection of information and technology. The security situation of SMB seems to have worsened. As shown in Figure 1, a periodical security check of SMB decreased from 46.5% in 2010 to 35.8% in 2011.

According to the survey report of the small and medium business administration on industrial security, in addition, 61.5% of SMB respondents answered that the government's online security control services are necessary for industrial security. Most of the companies surveyed also answered to apply for online security control service or consider applying for the service if provided. The 34.5% of the respondents would apply for the service and 50.1% answered to consider it. They also wanted the government to help them build security system with the support of industrial security education and security vulnerability assessment. Such requests would reflect the increasing needs of industrial security for SMB which could not afford to apply online security control services and hire more security personnel due to financial difficulties. It seems to be urgent that most of SMB need to build an effective security management system, which could be materialized with the strong governmental support.

3.2. Utilization of Technology Deposit System. Some large companies are trying to steal the cutting-edge technology developed by SMB which usually supplies its products to the large company. Large companies extract the technology by various methods such as demanding a detail drawing of design under the pretense of contract. The SMB would have to suffer such unfair acts by the large company due to its predominant position.

A technology deposit system was, thus, introduced to solve the problem in 2007. According to the technology deposit system, the SMB with core technology or industrial secrets can keep them at reliable public places by which its technology could be protected. When the industrial technology of the SMB is leaked out, the SMB could demonstrate and verify its development of the technology and exclusive rights by showing it stored at the deposit center.

However, a lack of awareness about the technology deposit system restricts its utilization. Only 29.4% of SMB surveyed, as indicated in Table 6, was shown to recognize the deposit system. More than 2/3 of the respondents did not know the presence of the deposit system, which reveals the problem of promotion. In addition, the burden of deposit expenses and one-year contract renewal would hamper the utilization of the system. The expansion of the technology deposit system requires, therefore, the financial support of the government to reimburse SMB for the deposit expenses, along with the active promotion of the system.

4. Conclusion

The damage of SMB from the leakage of industrial technology has been ever increasing; see Table 1. The low security awareness and financial difficulties, however, make it difficult for SMB to build the effective security management system which would protect the company from industrial espionage and leakage of its technology. The growing dependence of

Table 5: Main causes of SMB industrial technology leakage (multiple responses, %).

	Loosened security management	Lack of security awareness	Individual profit pursuit	Complaint on treatment	Financial difficulty of security investment
Percentage	52.7	46.4	30.3	22.4	22.4

Source: small and medium business administration, *The Survey Report of the Small and Medium Business Administration on Industrial Security,* 2012 [10].

Table 6: Awareness of technology deposit system (%).

	Know	Do not know
Manufacturing	32.3	67.7
Service	25.9	74.1
Construction	22.9	77.1
Total	29.4	70.6

Source: Small and medium business administration, *A Report on Technology Leakage of SMB*, 2013.

SMB on network such as internet, furthermore, puts the SMB at risk of leaking its technology through hacking or similar ways. It requires new measures to confront and control such a risk.

Online security control services and technology deposit system are suggested for such measures. These measures could enhance to a certain extent the industrial security of SMB. The low security awareness and financial difficulties seem to be the main obstacles to equip the SMB with such measures. However, these obstacles cannot be removed without a strong governmental support in financial and political ways. The economic competitiveness can be achieved with the balanced development between large companies and SMB. This is why the government should give more attention and resources to SMB to attain the goal.

Conflict of Interests

The author declares that there is no conflict of interests regarding the publication of this paper.

References

[1] C. Lee, D. Hyun, and H. Chang, *Industrial Security*, Pakyoungsa, Seoul, Republic of Korea, 2012.

[2] H. Snyder and A. Crescenzi, "Intellectual capital and economic espionage: new crimes and new protections," *Journal of Financial Crime*, vol. 16, no. 3, pp. 245–254, 2009.

[3] W. A. Stadler, "The quiet threat: fighting industrial espionage in America," *Security Journal*, vol. 25, no. 1, pp. 90–93, 2012.

[4] O. Thonnard, L. Bilge, G. O'Gorman, S. Kiernan, and M. Lee, "Industrial espionage and targeted attacks: understanding the characteristics of an escalating threat," in *Research in Attacks, Intrusions, and Defenses*, vol. 7462 of *Lecture Notes in Computer Science*, pp. 64–85, Springer, Berlin, Germany, 2012.

[5] Digital Times, "Science Technology Law should be legislated as soon as possible," January 2014.

[6] WIPO, *PCT Yearly Review: The International Patent System*, World Intellectual Property Organization, Geneva, Switzerland, 2013.

[7] Korea JoongAng Daily, "US firm ranks ETRI first for number of patents granted," April 2014.

[8] Korea National Industrial Security Center, *Industrial Security Information*, http://service4.nis.go.kr/page?cmd=preservation&menu=AAA00.

[9] H. M. Leith and J. W. Piper, "Identification and application of security measures for petrochemical industrial control systems," *Journal of Loss Prevention in the Process Industries*, vol. 26, no. 6, pp. 982–993, 2013.

[10] Korea Small & Medium Business Administration, *The Survey Report of the Small & Medium Business Administration on Industrial Security*, Small & Medium Business Administration, Seoul, Republic of Korea, 2012.