A Study on Insider Behavior Scoring System to Prevent Data Leaks

Young-Hwan Lim* · Jun-Suk Hong** · Kwang Ho Kook** · Won-Hyung Park***

Seoul National University of Science&Technology, Hyundai-Autoever

ABSTRACT

The organization shall minimize business risks associated with customer information leaks. Enhance information security activities through voluntary pre-check and must find a way to detect the personal information leakage caused by carelessness and neglect accident. Recently, many companies have introduced an information leakage prevention solution. However, there is a possibility of internal data leakage by the internal user who has permission to access the data. By this thread it is necessary to have the environment to analyze the habit and activity of the internal user. In this study, we use the SFI analytical technique that applies RFM model to evaluate the insider activity levels were carried out case studies is applied to the actual business.

요 약

조직은 고객 정보 유출과 관련된 비즈니스 위험을 최소화하고, 자발적인 사전 검사를 통해 정보 보안 활동을 강화하고 부주의 방치 사고에 의한 개인 정보의 누출을 검출하는 방법을 발견해야 한다. 최근 많은 기업들이 정보유출방지솔루션을 도입하였으나, 업무산 필요에 의한 허용된 권한을 가진 내부 사용자에 의한 유출가능성이 존재한다. 이에 정보 취급행위 및 활동에 대한 정보를 수집하여 분석할 수 있는 환경이 필요하다. 본 연구에서는 내부자의 활동 수준을 평가하기 위해서 RFM 모델을 응용한 SFI 분석기법을 활용, 실제 기업에 적용하여 사례 연구를 수행하였다.

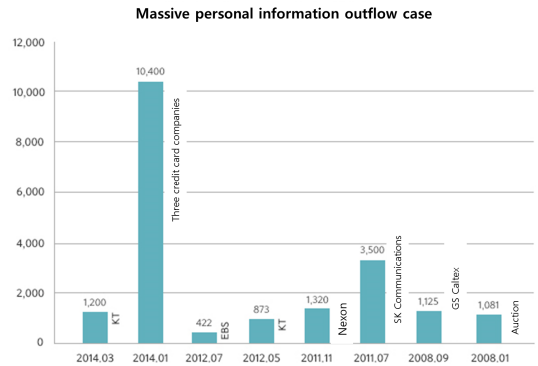
Key words : Data Leaks, Internal Controls, Security Monitoring System, Insider Threats, Insider Activity, SFI Analysis, RFM Model

접수일 2015년 8월 8일 , 수정일(1차: 2015년 9월15일), 게재확정일 2015년 9월 24일

* Hyundai-Autoever, Seoul National University of Science&Technology
** Seoul National University of Science&Technology
*** Far East University

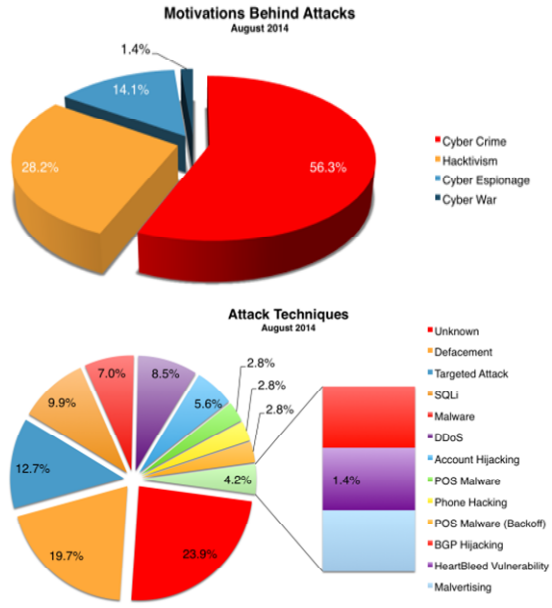
1. Introduction

The development of the Internet has provided the opportunity to live a more abundant life in addition to Swiftness activation as well as the convenience of e-government services and at the same time led to the treatment of people living with the advent of e-commerce. Nestled up to the universal service in a more interactive user with the advent of Web2.0 communication becomes possible , such as people's lives [1]. According to the Korea Internet & Security Agency (KISA) has increased more than doubled between private information practices the past three years , and manipulative attacks to steal the personal information and pointed out that developing intelligent [2]. Privacy and disclosure of personal information over the Internet when you view the leaked case can be said to be more important issues at the national level to protect the individual , not the problem.



(Figure 1) Recently , the outflow case of personal information

Privacy look at the spill type can be divided into four. First personal information DB hacked , leaked by insiders Second , Third privacy neglect , misuse due to unauthorized Fourth personal information is provided. Personal information is theft , Internet fraud , the problem on illegal spam and online , as well as voice phishing and illegal Phones(accounts) are likely to be exploited by illegal establishment , offline crime has become a serious social problem. Cyber Security Watch Survey 2011 in 21% of security incidents that occurred during the year 2010 has come to light that caused by insider [3]. Has been steadily increasing the amount of log information in the record of the leave -in and uses the current user's web environment , this log data can be used as evidence to analyze the user's behavior.



(Figure 2) August 2014 Cyber Attacks Statistics: hackmageddon.com

<Table 1> Recent security accidents

Year	Accident	Contents
2014	Three credit card companies customer information leaks	- Credit rating company of dispatch service personnel outflow customer information of three card bereavement several tens of million people - Secondary damage occurs leaked personal information (voice phishing , spam , etc.)

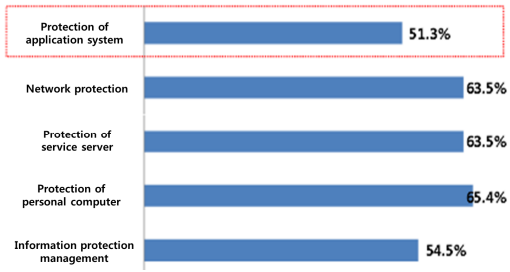
2013	Financial institutions / broadcasters computer network attack	- Diffusion of Web server hacking and malware that exploits this vulnerability - Major broadcasters three companies , Shinhan , function paralysis of warrior organi-zations such as agricultural cooperatives - 30,008 thousand units of the PC and the ATM damage
2011	SK Communicati ons information spill	- 35 million people of name and address , mobile phone number , the outflow of personal information such as encrypted password has been incorpor-ated - Secondary damage occurs leaked personal information (such as spam mail)
2011	Information spill of Hyundai Capital	- Personal information of 420,000 by hackers invaded from outside the outflow , will leak financial transaction informa-tion of 10 003 thousand people

In this study would predict that disclose personal information using their legal rights in the private insider information disclosure aspects of the insider threat. Analyzing the relevance of each log data is based on the ID / IP address to gain access to the system to deal with personal information through the Web page. This result is based on the relevance hacking , weak information , related organizations and manage the shared information between the resources in association with the log analysis system designed to provide a significant security information , and to implement.

2. Background

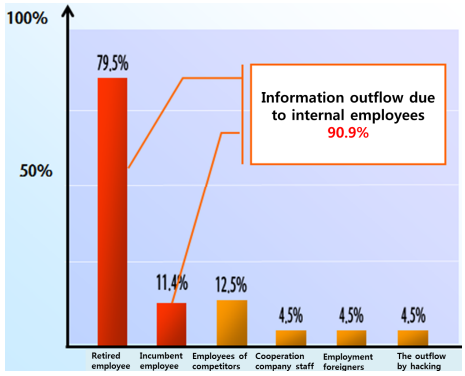
2.1 Status of internal information leakage prevention

Most of the activities to minimize internal information leakage is still limited to a personal computer, server, security and service security building. 1000 or more businesses or while going a variety of security activities , small businesses with less than 50 internal information leakage prevention activities are very vulnerable. Short sex industry technology requires a consistent and secure environment, protected , rather than building a coherent organizational level.



(Figure 3) Current status of the internal information flow prevention activities [4]

90% of all information leaks have been reported by insiders of the insider information leaks.Insider incidents are very difficult to pre-screen the IT systems of control in an accident that occurs during normal work done by the authorization woman.



(Figure 4) Insider information leaks

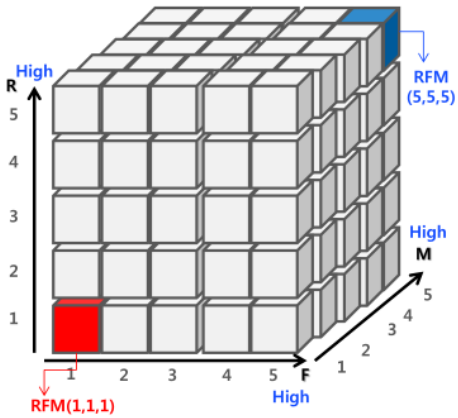
Existing literature can be summarized <Table 2>. The existing research on insider threats available through the existing literature are interspersed with researchers in the study area, their interests.

<Table 2> Existing literature related to the threat of insider

Author	Author Title	Content
J. H. Eom, S. H. Park, T. M. Chung	An Architecture of Access Control Model for Preventing Illegal Information Leakage by Insider, Journal of The Korea Institute of Information Security and Cryptology. (2010)	Insider and , for the information assets of the organization, it has a legitimate access privileges, security policy, means procedures, and employees have the knowledge and technical.
H. J. Jang	The Insurance Method of Respond Ability on Insider Cyber Threat, 2012 ROKAF Information & Communications Development International Seminar, (2012)	Insiders, full-time employees, temporary / contract employees contractors, are included, such as subcontractors.
Magklaras G.B, Furnell S.M.	A preliminary model of end user sophistication for insider threat prediction in IT systems", Journal of Comput. Secur. (2004)	Beginner in the evaluation element of knowledge and technology , general, and is distinguished from the luxury. Knowledge is a legitimate user the ability that can be part of or to win without permission or knowledge doubt that knows well all of the operational behavior of the attack system.
Shari Lawrence Pfleeger, Hunker J., Bulford, C.	Insiders Behaving Badly: Addressing Bad Actors and Their Actions, IEEE Transaction on information forensics and security. (2010)	Insider of segments, who people , important information and information people access reliable available to the system , has been granted the privilege level to allow access to information system which operates the system from the inside of the computer security boundary of, it is the people who have access of information systems and services.
Dawn Cappelli, Andrew Moore	Common Sense Guide to Prevention and Detection of	Motivation for insider to the malicious behavior is a personal financial benefit,
Randall Trzeciak, Timothy J. Shimeall	insider Threats, SEI Carnegie Mellon, (2009)	business advantage, destruction of information assets by hostile feelings of organization.
H. W. Shin	Methodology to analyze insider risk for the prevention of corporate data leakage, Journal of Korea University Graduated School, (2012)	It is internal information flow to the most serious and frequent occurrence in the threat of insider. In particular, the main data of the company , information leakage of personal information and national institutions, and that suffer major damage to companies and organizations.

2.2 Insider conduct evaluation methodology

RFM (Recency, Frequency, Monetary) model is when a business or hospital customers and patients in three kinds of indicators , frequency, based on the value of a method for classifying major customers or patients. Modern analytical methods in the most widely used in customer management aspects in marketing [5]. RFM value is calculated as the product of these three factors , but , by weighting according to the importance of each element to obtain the score of REM.



(Figure 5) RFM analysis

- Recency : When did a customer recently purchased?
- Frequency : How often did the customer purchase?
- Monetary : What is the value of goods purchased by the customer ?

In this study, a user customers from RFM model , to replace with the data to evaluate the activity level of insider. Also apply to the object you are trying to access insider assessment element of the RFM model based on the destination and use to change based on the SFI analysis.

- Span : Did insider recently when trying to access the object after the final approach?
- Frequency : How often did you insider access to the object?
- Importance : What is the significance of the objects that insiders are trying to access ?

S values are divided into five grades on the basis of the recent insider access the object. The RFM model only considers the recent visit time. However, SFI (Span, Frequency, Importance) analysis means the period of the last access date of the date of the last access to the object. The reason for this is that the insider access from time to time because the objects can be determined by the amount of activity that there are many.

Expressed insider activity level evaluation method by a formula as follows.

$$SFI = a^{*}S + b^{*}F + c^{*}I \quad (1)$$

S-values that can affect the activity level where, F value, were selected according to the weight ratio of I value [24]. It means that the frequency-wise wise this activity by that, what is the importance of the object by determining that the higher the weight, perform the core tasks of 0.2, 0.5, was determined to 0.3.

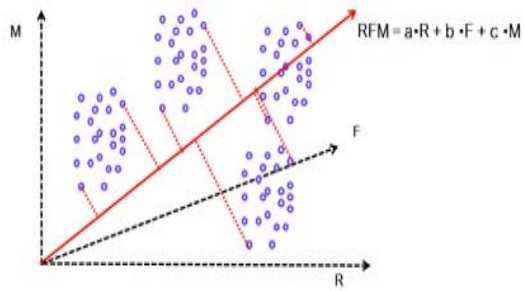
$$SFI = 0.2^{*}S + 0.5^{*}F + 0.3^{*}I \quad (2)$$

SFI score has a value between 1 and 10, and again in terms of the percentage of this by calculating the SFI score calculation expression of each ball as shown below insider.

$$SFIScore = (SFI^{*}100)/10 \quad (3)$$

The SFI score by summing the number of objects that can be accessed because the insider object can be several calculate the final SFI scores and calculate the average score for individual activity level assessment.

$$SFIAverageScore = \sum((SFI^{*}100)/10) \quad (4)$$



(Figure 6) Projection of RFM

3. Evaluation System Case

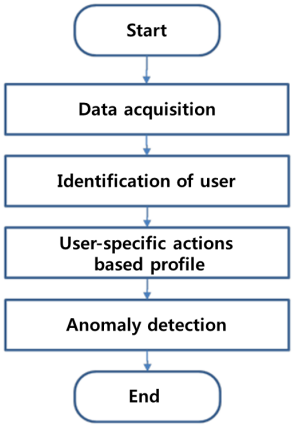
3.1 Rule-based log collection and scenario analysis

Profiling using heterogeneous devices / applications system logs the user by various acts, which is a key element to produce useful results [6].

- Step 1 (Step Rule established) : To account for the additional security features required for effective security controls and strengthening of

the system and establish a basis Rule in the individual system.

- Step 2 (Unit Classification Rule) : Rule by the nature of the individual units of the system is established and categorized by region.
- Step 3 (Correlation Rule) : It performs the correlation between Rule based on the classification units Rule. To respond more effectively to implement grouped into 1-3 steps developed through the analysis of severity. To increase the security controls associated synergies through jeongjaek interworking between the target system.
- Step 4 (Correlation analysis) : Possible leakage of inside information by a malicious act in a real environment with external or internal information handling, creating a history of performing an anomaly, pursuant to spill scenarios specific to Case. The created and developed a scenario based on Rule spill scenario.



(Figure 7) Behavior based profiling

3.2 Formal Analysis private information act

Here is a classification based on personal information life-cycle of a possible privacy threat to my personal information handling system environment [7].

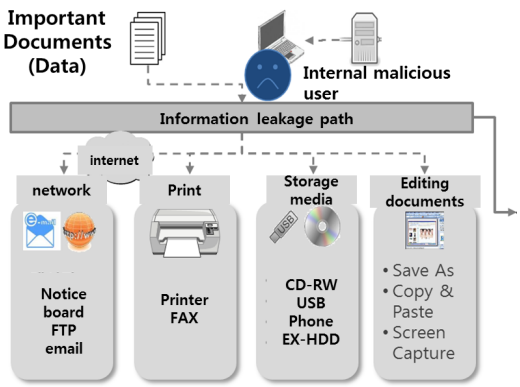
<Table 3> Threat of personal information in accordance with the life cycle

Step	Infringement Type	Threats and factors of personal information infringement
Collection	Inappropriate Collection of personal information	- Such as by using the SW the user is not aware , the collection of personal information - By crawling the content that contains personal information , collection of personal information
	There is no agreement Privacy monitoring	- By crawling the content that contains personal information , collection of personal information - Without permission , and collection of personal location information Unnecessary
	Unnecessary Collection of personal information	- On the grounds of commercial or ease of management , and collection of unnecessary personal information - Collection of sensitive information without legitimate purpose
Storage and management	Database / Protection of system rice	- Management lack of DB / system personal information is saved
	Inadvertent Disclosure of personal information	- Outflow of personal information by mistake with the system trespassing - Personal information Yu permission error, Exposure
Use and provide	Improper analysis	- And use a service that has been customized by analyzing such as purchase history without user consent - By analyzing the movement path of the user , used for the purpose of malicious Without consent of advertising
	Provision of information	- Provide product advertising and advertising of information without going through the prior consent - Advertising of spam to provide to third parties of personal information without the user's consent , SMS text , phone shipment

Destruction	Also undiscovered after holding period	- Even after holding period , personal information and location information , the US destroyed - Personal information is saved and left without deleting the stored information of the hard disk
	Illegal personal information discarded	- Arbitrarily discard the personal information those who do not have the discard privileges - Personal information discarded by the administrator of the mistake

3.3 Log collection and management in accordance with the Data Life Cycle

Log incorporate a variety of secure channel data in the Life Cycle. Collecting data in a massively parallel processing system using a dedicated collection agent. Refer integrated account information, your network credentials such as user identification is possible secure channel data, and maps the user logs in all Unified. The collected data Automatic / manual delete with archiving period setting.



(Figure 8) Structure of the evaluation system of insider Acts

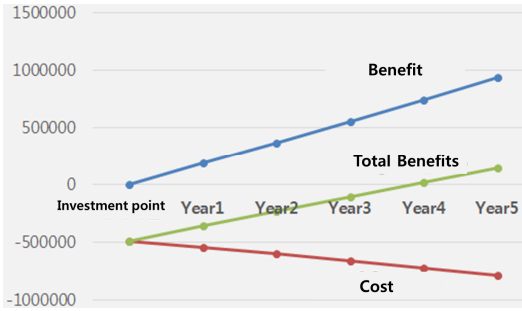
3.4 core calculation and utilization

Exponential analysis by integrating the activities of the individual observation target and integrate insider actions based on this analysis, to show the extent of the relative risk. Looking in stages collecting insider activity information, and calculates the scores for the individual activities. Give the total score for the individual actions, and individuals given a composite score ranking and grading. This compares to conduct risk between insiders and displays the relative degree of risk behavior. A relatively high risk of acts preferentially check your details. Determines a call request according to the derived risk behavior.

The basic Scoring, weighting, reflecting the monthly basic scenario scores calculated by the ratio of the sum score an individual act of ranking, rating, rating system, depending on the calculation of the 10 percentile.

3.5 Data Loss Prevention corresponding cost-benefit analysis

Insider behavior assessment system is proposed in this study can be used in conjunction with a variety of applications. How to measure cost-effectiveness of the use of insider behavior assessment system in 2009, Jinho Yoo, Sangho Jie, Jongin Lim, was the application of "Estimating Direct Costs of Enterprises by Personal Information Security Breaches" [24].



(Figure 8) Analysis of the effects that are expected to cost investment ratio of

The main cost of investment solutions,

introducing history, customization, etc. 4.9 billion in new investments, existing S / W maintenance, and maintenance personnel are expected to total 2.97 billion 7.87 billion. The main effect of spill prevention, incident response based on historical cost 6.9 billion, and security monitoring cost savings are expected to total 2.4 billion 9.3 billion.

Therefore, the net present value (total investment - total investment use) / total investment cost x ask for 100% the same as the next, investment sonsuik is reasonable investment in IT is seen to 18.5%.

$$ROI = 145{,}374/786.832X100 = 18.5\%$$

Qualitative analysis can enhance the control capabilities through a structured internal control, and to prevent leakage of customer information through awareness raising.

4. Conclusion

Using a modification of the SFI scheme RFM techniques in marketing techniques were used to build a system that evaluates the behavior of insiders. Raising the security awareness of internal staff costs and was about privacy spill response. In addition, loss of business opportunity, as well as to prevent leakage of personal information in accordance with the degree, and laid the foundation of enterprise internal control system. The subject of significant businesses and organizations must constantly monitor insider to form a high-risk group. Score model to predict future risk of an Entity study unit is based on a more historical data is also required. In more than a pattern (Anomaly Pattern) Analysis of sensitivity for visualizing the center plans to combine. To ensure the immediate data, and will be able to take a risk analysis for the behavioral symptoms associated with past data and Entity at least act.

References

[1] National Cyber Security Center, “Monthly Cyber Security” , pp.2-12, 2007.

[2] National Internet Development Agency of Korea, “Survey on the Internnet Usage” , pp 11, 2008. 11.

[3] 2011 Cyber Security Watch Survey, “CSO Magazin, U.S. Secret Service and Carnegie Mellon University&Deloitte”, 2011

[4] Chang, Hang-Bae, Song, Ji-Hoon,” The Exploratory Study on the Evaluation of Security System for Industrial Technology Leakage Prevention”, The Journal of Korea Association for Industry Security, Vol.1 No.1 2009.12

[5] Jo-Ting Wei, Shih-Yen Lin, Hsin-Hung Wu, “A review of the application of RFM model”, Journal of Business Management, Vol.4 No.19,.2010

[6] Seung Pyo Huh , Dae Sung Lee , Kui Nam Kim , “A Study on The Leak of Core Business Technologies Using Preventative Security Methods Such as Clustering”, Convergence security journal 2010.09

[7] Yeonwoo Lee Hyun-mi Jang Seng-phil Hong , “Design plan personal information management model large to protect the personal information Big data environment” , Korea Internet Information Society national conference of the Papers, VOL 13 NO. 02 PP. 0029 ~ 0030 (2012. 11)

[8] Salvatore J. Stolfo, Steven M. Bellonvin, Angelos D. Keromytis, Sara Sinclair, Sean W. Smith, “Security Beyond the Hacker”, Springer,

2008

[9] Rebecca Bacel and Peter Mell, "Intrusion Detection Systems", NIST, 2003.

[10] Carl Endorf, Eugene Schultz, Jim Mellander, "Intrusion Detection & Prevention", McGrawHill, 2004.

[11] H. Debar, M. Dacie, and A. Wepsi, "A Revised Taxonomy for Intrusion- Detection Systems", IBM Report, 1999.

[12] F.Apap, A. Honnig, S.Hershkop, E.Eskin, and S.Stolfo. Detecting malicious software by monitoring anomalous windows registry accesses. Proceedings of the Fitth International Symposium on Recent Advances in Intrusion Detection(RAID 2002), 2002.

[13] Stelios Sidiroglou, John Ioannidis, Angelos D. Keromytis, and Salvatore J. Stolfo. An Email Worm Vaccine Architecture. Proceeding of the First Information Security Practice and Experience(ISPEC 2005), 2005.

[14] Apap, F., Honkg, A., Hershkop, S., Eskin, E., Stolfo, S.J : Detecting Malicious Software by Monitoring Anomalous Windows Registry Accesses. In: Proceedings of the 5th International Symposium on Recent Advances in Intrusion Detection(RAID). 2002.

[15] Carsten Willems, Thorsten Holz, and Felix Freiling, : Toward Automated Dynamic Malware Analysis Using CWSandbox. IEEE Security & Privacy. 2007.

[16] Jong-Ho Eom, The Quantitive Evaluation of a Level of Insider Activity using SFI Analysis Techniques, Journal of Security Engineering (2013), Vol.10 No.2

[17] H. W. Shin, Methodology to analyze insider risk for the prevention of corporate data leakage, Journal of Korea University Graduated School, (2012)

[18] D. J. Ha, Customer Relation Management based on Association rule and RFM Techniques, Journal of Korea University Graduated School, (2006)

[19] J. H. Eom, S. H. Park, T. M. Chung, An Architecture of Access Control Model for Preventing Illegal Information Leakage by Insider, Journal of The Korea Institute of Information Security and Cryptology.(2010), Vol.20, No.5, pp.59-67.

[20] H. J. Jang, The Insurance Method of Respond Ability on Insider Cyber Threat, 2012 ROKAF Information& Communications Development International Seminar, (2012)

[21] Magklaras G.B, Furnell S.M., A preliminary model of end user sophistication for insider threat prediction in IT systems", Journal of Comput. Secur. (2004), Vol.24 No.5, pp.371-380.

[22] Shari Lawrence Pfleeger, Hunker J., Bulford, C., Insiders Behaving Badly: Addressing Bad Actors and Their Actions, IEEE Transaction on information forensics and security. (2010), Vol.5, No.1, pp.169-179.

[23] Dawn Cappelli, Andrew Moore Randall Trzeciak, Timothy J. Shimeall, Common Sense Guide to Prevention and Detection of insider Threats, SEI Carnegie Mellon, (2009)

[24] Jinho Yoo, Sangho Jie, Jongin Lim, Estimating Direct Costs of Enterprises by Personal Information Security Breaches, , Korea Institute of Information Security & Cryptology (2009.08)

[Author]

Young-Hwan Lim

(E-mail:yhlim@seoultech.ac.kr)
Graduate School of Public and Information Technology, Seoul National University of Science and Technology Hyudai-Autoever

Won-Hyung Park

(E-mail:whpark@kdu.ac.kr)
Department of Cyber Security, Far East University

Jun-Suk Hong

(E-mail:jun0817@kaits.or.kr)
Graduate School of Public and Information Technology, Seoul National University of Science and Technology

Kwang Ho Kook

(E-mail:khkook@seoultech.ac.kr)
College of Business and Technology, Seoul National University of Science and Technology