Copyright ⓒ 2019 KSII

Advanced insider threat detection model to apply periodic work atmosphere

Junhyoung Oh[1], Tae Ho Kim[1] and Kyung Ho Lee[1]
[1] Institute of Cyber Security & Privacy (ICSP), Korea University
Seoul, South Korea
[e-mail: {ohjun02, officialtaeho, kevinlee}@korea.ac.kr]

Received September 30, 2018; accepted March 10, 2019; published March 31 2019

Abstract

We developed an insider threat detection model to be used by organizations that repeat tasks at regular intervals. The model identifies the best combination of different feature selection algorithms, unsupervised learning algorithms, and standard scores. We derive a model specifically optimized for the organization by evaluating each combination in terms of accuracy, AUC (Area Under the Curve), and TPR (True Positive Rate). In order to validate this model, a four-year log was applied to the system handling sensitive information from public institutions. In the research target system, the user log was analyzed monthly based on the fact that the business process is processed at a cycle of one year, and the roles are determined for each person in charge. In order to classify the behavior of a user as abnormal, the standard scores of each organization were calculated and classified as abnormal when they exceeded certain thresholds. Using this method, we proposed an optimized model for the organization and verified it.

Keywords: Insider threat detection, Machine learning, Unsupervised learning, Security, Privacy Behavior

A preliminary version of this paper was presented at APIC-IST 2018, and was selected by the conference review process.
This research was supported by the MSIT(Ministry of Science, ICT), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2018-2015-0-00403) supervised by the IITP(Institute for Information & communications Technology Promotion)
Kyung Ho Lee is corresponding author of this paper.

http://doi.org/10.3837/tiis.2019.03.035 **ISSN : 1976-7277**

1. Introduction

As the information system evolves, organizations will continue to be exposed to various threats. Detecting and blocking attacks from the outside is important, but theft by insiders called "insider threat" is also one of the key challenges faced by organizations. We must address such malicious behavior, because it is greatly affecting and threatening organizations.

The subject of insider threat is an area of great interest. An insider can be defined as a "system user who is entitled to certain rights and use" [1], a "user who is legally authorized to access or determine one or more assets in an organization's structure" [2], and “An authorized user who performs unauthorized actions that loses control of computational resources” [3]. Malicious insiders are "individuals who have access to an organization's network, system, or data, or who intentionally exceed or misuses access in a way that negatively affects confidentiality, integrity, or the organization's information or information system security issues" [4]. As such, research is currently underway worldwide to prevent threats from human resources as opposed to threats caused by system flaws or vulnerabilities.

According to the 'Vormetric Insider Threat Report' [5] in 2015, 93% of the 408 respondents surveyed indicated that their organizations were vulnerable to insider threats. Examples of insider threats that have gained global attention include the cases of Bradley Manning and Edward Snowden. Bradley Manning, a former army intelligence analyst in Iraq from 2009 to 2010, withdrew hundreds of thousands of classified documents, diplomatic documents, and videos related to the Afghan and Iraqi wars from the U.S. military network and posted them on a website [6]. Edward Snowden, a computer technician in the U.S. who worked for the Central Intelligence Agency (CIA) and the National Security Agency (NSA), released various confidential NSA documents in an effort to inform the public [7].

Looking at these incidents suggests that insider threats are a threat to not only businesses but also governments and military organizations, as massive national losses could result from information leakage depending on the sizes and impacts of the organizations involved. It is crucial for government agencies to proactively detect and respond to insider threats in a timely manner. The process of detecting insider threats differs depending on the nature and function of the organization. Public organizations, military organizations, and other organizations of a public nature often repeat similar tasks each year [8]. This paper suggests a model with which to detect insider threats based on the user's behavior, limited to organizations that repeat tasks at regular intervals. Further, while various models to detect insider threats are currently being researched, studies that have been validated using actual data are rare. Therefore, this paper validates this model by applying data from an actual public institutions.

The rest of this paper is as follows. The related work on insider threat detection based on user behavior and machine learning is presented in Chapter 2. Details of the advanced insider threat detection model proposed in this paper are described in Chapter 3. The results of applying the proposed model to an actual organization are shown in Chapter 4. Finally, Chapter 5 concludes this paper.

2. Related Work

In this section, we focus on the existing studies on insider detection based on user behavior and insider threat detection using machine learning. As the number and variety of information systems are continually increasing, it is impossible to create a normal pattern of all actions in

order to detect insider threats based on scenarios or rules. Researchers have thus proposed models that can detect and prevent insider threats in advance based on an insider's psychological expression or behavior based on the records remaining in the active area of the organization. For example, Myers et al. [9] considered using a web server log file to detect malicious insiders trying to exploit internal systems. Eldardiry et al. [10] divided the activity area of the insider into the system log-on, the storage medium, the file, the HyperText Transfer Protocol (HTTP), and the e-mail domain. Philip et al. [11] detected insider threats by calculating the activity score, separating all activities performed within the organization into users and roles, and creating a tree-structured profile that makes it easy to compare one's activities with those of their other peers. Magklaras et al. [12] developed an insider threat detection tool that measures the threat levels that might originate from specific insiders based on a specific user behavior profile. Brdiczka et al. [13] developed an architecture for detecting insider threats by combining personal psychological profile information with a structural anomaly detection model, and examined ways to improve the detection accuracy. Okolica et al. [14] conducted a Probabilistic Latent Semantic Indexing (PLSI) technique with which to potentially detect employees related to insider threats using indexes related to internal data leakage. Liu et al. [15] proposed the Sensitive Information Dissemination Detection (SIDD) framework by applying statistical and signal processing techniques for traffic flow. Nurse et al. [16] presented a framework for marking the malicious threats and human factors of an attacker, as well as descriptions of the potential attacks that may occur. Matthews et al. [17] developed an active indicator using stimuli that triggered a characteristic response from the insider and detected insider threats. Maasberg et al. [18] analyzed the relationship between dark triad personality traits and insider threats. Kauh et al. [19] developed an Indicator-Based Behavior Ontology (IB2O) with which to detect potential threats based on behavioral ontology in the early stages of social networks and corporate networks.

As the size of the system grows with the incoporation of technology such as big data and cloud, the number of accumulated logs and the complexity of the analysis have increased, along with the difficulty in detecting insider threats. In order to solve these problems, studies using machine learning in the field of insider threat are being conducted. Parveen et al. [20] used unsupervised learning-based compression-based techniques to model common user behavior patterns and achieved high accuracy in classifying data streams for insider threats with unusual patterns. Parveen et al. [21] proposed an efficient approach for identifying internal threats and hiding non-ideal activities from internal threats using ensemble-based stream mining, unadjusted learning, and graph-based approaches to large data streams. Wangyan et al. [22] proposed an insider threat detection model that works by applying the cloud file share access data to three unsupervised learning algorithms to create indicators for outliers. Tuor et al. [23] developed a model for analyzing the system log in real time and scoring the abnormal behaviors of individual users. Kim et al. [24] used the Markov chain model to classify their state according to user behavior over time, and to detect insider threats using machine learning algorithms.

3. Methodology

3.1 Pre-processing

Determine if the organization is suitable for use with this model and perform data preprocessing. It is imperative to determine whether this model is available for the organization. This model is intended for organizations that repeat similar types of tasks at

given intervals. A public institution or army is a prime example of such an organization. The activities of organizations such as startup companies may vary from year to year, so this model cannot be used to effectively detect insider threats in such situations. Therefore, before using this model, it should be verified that the organization is suitable for the model.
In general, the collected data cannot be used as is. The data collected should be verified and corrected to make it usable. Keyword extraction, categorization, and normalization are carried out to convert data into a format in which it can be processed.

3.2 Feature Selection

Select various feature evaluator algorithms and search method algorithms. Feature selection is a process that involves identifying the subset of data that shows the best performance from the original data by selecting related attributes that have the most significant effect on detection or prediction among a large amount of data [25]. If there is an unrelated attribute without a feature selection process, there is a high possibility that the classification is only appropriate for the experimental data, and that it will be erroneously determined when actual new data is added. In addition, it has been proven to be efficient by extracting only closely related attributes in data mining and machine learning problems, thereby improving the analysis speed by reducing the dimension of data [26, 27]. Therefore, the efficiency of this model can be improved by using the feature selection algorithm.

The feature selection algorithm is divided into a feature evaluator algorithm and a search method algorithm [28]. In this step, the desired feature evaluator algorithms and search method algorithms are selected in order to perform the next step.

3.3 Unsupervised Learning

Select various unsupervised learning algorithms to apply to the model. Unsupervised learning [29] is a machine learning method that aims to classify unlabeled data and combine it into groups with similar functions. In general, the accuracy of supervised learning is higher than that of unsupervised learning. The reason for using unsupervised learning with this model is that unsupervised learning is more universal; in order to use supervised learning, it is necessary to detect a case in which insider detection occurs at a certain level or higher in the relevant organization. However, due to the nature of insider threats, only a few cases have been found in general organizations. Therefore, this model is employed in many organizations by using unsupervised learning.

In this study, clustering is used as a representative model of non-instructional learning. Clustering [30] collects data based on high similarity and applies the autonomous learning algorithm to the selected attributes of unlabeled data in the grouping process in order to obtain classified results. In this step, we select the desired clustering algorithms and proceed to the next step.

3.4 Optimization

Apply all of the combinations of feature selection algorithms, unsupervised learning algorithms, and standard scores to the data and derive an optimized model based on the priority criteria. The proposed insider threat detection model identifies the optimal model that changes the attribute selection algorithm, non-supervised learning algorithm, and standard score in 3D, as shown in **Fig. 1**.

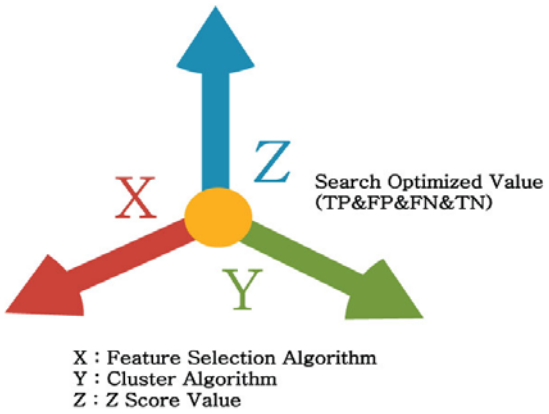


Fig. 1. Optimized model for insider threat detection

3.4.1 Criteria for insider threat

In this model, the standard score (z score) is used as a criterion for dividing the abnormal pattern of the system user and the normal pattern. The standard score [31] is a non-dimensional value that shows a statistically normal distribution as well as the position of each case on the standard deviation from the mean. The standard score is obtained using the following formula.

$$Z = \frac{X - \mu}{\sigma} \tag{1}$$

As shown in **Fig. 2**, numbers exceeding a certain standard score are classified as instances of abnormal behavior.

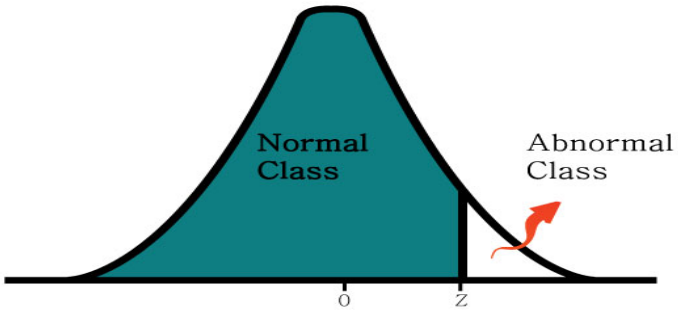


Fig. 2. Insider threat classification

x: The number of times a task person has performed a particular action
μ: Average number of times a person has been in charge of a specific action
σ: the standard deviation of the number of times a person has been in charge of a particular action

The search order is changed according to the above process, and the maximum and minimum standard scores are set to 2.0 (97.7%) and 1.2 (84.1%), respectively.

3.4.2 Priority criteria for optimization models

At the end of each cycle of the process, a model is formed, and it is determined whether the result of the verification step is an optimized model based on the priority criteria presented in **Table 1**.

Table 1. Priorities in determining optimized model

Priority ①	Does the model have a higher Accuracy than the previous model?
Priority ②	Does the model have a higher AUC than the previous model?
Priority ③	Does the model have a higher TPR than the previous model?

Scores of True Positive, True Negative, False Positive, and False Negative are required to calculate Accuracy, Area Under the Curve (AUC), and True Positive Rate (TPR). True Positive is a correct detection in the clustering algorithm when a worker classified into the abnormal cluster has exhibited an abnormal job pattern on a certain standard score basis. False Negative is a case in which a clerk classified as having a the normal business pattern in the clustering algorithm shows an abnormal business pattern according to the standard score. False Positive is a mistake in the clustering algorithm when a person classified as showing an abnormal business pattern shows a normal working pattern according to a certain standard score standard. True Negative is the correct detection in which the clusters are classified according to the normal task pattern in the clustering algorithm and the standard score is normal. These are described in **Table. 2**.

Table 2. Confusion matrix

		Predicted Class	
		ANC	NC
Class (Z Score)	ANC	TP	FN
	NC	FP	TN

※ Normal Class - NC, Abnormal Class - ANC

Accuracy is one of the key measures for assessing whether the classification is correct [32]. Accuracy indicates how much the true positive and true negative account for all scores, where the closer the ratio is to 1, the better the classification is evaluated. Accuracy is calculated using the following formula.

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN} \tag{2}$$

The ROC Curve is widely used to determine the efficiency of diagnostic methods, and is a suitable way for visualizing the performance of the classifier in order to select the appropriate operating point or decision threshold [33]. The ROC curve shows sensitivity and specificity in a two-dimensional plane. Sensitivity refers to the True Positive Rate (TPR) as a measure of

how well a model detects abnormal users, based on a certain standard score. Specificity is represented by 1-FPR (False Positive Rate), which is a numerical value of whether the model selects a normal user among the normal users. TPR and FPR are calculated using the following formulas.

$$TPR = \frac{TP}{TP + FN} \tag{3}$$

$$FPR = \frac{FP}{FP + TN} \tag{4}$$

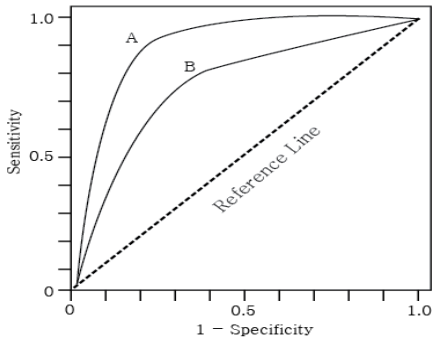


Fig. 3. Example of ROC

AUC is the abbreviation for Area Under the ROC Curve, which refers to the area under the curve [33]. The reference line shows 0.5 in **Fig. 3**, which represents a meaningful test when the curve is to the left of the reference line. Curve A is more suitable as a diagnostic model based on the fact that it has a larger area than curve B on the lower right.

4. Case Study

4.1 Pre-processing

The developed model was applied to a public institution in South Korea. This model is not targeted toward all organizations, but it is necessary to validate it, because it targets organizations that are repeatedly working at regular intervals. The organization applied to this model is divided into groups A, B, and C (A is a higher group of B and B is a higher group of C.) The tasks of each group are mutually complementary, and they repeat every year. The detailed business processes are described in **Table 3**.

This data consists of a log of approximately four years from 2014 to 2017. **Fig. 4** shows the number of workers that have accessed sensitive information on a monthly basis over the four-year period. Although there are some differences, it can be seen that the monthly access frequency exhibits a constant pattern every year. Because the business process is assigned to each group in a cycle of one year, the model can be used to evaluate threats to insiders that fall outside of the business pattern. In September and October, the portion of task force team was so high that it did not repeat the work at regular intervals and was excluded at a later stage.

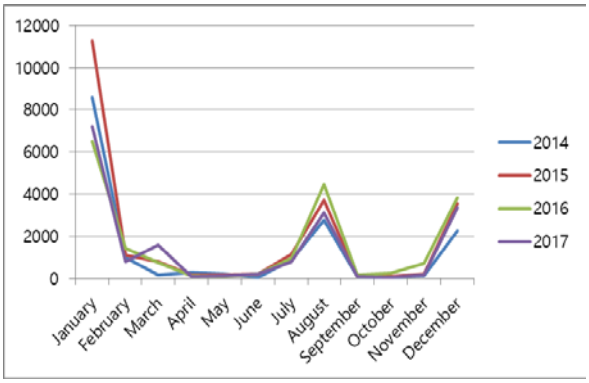


Fig. 4. Number of sensitive information accesses over four years (monthly)

Since this data contains sensitive information, it was analyzed by a relevant worker in charge of the institution. The data used in this study are log records of user-specific sensitive information access from 2014 to 2017. The actual data consists of 88410 records (2014: 22,067, 2015: 20,782, 2016: 22,077, 2017: 23,484). Each record consists of access time, access IP, access method, and accessor ID, as shown in **Table 4**.

Table 3. Processes between each group for one year

Month	Group	Work
January	A	▪ Make guideline
	B,C	▪ Identify requirements
February	A	▪ Notify groups B and C of instructions
March	C	▪ Carry out business according to guidelines ▪ Submit the results to Group B
April		
May	B,C	▪ Group B reviews the results of Group C ▪ Group C modifies results according to instructions
June		
July	B	▪ Submit the results to Group A
August	A	▪ Group A reviews the results of Group B
	B,C	▪ Groups B and C modify results according to instructions
September	-	-
October	-	-
November	B,C	▪ Identify requirements for next year
December		

Table 4. Log Format of the data

Attributes	Format	Content
Time	Date	Accessed Year-Month-Day Hour-Minute-Second
User IP	String	Accessed User IP
Action	String	One of Download, Print, or View
User ID	String	Accessed User ID

In order to analyze the work pattern in the business process over a one-year cycle, the four-year dataset is divided into months. As the sensitive information access method is limited to inquiry, downloading, and output, the pattern for each user is converted into a continuous data form which is easy to analyze. In order to analyze the successive work patterns by year, we excluded the task force team.

In order to identify the difference in the access amount of sensitive information by the characteristic of annual business process, the values of the average and standard deviation of downloading, output, and number of inquiries are extended to the attributes as shown in the table below. The standard deviation was used to determine the deviation from the mean, which is the representative value, in order to determine the reference value.

Table 5. Extended Attributes

	Mean(M)	Standard Deviation(S)
Download(D)	MD	SD
Print(P)	MP	SP
View(V)	MV	SV

In this study, these attributes are used as features and become the input values of the feature selection algorithm in the next step.

4.2 Feature Selection

We used Weka, a machine learning tool, in this study, so Weka's typical feature selection algorithms were applied. The feature evaluation algorithms used include CfsSubsetEval, SymmetricalUncert AttributeEval, CorrelationAttributeEval, InfoGainAttributeEval, and GainRatioAttributeEval. The search method algorithms used are BestFirst, Greedy Stepwise, and Ranker. The details of these algorithms are presented in **Table 6**.

Table 6. Feature Selection Algorithms [34]

	Algorithm	Content
Feature Evaluator	CfsSubsetEval	▪ Evaluating subsets value individually based on the degree of duplication. ▪ Selecting features based on the correlation between features.

	Symmetrical Uncert AttributeEval	▪ Evaluating the worth of an attribute by measuring the symmetrical uncertainty with respect to the class.
	Correlation AttributeEval	▪ Evaluates the worth of an attribute by measuring the correlation (Pearson's) between it and the class.
	Info Gain AttributeEval	▪ Evaluating the worth of an attribute by measuring the information gain with respect to the class.
	Gain Ratio AttributeEval	▪ Evaluating the worth of an attribute by measuring the gain ratio with respect to the class.
Search Method	BestFirst	▪ Searches the space of attribute subsets by greedy hill climbing augmented with a backtracking facility.
	Greedy Stepwise	▪ Performing a greedy forward or backward search through the space of attribute subsets.
	Rank	▪ Ranks attributes by their individual evaluations.

4.3 Unsupervised Learning

In this step, we used algorithms provided by Weka among the representative clustering algorithms. The corresponding algorithms are the Expectation-Maximization algorithm (EM), K-Means, Canopy, and Density-based algorithms. The details of these algorithms are presented in **Table 7**. The means and standard deviations of clusters are obtained through unsupervised learning. We then use the mean and standard deviation to determine the z value for each record.

Table 7. Unsupervised Learning Algorithms [35]

	Algorithm	Content
Unsupervised Learning	EM	▪ As a general technique for obtaining the maximum likelihood of a probabilistic model in which latent variables exist, the optimal value is derived by repeating the Expectation step and the Maximization step.
	K-means	▪ As a typical clustering algorithm, clustering is repeated using the distance to the center point of the cluster.
	Canopy	▪ This is used as a preprocessing step for other algorithms such as K-means, and is mainly used to increase clustering operation speed.

	Density Based	▪ This is an algorithm that estimates the probability distribution of the basic probability density function that cannot be observed based on the observed data.

4.4 Optimization

Accuracy, AUC, and TPR were calculated for all of the cases of feature selection (Feature Evaluator, Search Method) algorithms, Unsupervised learning algorithms, and Z-score (1.2 ~ 2.0) using the SPSS statistical tool. Based on the priority criteria, the most optimized model was derived on a monthly basis. The details are presented in **Table 8**.

For every month except January, accuracy is 0.9 or more, and the AUC has a value of 0.5 or more above the reference line in all months, with March and June each showing a maximum of 1.0. TPR shows the detection rates for insiders with abnormal patterns, which are 100% for 3, 4, 5, 6, 8, and November. Looking at the graph, we can see that the monthly accuracy, TPR, and AUC are universally constant, and we can see that the accuracy and TPR are 0.9 or higher when looking at the average. The overall score is summarized in **Fig. 5**.

Table 8. Evaluation results of the proposed insider threat detection model (monthly)

	January	February	March	April	May
Z Score	1.4	2.0	2.0	1.4	1.4
Feature Selection	Ranker	Best First	Ranker	Best First	Ranker
	InfoGain Attribute Eval	Cfs Subset Eval	InfoGain Attribute Eval	Cfs Subset Eval	Correlation Attribute Eval
Unsupervised Learning	Density Based	Canopy	K Mean	Canopy	K Mean
Accuracy	0.88	0.98	1.00	0.92	0.95
TPR	0.71	0.75	1.00	1.00	1.00
FPR	0.09	0.01	0.00	0.08	0.05
AUC	0.76	0.79	1.00	0.61	0.63

	June	July	August	November	December
Z Score	1.4	1.6	2.0	1.6	2.0
Feature Selection	Ranker	Best First	Ranker	Ranker	Ranker
	InfoGain Attribute Eval	Cfs Subset Eval	InfoGain Attribute Eval	Correlation Attribute Eval	InfoGain Attribute Eval
Unsupervised Learning	EM	EM	Density Based	K Mean	Canopy
Accuracy	1.00	0.99	0.93	0.93	0.95

TPR	1.00	0.67	1.00	1.00	0.83
FPR	0.00	0.00	0.07	0.07	0.05
AUC	1.00	0.99	0.62	0.59	0.63

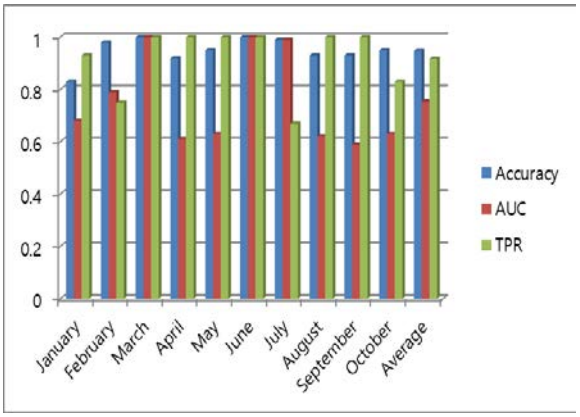
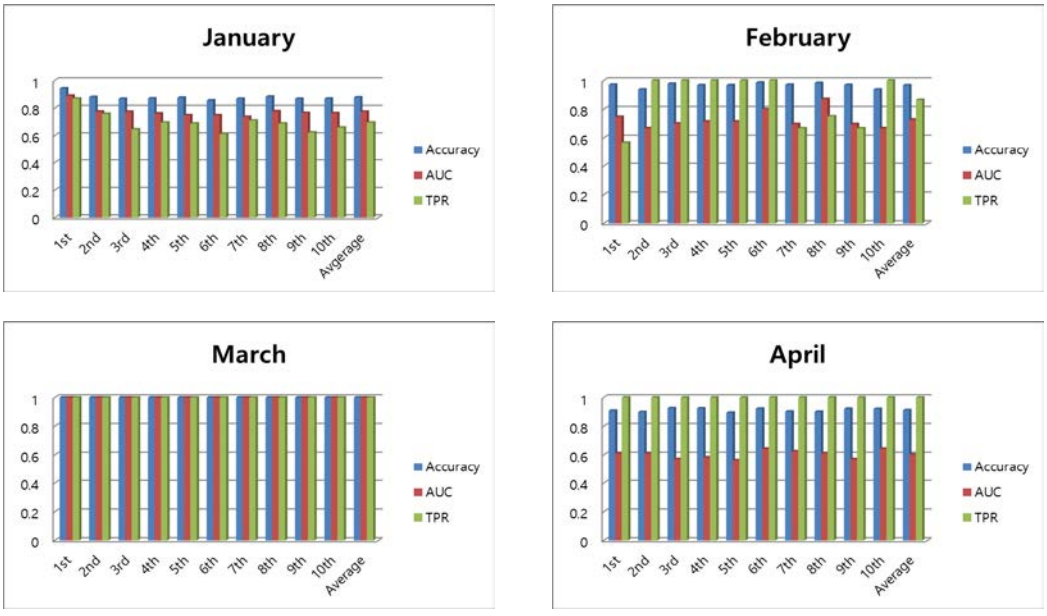


Fig. 5. Evaluation results of the proposed insider threat detection model(monthly)

4.5 Validation

In order to show that the proposed model is valid, 80% of the data is extracted at random, and the optimization model is constructed. Then, we applied the remaining 20% of the data to the optimization model. This procedure was repeated ten times, with the detailed results shown in **Fig. 6**.



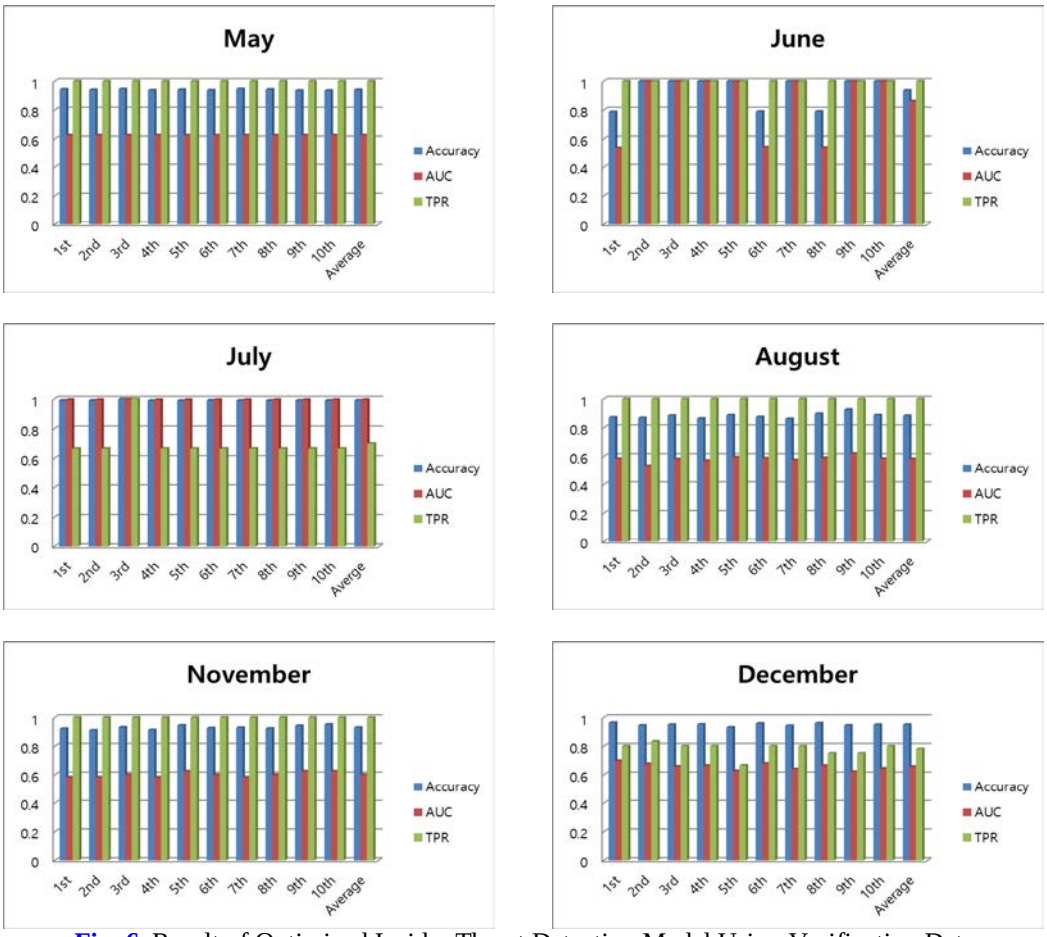


Fig. 6. Result of Optimized Insider Threat Detection Model Using Verification Data

Overall, the values of monthly accuracy, AUC, and TPR are stable. In particular, it can be seen that the verification results are constant in March, April, May, August, and November. From the verification results, we can see that the values of monthly accuracy, AUC, and TPR are similar to or better than the values shown in the optimization model. The results show that the average for each accuracy, AUC, and TPR of the verification results is similar to that shown in the optimization model. Further, this result indicates lower overall AUC and higher accuracy than the latest studies. (Lo et al. [36]: Accuracy 69%, Yuan et al. [37]: AUC 0.9449)

5. Conclusion

Insider threats do not happen very often, but many organizations are fearful of such threats they can cause huge damage if they do occur. However, there are few practical examples of insider threats and few effective tools to detect such threats. In order to solve this problem, we developed an Insider threat detection model. Since there are many ways to detect Insider threats according to the characteristics of the organization, this model focuses on the general characteristics of repeating tasks in a certain cycle and makes them available to the concerned organizations. The inspirations that the work process of the organization under study is periodic and the role of the person in charge is fixed have become the basis of the model. The model is applicable to organizations that repeat tasks at specific intervals, such as military or

public agencies. In this model, standard scores were used to classify abnormal users for insider threat detection. After repeatedly adjusting the standard scores and performing various feature selection algorithms and Unsupervised learning algorithms, an optimized model was derived by comparing Accuracy, AUC, and TPR across each result.

We applied this model to the data of actual public institutions. The data includes key features such as access frequency, IP address, and access time based on four years of logs. We presented a model that is optimized for the data by using various feature selection algorithms provided by Weka as well as unsupervised learning. In order to verify this optimized model, 80% of the data was used to generate the model; the remaining 20% of the data was applied to this model, which was then proven to be effective.

The quality of the feature is good in the case study, but it has a limitation in that the amount of features is small. Therefore, in future research, a big data analysis processing system which can process large logs should be applied to collect and analyze logs generated from a complex area such as a system user's terminal, e-mail, and web record. Therefore, more accurate insider threat detection models can be proposed.

References

[1] Neumann, Peter G. "Combatting insider threats," *Insider Threats in Cyber Security*, Springer, Boston, MA, 17-44, 2010. Article (CrossRef Link)

[2] Probst, Christian W., et al. "Countering insider threats," 2008. Article (CrossRef Link)

[3] Anderson, R. H., Bozek, T., Longstaff, T., Meitzler, W., & Skroch, M., "Research on mitigating the insider threat to information systems-# 2 (No. RAND-CF-163-DARPA)," *Santa Monica*, CA: Rand National Defense Research Institute, 2000. Article (CrossRef Link)

[4] Cappelli, D., Moore, A., Trzeciak, R., & Shimeall, T. J., "Common sense guide to prevention and detection of insider threats 3rd edition 1003)," *Software Engineering Institute*, Carnegie Mellon University: Published by CERT, 2009. Article (CrossRef Link)

[5] Poll, H., and A. Kellett. "Vormetric insider threat report," 2015. Article (CrossRef Link)

[6] THORSEN, Einar; SREEDHARAN, Chindu; ALLAN, Stuart. Wikileaks and whistle-blowing: The framing of Bradley Manning. In: Beyond WikiLeaks. Palgrave Macmillan, p. 101-122, 2013. Article (CrossRef Link)

[7] GREENWALD, Glenn. No place to hide: Edward Snowden, the NSA, and the US surveillance state. Macmillan, 2014. Article (CrossRef Link)

[8] WRIGHT, Bradley E.; DAVIS, Brian S., "Job satisfaction in the public sector: The role of the work environment," *The American Review of Public Administration*, 33.1: 70-90, 2003. Article (CrossRef Link)

[9] Myers, Justin, Michael R. Grimaila, and Robert F. Mills. "Towards insider threat detection using web server logs," in *Proc. of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies*, ACM, 2009. Article (CrossRef Link)

[10] Eldardiry, Hoda, et al., "Multi-domain information fusion for insider threat detection," in *Proc. of Security and Privacy Workshops (SPW), 2013 IEEE*, 2013. Article (CrossRef Link)

[11] Legg, Philip A., et al. "Automated insider threat detection system using user and role-based profile assessment," *IEEE Systems Journal*, 11.2, 503-512, 2017. Article (CrossRef Link)

[12] G. B. Magklaras and S. M. Furnell, "Insider threat prediction tool: Evaluating the probability of IT misuse," *Comput. Security*, vol. 21, no. 1, pp. 62–73, 1st Quart. 2002. Article (CrossRef Link)

[13] O. Brdiczka et al., "Proactive insider threat detection through graph learn- ing and psychological context," in *Proc. of IEEE Symp. SPW*, San Francisco, pp. 142–149, 2012. Article (CrossRef Link)

[14] J. S. Okolica, G. L. Peterson, and R. F. Mills, "Using PLSI-U to detect insider threats by datamining e-mail," *Int. J. Security Netw.*, vol. 3, no. 2, pp. 114–121, 2008. Article (CrossRef Link)

[15] Y. Liu et al., “SIDD: A framework for detecting sensitive data exfiltration by an insider attack,” in *Proc. of 42nd HICSS*, Jan, pp. 1–10, 2009. Article (CrossRef Link)
[16] Nurse, Jason RC, et al. "Understanding insider threat: A framework for characterising attacks," in *Proc. of Security and Privacy Workshops (SPW)*, IEEE, 2014. Article (CrossRef Link)
[17] Matthews, G., Reinerman-Jones, L., Wohleber, R., & Ortiz, E., “Eye Tracking Metrics for Insider Threat Detection in a Simulated Work Environment,” in *Proc. of the Human Factors and Ergonomics Society Annual Meeting*, vol. 61, no. 1, pp. 202-206, 2017. Article (CrossRef Link)
[18] M. Maasberg, J. Warren and N. L. Beebe, "The Dark Side of the Insider: Detecting the Insider Threat through Examination of Dark Triad Personality Traits," in *Proc. of 2015 48th Hawaii International Conference on System Sciences (HICSS)*, pp. 3518-3526, 2015. Article (CrossRef Link)
[19] Kauh, Janghyuk, et al. "Indicator-based Behavior Ontology for Detecting Insider Threats in Network Systems," *KSII Transactions on Internet & Information Systems*, 11(10), 2017. Article (CrossRef Link)
[20] Parveen, Pallabi, et al. "Unsupervised ensemble based learning for insider threat detection," in *Proc. of Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom)*, IEEE, 2012. Article (CrossRef Link)
[21] Parveen, Pallabi, et al., "Insider threat detection using stream mining and graph mining," in *Proc. of Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing (SocialCom), 2011 IEEE Third International Conference on. IEEE*, 2011. Article (CrossRef Link)
[22] Wangyan Feng et al. "Wavelet transform and unsupervised machine learning to detect insider threat on cloud file-sharing," in *Proc. of Intelligence and Security Informatics (ISI), 2017 IEEE International Conference on*, pp.155-157, 2017. Article (CrossRef Link)
[23] Tuor, Aaron, et al. "Deep learning for unsupervised insider threat detection in structured cybersecurity data streams," *arXiv preprint arXiv:1710.00811*, 2017. Article (CrossRef Link)
[24] Kim, Hong, et al. "A study on Classification of Insider threat using Markov Chain Model," *KSII Transactions on Internet and Information Systems (TIIS)*, 12(4), 1887-1898, 2018. Article (CrossRef Link)
[25] Li, Jundong, et al. "Feature selection: A data perspective," *ACM Computing Surveys (CSUR)*, 50.6 : 94, 2017. Article (CrossRef Link)
[26] Zhao, Zheng, and Huan Liu. "Spectral feature selection for supervised and unsupervised learning," *in Proc. of the 24th international conference on Machine learning*, ACM, 2007. Article (CrossRef Link)
[27] Baksai, Karim Elías Pichara, “Feature Selection to Detect Patterns in Supervised and Semi Supervised Scenarios,” *Diss. Pontificia Universidad Católica de Chile*, 2010.
[28] Khonji, Mahmoud, Andrew Jones, and Youssef Iraqi, "A study of feature subset evaluators and feature subset searching methods for phishing classification," in *Proc. of the 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference*, ACM, 2011. Article (CrossRef Link)
[29] Hastie, Trevor, Robert Tibshirani, Jerome Friedman, "Unsupervised learning," *The elements of statistical learning*, Springer New York, pp. 485-585, 2009. Article (CrossRef Link)
[30] Sharma, Narendra, Aman Bajpai, and Mr Ratnesh Litoriya, "Comparison the various clustering algorithms of weka tools," *facilities 4.7*, 2012. Article (CrossRef Link)
[31] Moos, Rudolf H., and Bernice S. Moos, “Family environment scale manual,” *Consulting Psychologists Press*, 1994.
[32] POWERS, David Martin. Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation, 2011. Article (CrossRef Link)
[33] James A Hanley and Barbara J McNeil, “The meaning and use of the area under a receiver operating characteristic (ROC) curve,” *Radiology 143.1*, pp. 29-36, 1982. Article (CrossRef Link)
[34] Lee, Hojin, et al. "FEATURE SELECTION PRACTICE FOR UNSUPERVISED LEARNING OF CREDIT CARD FRAUD DETECTION," *Journal of Theoretical & Applied Information Technology*, 96.2, 2018. Article (CrossRef Link)

[35] Nasrabadi, Nasser M. "Pattern recognition and machine learning," *Journal of electronic imaging*, 16.4 , 2007. Article (CrossRef Link)
[36] Lo, Owen, et al., "Distance measurement methods for improved insider threat detection," *Security and Communication Networks*, 2018. Article (CrossRef Link)
[37] Yuan, Fangfang, et al., "Insider threat detection with deep neural network," in *Proc. of International Conference on Computational Science*, Springer, Cham, 2018. Article (CrossRef Link)

Junhyoung Oh received the B.S. degree in electrical engineering from Korea University, Seoul, Korea. He is currently pursuing the Ph.D. degree with the graduate school of information security at Korea University. His research interests include Usable Security, Privacy, and Internet of Things.

Tae Ho Kim received the M.S. degree in information security engineering from Korea University, Seoul, Korea. His research interests include Insider Threat and Machine Learning,

Kyung Ho Lee received his Ph.D. degree from Korea University. He is now a professor in the graduate school of information management and security at Korea University, and has been leading the risk management laboratory in Korea University since 2012. He was a former CISO at Naver Corporation, and he was the former CEO of SecuBase Corporation.