International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 22 (2017) pp. 12597-12607
© Research India Publications. http://www.ripublication.com

The Judgment System for the Risk Class of Internal Data Leakage based on GRU Model

[1]Ye-Seul Lee and Myung-Ho Kim[2]

[1]M.S. Student, Software Convergence Department, Soongsil University, Seoul, 156-743, Korea.
[2]Professor, Software Convergence Department, Soongsil University, Seoul, 156-743, Korea.
[1]Orcid: 0000-0002-1713-1299

Abstract

Recently, there has been an increase in the leakage of internal data in the company. The subject of internal data leakage is the majority of Insiders. Companies are applying several security solutions to prevent data leakage. However, there is still a lack of research on solutions applying Deep Learning to detection of data leakage, which have limitations to prevent leakage beforehand. This paper proposes a method to determine the risk of internal data leakage by applying GRU among various Deep Learning models. Security events are generated for each user by mapping the security log and user data obtained through the security device to determine the risk of internal data leakage. Training data is generated based on the mapped data and it is applied to the GRU model to examine the effect of the number of hidden layer nodes and the presence or absence of the activation function dropout. Different Deep Learning models are also applied to see if GRU model is more effective than other models. Through experiments, it was confirmed that the accuracy of internal data leakage per user is determined with accuracy of about 92.2% and it was shown that the method classifying the serious category into the serious category had almost 100% accuracy rate.

Keywords: Insider Data Leakage, Risk Class, Deep Learning, GRU

INTRODUCTION

Recently, as the IT technology is advanced, it enters the Internet & dataization age. In the past, companies managed important data in form of documents in a safe. As technologies have developed, they handle their important data by saving them in a storage unit like DB. As the data possessed by companies have some economic values and their importance is increased contrary to the past, so there are increased people trying to leak such important data from companies. According to the Industrial Confidential Data Protection Center in the National Intelligence Service Korea's 'Industry Spy Exposure Status', it is found that the number of exposed cases of company's data leakage was increased about 10 times as 63 ones in 2014 compared to 6 cases in 2003. The center stated that the expected monetary loss of data-leaked companies is annual average 50 trillion KWR, equal to the annual turnover of about 4,700 small & middle firms. Data leakage accidents are more happened in companies than outside. According to the National Intelligence Service Korea's 'Status of Data Leakage by Leakage Subject', it was appeared that the rate of data leakage cases by Insiders occupied over 80% of all data leak accidents[1].

Therefore, most companies invest in the data protection like introducing various security devices for preventing data leakage. DLP(Data Loss Prevention), DRM(Digital Rights Management), NAC(Network Access Control) are representative security devices being used in companies. Besides, there are developed some systems reacting against any intrusion trial including IPS (Intrusion Prevention System) and IDS (Intrusion Detection System). However, as the increase of security devices being established separately and the variety of analysis works, there is limited in comprehensively controlling and monitoring a company's data, but trials to leak company's data are increased and tracing the intrusion route becomes more difficult.

There have been established various devices to monitor any trial to leak data from companies and to analyze such trial patterns. But, for existing devices, a security manager directly calculates the risk level of data leakage through the scenario-based analysis concerning various leakage routes and the statistical analysis, and such devices monitor the data and detect any trial to leakage them according to the calculated risks. Existing technology to monitor and detect any data leakage trial can't effectively detect any data leakage trial in advance due to limits like the increase of management points, the fragmentary monitoring work and the limited reaction .

This paper was intended to judge the risk class of Insider data leakage in using Deep Learning model in order to overcome such limits and to efficiently detect any data leakage trial in advance.

Currently, Deep Learning technology is utilized in many fields. Especially, the technology displays its good ability in the fields of image-recognition, natural language-process, voice-recognition and auto-driving, etc. However, in the security solution field detecting any data leakage trial, there lack researches utilizing Deep Learning technology. This paper proposed a system judging the risk class of Insider data leakage in using the GRU (Gated Recurrent Unit)[2] model, one of Deep Learning models.

This paper is composed as follows. Firstly, relevant researches are described and a GRU model-based system judging the risk.

Also, the proposed system's performance through an experiment of risk class judgement of Insider data leakage is evaluated and the conclusion and future researches are described.

RELEVANT RESEARCHES

Security Devices

There existed various security devices for preventing any Insider data leakage and their features were listed in the Table 1.

Table 1: Summary of Security Devices

Classification	Security Devices	Features
Network Security Devices	NAC	Solution detecting any traffic detecting a traffic trying to hack among the network traffics
	IPS	Progressive security device real-time reacting any intrusion trial before real intrusion and blocking harmful traffics by using various security technologies
	IDS	Automated system enabling to detect and react any intrusion trial by monitoring events occurred through PCs and networks
	Fire Wall	Control any access to the user's PC from outside via a network.
Sever Security Devices	DB Security	System the minimal data required for a work to the designed user by controlling an access to data and encoding the data
	Session Logging	Audit the session logs of an account including the work history and the connection history in order to judge the manager and the user's misuse of system or not.
Hard Disk Security Devices	Syslog	Save messages created by various programs and provide log messages for enabling various analysis on the created messages.
	Trip Wire	Utility discerning whether a system is hacked or not
File Security Devices	DRM	Composed of protection technology for intellectual property right of digital contents, the management technology for management efficiency, and the distribution technology for more convenient distribution environment.
	DLP	Means the prevention from company's data leakage, and real-time monitors any trail leaking a company's confidential data to outside, and blocking such trial according to the company's policy.

Deep Learning

Deep Learning is the technology classifying the data set and finding out the correlation between data by utilizing the deep neural network imitating the connectivity of human's brain and the data. The neural network of Deep Learning is composed of the input layer, the output layer and the hidden layer between the both layers. The hidden layer may be consisted of multi layers and each layer receives input signal emitted from previous layer and uses it as a new output. In each neuron, there exists an activation function for drawing out an output, and as the types of activation functions, there are the step function, the sigmoid function and the softmax function.

The algorithm of Deep Learning can be largely classified into the supervised learning, the unsupervised learning, and the reinforcement learning. The supervised learning is the way learning a computer in the situation where the label for data, that is, the explicit right answer is given. Questions can be fallen into the classification question or the regression question depending on the expected result value. Unsupervised learning is the way learning a computer in the state not giving the explicit right answer about the data differently from the supervised learning. This learning way is used in discovering any hidden feature or structure of data, and the representative way is the clustering algorithm. The reinforcement learning is the way developing the learning with gaining a certain compensation at taking any action to the given environment differently from the both ways of supervised learning and unsupervised learning. As representative models of Deep Learning, there are the Perceptron, the most basic model consisted of input layer and output layer, the Multi-Layer Perceptron[3] adding the hidden layer between the both layers for correcting the disadvantage of Perceptron impossible to learn the XOR calculation, and the RNN (Recurrent Neural Network) for processing sequent data[4], the LSTM(Long Short Term Memory)[5] complementing the long-term dependency matter of RNN, as well as the GRU(Gated Recurrent Unit), the LSTM-transforming model simply processing the structure of LSTM.

Previous Researches

As the number of Insider data leakage cases is increased contrary to the past, there have developed various researches about the solutions to detect the Insider data leakage.

Park and Jeong[6] suggested the behavior attributes for finding out an Insider with high possibility to leak Insider data of company and a technical solution handling such matter. First, they considered that an Insider’s intentional data leakage can cause substantial loss for his/her company compared to any unintentional leakage or leakage by outsider. Second, they also considered that it would be very possible to realize an effective security function. As the ways identifying the leakage-risk group among a company’s Insiders, the researchers suggested two ways as follows.

As a kind of cross-section analysis, the first way was that Insiders mutually compare and analyze each other’s behavior attributes and finding out an extraordinary candidate. The other way, a type of time-series analysis was the method finding out a person showing extraordinary change while continually observing Insiders’ behavior attributes. This way identified the leakage-risk group in considering the Insiders’ attributes, and then closely observed the candidates falling into the group and tracing their extraordinary behaviors. Rashid et al[7] proposed a way modeling a user’s normal behaviors and detecting the Insider in order to detect his/her behavioral abnormality to lead to the Insider leakage accident by using the hidden Marcov Model (HMM)[8], a statistical model being used in various fields including the voice-recognition, the natural language-process, and the pattern-recognition.

Kim[9] suggested a technique detecting an accident of company-Insider data leakage by an Insider. In his paper, the researcher suggested a technique detecting an Insider data leakage by detecting a user’s abnormal behavior based on his/her normal behaviors after modeling the Insider’s normal behavior data utilizing the Hidden Marcov Model(HMM). In order to find out the optimal performance of detection technique of Insider data leakage, the researcher carried out an experiment determining the parameters of Hidden Marcov Model, and identified that as the number of conditions was increased, the leakage detection rate was increased, too. At applying the HMM, there were 80% of detection rate and 20% of error detection rate.

In the existing paper, while the proposed leakage-risk detection technique showed improved detection effect comparing to conventional techniques in case of detecting Insider data leakage, but the technique still had the disadvantage that the responsible manager had to directly detect the patterns of data leakages and monitor data leakage risks. In case of a person leaking company's data on the basis of his/her behavior, this technique could identify a leakage-risk group by considering only the attributes having been selected, so an Insider not being fallen into the risk group might be excluded from the monitoring target. The way closely observing the people classified as the risk-group and tracing their extraordinary behaviors has the disadvantage that the manager should directly apply the way. Besides, a study proposing a way detecting any insider data leakage trial in using the Hidden Marcov Model(HMM) showed the research needs for identifying a way to finely improve the detection performance with utilizing Deep Learning algorithm like the LSTM and for modeling the Insider’s normal behaviors in detail.

In order to judge the risk classes of insider data leakages, the researcher mapped the user’s data and security events and applied them to Deep Learning model, so that any Insider data leakage can be detected in advance.

ANALYSIS AND DESIGN

Analysis of Input Data

In order to judge a risk class of Insider data leakage case, this experiment analyzed the data in using the security log by security device and the user’s data. For this purpose, it utilized the logs of security systems like the DRM, the DLP and the NAC, which were the most widely distributed and commonly used. The sample of logs being used in this experiment had the same patterns with those listed in the Table 2.

Table 2: Log data sample by device

Device Classification	Log Sample
DLP	20171111;114620;409;S7300-15;;...;203.253.25.86;A008;[SHAREFOLDER] (E:\) access to the folder. - blocks it. 20171111;131552;Credit Review Department;...;21215;...;203.253.25.10;A061;Allow to print: Allow to print the from [...] to […] of [...]. [Printing Classification:SECUMARK]
NAC	"LOG_SENSORIPSTR":"","LOG_MSG":"Agent Action Outcome. RESULT=SUCCESS, ACTION=Block the wireless LAN access, TYPE=NEW","LOG_PARENTID":"1bed89de-2f30-1034-9992-448a5bdc64bc-5c3031f3","LOG_LOGID":111,"LOG_SENSORIP":0,"LOG_IP":372465741,"LO

	G_EXTRAINFO":"","LOG_IDX":53545829,"LOG_PARENTNAME":"409"LOG_MAC":"50:B1:C3:A6:44:EF" ,"_id":75369,"LOG_DETAIL":"","LOG_USERNAME":"","LOG_DEPTNAME":"","_table":"LOG2","LOG_IPSTR":"22.48.47.135","LOG_USERID":"","LOG_TYPE":2, "_time":"2017-11-11 20:43:14+0900","LOG_TIME":"2017-11-11 20:43:14+0900","_host":"alder4"

The user's data includes the employee id, his/her full name, the date being hired, his/her position and department, and others. This leakage detection system analyzes the collected security logs and maps them with a user's data, and then saves the mapped data in an event table by Insider use, and this system has the way shown in the below Fig. 1. The system generates the data set for training by user on the basis of mapped data, which was required for this experiment.

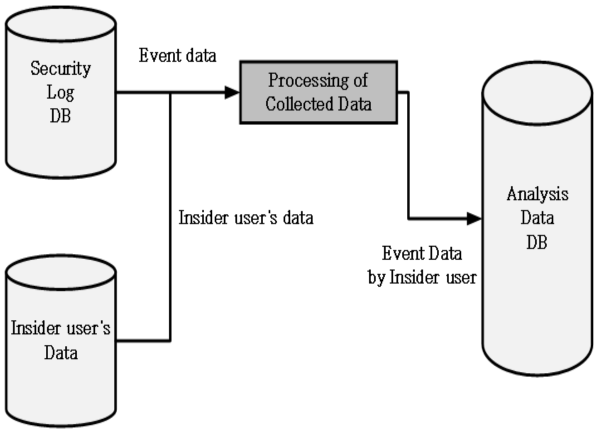

Figure 1: Mapping Method of security logs and Insider user's data

DEFINITION OF RISK CLASS

An input datum calculates the risk level value by user between 0 and 1 on the basis of unit event use by user, and are classifies into one risk group among 4-Step risk classes of normal, attention, caution and serious categories as shown in the Table 3. For a user being classified into the caution or serious classes, this leakage risk detection system gave an alarm about the user being classified into the caution or serious classes, and specially manages the user being classified into the attention class by weighting separately.

Table 3: Classification of Risk Classes

Classification of Risk Classes	Feature
Normal	Normal User
Attention	Several security events are occurred among normal users.
Caution	Weighting over 50% possibility to leak Insider data and specially controlling
Serious	Having over 90% possibility to leak Insider data and giving the risk alarm to the manager.

Judgement Process of Insider Data Leakage's Risk Class

This paper suggested a way judging the risk class of Insider data leakage in using Deep Learning Model. The proposed system's whole process course was divided into the 3 categories of Data Collection, Data Pre-Process, and Appliance of Deep Learning Model as seen in the Fig. 2.

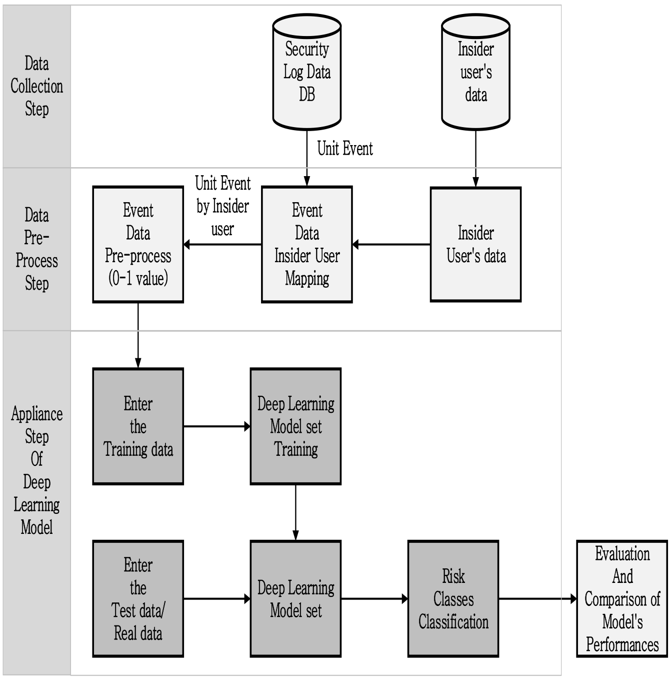
Data Collection Step
Security Log Data DB
Insider user's data
Unit Event
Data Pre-Process Step
Event Data Pre-process (0-1 value)
Unit Event by Insider user
Event Data Insider User Mapping
Insider User's data
Appliance Step Of Deep Learning Model
Enter the Training data
Deep Learning Model set Training
Enter the Test data/ Real data
Deep Learning Model set
Risk Classes Classification
Evaluation And Comparison of Model's Performances

Figure 2: The System Chart for Judging the Risk Classes of Insider data Leakage

As the input value, this system had the value between 0 and 1 being pre-processed, and as the output value, it has a value being classified into a risk class among 4-Step risk classes. Representative Deep Learning models for solving the classification problem are the MLP, the LSTM, and the GRU, and others, and each model's features are listed in the Table 4.

Table 4: Feature of Deep Learning Models

Deep Learning Models	Features
MLP	• The most common neural network model • Slow learning speed • Problem of Excessive Suitability
RNN	• Suitable for processing sequent data like voices and characters • Network structure to accept inputs and outputs regardless the length of sequence • Problem of Gradient Loss
LSTM	• Model complementing the problem of RNN. • LSTM remembers a longer sequence than that of GRU. • LSTM has many parameters in the recurrent unit, so is difficult for training in case of insufficient training data.
GRU	• Model reducing the complexity in the calculation with keeping the advantages of LSTM • Easy to add an input or to corrected data • As the structure of GRU is simple and the number of variables is few, so its learning hour is taken shorter than that of LSTM, and the excessive suitability is fewer occurred. • The purpose of GRU is the same with that of LSTM.

After considering the training data and the number of variables because the use purpose of LSTM model and GRU model is coincided, the researcher judged that the GRU model would be suitable for judging the risk class of Insider data leakage in that its structure was simpler and easier to add and correct a new user's data a new event being occurred in a new security device to the input data in future, so applied the GRU model to the proposed system.

Analysis on Factors of Deep Learning

Deep Learning Model can significantly affect the result depending on factors like the number of hidden layers, the number of nodes in hidden layer, the learning rate, the momentum, the dropout technique or not, the activation function and the loss function. However, as it was impossible to experiment the all factors, so this experiment measured the performance of GRU model according to the number of nodes in hidden layer, the dropout technique or not, and the activation function.

Most Deep Learning models are composed of the input layer, the output layer and the hidden layer. The input layer means the input factors necessary for the learning. While these nodes are connected with each node of hidden layer in the perfect connection pattern, but are not mutually connected with the nodes in the same layer. Also, there is no explicit rule determining the most suitable number of nodes by hidden layer. The number of nodes are determined through trials and errors.

From Tam & Kian's study, as the results from comparing the case of the neural network having no hidden layer with the case of the neural network having one hidden layer, it was revealed that the network having one hidden layer showed better result[10]. Besides, according to Collins et al.'s study and Dutta & Shekhar, Slchenberger et al's study, when a neural network increasing the number of hidden layers to over two ones was compared with a neural network having one hidden layer, it was appeared that the risk prediction rate was not enhanced in spite of the increase of hidden layers. So, most other previous studies used a neural network having 1 hidden layer rather than over 2 hidden layers in order to shorten the learning time about the essence of neural network's performance[11].

Furthermore, there is no rule determining the number of nodes in hidden layer. However, if the number of nodes in hidden layer were excessively increased, then the excessive connection phenomenon is occurred. As that can have the explanation ability but the case becoming meaningless value is frequent, so a leakage-risk detection model should be designed in using suitable-level nodes[12]. In order to shorten the learning time and the proposed system's performance, this experiment changed the number of nodes in hidden layer with the use of one hidden layer, and tried to find out the optimal number of nodes in hidden layer to generate the best performance.

Of the classification models, it is general that the binary classification model uses the logistic function as its activation function in input nodes, and the multi classification model uses the softmax function. In the multi-classification model, an output node should compare its relative size with other output node in order to accurately interpret its output value. As the softmax activation function outputs a value in considering relative sizes of all output values, so it is the most suitable activation function in using the multi-classification model having more than 3 outputs[13]. The researcher applied some activation functions like the softmax, the sigmoid and the tanh to this experiment having 4 outputs, and investigated whether the softmax activation function would show better performance.

Few methods normalizing the RNN-type models have been suggested, and the dropout technique has not been correctly applied. And, if the Dropout would be applied to the LSTM model or the GRU model which were created after expanding and complementing the RNN model, the performance of both models might rather decreased[14]. Also, if the Dropout would be applied to a simple model, the model's performance might be reduced. In this experiment, the researcher would apply different rates of dropout to a model having other number of nodes in hidden layer, and tried to prove this hypothesis.

EXPERIMENT FOR RISK CLASS JUDGEMENT OF INSIDER DATA LEAKAGE

Experiment Data

For judging risk classes of Insider data leakage, this experiment used the DRM and the DLP logs, the security devices commonly used in companies. And, it selected 18 Deep Learning input layers after considering users' IDs, departments, positions, continuous service year, unit event, retirement or not with 300 users' data and generated the training data.

By analyzing the Insider user's data and the event data being saved in the collected security log DB, the associations among the IP, the user's ID and his/her employee identification No were identified. Then, each Insider user table's ID and collected data table's ID were saved in the event table by Insider user according to the identified results. The format of event table by Insider user was seen in the following Table 5.

Table 5: Event Table by Insider User

Column Name	Data Type
id	INTEGER
user_id	INTEGER
dept	STRING
join_date	DATE
position	STRING
event_id1	INTEGER
event_count1	INTEGER
event_id2	INTEGER
event_count2	INTEGER
...	...
event_idn	INTEGER
event_countn	INTEGER

In pre-processing the data, the list-type values and the parameters not influencing on the results of experiment were treated as dummy variables, and the continuous values were normalized as a value between 0 and 1. As the department could not be expressed as a continuous value, so the value of department was expressed in a binary value between 0 and 1 through giving input layers as much as the number of departments. For considering the continuous service years, the data were normalized as a value between 0 and 1 after subtracting each user's hiring date from today's date. And, the event by user was differently weighted by unit event with considering the occurrence frequencies of each event. Table 6 showed the event table patterns by user after normalizing the collected data.

Table 6: Event Table by Insider User after Normalization

Column Name	Data Type
id	INTEGER
user_id	INTEGER
dept	INTEGER
years	DOUBLE
position	DOUBLE
event_id1	DOUBLE
event_count1	DOUBLE
event_id2	DOUBLE
event_count2	DOUBLE
...	...
event_idn	DOUBLE
event_countn	DOUBLE

Besides, as the category or the frequency to access the data were different depending on each user's position and department, so the data leakage or not should be judged on the basis of user's data. So, this experiment weighted each user's data in order to differentiate the data leakage risk by user.

Table 7: Weighting Target By User

Weighting Target by User
Average Continuous-Service Years by Position < Continuous-Service Years
Average Continuous-Service Years by Position > Continuous-Service Years
Prospective Retirement
Prospective Retirement and Average Continuous-Service Years by Position < Continuous-Service Years
Prospective Retirement and Average Continuous-Service Years by Position > Continuous-Service Years
Senior Executive
DB Manager
System Operation Manager
Prospective Retirement and Senior Executive
Prospective Retirement and DB Manager
Prospective Retirement and System Operation Manager

The conditions weighting each risk level differently in order to discern risk classes by user were provided in the Table 7. First, at considering the positions and the continuous service years, if a user's position was senior at comparing with his/her continuous service years, then it might be guessed that he/she had changed from any other firm to this company as an experienced man. In case that such type of user accesses the company's data so frequently and generates a lot of unit events, then this experiment weighted the user in doubting that he/she might be an industrial spy from other company having changed to this company for the purpose of leaking this company's data, even though such possibility would be low. Contrary to that, if a user's position was lower at comparing with his/her continuous service years, it could be guessed that he/she might be lost in the competition against promotion. Considering the possibility that he/she might leak the company's data in the sense of resentment or revenge toward the company, this experiment weighted the user. Apart from that, for the case of person to be retired (prospective retirement), there have been many trials to leak the company's data for the purpose of gaining profits, so this experiment needed to differentiate this type of users from other employees. Also, senior executives or the DB manager as well as the system operation manager were weighted because they had more authorities to access the company's data and could easily access to such data.

Experiment Method

This experiment proposed a system for judging a risk class of Insider data leakage in using the GRU model. This experiment was carried out with the factors like number of nodes in hidden layer, dropout technique or not, and activation function among several factors swaying the performance of Deep Learning. Besides this experiment used one hidden layer, the Cross Entropy as the loss function, the Adam as the optimization function, and total 200 learning epochs as learning frequency and the data were experimented under the same conditions.

The summarized results of proposed system using the GRU model were listed in the following Table 8.

Table 8: Summary of Experiment Model

Deep Learning Model	**Drop Out**	**Number of Nodes on the Hidden Layer**	**Activation Function**
GRU	Use	5	ReLu, softmax, sigmoid, tanh
		10	
		15	
		200	
	Not	5	
	Use	10	
		15	
		200	
	Number of Hidden Layer: 1 Loss Function: Cross Entropy Optimization Function: Adam Learning epochs: 200		

EXPERIMENT RESULTS

Evaluation Scale of GRU Model's Performance

ROC(Receiver Operating Characteristic) Curve and AUC(area under the curve)

The ROC[15] curve is the curve judging the performance of a classification model being established by the sensitivity and the specificity, so its horizontal axis represents the specificity and its vertical axis represents the sensitivity. Here, the sensitivity is indicated as TPR meaning the true positive rate, and the rate mistakenly classifying non-risky user into the risk category is indicated as FRP meaning the false positive rate.

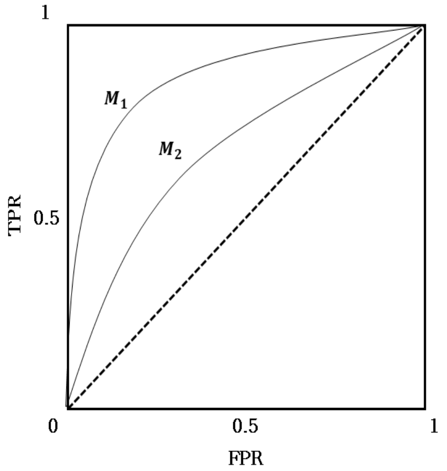

Figure 3: ROC Curves of Two Classification Models

The above Fig. 3 was the ROC curves of two classification models. Generally, as a ROC curve is located in a higher place toward the axis χ, it means that the TPR is higher at comparing to the FRP mistakenly classifying non-risky user into the risk category. At seeing the Fig. 6, it could know that the M1 models' classification performance was relatively better than that of M2.

The AUC, the value calculating the area under the ROC curve could evaluate how good a classification model's performance was good. For the idea classification model, its FRP value should be 0 and the TPR value should be 1, and when a model has these values, the area becomes 1. So as the value of AUC is closer to 1, it can be considered the classification model is the model having better performance.

Results Applying the GRU Model

In order to judge risk classes of Insider data leakage and to classify the most suitable categories, the investigatory carried out an experiment determining the number of nodes in hidden layer and the activation function as well as the dropout or not. To measure the applied GRU model's performance, the experiment used the accuracy of test set, the loss function and the ROC-based AUC value as the evaluation scales.

Performance Differences Depending On Number of Nodes in Hidden Layer

In order to identify the performance difference depending on the number of nodes in hidden layer, this experiment applied 5, 10 and 20 nodes to the GRU model, and compared the loss rate and accuracy rate by number of nodes, and the results were summarized in the Table 9 and the Figure 4.

Table 9: Loss Function, Accuracy Rate and AUC Value depending on the Number of Nodes at 200 Learning Epochs

Number of Nodes	5	10	15	20
Loss	0.3078	0.2835	0.2723	0.2884
ACC	88.89%	92.22%	91.11%	90.00%
AUC	0.9866	0.9907	0.9891	0.9897

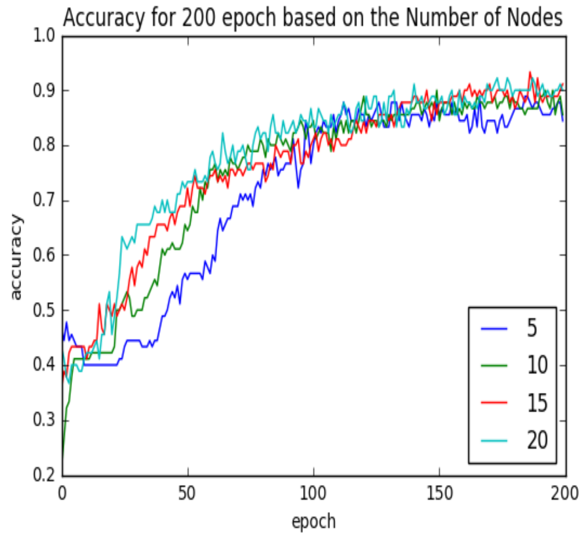

Figure 4: Accuracy Rates Depending on the Number of Nodes at 200 Learning Epochs

It was found that as the number of nodes in hidden layer became increased, the GRU model's performance classifying the leakage risk class, and showed somewhat higher accuracy rate and lower loss function values. However, after exceeding a certain number of nodes, the accuracy of model was not improved any longer. From the results of this experiment, it could be identified that at applying the 10 nodes in hidden layer to the model, its accuracy rate became 92.22% and its AUC value was 0.9907 very close to 1, indicating that the 10 nodes showed the best classification performance for the GRU model.

As seen in the above result, it could be identified that however the number of nodes in hidden layer was increased, the classification performance was not obscurely improved according to the increase of nodes. If the number of nodes in hidden layer were increased, then the calculations would become increased, causing the increase of learning epochs, and might reduce the GRU model's classification performance. So it is important to find out suitable number of nodes in hidden layer for an applying model.

Performance Differences Depending On Activation Functions

In order to identify the performance differences of models depending on activation functions, this experiment applied 3 activation functions of softmax, sigmoid and tanh to the GRU model. And the loss functions and accuracy rates by activation functions were shown in the Table 10 and Fig. 5.

Table 10: Loss Function, Accuracy Rate and AUC Value depending on Activation Function at 200 Learning Epochs

Activation Functions	softmax	sigmoid	tanh
Loss	0.2835	0.3155	7.1761
ACC	92.22%	88.89%	34.44%
AUC	0.9907	0.94547	0.6656

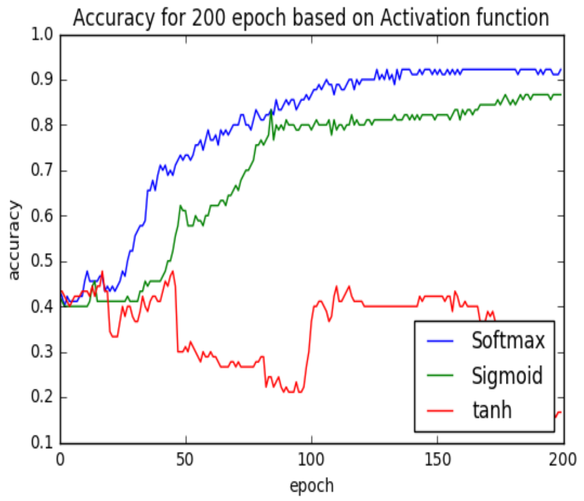

Figure 5: Accuracy Rates Depending On Activation function at 200 Learning Epochs

From the results, it could know that among 3 activation functions, the softmax activation function was the most suitable activation to a multi-classification model, showing the highest accuracy rate. And the researcher also got the result coinciding with the hypothesis that for more than 3 classification models being mentioned in the Chapter 3, the models applying the softmax activation function generally showed good performance. And it could be seen that at applying the tanh activation function to the GRU model, the learning was not be carried at all.

Performance Difference Depending On the Dropout or Not

In order to compare the performances depending on the appliance of dropout or not, this experiment did not apply the dropout in one case, and in two other cases, 0.2 and 0.5 of dropout probabilities were applied, respectively. The results comparing these cases were seen in Table 11, and Fig. 6 and Fig. 7.

Table 11: Loss Function, Accuracy Rate and AUC Depending on Dropout Rates at 200 Learning Epochs

The Number of Nodes	Dropout	0.2	0.5	None
10	Loss	0.3044	0.4124	0.2835
	ACC	85.56%	81.11%	92.22%
	AUC	0.98405	0.98302	0.99074
200	Loss	0.4132	0.3094	0.4469
	ACC	87.78%	90.00%	90.00%
	AUC	0.98611	0.98765	0.98714

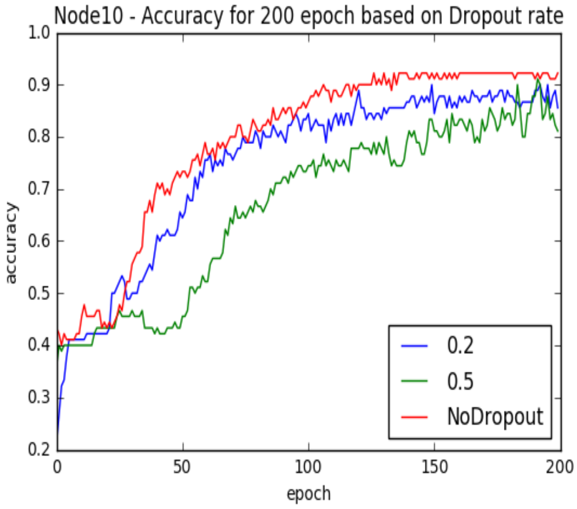

Figure 6: Node 10 - Accuracy Rates Depending on the Dropout Rates at 200 Learning Epochs

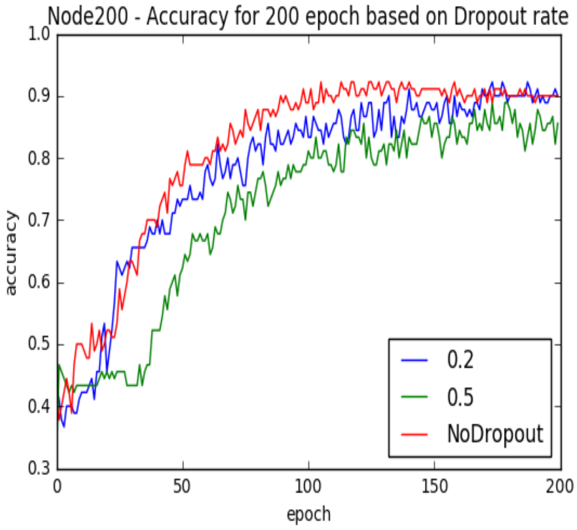

Figure 7: Node 200 - Accuracy Depending on the Dropout Rates at 200 Learning Epochs

Seeing the results applying the dropout to 10 nodes and 20 nodes in hidden layer, respectively, it could be identified that the performance was improved in both cases applying 0.2 and 0.5 probabilities of dropout to 200 nodes in hidden layer. But when the dropout was applied to the case which few calculations because of a few nodes in hidden layer, it could be identified that the performance of GRU model became rather worse. Additionally, like the content mentioned in Chapter 5, this experiment could verify that for the model applying the Dropout technique to RNN-type models, its performance was reduced.

Results Applying Other Deep Learning Models

In this experiment, the researcher conducted several experiments based on the GRU model, one of Deep Learning models. For the Deep Learning model developed for solving the classification problem, there exist various models apart from the GRU model. In order to find out whether the GRU model among various Deep Learning models was the most suitable model in judging a risk class of insider data leakage, the MLP model and the LSTM model were applied to this research subject and their risk detection performances were compared with that of GRU model. Table 12 showed the results comparing activation functions, loss functions and accuracy rates by model depending on the dropout or not for various Deep Learning models**.**

Table 12: Comparison of Loss Functions and Accuracy Rates by Activation Functions and Dropout or Not for Various Deep Learning Models

	Activation Function		**softmax**	**sigmoid**	**tanh**
MLP	With Dropout	Loss	0.0525	0.0542	0.0600
		Acc	85.56%	88.89%	86.67%
	Without Dropout	Loss	0.1072	0.1081	0.0925
		Acc	72.22%	72.22%	77.78%
LSTM	With Dropout	Loss	0.0801	0.1299	0.1051
		Acc	78.89%	65.56%	71.11%
	Without Dropout	Loss	0.3041	0.3314	6.8054
		Acc	90.00%	88.89%	34.44%
GRU	With Dropout	Loss	0.3044	0.4415	3.0623
		Acc	85.56%	85.56%	38.89%
	Without Dropout	Loss	0.2835	0.3155	7.1761
		Acc	92.22%	88.89%	34.44%

As seen in the Table 11, when several experiments were carried out in applying the dropout and generally using the GRU model except the experiment, the researcher could identify good performances of GRU model in most experiments except the experiment using the MLP model applying the Sigmod activation function. And at seeing the performance differences among the MLP model, the LSTM model and the GRU model depending on the dropout or not, it could find out that the model not applying dropout in the LSTM and the GRU model which were the RNN-type models showed superior performance and the MLP model showed relatively low performance than the above two models, but at applying the dropout, the MLP model showed better performance than them. Additionally, it was also identified that in case of applying the tanh activation function, the learning rarely was done in the GRU model, but at applying the dropout of MLP model or LSTM model, the learning was possible. However, from the comparison results, it could know that the hypothesis that the softmax activation function in over 3 classification models as mentioned was also true in the MLP model or the LSTM model.

EXPERIMENT RESULTS

It is not largely problematic to classify the normal category into the attention category or the attention category to the caution category at classifying a risk class, but a case classifying the normal category into the serious class or the serious category to the normal or attention category can be substantially problematic. In order to verify that this argument was true, the researcher made test sets by category and applied them to the GRU model. As the result from that, it was shown that the method classifying the serious category into the serious category had almost 100% accuracy rate. At experimenting with the est set of caution category, the accuracy rate was 94%. Here, it should be state that there were rare cases classifying the attention category into the serious category, but there were about 6% of cases classifying the caution category into the attention category. Through this verification, it could identify that the accuracy rate of classifying serious category was almost 100%.

In order to differently evaluate the performance of risk class judgement models of insider data leakage, the researcher calculated the AUC value using the ROC curve. In models except the tanh activation function, AUC values close to 1 could be gotten, and this experiment result was almost coincided with the results of accuracy rate experiment seen in the above.

Through the all experiments, it could identify that the GRU model used in this experiment was the most suitable model for the risk class judgement system of insider data leakage. Among the models, the model applying 10 nodes in hidden layer, using the softmax activation function, and not applying the dropout showed 92.22% of accuracy rate, 0.2835 of low loss function rate, and 0.99074 of AUC value almost close to 1, indicating that it was the model creating the best performance.

CONCLUSION

This paper proposed a method discerning risk classes of insider data leakage in using various Deep Learning models. This paper carried out experiments based on the security log data of security devices being commonly used in companies and user's data. Through the experiments, it could identify that when the Deep Learning models were applied to the research subject of this paper. they could suitably judge risk classes. Also, at changing various factors of Deep Learning differently and applying them to GRU models, it could find out that the GRU using the softmax activation function and not applying the dropout showed the best performance with 92.2% of accuracy rate. From the results of experiment, it could identify that this model could almost perfectly (100%) classify the serious class which was the most risk among 4 risk classes.

Future studies need to develop ways to improve the classification system's performance in considering more various factors to influence on the insider data leakage as input data. And they also need to improve data leakage risks classification systems in order to classify risky users more exquisitely by more specifying the current risk classes classification scale.

REFERENCES

[1] “2016 Survey on Information Security(Business)”, National Intelligence Service Korea, 2017

[2] J. Chung, C. Gulcehre, K. H. Cho, and Y. Bengio, “Empirical evaluation of gated recurrent neural networks on sequence modeling", arXiv preprint arXiv:1412.3555, 2014

[3] W. S. McCulloch, and W. Pitts, “A logical calculus of the ideas immanent in nervous activity", The bulletin of mathematical biophysics, Vol. 5(4), pp. 115-133, 1994.

[4] W. Zaremba, I. Sutskever, and O. Vinyals, “Recurrent neural network regularization", arXiv preprint arXiv:1409.2329, 2014.

[5] S. Hochreiter, and J. Schmidhuber, “Long short-term memory", Neural computation Vol. 9(8), pp. 1735-1780, 1997.

[6] S. M. Park, and J. C. Kyo, “Enterprise Data Loss Prevention Using Behavior-Based Outlier Detection", The Korean Institute of Communications and Information Sciences, pp. 94-95, 2016

[7] T. Rashid, I. Agrafiotis, and JRC Nurse, “A New Take on Detecting Insider Threats: Exploring the use of Hidden Markov Models", Proceedings of the 2016 International Workshop on Managing Insider Security Threats, pp. 47-56, 2016

[8] S. R. Eddy, “Hidden markov models”, Current opinion in structural biology, Vol.6(3), pp. 361-365, 1996

[9] H. S. Kim, “A Study on Method for Insider Data Leakage Detection”, The Journal of The Institute of Internet, Vol. 17(4), pp. 11-17, Aug. 2017

[10] K.Y. Tam, and M. Y. Kiang, “Managerial applications of neural networks: the case of bank failure predictions", Management science, Vol.38(7), pp. 926-947, 1992.

[11] E. Collins, S. Ghosh, and C. Scofield, “An application of a multiple neural network learning system to emulation of mortgage underwriting judgments", Proceedings of the IEEE International Conference on Neural Networks, Vol. 2, pp. 459-466, 1988.

[12] I. D. Jang, and S. M. Wee, “The Analysis Telecommunication Service Market with Data Mining”, Journal of KIISE, Vol 28(2), pp. 1-3, Oct. 2001.

[13] R. A. Dunne, and N. A. Campbell, “On the pairing of the softmax activation and cross-entropy penalty functions and the derivation of the softmax activation function", Proc. 8th Aust. Conf. on the Neural Networks, pp. 181-185, 1997.

[14] R. Rana, “Gated Recurrent Unit (GRU) for Emotion Classification from Noisy Speech", arXiv preprint arXiv:1612.07778, 2016.

[15] J. P. Egan, "Signal detection theory and {ROC} analysis", 1975.