New Approach for Detecting Leakage of Internal Information; Using Emotional Recognition Technology

Ho-Jae Lee[1], Min-Woo Park[1], Jung-Ho Eom[2] and Tai-Myoung Chung[1]
[1] Department of Electrical and Computer Engineering Sungkyunkwan University
Suwon, Republic of Korea
[e-mail: hjlee72@gmail.com], [e-mail: mwpark@imtl.skku.ac.kr], [e-mail: tmchung@ece.skku.ac.kr]
[2]Department of Military Studies, Daejeon University
Daejeon, Republic of Korea.
[e-mail: eomhun@gmail.com]
*Corresponding author: Jung-Ho Eom

Received May 14, 2015; revised June 2, 2015; revised August 19, 2015; accepted September 11, 2015; published November 30, 2015

Abstract

Currently, the leakage of internal information has emerged as one of the most significant security concerns in enterprise computing environments. Especially, damage due to internal information leakage by insiders is more serious than that by outsiders because insiders have considerable knowledge of the system's identification and password (ID&P/W), the security system, and the main location of sensitive data. Therefore, many security companies are developing internal data leakage prevention techniques such as data leakage protection (DLP), digital right management (DRM), and system access control, etc. However, these techniques cannot effectively block the leakage of internal information by insiders who have a legitimate access authorization. The security system does not easily detect cases which a legitimate insider changes, deletes, and leaks data stored on the server. Therefore, we focused on the insider as the detection target to address this security weakness. In other words, we switched the detection target from objects (internal information) to subjects (insiders). We concentrated on biometrics signals change when an insider conducts abnormal behavior. When insiders attempt to leak internal information, they appear to display abnormal emotional conditions due to tension, agitation, and anxiety, etc. These conditions can be detected by the changes of biometrics signals such as pulse, temperature, and skin conductivity, etc. We carried out experiments in two ways in order to verify the effectiveness of the emotional recognition technology based on biometrics signals. We analyzed the possibility of internal information leakage detection using an emotional recognition technology based on biometrics signals through experiments.

Keywords: Data Leakage, Insider Threat, Biometric Signals, Emotional Recognition, Detection Technique

This research was supported by a Daejeon University research fund (2014) and the ICT R&D program of MSIP/IITP. [2014-044-072-003 , Development of Cyber Quarantine System using SDN Techniques].

http://dx.doi.org/10.3837/tiis.2015.11.023 **ISSN : 1976-7277**

1. Introduction

In 2011, a former Goldman Sachs Group director leaked hedge fund related corporate secrets in the U.S [1,2]. He obtained personal a pecuniary advantage by selling the stolen corporate information to a competition company. A sensitive data leakage by insiders has become a critical security issue in business and public institutes. The possibility of leakage of internal information has increased because there are increasingly more information leakage paths in the enterprise computing environment. In a 2012 Cyber Security watch survey [3], it was revealed that 32% of common cyber incidents by insiders constitute theft of internal information. The 'Top 10 Guide' for protecting sensitive data from malicious insiders [4] also stated that database security is one of the most critical areas that need sensitive data protection from insiders because it saves attractive information desired by insiders. Insiders are capable of saving data on USB memory sticks and portable disks, and they can illegally use the data from outside by bypassing the firewall, the intrusion detection system (IDS), and the monitoring system at a later time [5]. Insider threats are considered as one of the greatest threats to information security as organizations are becoming more dependent on enterprise information systems. Malicious insiders can use their legitimate access authorization to leak sensitive data and extend their privileges in a manner that breaks the access control rules [6]. In the past, most security systems focused on detecting threats from the outside, not necessarily on insider threats. Data leakage protection techniques were mainly based on a firewall, DLP, DRM, and encryption. However, traditional security techniques are not effective for detecting the leakage of internal information by malicious insiders with legitimate access authorization [5]. Therefore, we attempted to apply a new approach to the detection method. We focused on human biometrics signals that represent human emotional conditions. In other words, we applied an emotional recognition technology to the detection algorithm of our proposed security system. When a malicious insider attempts to leak sensitive information in the database, he/she may show abnormal emotional conditions such as tension, agitation, and anxiety, etc. These could be detected by biometrics signals such as the pulse, temperature, and skin conductivity, etc. The proposed security system will be assumed that only apply to employees with access to critical internal data during the working hours in the company.

In this paper, we will describe the related works in Section 2 and explain the proposed system in Section 3. We then explain the application and analysis of the proposed system in Section 4 and conclude the work in Section 5.

2. Related Works

2.1 Security Research to Detect Data Leakage

Recently, insider threats have emerged as one of the most important security concerns of business in information system environments. Especially, information leakage caused by malicious insiders is considered the most serious risk to businesses' intellectual property and privacy information in their databases. Information leakage by malicious insiders is very serious because insiders have a legitimate access authorization to the database and can bypass logical and physical security measures. Moreover, they already know the ID&P/W for log on database, the security system, and the main location of sensitive data. **Table 1** shows examples of data leakage by malicious insiders in the Republic of Korea [7].

Table 1. Examples of data leakage by malicious insiders

Date	Incident	Path
Jan. 2014	Korea Credit Bureau (KCB) employee leaked personal information (over 100 million users) from 3 card firms (KB, Lotte, NH) * He was in charge of setting up a fraud detection system (FDS) for the three card firms	USB
Apr. 2013	Local employee leaked personal information of 34,000 users from Citibank	Printed paper
May 2012	Lieutenant Colonel working in Army Training Command leaked a total of 38 hard copy military secrets	Physical Access
Sept. 2011	A support staff responsible for Hana SK Card telemarketing leaked a total of 90,000 items of the personal information	E-mail
Aug. 2011	Samsung Card customer care sales staff leaked customer information by hacking the server for 8 months	Server Hacking
Mar. 2010	The staff working at the Samsung Electronics Semiconductor cooperation supplier leaked the business proprietary documents and core technology under A/S	Physical Access

While security research has been actively performed in the insider security field, the research focuses on access control, profiling, and monitoring. Jiangjiang Wu et al. [8] proposed an active data leakage prevention model for insider threats. Their proposed model combined trusted storage with virtual isolation technologies. The trusted storage is a secure data container that is a dynamic virtual isolation environment for processes that controls file access, network access, and inter-process communication for processes accessing sensitive content. It performs 3 dynamic isolation processes including read isolation, write isolation, and communication isolation to ensure data leakage protection. Frank L. Greitzer et al. [9] proposed predictive modeling for insider threat mitigation. Their proposed model focuses on a possible structure of a predictive model combining psychosocial and traditional digital data. A key challenge of this research is to define the possible precursors to insider threat exploits in terms of observable cyber and psychosocial indicators and to integrate these indicators in an analysis model. You Chen et al. [10] proposed the community anomaly detection system for detecting anomalous insiders in collaborative information systems. The proposed system is an unsupervised learning framework to detect insider threats based on the access logs. It is based on the insider access pattern and consists of two components; relational pattern extraction and anomaly prediction. The former derives community structures while the latter leverages a statistical model to determine a point time of deviation from communities.

Insider security technologies and systems are being actively studied. The representative technologies are document-based DRM and DLP. Especially, a document-based DRM is used for preventing leak electric documents by insiders. A document-based DRM has been developed for copyright security and piracy prevention of digital contents. This has been used as a means to prevent illegal access to a document or block leakage of internal sensitive documents [11]. DLP monitors packets transferred in the internal network, and logs & blocks services related to information disclosure by email, messenger, web hard, P2P, and remote control. It inspects every packet communicated with the outside network at the point where the internal network is connected to the external internet. It also detects anomaly behavior when an insider attempts to leak internal data by email or messenger via the PC, then blocks

the service requested by the insider and alerts the security manager. **Fig. 1** describes a typical DLP structure.

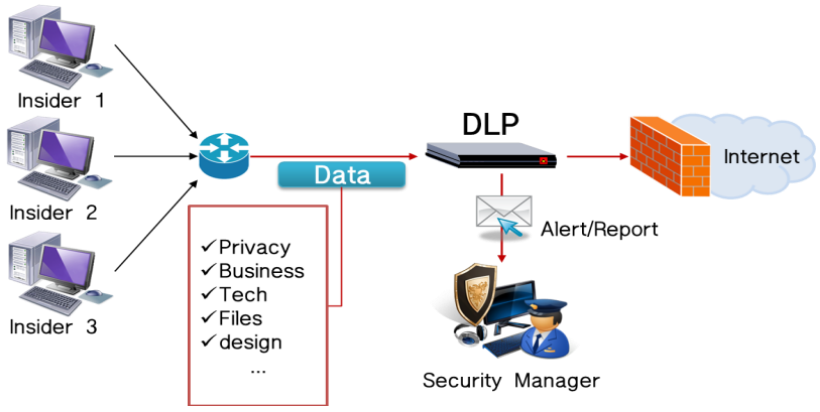

Fig. 1. DLP

2.2 Security Technologies using Biometrics

Biometrics [12] refers to the identification of humans according to their physiological and/or behavioral characteristics or traits. A system using biometrics provides an automated technique of identifying an individual based on his/her biometric characteristics. The types of biometric commonly include face, iris, retina, fingerprint, voice, signature, vein pattern, and hand geometry [12,13]. Biometrics is commonly used to identify and authenticate humans because it provides a more reliable authentication than traditional authentication methods such as P/W, ID cards, and keys. Biometrics based authentication mechanisms are more reliable than traditional authentication methods [14]. They are also used to control access to physical assets or logical data. A biometric system is essentially a personality recognition system that operates by extracting biometric data from an individual, and compares this personality set with the template set in the database. A biometric system operates in a simple manner as shown in **Fig. 2**.

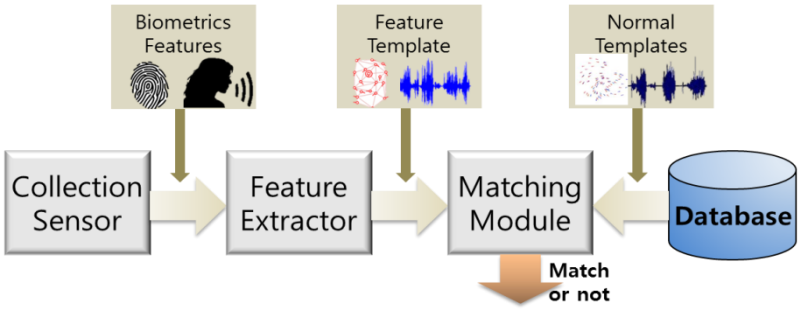

Fig. 2. Biometrics based Authentication System

The collection sensor collects the user's biometric features using sensors such as a camera, a fingerprint scanner, etc. The feature extractor processes the extraction and encoding of specific features from the user's biometric features to convert to feature templates. In the

case of fingerprints, the location and direction of the ridges and bifurcations are extracted from the fingerprint image. The new feature template is then compared with stored templates in a database to determine the degree of similarity or correlation. If a new feature template matches individual template stored in a database, it permits access to resources [12,13,15].

Biometrics based security systems offer several advantages. A specific personalized key could be created for each user because biometrics are unique to each person. In addition, an authentication key does not need to change periodically like a password because biometrics characteristics are permanent and not changeable. It cannot be transferred, and a user cannot spoof their own biometrics characteristics to other users because biometrics characteristics are only measured in real time when the user requests authentication to the system. Because of these advantages, biometrics is popularly used in security systems such as database security and access control in physical security fields such as in buildings, gates, and offices.

However, in spite of their various advantages, security technologies using biometrics are limited to the authentication system because inherent disadvantages of biometrics still have not been overcome. Firstly, the false rejection rate poses a limitation. There is a probability of failure to match the input template to the correct template stored in the database. The second limitation is that not all users can utilize a given biometric system; for example, impaired people. The third limitation is that some biometric sensors do not accurately collect the necessary biometric information. Lastly, biometric systems may violate a user's privacy because biometric characteristics contain a great deal of personal information. Because of these problems, a security system using biometrics does not expand the security functions related to detection, prevention, and firewall, etc. [16,17].

3. Proposed Internal Information Leakage Detection System

3.1 Biometrics Signals related to Emotional Recognition

According to the basic classification by psychologists, "emotions are classified into joy, sadness, anger, surprise, fear, and disgust". Emotions can be detected by biometrics signals such as brain waves, pulse, voice, and skin conductivity, etc. In this paper, we selected emotional recognition elements which have proven effectiveness in the polygraph technique and previous research. We also selected the proven elements through the existing emotional function mouse research [18]. We researched 3 biometrics signals including pulse, temperature, and skin conductivity to identify the emotional changes.

The pulse is a significant physiological signal of the human body. It is the periodic wave of the arteries occurring from human heart beats. Research has been carried out on pulse based emotional recognition. The pulse accelerates when the heart rate increases as soon as physiological and/or physical stress is applied. When the emotional change is recognized, the technique using the pulse is 87~97 percent of effectiveness in the emotional recognition field [18,19]. Temperature used in this paper is the skin temperature, and the average temperature is 34~35℃. This usually changes with mental excitement or exercise, etc. This is commonly used to observe the human physiological changes with respiration, pulse, and blood pressure [20]. Skin conductivity is the electrical conductance of the skin, which varies with skin moisture. The degree of skin moisture changes according to the response of skin stimulation. Thus, skin conductivity is used as an indication of psychological or physiological arousal. According to Ahyoung Choi's paper, 'Feature extraction for emotion analysis based on physiological signal', when the emotional change is recognized, a technique measuring the skin conductivity has an effectiveness of 87.5~ 98 percent [20,21].

3.2 Proposed Detection Mechanism

Our proposed detection mechanism focuses on the subject rather than an object. In other words, the detection target is the malicious insider. We applied emotional recognition technology using biometrics signals as a detection mechanism. Our idea of applying emotional recognition was inspired by the polygraph technique and an authentication system using biometrics. The polygraph technique [22] measures and records the change values of biometrics signals such as blood pressure, pulse, skin conductance. It identifies condition that can be deviated from normal condition when they deliberately attempt to lie.

The concept of the proposed detection mechanism is shown in **Fig. 3**.

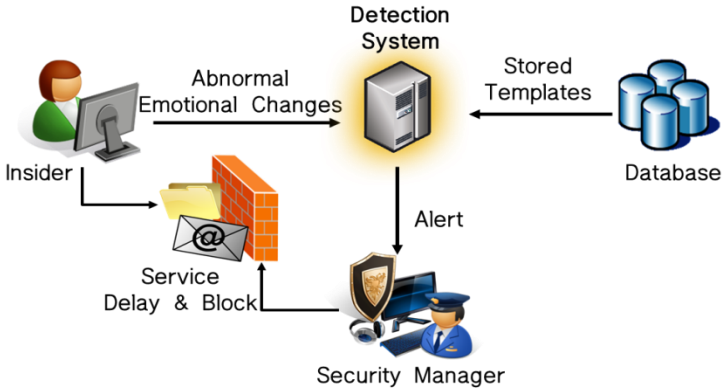

Fig. 3. Concept of Proposed Detection Mechanism

The system monitors the insider's biometrics signals when he/she attempts to access sensitive data in the database, and compares the acquired value of insider's biometrics signal with the normal values of biometrics signals stored in the database. If the acquired value of the biometrics signal is deviated from the normal boundary, the system checks the insider's emotional changes. If the emotional changes indicate abnormal behavior such as information leakage, deletion, changes, etc., it alerts the security manager, and delays or blocks the requested services.

3.3 Architecture of Proposed Internal Information Leakage Detection System

Our proposed system is composed of an emotional recognition based detection system that is installed on the user's PC, a security manager that manages the security policy of the internal system, and a human interface that is an input device attached to the sensors to collect the insider's biometrics signals, as shown in **Fig. 4**. The proposed system is an expanded model of that in [23]. We improved and added new functions to the detection, response, security controller module, and human interface in the system proposed in the paper.

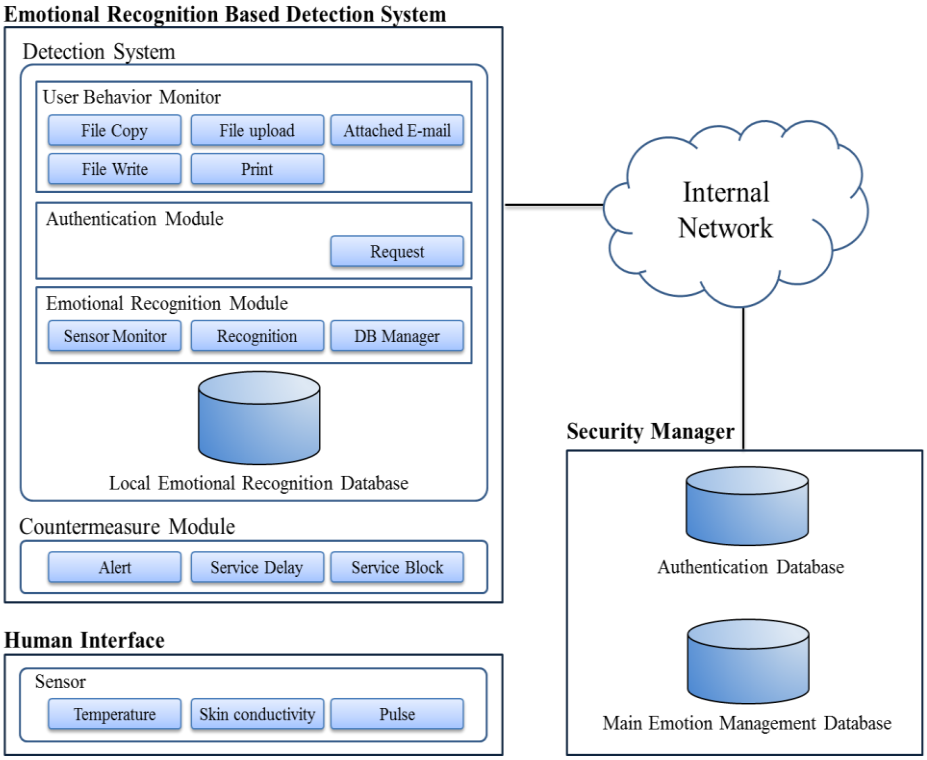

Fig. 4. Architecture of Proposed Detection System

The emotional recognition based detection system analyzes the insider's emotional condition by biometrics signals. And it detects the indication of information leakage and corresponds according to the risk degree of information leakage. It is composed of a detection system and a countermeasure module. The detection system monitors the user's emotional changes while he/she is working, and identifies any unusual rapid changes of biometrics signals. It is composed of a user behavior monitor, an authentication module, an emotional recognition module, and a local emotional recognition database. Functions of these components are as follows.

- User behavior monitor: monitors insider's behaviors such as sensitive documents copies, uploading, sending mail attachments and prints, etc. Sensitive documents are determined by the security policy, and monitoring is performed by hooking the main system call.
- Authentication module: authenticates user with ID & P/W before the user performs any action on sensitive data. The insider can access sensitive documents after being authenticated by the authentication process.
- Emotional recognition module: detects suspicious behavior, and compares and analyzes the change values of the collected biometrics signals with his/her normal (average) values saved in a database when biometrics signals are received from human interface. It performs the 3 functions of sensor monitor, recognition, and database manager. A sensor monitor periodically calls the insider's biometrics signals from the human interface, and generates the normal (average) values of the biometrics signals after collecting the insider's biometrics signals during the several months. The recognition function compares the values of biometrics signals received from the sensor monitor with the insider's

normal values in the database. If the values of the collected biometrics signals are deviated from the boundary of the normal value, it suspects the information leakage. The D/B manager measures the normal values of the insider's biometrics signals, using the value saved in local emotional recognition database as the initial values. If data is not stored in the emotional recognition database of the local system, it measures the values of the insider's biometrics signals based on the value stored in the main emotion management database.

- Local emotional recognition database: stores the value of the insider's biometrics signals received from the human interface while the insider is working.

A countermeasure module defense insider suspicious behavior related to information leakage with response methods such as alert, service delay, and block, etc. according to the risk degree of the information leakage. The change of the insider's biometrics signals is used as an indicator to identify the potential information leakage, rather than to diagnose the exact information leakage. Thus, a differentiated response is required, depending on the width and depth of the insider's emotional changes. For example, if the risk degree of information leakage is low, it alerts the security manager. When the degree of risk of information leakage is high, it performs a delay or blocks the requested service.

The security manager consists of two databases; an authentication database and a main emotion management database. The former stores user information related to insider authentication. The latter stores the value of the insider's normal (or average) biometrics signals. The value of the user's biometrics signals is encrypted to prevent hacking.

The human interface is a set of input devices that are attached sensors to collect the insider's biometrics signals. Sensors periodically measure the insider's pulse, temperature, and skin conductivity. It sends these values to the sensor monitor in the emotional recognition module. If the sensor monitor requests the measurement results, the sensors immediately measure the insider's biometrics signals and report these to the sensor monitor.

The proposed system operates in two phases; a monitor and a detection phase, as shown in **Fig. 5**.

In a monitor phase, a security policy is established, a database is built, and the normal values of the insider's biometrics signals are set. A human interface periodically measures the insider's biometrics signals, and sends these to an emotional recognition module. An emotional recognition module creates the normal (average) value of the insider's biometrics signals based on the results collected from a human interface. A security manager establishes a security policy for detecting suspicious insider's behaviors based on emotional recognition. Security policies include the specification of the valid boundary of authentication (valid number and expiration data, etc.), a set of the normal (average) value of the insider's biometrics signals, and a response methods (alert, service delay, and block, etc.) according to the risk degree. The security manager also builds the database related to authentication and emotional recognition.

In the detection phase, the insider's biometrics signals collected from a human interface are analyzed and the values of the insider's emotional changes are compared with the normal values in the database. In addition, it detects insider's suspicious behaviors, and responds according to the risk degree. The authentication module checks whether the insider has access authorization when the insider attempts to access a sensitive data. User authentication is only performed when authentication is unsuccessful in advance or is beyond the valid conditions. The result of user authentication is sent to the user behavior monitor. If authentication failed, the requested service is blocked. If authentication is successful, the next detection process progresses, and the emotional recognition module is initiated. The

emotional recognition module checks the biometrics signals, which are managed periodically to identify the emotional change of the insider. If an unusual change of biometrics signals is detected, it immediately requests the measured value of insider's biometrics signals to the human interface. The human interface measures the insider's biometrics signals in real time, and immediately returns the results to the emotional recognition module. The emotional recognition module compares the value of insider's biometrics signals received from the human interface with the value of the insider's normal (average) biometrics signals in the database, and determines the possibility of information leakage. The emotional recognition module sends analysis results to the user behavior monitor. The user behavior monitor calls a countermeasure module when data leakage is determined. Otherwise, the detection process is terminated. A countermeasure module performs an alert, and delays or blocks the requested service according to the risk degree of information leakage.

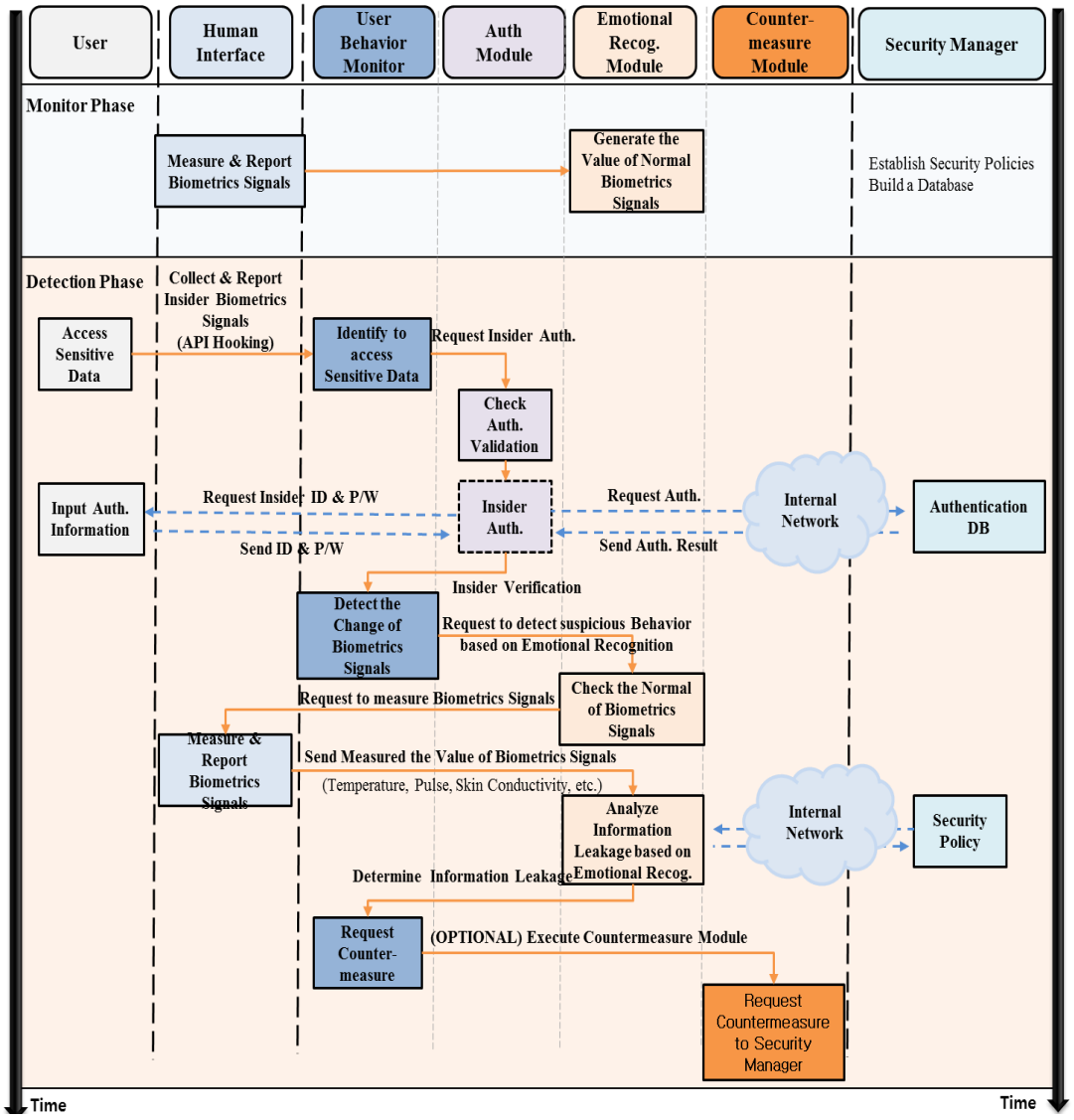

Fig. 5. Operational Procedure of Proposed Detection System

4. Application and Analysis

4.1 Detection Test by Pattern of the Pulse Graph

We will show how to detect the leakage of internal information using the biometrics signals measuring device, the 'BioGraph Infiniti' program used in [20]. The biometrics signals measurement system installed in this program is composed of a sensor, an encoder, and software made in Thought Technology as shown in **Fig. 6**.

A Blood Volume Pulse (BVP) sensor can measure heart rate, pulse, blood temperature, and skin temperature. The 'BigGraph Infiniti' sensor is very sensitive to the movement of the test subject because it is usually used for checking the health condition of the subject. Therefore, this does not exactly fit our research, but it can show us how to detect any abnormality precursor from the change of the insider's biometrics signals. In this test, we will use only the pulse, which has a fairly high accuracy to detect any abnormality precursor of the subject. The BioGraph Infiniti program [24] presents the biometrics signals and reaction times. We measured the change of the test subject's biometrics signals while watching a horror movie. In other words, we observed whether the emotional change could be measured from the change of biometrics signals.

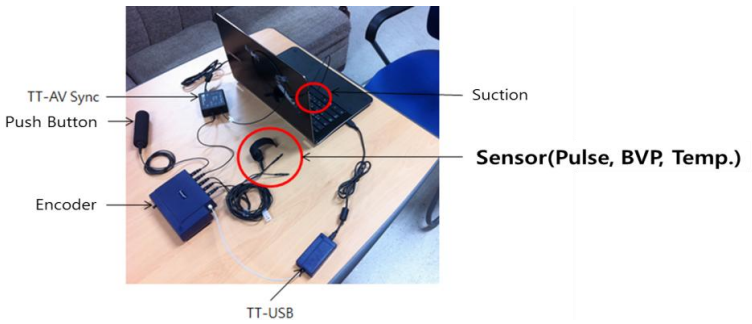

Fig. 6. Biometrics Signals Measurement System

Fig. 7 shows the capture screen of the biometrics signals in the BioGraph Infiniti program. The pulse is represented in the graph of the top of the screen.

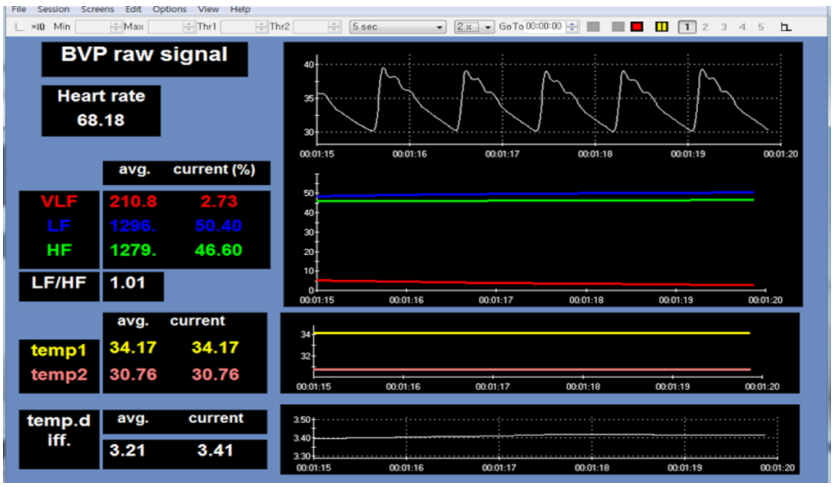

Fig. 7. Measurement Screen of the BioGraph Infiniti Program

We measured the BVP of three persons, three times daily for 10 days. **Table 2** shows the information gathered on the test subject group.

Table 2. Information of the Test Subject Group

Test Subject	Gender	Age	Physical Size		Job
			Height	Weight	
A	Male	28	176cm	65kg	Student
B	Male	26	182cm	68kg	Student
C	Female	27	160cm	42kg	Student

Fig. 8 shows a graph of the BVP measurement results. As shown in the figure, there is no consistency of the graph patterns for each person. This means that a correct mean graph pattern cannot be represented.

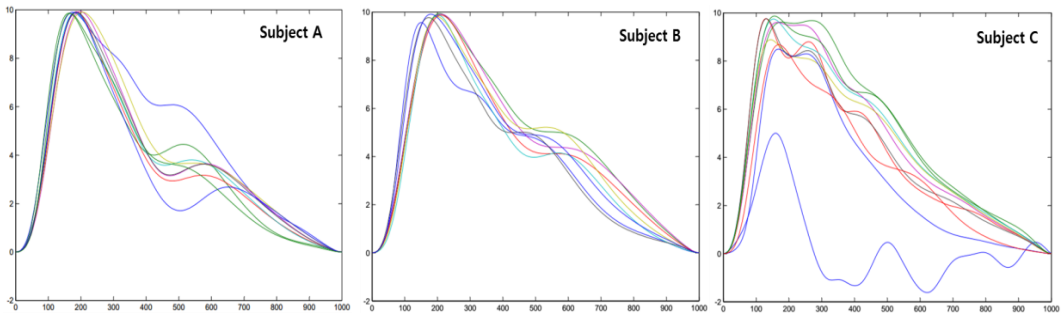

Fig. 8. Graph Pattern of BVP Measurement Results

While measurement was being carried out, we faced some problems that could have affected the test results due to the inconsistency with the subjects' conditions. First, the measurement result is influenced by measurement environment factors such as indoor temperature, noise, air, smell, etc. Secondly, the signal graph is irregular according to the condition of the test subjects. After the test subject exercises or eats food, the span of the graph becomes narrow. When the test subject's condition is poor, the span of the graph becomes wide. Lastly, when measuring, if the test subject moves, the value of the biometrics signals cannot be accurately collected. Also, the sensor of the measurement system is very sensitive to the subjects' movements. We revealed that the average graph cannot accurately represent a pulse graph of the test subject due to the measurement environment and the test subject's condition. Therefore, we purchased a new upgraded sensor and implemented an improved analysis tool for analyzing the biometrics signals. We used the experimental results from the pulse pattern in the authentication research [25]. It is difficult to detect abnormal behavior with only pulse wave patterns. However, if we derive the unique pattern of the user's pulse wave, it is possible to apply it to the authentication system.

4.2 Detection Test according to Heart Rate (HR) Interval

Our purchased sensor is the Ubpulse 360, which can measure the photoplethysmography (PPG) pattern, Heart Rate (HR), HR interval, and blood flow index, etc. This sensor sends

the measured result to a smart device or PC using Bluetooth or USB. The analysis tool for biometrics signals extracts the measurement information entering through the serial port communication, and then outputs the information to re-produce meaningful values. And then it analyzes the experimental results data. **Fig. 9** shows the biometrics signals analysis tool and Ubpulse 360.

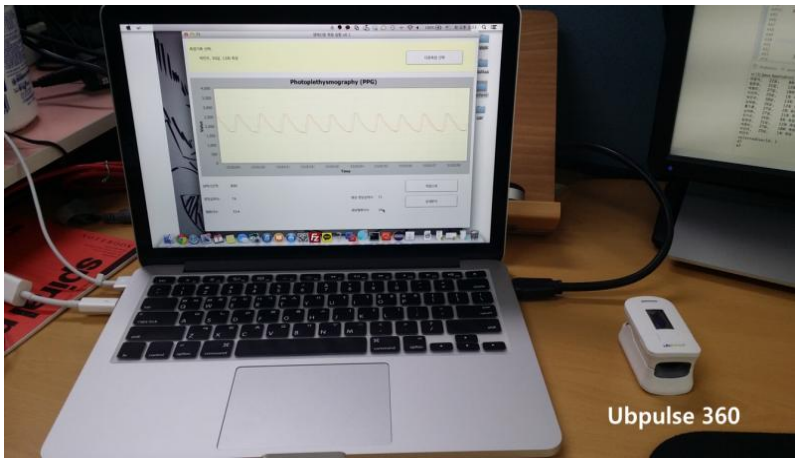

Fig. 9. System to measure HR interval

As shown in **Fig. 10**, we designed the additional detailed biometrics signals analysis tool to view the user. Each function is the same as the function of the emotion recognition module shown in **Fig. 4**.

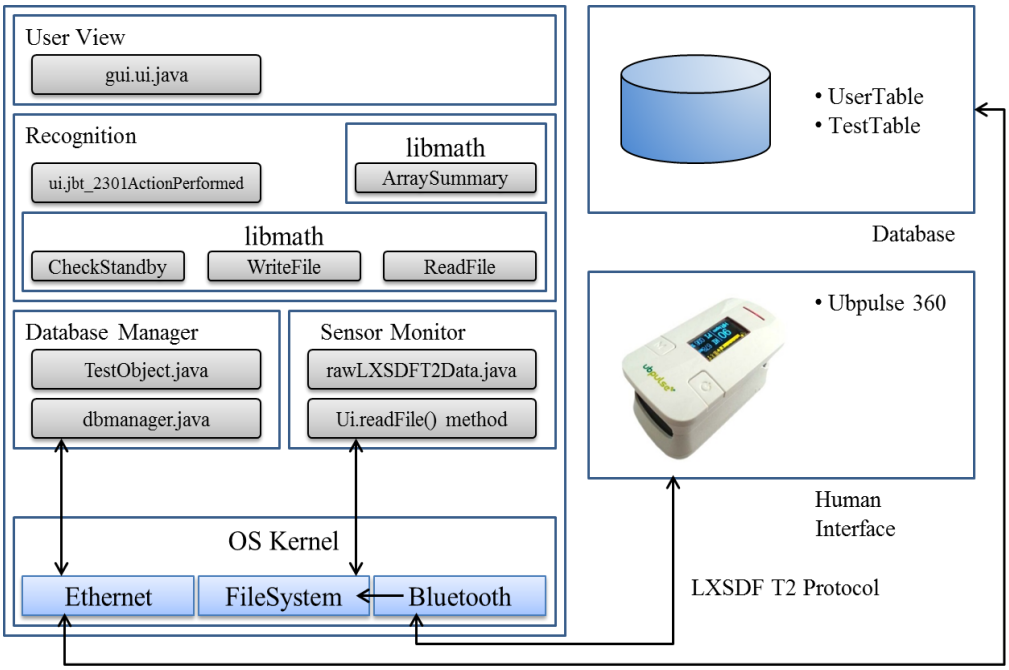

Fig. 10. Detailed Architecture of Biometrics Signal Analysis

Table 3 shows information of the test subject group.

Table 3. Information of Test Subject Group in 2nd Test

Test Subject	Gender	Age	Physical Size		Job
			Height	Weight	
A	Male	30	181cm	105kg	Researcher
B	Male	26	182cm	68kg	Student
C	Male	27	169cm	63kg	Student
D	Male	27	172cm	50kg	Student
E	Male	32	182cm	79kg	Student
F	Male	25	178cm	69kg	Student

The biometrics signals of each subject were measured at a normal condition for 10 minutes. The subjects' biometrics signals were also measured for 10 minutes while watching the horror film, to measure the stress condition in order to confirm the emotional change. We decided to exclude subject B, D from the measurement results because his biometrics signal was too irregular. **Fig. 11** shows HR interval distribution of subjects according to the emotional change.

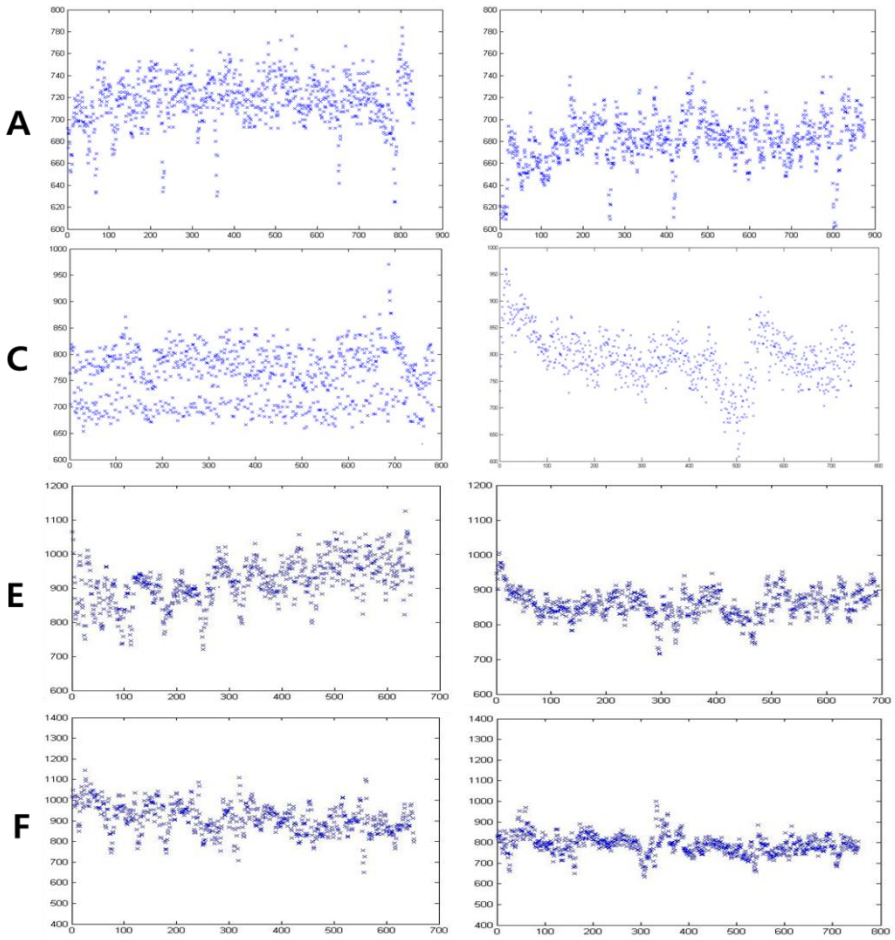

Fig. 11. HR Interval Distribution of Subjects; Normal (Left) and Stress (Right) Conditions

The HR interval distribution of subject A did not significantly change when comparing he normal condition as shown **Fig. 11**. However, we confirmed that the HR interval distribution of subject C is significantly lower (778.7ms) than the average value (794.6ms) of normal condition. We confirmed that subject E and F are differentiated normal and stress conditions through additional experiments. HR of subject E and F are significantly lower value (each 705.3ms and 900.3ms) than the average value (each 1,020.2ms and 1037.1ms) of normal condition. We knew that the HR interval distribution of subjects changes when comparing the normal condition to stress condition. In other words, subjects display emotional change when he watches the scene being scared suddenly during the horror movie watching time.

Fig. 12 shows pulse pattern of subjects.

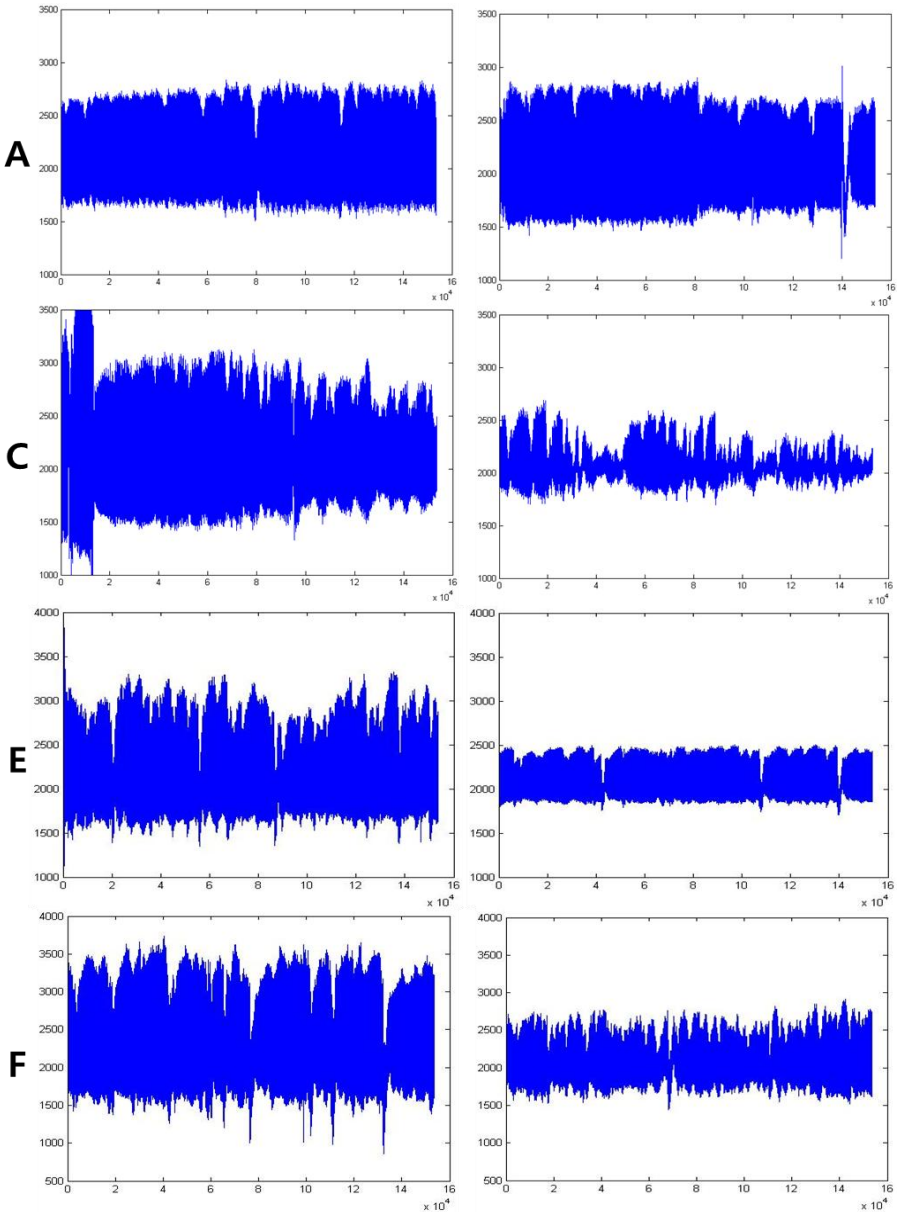

Fig. 12. Pulse Patten of Subjects; Normal (Left) and Stress (Right) Conditions

We found that there are emotional changes in the pulse pattern of subject C, E and F except subject A because the pulse pattern of each subject is not similar between normal and stress condition as shown **Fig. 12**. The longitudinal width of pulse pattern of each subject C, E and F became narrow in stress condition as shown graph E in **Fig. 12**. It means that subjects become a state of tension in terrible scene. But the continuous experiment is required because the graph pattern is fixed in shape in the supplementary experiment. So, we apply the pulse pattern to the factor of detection mechanism, we are considered to use as the secondary detection factor.

We found the other detection factor in a supplementary experiment. It is LF/HF ratio that represents the balance of the autonomic nerve. It can be calculated by the analysis tool as shown in the middle of **Fig. 7**. In the second experiment, we cannot see in the program display because it receives the analysis result after analyzing. LF (Low Frequency) reflects an activity of the blood pressure control mechanism. HF (High Frequency) reflects the indicators related to respiratory activity. For example, subject E's LF/HF ratio is lowered to 1.2 in the excited condition from 1.4 in a normal condition. Also, subject F's LF/HF ratio is lowered to 1.1 in the excited condition from 1.7 in a normal condition. The exact analysis of this indicator (LF/HF ratio) is planned to proceed through a supplementary experiment in the future.

We confirmed that the subject's emotional changes can be detected from his biometrics signals (HR Interval Distribution) through the experiments. In other words, it is possible to detect the change of an insider's biometrics signals because an insider's emotional change occurs when he/she abnormally responds to internal information such as data leakage. For example, if the insider intentionally responds to leaking internal information, he/she will be detected in real time because his/her biometrics signals change due to emotional changes such as tension, nervousness, etc. Moreover, the requested service will be limited at each step depending on the degree of emotional change. However, if the insider unintentionally changes or deletes the internal information, it cannot be detected from the biometrics signals because the emotional change did not occur.

In order to completely apply the emotional recognition technology to the internal information leakage detection system, some issues need to be addressed. First, sensors that are not affected by movement are needed because the existing sensors are sensitive to a user's movement. The existing sensors show a lot of noise when collecting biometrics signals. If we use the existing sensors, the measured value and the average value of the user's biometrics signals are not accurate and False Reject Rate (FRR) increases. Therefore, if a sensor is developed that is not sensitive to motion and can filter the unnecessary values, an accurate average value can be obtained and FRR can also be reduced. The accuracy of normal templates stored in the database is also a problem. To improve the accuracy, a considerable amount of raw data is needed. It is not sufficient to calculate the average value using a small dataset such as used in our test. Although the average was calculated with a small dataset, it is easy to determine the incorrect average value. Therefore, in most biometrics system research, a mathematical and statistical algorithm is recommended to calculate normal templates. We will solve these issues individually as the research continues. We also confirmed the possibility of detecting the leakage of internal information based on the emotional recognition system using the user's biometrics signals through this research experiment.

5. Conclusion and Future Work

In this paper, we proposed a real-time internal information leakage detection system based on emotional recognition technology using biometrics signals. We applied emotional recognition technology using insider's biometrics signals as a detection mechanism. When the insider performs abnormal behavior when accessing sensitive documents, emotional changes could be identified by the change of biometrics signals, which are detected, similarly to a polygraph technique.

We applied a new approach for the detection target, whereby the subject (insider) is the detection target rather than an object (internal information). The new approach was based on the fact that emotional changes occur when humans switch from normal to abnormal conditions, and these changes could be detected through biometrics signals. We carried out an experiment two times in order to verify the effectiveness of the emotional recognition technology based on biometrics signals. First, we used the pattern of a pulse graph as a detection basis, but it was difficult to obtain a normal value due to external states such as user's condition, and sensor performance, etc. Therefore, we decided to stop this method because of its false detection rate. Second, we tested the HR interval distribution with new biometrics signals analysis tool and sensor equipment. The second experiment result showed greater effectiveness than the first experiment. The equipment was able to distinguish between normal and abnormal conditions from the HR interval distribution and the LF/HF ratio. Therefore, we could confirm the possibility of internal information leakage detection using an emotional recognition technology based on biometrics signals through experiments.

We will continue to address this technical problem through research and experiments. In particular, we will address the sensor problem by developing a detection optimized sensor through cooperative research with the biometrics signals laboratory.

References

[1] Jung ho Eom, Sung Hwan Kim and Tai Myoung Chung, "Analysis of Insider Access Pattern for Monitoring Misuse in the DCD," *Internal Journal of Multi and Ubiquitous Engineering*, vol.8, No.3, pp.431-440, 2013.

[2] http://online.wsj.com/article/SB10001424052970203897404578077050403577468.html.

[3] "2012 CyberSecurity Watch Survey," Software Engineering Ins, Carnegie Mellon University, 2012.

[4] "Top-10 Guide for Protecting Sensitive Data from Malicious Insiders," Imperva White Paper, iMPERVA, 2009.

[5] Imad M. Abbadi, Muntaha Alawneh, "Preventing Insider Information Leakage for Enterprises," *The Second International Conference on Emerging Security Information, Systems and Technologies (SECURWARE '08)*, IEEE Press, pp.99-106, 2008. Article (CrossRef Link)

[6] Jung ho Eom, "Modeling of Document Security Checkpoint for Preventing Leakage of Military Information," *Internal Journal of Security and Its Application*, Vol.6, No.4, pp.175-182, 2012.

[7] Jung ho Eom, "The Quantitative Evaluation of a Level of Insider Activity using SFI Analysis Techniques," *Journal of Security Engineering*, Vol.10 No.2, pp.113-122, 2013.

[8] Jiangjiang Wu, Jie Zhou, Jun Ma, Songzhu Mei, Jiangchun Ren, "An Active Data Leakage Prevention Model for Insider Threat," *The journal of International Symposium on Intelligence Information Processing and Trusted Computing*, IEEE Press, pp.39-42, 2011. Article (CrossRef Link)

[9] F. L. Greitzer, P. R. Paulson, L. J. Kangas, L. R. Franklin, T. W. Edgar and D. A. Frincke, "Predictive Modeling for Insider Threat Mitigation," *Pacific Northwest National Laboratory Report, U.S Department of Energy*, 2009.

[10] Y. Chen, S. Nyemba and B. Malin, "Detecting Anomalous Insiders in Collaborative Information Systems," *IEEE Transactions on Dependable and Secure Computing*, vol.9, No.3, pp.332-344, 2012. Article (CrossRef Link)
[11] Jung ho Eom, Nam uk Kim, and Tai myoung Chung, "An Architecture of Document Control System for Blocking Information Leakage in Military Information System," *International Journal of Security and Its Applications (IJSIA)*, Vol.6, No.2, pp.109-114, 2012.
[12] Neha Dahiya and Chander Kant, "Biometrics Security Concerns", in *Proc. of Second International Conference on Advanced Computing & Communication Technologies*, IEEE Press, pp.297-302, 2012. Article (CrossRef Link)
[13] "Biometrics Security Considerations," System and Network Analysis Center Information Assurance Directorate, www.nsa.gov/snac.
[14] Xinyi Huang, Yang Xiang, Elisa Bertino, Jianying Zhou, and Li Xu. "Robust Multi-Factor Authentication for Fragile Communications," *IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)*, IEEE Computer Society, Vol.11, No.6, pp.568-581, 2014. Article (CrossRef Link)
[15] Jong Yeol, Kim, "A study on a Reinforced Certification Technique Using an Accredited Certificate and Bioinformation," *Master's thesis*, Graduate School of Information Sciences Soongsil University, 2012.
[16] Reetu Awasthi and R.A.Ingolikar, "A study of biometrics Security System," *International Journal of Innovative Research & Development*, Vol.2, Issue4, pp.737-760, 2013.
[17] A. A. E. Ahmed and I. Traore, "Anomaly Intrusion Detection based on Biometrics," in *Proc. of the 2005 IEEE Workshop on Information Assurance and Security*, pp.452-453, 2005. Article (CrossRef Link)
[18] Kim Hyun, Heo Chang-Wook and Choi Jun-Hyung, "Evaluation of Reliability of the Emotional Function Mouse," *the Journal of the Korean Society of Jungshin Science*, Vol.5 No.1, pp.28-36, 2001.
[19] Huiling Zhang and Guangyuan Liu, "Research of Emotion Recognition Based on Pulse Signal," in *Proc. of 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, pp.506-509, 2010. Article (CrossRef Link)
[20] Jung ho Eom, et al, "Application of pilot's biomedical signals for safety management," *ROKAF Research Report*, pp.18-19, 2013.
[21] Ahyoung Choi and Woontack Woo, "Feature extraction for emotion analysis based on physiological signal," in *Proc. of 2005 Korea HCI conference*, pp.624-629, 2005.
[22] Byoung Sun Cho, "Lie detector," *The Journal of Notice*, Vol.549, pp.5-16, 2002.
[23] Jung-ho Eom , et al, "An Architecture of Emotional Recognition based Internal Information Leakage Prevention System," in *Proc. of The 4th International Conference on Security-enriched Urban Computing and Smart Grid*, Vol.26, pp.60-63, 2013.
[24] "SA7913 V5.1.2 BioGraph Infiniti Getting Started.pdf", http://www.thoughttechnology.com.
[25] Jung ho Eom, "The Design of Robust Authentication Mechanism using User's Biometrics Signals," *Internal Journal of Security and Its Application*, Vol.8, No.6, pp.71-80, 2014. Article (CrossRef Link)

Ho Jae Lee received his first B.S. degree in Information Engineering from Sungkyungkwan University, Korea in 1999. He received his M.S. degree in Computer Engineering from Sungkyungkwan University 2002. He was work for Korea Information Security Agency and LG Electronics more than 10 years. He is now senior engineer in Samsung Electronics.

Min Woo Park is currently a Doctor candidate at Sungkyunkwan University, Suwon, Korea. He received his B.S. degrees in Information & Communication Engineering from the SungKyunKwan University, Suwon, Korea, in 2008. He received his M.S. degrees in the Department of Electrical and Computer Engineering from the SungKyunKwan University, Suwon, Korea, in 2010. His research interests include security of Sensor Networks and Cloud Computing.

Jung Ho Eom received his M.S. and Ph.D. degrees in Computer Engineering from Sungkyunkwan University, Suwon, Korea in 2003 and 2008, respectively. He is currently a professor of Military Studies at Daejeon University, Daejeon, Korea. His research interests include information security, cyber warfare, and network security.

Tai Myoung Chung received his first B.S. degree in Electrical Engineering from Yonsei University, Korea in 1981 and his second B.S. degree in Computer Science from University of Illinois, Chicago, USA in 1984. He received his M.S. degree in Computer Engineering from the University of Illinois in 1987 and his Ph.D. degree in Computer Engineering from Purdue University, W. Lafayette, USA in 1995. He is currently a professor of Information and Communications Engineering at Sungkyunkwan University, Suwon, Korea. He is now a vice-chair of the Working Party on IS & Privacy, OECD.