A Feasibility Study on Detection of Insider Threats based on Human Bio-signals

Young A Suh [a], Man-Sung Yim [a]*

[a] Nuclear Environment & Nuclear Security Lab, Department of Nuclear And Quantum Engineering, Korea Advance Institute of Science and Technology(KAIST)
[*]Corresponding author: msyim@kaist.ac.kr

1. Introduction

The insider threat means that trusted workers in an organization might carry out harmful acts from the negligent use of classified data to potentially sabotage the workplace. Surveys and studies [1-3] conducted over the last decade have consistently shown the critical nature of the insider threats problem, in both government and private sectors. Despite the significance of insider threats in NPPs, it is difficult to measure the insider threat and develop a system for detecting and predicting their actions since individuals are unpredictable. The shortcomings of existing systems, such as mental self-assessment and peer review, are very subjective, biased-assessments and employed infrequently. To overcome these limitations, this study investigates the feasibility of detecting and predicting an insider threat by using human biodata, from smart wearable devices.

2. Experiment Setup

The premise of this study starts by assuming that bio-signals from the human body do not lie. It is difficult for humans to manipulate their bio-signals. This paper chose particular bio-signals such as Electroencephalogram (EEG), Galvanic Skin Response (GSR) and Electrocardiogram (ECG) to detect and predict a "non-initiating insider" (insider who has not yet committed an action). The behavior of an insider may be related to cognitive processes that can be measured by EEG. In addition, when one initiates a bad action, their heart rate (ECG) and skin conductivity (GSR) will respond to changes in their nervous system.

2.1. Research hypotheses

Using the EEG, GSR and ECG bio-signals, we can measure changes in a human's psychological and cognitive responses. If a normal worker becomes a non-initiating insider, his/her emotions could be revealed through specific bio-signals that respond to their deceit and lies.. Along with their change in feelings, the insider may be conflicted because of his/her life of values, so it arouses abnormal brain states when bad action and good action decisions are made.

Hypothesis 1: Based on normal and unusual emotional states, the values of skin conductivity from GSR and R-R intervals tracked by ECG data may provide a meaning difference.

Hypothesis 2: Based on decision including bad actions and good actions, the ratio of power spectrum density from EEG data may reflect a meaningful difference.

2.2. Experimental Setup

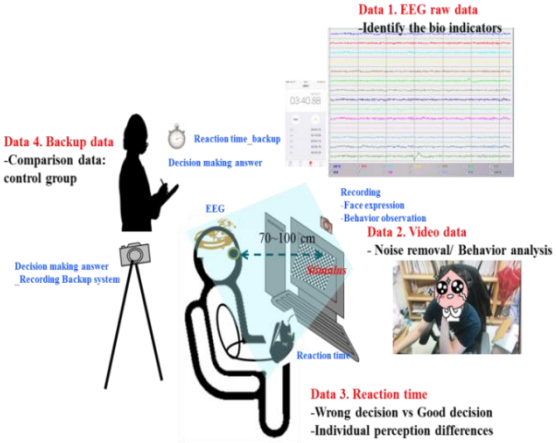

Fig.1. Example of experimental setup

Figure 1 shows the basic elements of the experimental setup. A feasibility study collecting EEG, GSR and ECG data was conducted on 10 men, around 23-28 years old, and were healthy. They performed two simple tests; a bad and good decision test and an emotion change test.

2.2.1 Emotion Test

When a normal worker thinks about becoming an insider, he/she must lie and be deceitful to colleagues. We conducted the lie-test five times using several different questions to reveal a variation in skin conductivity and heart rate, during the subject's lie and deceit testing. Typical questions during this phase of this experiment are "Have you ever watched porn?"; "Are you sitting on a chair now?"; and "Have you ever imagined killing someone ?". GSR and ECG data from Neulog sensors measured emotional changes while subjects answered these questions.

2.2.2 Bad and Good Decision Test

First, we developed a decision-making measurement tool using MATLAB to provide a menu of similar situations to instigate the typical reactions of an insider. Typically, workers become an insider when they feel dissatisfaction with their life internally or are

blackmailed by outsiders [4-5]. This tool consists of 140 scenarios, with Yes/No answers and a tic-toc program for checking the time needed to make a decision. This program suggests a number of difficulties a worker may encounter forcing them to participate in an insider event. For example, a terrorist might demand that you give them your security card to enter into a secure facility. . While we recording their EEG signal, we compile their Yes or No answers, using the Epoc Emotive wearable device, at a sampling rate of 128HZ. Each subject was fitted with a 14-channel electrode cap, with electrodes arranged in the extended international 10-20 system with a reference electrode on the top of the scalp.

3. Experimental Results

3.1. Emotion Results

Similar to the principle of lie detection, the results of deceit emotion have differences of skin conductivity and the value of R-R interval when they tell a lie. Someone hides something; they felt nervous and sweat a lot because it relates to human's nervous system. Figure 2 shows the representative sample of GSR and ECG analysis for the truth and lie. The skin conductivity graph by time series is monotonous when telling the truth, while the value of conductivity increases almost 7-8% with 5 sec duration when they are lying. In addition, R-R intervals related to measure the heartbeat increased when they tell a lie with regular pattern. However, during 5sec duration, the value of lowest point, called as S (Late depolarization of the ventricles) in Heart Rate Variability (HRV) analysis, has a slightly increase. Human can feel many emotions when they performed this test. To distinguish the difference on deceit feeling compared to other feelings, we tested the simple game which can be felt the fear. The reason why we chose the fear emotion as comparison feeling is that both of feeling (telling the lie and fear) are relatively negative but the difference between two feelings is from the intensity of energy (arousal). Figure 3 indicates the sample of GSR and ECG analysis when they felt fear. As you can be seen in Figure 3, the skin conductivity is highly increasing with long duration rather than telling a lie. In addition, the R-R interval after doing the simple game is shorter than before the test with irregular pattern. This means that it is possible to detect the insider's emotion when they hide something with distinguishing other emotion changes.

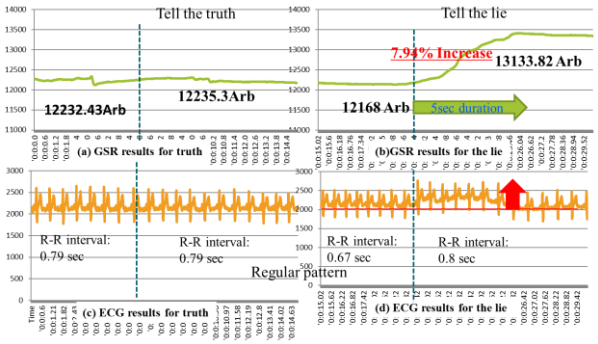

Fig. 2. GSR and ECG analysis for two cases: (a, c) Tell the Truth and (b, d) Tell the lie

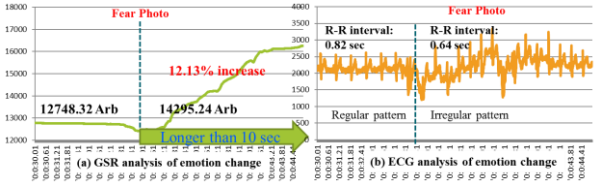

Fig. 3. GSR and ECG analysis for fear emotion

3.2. Bad and Good Decision results

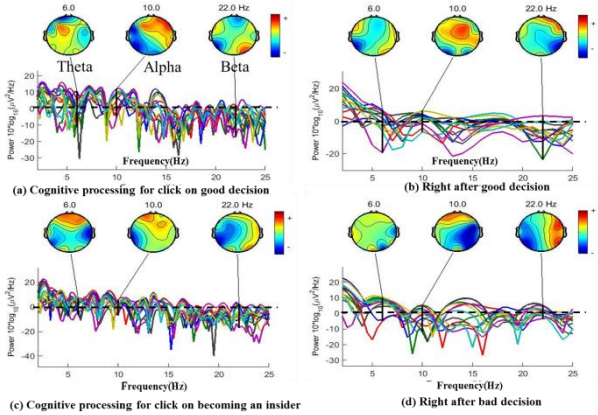

Fig.4. Power spectrum and frequency analysis for two cases: (a-b) Good decision and (c-d) Bad decision

Table.1. The EEG results for two cases: Good decision and Bad decision

	Cognitive process	Good decision	Cognitive process	Bad decision
[AF3]: Attention				
P_beta/P_alpha	1.7165	1.1232	1.1475	1.4487
P_gamma/P_alpha	0.7575	0.3844	0.3027	0.4469
[AF4]: Judgement				
P_beta/P_alpha	2.0453	0.8027	1.5123	1.6876
P_gamma/P_alpha	0.8714	0.3358	0.3713	0.6878
[P8]: Emotion understanding/Motivation				
P_beta/P_alpha	1.3091	0.884	0.9127	0.92
P_gamma/P_alpha	0.4204	0.3242	0.4681	0.4552
[P7]: Verbal understanding/Motivation				
P_beta/P_alpha	2.634	1.2233	1.4559	1.7081
P_gamma/P_alpha	1.4202	0.5329	0.4461	0.7233
[P3]: Cognitive processing				
P_beta/P_alpha	2.6863	1.6988	1.5162	1.5389
P_gamma/P_alpha	1.2617	0.5137	0.4305	0.9499

Figure 4 shows the qualitative results of power spectrum and frequency analysis between good decision and bad decision. During the thinking process indicated in Fig.4 (a) and (c), phase of these graph is complex and these seems like continuous frequently sine waveform,

while the graphs right after (b) bad or (d) good decision express the infrequent cosine waveform having steep gradient. When they think the bad action like coercion, unconscious area represented by theta brain wave was activated highly. Specially, the frontal lobe of brain, which takes charge of higher mental function such as attention and judgement, was activated. In addition, right after the decision whether good or bad action, beta brain wave was highly activated in the right front lobe of brain related to judgement. Interestingly, in case of right after bad action, the backside of right lobe, which takes charge of emotion and motivation, was activated together with front side. It means that the bad decision like becoming the insider is not easy to judge without emotional understanding and critical motivation.

To identify the trigger becoming an insider quantitatively, we calculated the ratio of power spectrum density. Table 1 shows the EEG results for two cases: good decision and bad decision. For comparison, we developed the two EEG indicators such as power ratio beta of alpha and gamma of alpha. This is because beta band (13-30Hz) represents active thinking and focusing; gamma band (30-50Hz) indicates the willingness and emotion; and alpha band (7-13Hz) is relaxed states in the consciousness state [6]. As shown in Table 1, the value of two indicators is increasing when they select the bad action but, the value is almost same or decreasing when they decided the good action. It means that it is possible to use EEG signals for detecting the insider.

4. Conclusions and Discussion

This paper showed the feasibility of predicting and detecting insider threats using EEG, GSR and ECG signals. In the section 2.1, two research hypotheses were established to identify the significant difference on EEG, GSR and ECG signals when the subject decided bad action and is the placed in deceit situation. These hypotheses were tested using two kinds of pilot experiments in the form of input (stimulus) and output (checking response of physiological signals and reaction time). The results from tests in Figures 2-4 and Table 1 proved the null hypotheses (Hypothesis 1 and 2) should be dismissed. Therefore, we confirmed the feasibility of insider detection using bio-signals from smart wearable devices. Despite necessary demand on an expansion into a formative experiment with large sample size (different sex, age, nationality and so on) and statistical analysis, this study is meaningful itself because this is the first try to reveal the potential for preventing and detecting insider threats using bio-signals.

At this stage, we have many problems to solve. First, bio signals because of sensitive characteristics tend to be very noisy. Second, EEG, GSR and ECG signals for identifying the potential insider generally lacks ground truth and these are very subjective depending on the person. Future work will address the uncertainty and sensitivity analysis that needs to be taken into consideration when overcoming the lack of ground truth and differences in individual perception when responding to stimulus. In the near future, it will be possible to use these monitoring technics in critical infrastructures of airports, NPPs and government installations, for improving national security.

REFERENCES

[1] DoD Office of the Inspector General, DoD Management of Information Assurance Efforts to Protect Automated Information Systems (Washington, D.C.: U.S. Dept.of Defense, 1997).

[2] Keeney, M., E. Kowalski, D. Cappelli, A. Moore, T. Shimeall, & S. Rogers. (2005) Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. U.S. Secret Service and CERT Coordination Center, Carnegie Mellon Software Engineering Institute, May 2005.

[3] U.S. Secret Service, Software Engineering Institute, CERT Program at Carnegie Mellon University and Deloitte, "2010 CyberSecurity Watch Survey—Survey Results," CSO Magazine, 2010, available at: http://www.sei.cmu.edu/newsitems/cyber_sec_watch_2010_release.cfm.

[4] Schultz, E.E.: A framework for understanding and predicting insider attacks. Comput.Secur. 21(6), 526–531 (2002)

[5] Nurse, Jason RC, et al. "Understanding insider threat: A framework for characterising attacks." Security and Privacy Workshops (SPW), 2014 IEEE. IEEE, 2014.

[6] J. G. Webster, “Electroencephalography: Brain electrical activity”, Encyclopedia of medical devices and instrumentation, Vol.2, pp. 1084-1107, 1988.