IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 9, 2021, accepted April 30, 2021, date of publication May 10, 2021, date of current version May 21, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3078470

Development of an Information Security-Enforced EEG-Based Nuclear Operators' Fitness for Duty Classification System

JUNG HWAN KIM[1], YOUNGGEOL CHO[2], YOUNG-A SUH[3], AND MAN-SUNG YIM[1]

[1]Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology, Daejeon 34141, Republic of Korea
[2]Agency for Defense Development, Daejeon 34186, Republic of Korea
[3]Korea Institute of Nuclear Safety, Daejeon 34142, Republic of Korea

Corresponding author: Man-Sung Yim (msyim@kaist.ac.kr)

This work was supported in part by the Nuclear Safety Research Program through the Korea Foundation Of Nuclear Safety (KoFONS) using the financial resource granted by the Nuclear Safety and Security Commission (NSSC) of the Republic of Korea under Grant 2003023, and in part by the Khalifa University of Science, Technology and Research-Korea Advanced Institute of Science and Technology (KUSTAR-KAIST) Institute, KAIST, South Korea.

ABSTRACT In a nuclear power plant (NPP), operator performance is a critical to ensure safe operation of the plant. The fitness for duty (FFD) of the operators should be systematically assessed before they engage in duties related to reactor operations. This study proposes the use of an electroencephalography (EEG)-based deep learning algorithm to classify an operator's FFD. To determine the suitability of this approach, EEG data were collected during simple cognitive exercises designed to examine the mental readiness of nuclear operators. The EEG-based FFD classification system designed could successfully determine an operator's sobriety, stress, and fatigue in a timely and cost-effective manner. As protecting personal information of the operators while using their EEG data is important and necessary, this study also investigated schemes for providing information security to the EEG-based FFD status classification system by following the International Organization for Standardization/International Electrotechnical Commission standard. Data confidentiality, integrity, and unlinkability were considered in the resulting schemes of information security for the EEG data. The resulting system provides the necessary protection of personal information and the FFD databases without significantly affecting the overhead of FFD classification through near real-time analysis.

INDEX TERMS Information security, brain computer interface, electroencephalography (EEG), deep learning, nuclear safety, fitness for duty (FFD).

I. INTRODUCTION

In a nuclear power plant (NPP), operator performance is a key factor for achieving safe operation. According to the United States Nuclear Regulatory Commission (USNRC), 65% of all US commercial NPP accidents are caused by human error [1].

Therefore, operators must be fit to undertake their work duties in an NPP [2]. The USNRC developed 10 Code of Federal Regulations (CFR) Part 26 to assist the licensee in implementing good practices to manage their NPP operators and to determine their fitness for duty (FFD). FFD programs are designed to provide reasonable assurance that NPP operators are trustworthy, are capable of performing their tasks in a reliable manner, are not under the influence of any substance, legal or illegal, that may impair their ability to perform their duties, and are not mentally or physically impaired from any cause that can adversely affect their ability to safely and competently perform their duties.

Among the various features contained in 10 CFR Part 26, the USNRC's focus is on alcohol testing, stress management, and fatigue management [3]. However, there are some limitations in the implementation of this approach. Alcohol testing is conducted only a few times a year, whereas stress and fatigue management are based on self-evaluations, which are subsequently assessed by qualified technicians and in some cases, may include a doctor's interview. These tests are infrequent and the interpretation of the results can be subjective. There remains a need to develop a comprehensive, timely, and cost-effective system that supports frequent and objective analyses of an operator's sobriety, stress, and fatigue [4].

The associate editor coordinating the review of this manuscript and approving it for publication was Ludovico Minati.

Such a system would result in more effective management of the workforce and enhanced workplace safety and security.

With the development of data science and information technologies, the use of electroencephalography (EEG) data, along with machine learning algorithms, has been widely applied in various fields, such as alcohol intake, stress, and fatigue evaluation [5]–[8]. Appropriate use of machine learning has made it possible to classify EEG data in a reliable manner.

Protecting personal information (PI) is an important requirement in the use of biosignals. In 2016, the European Union (EU) enacted the General Data Protection Regulation (GDPR) in recognition of the importance of handling PI. In GDPR, biometric data means personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic data.

Until now, there has been no concrete international consensus on protecting the PI associated with the use of EEG data. A user's private information is potentially vulnerable if an unauthorized person knows the position of the electrodes, extracted features, and frequency ranges measured during the examination. According to the reference, sensitive PI includes users' emotions, alcohol abuse behavior, the area of residence, medical conditions, and learning ability [9], [10]. It may be possible to link a subject's EEG data to some of these PI attributes. Without adequate data privacy, ethical and legal issues could stifle the collection of EEG data and its use [11], [12]. Hence, EEG data and any related PI must be protected and treated as sensitive information.

While a large number of studies continue to explore human performance based on EEG data, there is still a lack of research regarding the ways to ensure the privacy of the EEG data. This indicates the need to implement an adequate information security management system (ISMS) to protect the privacy of sensitive PI while applying EEG-based technology in the field.

Along with development of an EEG-based FFD evaluation system, protection of PI during the use of EEG data was examined in this study through the application of relevant information security technology. The EEG data were collected while the subjects performed cognitive tasks related to nuclear safety. This study explored the feasibility of using these data as the basis for classifying the FFD status of nuclear operators. The FFD status to be examined include alcohol intake, stress, and fatigue based on EEG signals.

The objectives of this study were: (1) to determine the feasibility of classifying an NPP operator's FFD using deep learning algorithm based on EEG data collected while performing cognitive tasks, (2) to investigate the methods to acquire and analyze the EEG data considering aspects related to information security, and (3) to examine the feasibility of an ISMS that can quickly and securely process the PI and the FFD results for immediate use in daily work planning. If successful, the proposed ISMS will remove the time delays and subjectivity that burden the current FFD in NPPs.

II. EEG-BASED OPERATORS' FFD EVALUATION

This section describes the development of the methods of EEG analyses to comprehensively evaluate operators' FFD.

A. SUBJECTS

To examine FFD status outlined in 10 CFR Part 26, the present study recruited four different groups: three groups related to FFD criteria (alcohol intake, stress, and fatigue) and a fourth group labeled the normal group. Ninety subjects (80 males and 10 females with ages ranging between 20 and 35, with a mean of 24) having engineering backgrounds were voluntarily recruited from the Korea Advanced Institute of Science and Technology (KAIST) student community. The subjects enrolled in the program had no history of neurological disorder, mental disorder, alcohol dependence, or drug dependence.

By carefully controlling factors that could affect their classification status, recruited subjects represented only one of the specific groups.

The Perceived Stress Scale (PSS-10) was performed on all the subjects as part of the recruiting procedure [13]. PSS scores ranging from 14-26 indicated a moderate perceived stress level while 27-40 was a high perceived stress level. The alcohol intake group, the fatigue group, and the normal group were recruited from subjects with PSS scores ranging from 14-26. In contrast, 24 subjects with PSS scores above 27 were placed in the stress group.

The alcohol intake group consisted of 19 subjects with a blood alcohol concentration (BAC) above 0.03% based on 10 CFR Part 26. The subjects in the alcohol intake group were instructed to consume the same amount of alcohol one hour and thirty minutes before the experiment. Over the next 30 minutes, each subject was fitted with an Ag/AgCl electrode cap arranged in the international 10-20 system of electrode placement. Exactly two hours after drinking, their BAC was measured using a breathalyzer.

The non-alcohol intake subjects were instructed to abstain from consuming alcohol for at least 24 hours before the experiment. Of these subjects, twelve were categorized into the fatigue group. The fatigue group was instructed to sleep less than four hours over a 48-hour period. The remainder of the subjects in the non-fatigue group were instructed to sleep for more than seven hours and to abstain from consuming caffeine for at least 24 hours before the experiment.

The remaining thirty-five subjects with no alcohol intake, no stress, and no fatigue were categorized into the normal group.

Prior to testing, the experimenter explained the experimental procedure to the subjects, as required by KAIST Institutional Review Board (IRB) guidelines. Subjects read an information sheet and signed an agreement regarding the data collection process. The EEG experiments were conducted in a dark room with soundproofing to support the subject's

concentration and to minimize the background light and noise. This protocol was essential, as the collection of a subject's EEG signals can be easily influenced by light and sound.

B. EXPERIMENTAL DESIGN

An experiment was designed to measure EEG data while the subjects performed cognitive tasks mimicking the mental activities of operators in advanced NPPs. The tasks in the experiment intended to test the patterns of EEG data while performing cognitive tasks before entering the main control room (MCR) for the identification of FFD for safe nuclear reactor operations.

The design of an advanced NPP MCR is based on the use of digital technologies. In these reactor's MCR, operators rely on using hard devices with soft controls such as mice and keypads to perform operator functions. Generally, the key activities of the MCR operator are related to safety in advanced NPPs demands cognitive work in order to monitor and diagnose situations involving visual matching ability, visual recognition memory, problem-solving ability, attention, and multitasking. These are related to the four major factors that contribute to human errors: observation, search, memory, and decision-making. In our previous research [14], EEG-based human attention monitoring, while performing related cognitive work was examined using an NPP simulator, called the Windows-based Nuclear Plant Performance Analyzer (Win-NPA). Win-NPA is a compact nuclear simulator capable of simulating 53 malfunctions in nuclear reactor operations. In the study, the subjects conducted operational tasks for both normal (i.e., startup and shutdown) and two accident situations with Win-NPA involving visual matching, visual recognition memory, problem-solving, attention, and multitasking.

The experiments in the study were performed by engaging the subjects with similar cognitive tasks using a computer program, Lumosity. Lumosity is a computerized program developed to improve cognitive skills including memory and attention. This program is widely used in the field of cognitive psychology [15]–[17]. Kim *et al.* found that the general tasks with observation, search, memory, and decision-making show similar classification accuracy with soft control-based tasks using Win-NPA as an advanced MCR mock-up [14].

Use of the Lumosity program to mimic nuclear operators' actions was based on the tasks such as the memory matrix (MM) test, a chalkboard challenge (CC), and the train of thought (TT) test.

In the MM test, the subjects were required to quickly memorize a group of tiles on a grid. This program challenges the memory of a subject to track the location and position of a tile within an environment. The memory of the subject temporally stores and manipulates the presented information. The MM test describes a situation of the Win-NPA tsk, which monitors and memorizes the indicator value in the key areas of interest (AOI) in the MCR.

The CC test measures quantitative reasoning and problem-solving skills for decision-making. The test uses numerical estimation to quantify a subject's ability to approximate numerical relationships quickly or with incomplete information. This test is similar to a situation of the Win-NPA task, which monitors the indicator in the key AOI and verifies that the indicator value is within the procedure range.

In the TT test, a subject guides an increasing number of trains to their predetermined stations using a computer mouse. The subject must divide their attention to guide all trains simultaneously thus experiences a situation similar to the Win-NPA multitasking task, which monitors various indicators in key AOI and identifies scenario (normal operation or accidents).

As shown in Figure 1, each experiment session consisted of five steps. The first step involved collection of the subjects' baseline EEG signals. This was performed by collecting EEG signals for two minutes with the subjects' eyes closed (EC). This step was followed by another EEG measurement for two minutes with the subjects' eyes open (EO). Subsequently, the EEG signals were measured for two minutes while the subjects performed each of the program's test (MM, CC, and TT). This timeline of testing was followed once each of the 90 subjects.

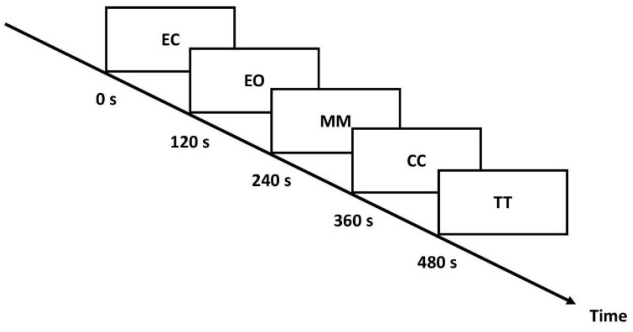


FIGURE 1. EEG experiment paradigm of the cognitive training programs.

C. EEG RECORDING AND PREPROCESSING

EEG signals were measured using the BrainMaster Discovery 24E system (BrainMaster Technologies Inc.). Each subject was fitted with an Ag/AgCl electrode cap arranged in the international 10-20 system of electrode placement. The EEG data were recorded from 19 channels Fp1, Fp2, F7, F3, Fz, F4, F8, T3, C3, Cz, C4, T4, T5, P3, Pz, P4, T6, O1, and O2 at a sampling rate of 1024 Hz. Reference electrodes were located on both earlobes. During the experiment, an electrode impedance of below 5 kΩ was maintained for all the channels. One of the related objectives of the use of these channels was to develop a minimum set of channels to minimize the use of EEG data while providing meaningful signals for FFD classification.

Data preprocessing was performed based on using Makoto's preprocessing pipeline using EEGLAB to remove artifacts in the collected EEG data [18]. The line noise

was removed with the CleanLine plugin [19]. Bad channels were rejected using the Clean Rawdata plugin, and continuous data were corrected using artifact subspace reconstruction (ASR). The Adaptive Mixture Independent Component Analysis (AMICA) program and postAmicaUtility toolbox were used to conduct an independent component analysis (ICA) [20]. The artifacts from body motions, rolling eyeballs, and blinking were excluded from the analysis based on a visual inspection of each component. The preprocessed data were divided into six 20-second epochs for each task (EC, EO, MM, CC, and TT) in the experiment. Thus, each task contained 540 20-second epochs, 114 from the alcohol intake group, 144 from the stress group, 72 from the fatigue group, and 210 from the normal group.

D. FEATURE CONSTRUCTION

Our previous work involving EEG-based classification, features extracted from the time domain that were found significant [11]. Based on these results, this study selected features from the time domain of the EEG signals that supported the development of a deep learning algorithm. In the time domain, the Hjorth features and the peak-to-peak values were calculated from each channel. Three Hjorth features reflected the characteristics of activity, mobility, and complexity [21]. Hjorth activity represents the signal power, the variance of a time function. Hjorth mobility is defined as the proportion of standard deviation of the power spectrum. It can be derived by calculating the square root of the variance of the first derivative of the signal divided by variance of the signal. Hjorth complexity represents the change in frequency and indicates the signal's similarity to a pure sine wave. It can be computed by calculating the mobility of the first derivative of the signal divided by the mobility of the signal. The peak-to-peak value is the difference between the maximum value and the minimum value of the time series. Consequently, four features from the time domain were extracted from each channel of EEG data. However, to evaluate operators' FFD, it may be necessary to include all the available features such as those based on connectivity, synchronization and nonlinear features. Using a large number of features may result in overfitting and adding time delay to the system. Furthermore, one of the related objectives of the use of these features was to minimize the use of EEG data while providing meaningful signals for FFD classification. Therefore, this study used the fewest features possible to minimize the leakage of PI that is technically required to identify individuals.

E. CHANNEL SELECTION

A user's private information is potentially vulnerable, if an unauthorized person knows the location of the electrodes and the extracted features. Information should be used to a minimum to minimize the leakage of PI that is technically processed to identify individuals. During the process of collecting EEG data, recording unnecessary data (e.g., full set of EEG data) should be avoided. To examine the issue, this study selected frontal and temporal where four to seven channels are located in comparison to the use of full brain scanning.

The brain areas and their corresponding electrode placements, consistent with the international 10-20 system of electrode placement are frontal (Fp1, Fp2, F3, F4, F7, F8, Fz) and temporal (T3, T4, T5, T6), as shown in Figure 2. Extracted features were measured on these parts of the brain. Therefore, 76 features (four time domain features with 19 channels) were used for total brain, 28 features (7 channels) for frontal lobe, and 16 features (4 channels) for temporal lobe.

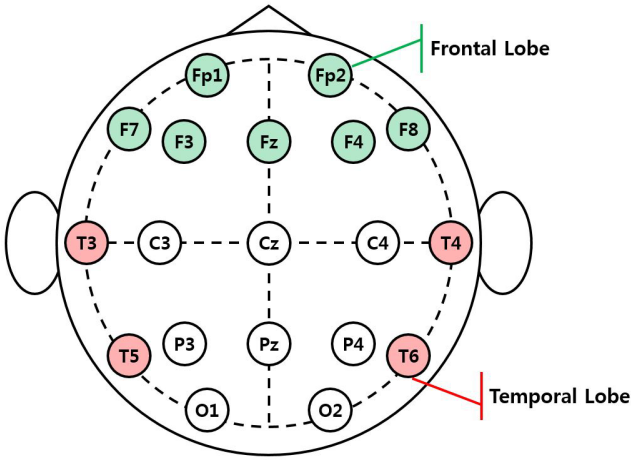


FIGURE 2. Selected channels corresponding to the international 10-20 system of electrode placement.

However, the possibility of leakage of PI that may identify individuals cannot be completely removed by simply minimizing the collected information. While dealing with the PI that may identify individuals, a system specifically designed to protect PI should be implemented. This study introduced an ISMS to protect private information resulting from EEG signals.

F. DEEP LEARNING ALGORITHM FOR FFD CLASSIFICATION

For the intended classification of FFD status of workers, this study employed several major machine learning algorithms for comparative evaluations. The methods used include multinomial logistic regression (MLR), support vector machine (SVM), convolutional neural networks (CNN), and long short-term memory (LSTM) algorithms.

The MLR is an extension to the logistic regression model that involves cross-entropy loss and predict probability distribution to support multi-class classification. The softmax function was used to find the predicted probability of each class.

The SVM is a supervised learning algorithm and formulates a separating hyperplane. Kernel SVM finds the optimum hyperplane into a higher dimensional space, which ensures that the distance between margins is maximum. This study specifically used the radial basis function (RBF) kernel to project input vectors into a Gaussian space.

The CNN consists of several convolution-pooling layer pairs and a fully connected layer at the output. A standard CNN is designed to recognize shapes in images and is partially invariant to the location of the shapes. To classify operators' FFD, EEGNet, a compact CNN for EEG-based brain–computer interfaces, was employed in this study [22]. It exhibits superior performance for detecting patterns in EEG for various applications. In the classification block, the features are passed directly to a softmax classification with 4 units, which represents the number of classes in the data. The model was fitted using the Adam optimizer. Altogether, 300 training iterations were run, validation was stopped, and the model weights that produced the lowest validation set loss were saved. The EEG raw data was used as an input for CNN analysis.

Since EEG signals constitute highly dynamic and non-linear time series data, LSTM algorithm exhibit a design advantage in isolating temporal characteristics of brain activity at different states [23]. Therefore, this study also evaluated the operators' FFD using the LSTM algorithm. To meet the irreversibility criteria, this study proposed a method to extract and store features through preprocessing without direct use of the EEG raw data.

As shown in Figure 3, the proposed LSTM algorithm consists of two LSTM layers (with 32 and 16 neurons, respectively), two dropout layers, and a dense layer. The LSTM structure is composed of two LSTM layers to obtain optimal performance while reducing the analysis time. The model was fitted using the Adam optimizer. Altogether, 300 training iterations were run, validation was stopped, and the model weights that produced the lowest validation set loss were saved. The dropout technique was used to help regularize the model with a dropout probability of 0.2 for classification to help prevent overfitting.

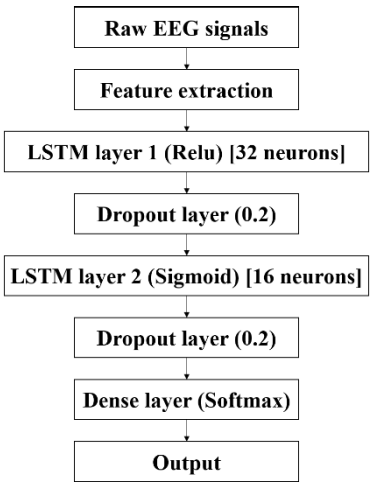


FIGURE 3. The structure of the proposed LSTM algorithm.

The EEG data were downsampled to a sampling rate of 256 Hz with 19 channels and 30720 time samples. A six-epoch size of 7680 time samples were used for analysis. For the MLR and SVM algorithms, 5-fold cross validation was used to classify a subject's group. In total brain classification, 116736 epochs were used as training data and 29184 epochs as testing data.

For both the CNN and LSTM algorithms, 60% of the observations were randomly selected and used as training data, 10% of the observations were used as validation data, and 30% of the observations were used as testing data to classify a subject's group.

III. ISMS DESIGN

The objective of this section is to examine the feasibility of an ISMS that can quickly and securely process the PI and the FFD results for immediate use in daily work planning.

The ISMS proposed in this study is based on the incorporation of the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 24745 standard "Information technology — Security techniques — Biometric information protection" [24]. ISO/IEC 24745 describes the requirements and guidelines necessary to protect personal and biometric information. Although the ISMS suggested in this study is not a biometric authentication system, it essentially performs the same function in the context of how EEG data and PI would be handled.

According to ISO/IEC 24745, an ISMS should meet the security requirements of confidentiality and integrity. Confidentiality is a property that protects the data against disclosure or unauthorized access [25]. This property makes the data indecipherable. Integrity is a property that protects the data from being forged or damaged. This property guarantees that the original data maintain their integrity.

An ISMS should also meet the privacy requirements of irreversibility and unlinkability. Irreversibility means transforming data irreversibly before they are stored. Thus, the transformed data can never disclose the information in the original data. This property prevents unintended use of the original data. Unlinkability prevents linking biometric or other data across applications or databases, thereby precluding an individual's data from being inadvertently linked to his/her identity.

In the following sections, the proposed ISMS, its implementation, and data use are described. The ISMS proposed in this research consists of five subsystems: the data capture subsystem, the preprocessing subsystem, the decision subsystem, the data storage subsystem, and the management subsystem, as shown in Figure 4.

A. DATA CAPTURE SUBSYSTEM

If the FFD classification is based on real-time EEG measurements, there are potential technical or regulatory issues regarding information security. Therefore, this study assumed that an operator performs cognitive tasks for 120 seconds before entering the MCR for evaluation of his/her FFD based on the baseline EEG data.

Before collecting PI and the EEG data, operators have to provide official consent for the acquisition and processing

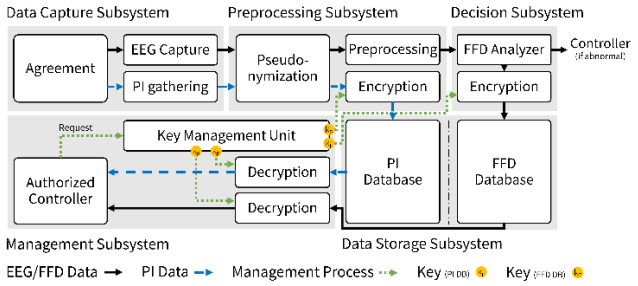


FIGURE 4. Proposed ISMS component diagram.

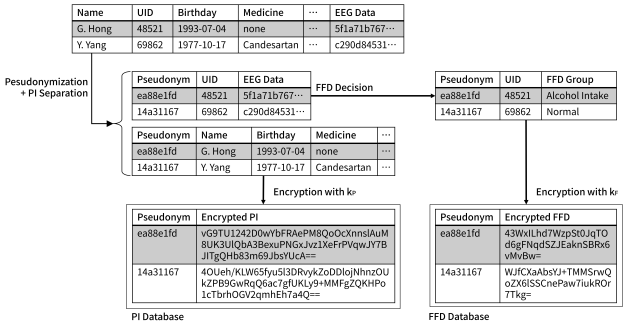


FIGURE 5. Dataflow diagram for saving PI and the FFD data using pseudonymization and encryption with authentication.

of the PI and the EEG data according to the Korean Act on Personal Information Protection (KAPIP). In Korea, this Act requires an NPP operator to understand and agree to the purpose of collecting PI and the EEG data and to understand the information that will be used, the way this information will be used, and the duration for which it will be used. This process is similar to the requirements of the EU GDPR.

In this study, it was assumed that the operators had proceed written consent for the collection of their PI and the EEG data to assess their readiness for operational duties. In addition, the data controller was required to secure a separate agreement for collecting health information. This was necessary because health information may be specified as sensitive information. After obtaining the users' agreement, the data controller could access the users' PI and record their EEG data.

B. PREPROCESSING SUBSYSTEM

To ensure PI security, three approaches are typically applied: data anonymization, encryption, and access control. Data anonymization eliminates personal identifiers such as names and personnel identification number from the collected data. This means that the subject cannot be directly identified from the anonymized data. However, once the EEG data analysis determines that one of the operators is not fit for duty, the anonymization of PI makes it impossible to link the EEG determination to the specific operator who has fitness issues.

The proposed ISMS needs a system that will not only protect the identity of the operator's PI and the FFD status, but will also allow tracking FFD to identify operators with any fitness issues. In such cases, pseudonymization can be used to replace personal identifiers with uncorrelated artificial identifiers called pseudonyms. Pseudonyms are used instead of data anonymization. As shown in Figure 5, an operator's name and unique identifier (UID) will be combined and replaced with a unique pseudonym to enable identification of each operator if necessary. Unique pseudonyms can be created using a hash function.

Hash function is an internationally accepted method to create pseudonyms. It maps arbitrary data to a fixed-size value called a hash value. A hash function with a specific length is often called one-way encryption because it converts one kind of data into another data type that does not contain any of the original information and is practically noninvertible. In addition, it always produces the same output when the same input is provided, but a highly different output when there is a very small change in the input (avalanche effect). This feature is important for the protection of the input information, i.e., the PI and the FFD databases (DBs) in the event of a potential attacker reaching the output information. For example, the hash value of a string "Mary Jung" using hash function Secure Hash Algorithm-256 (SHA-256) is "e86a6b461b88da6feb46388a89d6a4e9a20de9823af2402cf512ddda0c4db86," which is completely different from that of "Mary Jung." (Mary Jung with a period) as "91b027334cc5976eb2c84f9ebb48cb9ed2577b4b1f3cff5eb9607e4a848d2c2a."

Subsequently, the controller must take technical, administrative, and physical actions to securely process the pseudonymous data. It is essential that the pseudonymous data not to be lost, stolen, leaked, forged, modified, or damaged. In addition, the access key used to restore the pseudonymous data to its original state must be separately stored and managed.

C. DECISION SUBSYSTEM

The decision subsystem calculates an operator's FFD using a classification model as described in the previous section (II. F). The FFD classification results are transferred to the data storage subsystem and stored. To meet the irreversibility criteria, only the FFD classification results will be stored and not the EEG raw data. FFD classification results are encrypted before being stored in the FFD database. This process will be described in detail in the following section. When an off-normal FFD status (e.g. alcohol intake, stress, or fatigue) is identified, an authorized controller will be notified. Upon notification, the authorized controller can request a decryption key to access the identity of the operator with an off-normal FFD status.

D. DATA STORAGE SUBSYSTEM

To minimize the risk of privacy disclosure, it is recommended that PI and the EEG data be encrypted and stored separately. For further protection, a system can be set for access to the encrypted data requiring two authorized controllers who are

in possession of or can retrieve different portions of the access key. The input of both authorized controllers is necessary to create a complete access key to reach the encrypted PI and FFD databases.

Ideally, the FFD database should be completely independent from the PI database. However, as envisioned for the use of FFD assessment results, when an operator is classified as unfit, the authorized controller needs timely access to the PI database. Therefore, including minimal PI-related information such as an encrypted UID in the encrypted FFD database is necessary. As shown in Figure 5, timely access to PI data can be achieved through decryption of the FFD database, which makes the UID and FFD results accessible.

To ensure confidentiality and integrity of both the PI and the EEG data, the standard ISO/IEC 24745 standard suggests using encrypted and authenticated data. The following steps present how this study approached the security in data storage and the security necessary to link FFD issues to the employee in question.

Initially, data encryption is needed to guarantee confidentiality. Encryption algorithms use secret keys to encode plain text and to decode ciphertext. Encrypted data can be decrypted successfully only by using the correct key. There are two kinds of encryption algorithms: symmetric-key and asymmetric-key. The symmetric-key algorithm uses the same key for both encryption and decryption, whereas an asymmetric-key algorithm uses separate keys for each action. Generally, symmetric-key algorithms are used for efficiency, as asymmetric-key algorithms take significantly more time to encrypt or decrypt a large volume of data.

In this study, the Advanced Encryption Standard (AES) algorithm, the most commonly used algorithm among the symmetric-key algorithms with encryption and decryption capability was utilized. The AES algorithm has been adopted as a standard by the U.S. National Institute of Standards and Technology since 2001 and was approved by the U.S. Government for the security of classified information. Both PI and the FFD results should be encrypted before the databases are stored separately using different keys.

Data authentication is also needed to ensure integrity [26]. Data authentication guarantees that the original data have not changed. In this study, a message authentication code (MAC) was used for this purpose. MAC is similar to a hash but uses a secret key while generating the code. This feature securely provides integrity, and is called ''strongly unforgeable,'' since an attacker cannot forge the data without knowing the key. It was applied by attaching MAC to the ciphertext during data encryption and was used for verification during data decryption. Among the various ways to implement authenticated encryption, this study used encrypt-then-authenticate-then-translate (EAX) mode of AES to evaluate ISMS reliability with respect to processing time and security evaluation.

E. MANAGEMENT SUBSYSTEM

The aforementioned subsystems make the ISMS technically secure. However, the value of information security is extremely limited without appropriate management and process security by the system. While all NPP operators are educated in information security at the organization level through security education, establishing security teams, security screening of managers, or devising security processes, the ISMS is organized to address information security at the systems level.

In Figure 6, authorized controller is defined as the person approved to request access to the relevant information from the access control unit. This allows the authorized controller to request the decryption key and if approved, the data in the FFD database can be tied to an identified person using the decryption key. The same process was used to identify PI from the PI database.

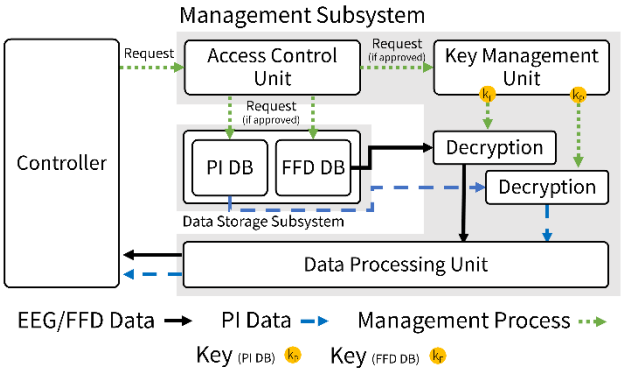


FIGURE 6. Overall process of the management subsystem from the controllers' perspective.

Physical access control and information access control are required to protect the security of a system. Therefore, only authorized controllers are allowed this access. In an NPP, physical access control can be achieved by defining security zones where databases are physically located and access to these areas is restricted. Permission for authorized controllers to access PI and the FFD databases should be granted only when necessary. To establish when access is necessary, procedures, processes, and conditions for information access control need to be established.

Managing the encryption keys requires the highest security because unauthorized use of encryption keys can destabilize the whole ISMS. For security, the keys should be stored in a designated, separate key management unit. ''Separate storage'' could be a physically separated device or a device without any network connection. A policy addressing access control to keys must define who has access and how they can access and use the keys. Encryption keys can be fixed passwords. However, for enhanced security, it is recommended that the passwords be changed periodically or generated as needed. Additionally, it is necessary to have two different controllers, each of whom has different portions of the password. Figure 7 shows the processes required to access the data from the databases.

Figure 8 shows the processes necessary to link the FFD and PI databases. Assuming that personal identifiers are

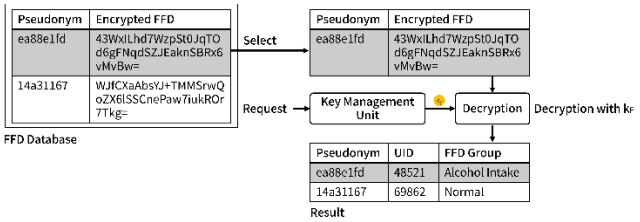


FIGURE 7. Dataflow diagram of fetching FFD data from the FFD database.

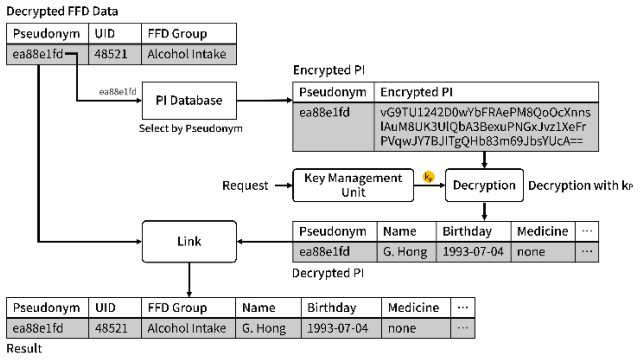


FIGURE 8. Dataflow diagram of linking FFD data to the PI data.

eliminated in the PI and the FFD databases, a pseudonym must be used to link the two databases with each operator's information. To cope with an unexpected security event, a system management process is needed to find a solution. Such a process requires identification of the data that were changed or leaked and the cause of the problem. To ensure a successful solution, the ISMS should identify and keep a log of every system event, such as access, modification, or data selection.

IV. CLASSIFICATION RESULTS

The results relevant to the development of the FFD classification models using the EEG data and their features are described in this section. As described in the feature construction section, four features from the time domain in the EEG data were used for the classification.

Table 1 shows the average classification accuracy of EC, EO, MM, CC, and TT across total, frontal, and temporal areas for all classification groups based on using the MLR, SVM, CNN, and LSTM algorithms. The classification accuracy was calculated as the total number of correctly classified samples by the model in the testing data divided by the total number of samples in the testing data. For EEG data, the average classification accuracy while performing cognitive activities in the Lumosity program (MM, CC, and TT) outperformed those obtained from EEG data measured during the EC and EO states. In addition, SVM, CNN, and LSTM algorithms exhibited higher classification accuracy across total, frontal, and temporal areas than MLR.

In general, the average classification accuracy increases when the number of epochs and channels increases (i.e., with total brain channels). The effect of increasing the size of

TABLE 1. All classification groups combined case: Comparison of average classification accuracy of MLR, SVM, CNN, and LSTM algorithms using different task EEG data from total, frontal, and temporal areas (Unit: %).

Task	Classifier	Total	Frontal	Temporal
EC	MLR	84.2	70.0	68.3
	SVM	87.1	82.5	86.0
	CNN	88.0	70.0	65.8
	LSTM	89.2	80.0	80.9
EO	MLR	81.2	64.1	68.0
	SVM	78.5	81.3	84.7
	CNN	85.2	61.8	58.8
	LSTM	84.5	77.7	80.6
MM	MLR	85.2	68.0	68.8
	SVM	91.5	87.2	85.1
	CNN	98.4	71.7	72.3
	LSTM	96.4	92.7	92.7
CC	MLR	84.9	69.8	62.3
	SVM	87.2	85.2	86.1
	CNN	97.5	72.2	70.3
	LSTM	94.3	91.2	89.9
TT	MLR	85.9	66.1	60.7
	SVM	92.6	90.7	91.7
	CNN	95.8	79.2	69.4
	LSTM	95.2	91.7	88.1

EEG data was particularly significant with the CNN analysis. Interestingly, the proposed LSTM algorithm exhibited higher performance than the CNN algorithm when only the data from the frontal or temporal areas are used. This indicates that LSTM can constitute a useful algorithm for EEG-based FFD classification employing a low number of channels. Therefore, using the proposed LSTM algorithm makes it possible to classify operators' FFD while protecting information quickly and accurately.

Table 2 shows the average classification accuracy of each classification group across total, frontal, and temporal areas based on the LSTM algorithm. As in all groups' combined cases, the average classification accuracy was also higher for cases using the Lumosity program's cognitive activities when compared to the EC and EO states. In addition, the classification accuracy of each group increased as the number of subjects increased (in most cases, higher performance was observed for the normal group and the stress group).

To examine potential errors in the classification, false positives (FPs) and false negatives (FNs) were calculated for the case using the LSTM algorithm. Here, FP is an error in which a test result incorrectly indicates that subjects are from the alcohol intake group, the fatigue group, or the stress group while they are actually from the normal group. In contrast, FN is an error where the test result incorrectly indicates that subjects are from the normal group when in reality they are not normal.

As shown in Table 3, the rates of FPs and FNs in the results corresponded to 0.00-10.00% with the FN rates lower than those of FP rates in most cases. Lower error rates and higher classification accuracy can be achieved when large number of EEG data can be accumulated for each subject. These

TABLE 2. Average classification accuracy of each classification group across total, frontal, and temporal areas with the use of the LSTM algorithm (Unit: %).

Task	Group	Total	Frontal	Temporal
EC	Alcohol	81.8	59.1	72.7
	Fatigue	93.3	66.7	80.0
	Normal	89.8	91.8	81.6
	Stress	91.2	82.4	85.3
EO	Alcohol	58.8	47.1	64.7
	Fatigue	85.0	75.0	65.0
	Normal	93.9	90.9	93.9
	Stress	87.9	81.8	84.8
MM	Alcohol	97.4	94.7	100.0
	Fatigue	100.0	85.2	77.8
	Normal	94.7	94.7	96.1
	Stress	96.1	92.2	90.2
CC	Alcohol	85.7	82.9	68.6
	Fatigue	90.0	80.0	90.0
	Normal	98.6	97.2	100.0
	Stress	97.0	93.9	90.9
TT	Alcohol	93.5	93.5	87.1
	Fatigue	96.2	88.5	80.8
	Normal	95.5	89.6	88.1
	Stress	95.5	95.5	93.2

TABLE 3. False positives (FPs) and false negatives (FNs) in FFD classification across total, frontal, and temporal areas based on the use of the LSTM algorithm (Unit: %).

Task	FP/FN	Total	Frontal	Temporal
EC	FP	4.17	7.50	10.00
	FN	4.17	3.33	7.50
EO	FP	2.91	7.77	8.74
	FN	1.94	2.91	1.94
MM	FP	1.56	3.65	1.56
	FN	2.08	2.08	1.56
CC	FP	1.89	6.29	5.66
	FN	0.63	1.26	0.00
TT	FP	2.38	2.38	4.17
	FN	1.79	4.17	4.76

findings indicated the feasibility of using EEG-based system for FFD classification, perhaps at lease as a supportive system for existing FFD evaluation systems.

V. ISMS RELIABILITY

The following section summarizes the results from the development of supporting ISMS to meet the European and Korean PI security system requirements.

The proposed near real-time data analysis in this research requires special considerations for its application in the nuclear industry. Any system that is essential for safe and secure operation of an NPP must be equipped with a reliable security system as required by law. The reliability of the information security approach should also be assessed quantitatively in terms of defense against unauthorized users. Moreover, a quick turnaround of the collected EEG data and identification of the FFD status are essential to the implementation of the proposed approach for its intended application in NPPs (to quickly determine an operator's FFD and to notify the appropriate authority before the operator begins the daily tasks). An EEG-based FFD evaluation system should also comply with regulatory requirements with minimal impact on the user.

A. PROCESSING TIME

The additional time required to implement information security, i.e., pseudonymization, authenticated encryption, and decryption, of the PI and the FFD data was assessed in this study using an Intel® Core™ Processor i5-7267U, 16GB RAM, and Mac OS X 10.14 with PyCryptodome package on Python 3.8.

Altogether, 100 datasets were randomly generated using four different lengths: 128bytes, 1KiB (2^{10}bytes), 32KiB, and 1MiB (2^{20}bytes). These lengths were used to conservatively represent the data to be processed in an ISMS at an NPP. The average time required was calculated for pseudonymization, authenticated encryption, and decryption for each set of the 1000 combinations. For pseudonymization, the SHA-256 hash function was used. For authenticated encryption and decryption, the AES-256 algorithm with the EAX mode was used. Table 4 summarizes the results of the overhead calculations for different lengths of the data. The results of the calculations indicated that the overhead was less than a few milliseconds. Typical PI is smaller than 32KiB, which can hold more than 8,000 characters when encoded by UTF-8. FFD results can have even fewer characters. Therefore, the addition of these three data security processes requires only a few milliseconds.

TABLE 4. Calculation of the additional time required, in milliseconds (ms) for pseudonymization, encryption, and decryption.

Data length	Pseudony -mization	Encryption	Decryption	Sum
128B	0.0273ms	0.2850ms	0.3070ms	0.6200ms
1KiB	0.0355ms	0.2980ms	0.3170ms	0.6510ms
32KiB	0.1920ms	0.4230ms	0.4350ms	1.0500ms
1MiB	5.7300ms	4.5500ms	4.1800ms	14.4000ms

B. SECURITY EVALUATION

When a data storage subsystem is attacked, the attacker can obtain only the pseudonymized identifier and encrypted data. The time required for the attacker to decrypt the encrypted data is important. This study calculated the time required to decrypt the data without keys and assumed the use of AES. AES supports key sizes of 128, 192, or 256 bits. The key length is directly related to the strength of the security, since the simplest method of attempting to decipher an unknown key is to try to input all the possible key values in the algorithm. This technique is called a brute-force key search. With a key of n-bit size, the number of attempts required during a brute-force key search is 2^n. On an average, 2^{n-1} attempts are needed to find the correct key. The number of attempts increases exponentially as the key size increases. Supposing that a processor can decrypt 10,000,000 AES-encrypted ciphertexts encrypted with a 128-bit key in 1 s

(10MHz rate), the average expected time for a brute-force key search is $2^{127} \times 10^{-7}\text{s} = 5.40 \times 10^{23}$ years, making decryption impractical. Currently, the best recorded attacks on AES require $2^{126.01}$ operations for a 128-bit key and the difficulty increases exponentially while using a 192-bit or 256-bit key, verifying the impracticality of a successful attack [27].

When an attacker attempts to forge an existing data entry in a database (change an entry from ABC to ACB), he/she must imitate the encryption process of the system. If this attempt is unsuccessful, the forged data will be discovered during the system's authentication process. The same encryption algorithm, key, and authentication logic are required to forge an original data entry. Among these three elements, finding the encryption key is impractical due to the time required according to the aforementioned calculations. This indicates that the security of the proposed system is appropriate for the intended application.

VI. DISCUSSION

The following discussion examines information security-enforced EEG-based nuclear operators' fitness for duty classification methodology.

A. EEG-BASED FFD CLASSIFICATION

While this study found that all of the algorithms examined are useful for EEG-based FFD classification, LSTM was found to be the best choice considering both classification accuracy and the information security. When a large amount of EEG data is available for each operator, the proposed LSTM algorithm makes it possible to quickly and accurately classify operators' FFD while protecting their PI.

The findings indicated the feasibility of using the proposed methodology to support worker FFD classification with the capability of simultaneously examining operators' sobriety, stress, and fatigue. For practical implementation, the methodology can serve the role of FFD screening without disclosing the subjects' identity. If necessary, the methodology can be supplemented with subject specific tests as a follow-up. In the case of stress and fatigue evaluations, subject-specific results can be collected and used for personalized health and mental assessment according to the existing protocol.

This study was based on the subjects' performing cognitive tasks mimicking the mental activities of nuclear operators in advanced NPPs. Although the subjects and the experiments do not represent the actual NPP workers and their professional tasks, the methodology may still prove utility in field applications. Future study should consider performing experiments by using various age group subjects with working knowledge in nuclear reactors and a full-scale nuclear simulator.

B. GUIDELINES

The six mandatory actions for secure PI handling required by the national and international communities are: (a) Establishment and enforcement of an inner management plan for secure PI handling, (b) Restriction of permission and control to access PI, (c) Application of encryption, or equivalent action, in order to save and transmit PI securely, (d) Keeping an access log to counteract a PI infringement accident and prevent forgery and falsification of PI, (e) Installation and updating of the security program for PI, and (f) Physical action such as placing the storage facility in a secure area or installing a lock for secure storage of PI. These requirements are similar to those of the European GDPR and the Korean E-KAPIP.

The ISMS can accomplish the six mandatory actions as discussed in the sections of the data capture subsystem, preprocessing subsystem, decision subsystem, data storage subsystem, and management subsystem. An organization level management plan is required for the implementation of the system (Item a). Permission and control to access PI are restricted and only authorized controllers are allowed the access to PI. A policy addressing permission and access control must define who has access and how they can access using the keys (Item b). To securely save and transmit PI, both the preprocessing and the decision subsystems must be encrypted (Item c). To cope with an unexpected security event, the ISMS should identify and keep a log of every system event such as access, modification, or data selection. This helps identify the data that were changed or leaked and the cause of the problem (Item d). Additionally, security programs such as pseudonymization, encryption algorithms, and encryption keys are updated periodically (Item e). Physical access control can be achieved by defining security zones where databases and EEG devices are physically located and by ensuring that access to these areas is restricted. To store encryption keys securely, a separate key management unit (e.g., separate storage) that includes a physically separated device or a device without any network connection can be used (Item f). Matching the regulatory requirements with the proposed design features suggests that the proposed ISMS is expected to meet the current privacy requirements.

C. ATTACK SCENARIOS

There are three potential scenarios by which the data can be attacked. The following section describes each of these scenarios.

First, there is a potential for PI and the FFD results to be disclosed while being transferred between the ISMS subsystem prior to the data storage subsystem. To prevent this situation, data should be encrypted and decrypted immediately after capture and before every transmission.

Second, the data storage subsystem can be made secure from data disclosure or forgery by not storing the EEG data in the ISMS. Thus, there is no link between an operator's identification and their PI, preventing it to be discerned from the EEG data.

Third, when the management subsystem is attacked, serious data disclosure is likely to occur. Strict enforcement of separate storage of the key along with strict access control should be designed against an attack as explained above.

Future studies are needed to address the bigger picture of organization level management in the implementation of the ISMS, which includes appropriate human resource management and security education. To achieve such a broad objective, it is necessary to implement ISO/IEC standard. This study assumed that the NPP network (intranet) was secure among subsystems. However, the vulnerabilities that can result from an insecure network should also be considered. In addition, relevant regulations to ensure key management security need to be developed.

VII. CONCLUSION

This study presents the development of an information security-enforced EEG-based classification system for evaluating an NPP operator's FFD. By applying the time domain analysis to multichannel EEG data, an operator's FFD could be classified with an accuracy of 88.1-96.4% (with cognitive training program based on LSTM algorithm).

This study also designed an ISMS to protect the PI and the FFD status for NPP operators whose FFD was determined using the proposed EEG-based classification system. The resulting system design considers the data collection, pseudonymization, encryption/decryption, and access control. Implementation of the information security measures in the proposed ISMS is expected to provide the necessary protection of the PI and the FFD databases without significantly impacting the overhead of FFD classification through near real-time analysis.

REFERENCES

[1] T. G. Ryan, "A task analysis-linked approach for integrating the human factor in reliability assessments of nuclear power plants," *Rel. Eng. Syst. Saf.*, vol. 22, nos. 1–4, pp. 219–234, Jan. 1988.

[2] J. C. Joe, J. O'Hara, J. V. Hugo, and J. H. Oxstrand, "Function allocation for humans and automation in the context of team dynamics," *Procedia Manuf.*, vol. 3, pp. 1225–1232, 2015.

[3] C. Moore, V. Barnes, and J. Hauth, *Fitness for Duty in the Nuclear Power Industry: A Review of Technical Issues*. Rockville, MD, USA: Nuclear Regulatory Commission, 1989.

[4] J. C. Higgins, J. M. O'Hara, P. M. Lewis, J. Persensky, and J. Bongarra, "Development of a risk screening method for credited operator actions," in *Proc. IEEE 7th Conf. Hum. Factors Power Plants*, Sep. 2002, pp. 7–8.

[5] A. Arsalan, M. Majid, A. R. Butt, and S. M. Anwar, "Classification of perceived mental stress using a commercially available EEG headband," *IEEE J. Biomed. Health Informat.*, vol. 23, no. 6, pp. 2257–2264, Nov. 2019.

[6] R. Foong, K. K. Ang, C. Quek, C. Guan, K. S. Phua, C. W. K. Kuah, V. A. Deshmukh, L. H. L. Yam, D. K. Rajeswaran, N. Tang, E. Chew, and K. S. G. Chua, "Assessment of the efficacy of EEG-based MI-BCI with visual feedback and EEG correlates of mental fatigue for upper-limb stroke rehabilitation," *IEEE Trans. Biomed. Eng.*, vol. 67, no. 3, pp. 786–795, Mar. 2020.

[7] R. Wang, Y. Zhang, and L. Zhang, "An adaptive neural network approach for operator functional state prediction using psychophysiological data," *Integr. Comput.-Aided Eng.*, vol. 23, no. 1, pp. 81–97, Dec. 2015.

[8] R. Wang, J. Zhang, Y. Zhang, and X. Wang, "Assessment of human operator functional state using a novel differential evolution optimization based adaptive fuzzy model," *Biomed. Signal Process. Control*, vol. 7, no. 5, pp. 490–498, Sep. 2012.

[9] R. K. Gäler, Å. Çapraz, and E. Bilir, "A novel fuzzy logic-based image steganography method to ensure medical data security," *Comput. Biol. Med.*, vol. 67, pp. 172–183, Dec. 2015.

[10] N. A. Rashid, M. N. Taib, S. Lias, N. Sulaiman, Z. H. Murat, and R. S. S. A. Kadir, "Learners' learning style classification related to IQ and stress based on EEG," *Procedia-Social Behav. Sci.*, vol. 29, pp. 1061–1070, Oct. 2011.

[11] J. H. Kim, C. M. Kim, and M.-S. Yim, "An investigation of insider threat mitigation based on EEG signal classification," *Sensors*, vol. 20, no. 21, p. 6365, Nov. 2020.

[12] E. Al Alkeem, C. Y. Yeun, and M. J. Zemerly, "Security and privacy framework for ubiquitous healthcare IoT devices," in *Proc. 10th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2015, pp. 70–75.

[13] E.-H. Lee, "Review of the psychometric evidence of the perceived stress scale," *Asian Nursing Res.*, vol. 6, no. 4, pp. 121–127, Dec. 2012.

[14] J. H. Kim, C. M. Kim, E.-S. Jung, and M.-S. Yim, "Biosignal-based attention monitoring to support nuclear operator safety-relevant tasks," *Frontiers Comput. Neurosci.*, vol. 14, Dec. 2020, Art. no. 596531.

[15] A. Al-Thaqib, F. Al-Sultan, A. Al-Zahrani, F. Al-Kahtani, K. Al-Regaiey, M. Iqbal, and S. Bashir, "Brain training games enhance cognitive function in healthy subjects," *Med. Sci. Monitor Basic Res.*, vol. 24, pp. 63–69, Apr. 2018.

[16] C. M. Clark, L. Lawlor-Savage, and V. M. Goghari, "Working memory training in healthy young adults: Support for the null from a randomized comparison to active and passive control groups," *PLoS ONE*, vol. 12, no. 5, May 2017, Art. no. e0177707.

[17] A. Richards, S. S. Inslicht, T. J. Metzler, B. S. Mohlenhoff, M. N. Rao, A. O'Donovan, and T. C. Neylan, "Sleep and cognitive performance from teens to old age: More is not better," *Sleep*, vol. 40, no. 1, Jan. 2017.

[18] A. Delorme and S. Makeig, "EEGLAB: An open source toolbox for analysis of single-trial EEG dynamics including independent component analysis," *J. Neurosci. Methods*, vol. 134, no. 1, pp. 9–21, Mar. 2004.

[19] T. Mullen, "Cleanline EEGLAB plugin," NITRC, San Diego, CA, USA, Tech. Rep., 2012.

[20] J. A. Palmer, K. Kreutz-Delgado, and S. Makeig, "AMICA: An adaptive mixture of independent component analyzers with shared components," Swartz Center for Computational Neuroscience, Univ. California San Diego, San Diego, CA, USA, Tech. Rep., 2012.

[21] B. Hjorth, "EEG analysis based on time domain properties," *Electroencephalogr. Clin. Neurophysiol.*, vol. 29, no. 3, pp. 306–310, Sep. 1970.

[22] V. J. Lawhern, A. J. Solon, N. R. Waytowich, S. M. Gordon, C. P. Hung, and B. J. Lance, "EEGNet: A compact convolutional neural network for EEG-based brain–computer interfaces," *J. Neural Eng.*, vol. 15, no. 5, Oct. 2018, Art. no. 056013.

[23] S. Alhagry, A. Aly, and R. A., "Emotion recognition based on EEG using LSTM recurrent neural network," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 10, pp. 355–358, 2017.

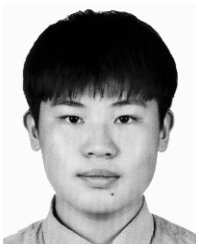
[24] *Information Technology—Security Techniques—Biometric Information Protection*, Standard ISO/IEC 24745, Geneva, Switzerland, 2011.

[25] E. A. Alkeem, D. Shehada, C. Y. Yeun, M. J. Zemerly, and J. Hu, "New secure healthcare system using cloud of things," *Cluster Comput.*, vol. 20, no. 3, pp. 2211–2229, Sep. 2017.

[26] C. Y. Yeun, K. Han, D. L. Vo, and K. Kim, "Secure authenticated group key agreement protocol in the MANET environment," *Inf. Secur. Tech. Rep.*, vol. 13, no. 3, pp. 158–164, Aug. 2008.

[27] B. Tao and H. Wu, "Improving the biclique cryptanalysis of AES," in *Proc. Australas. Conf. Inf. Secur. Privacy*, vol. 9144, pp. 39–56, Jun. 2015.

JUNG HWAN KIM received the B.S., M.S., and Ph.D. degrees in nuclear and quantum engineering from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Republic of Korea, in 2015, 2017, and 2021, respectively. He is currently a Postdoctoral Researcher with the Korea Atomic Energy Research Institute (KAERI). His current research interests include machine learning, biosignals, nuclear safety, nuclear security, probabilistic safety assessment, information security, and human factors engineering in nuclear power plants.



YOUNGGEOL CHO received the B.S. degree in computer science from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Republic of Korea, in 2019. He is currently a Research Officer with the Agency for Defense Development (ADD). His current research interests include machine learning, cyber-physical systems, and human–computer interaction.

YOUNG-A SUH received the B.S. and M.S. degrees in nuclear engineering from Seoul National University (SNU), Seoul, Republic of Korea, in 2010 and 2013, respectively, and the Ph.D. degree in nuclear and quantum engineering from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Republic of Korea, in 2018. She is currently a Senior Researcher with the Korea Institute of Nuclear Safety (KINS). Her current research interests include probabilistic safety assessment, decision-making tool, and human reliability analysis.

MAN-SUNG YIM received the B.S. and M.S. degrees in nuclear engineering from Seoul National University (SNU), Seoul, Republic of Korea, in 1981 and 1983, respectively, the Ph.D. degree in nuclear engineering from the University of Cincinnati, Cincinnati, OH, USA, in 1987, and the S.M. and Sc.D. degrees in environmental health science from Harvard University, Cambridge, MA, USA, in 1991 and 1994, respectively. He is currently the Associate Vice President of international office in Korea Advanced Institute of Science and Technology (KAIST), the Professor with the Department of Nuclear and Quantum Engineering, KAIST, and the Director of Nuclear Nonproliferation Education and Research Center (NEREC). His current research interests include nuclear fuel cycle, nuclear waste management, nuclear safety, and nuclear nonproliferation.