A Multi-Modal Neuro-Physiological Study of Malicious Insider Threats

Yessir Hashem, Hassan Takabi, Ram Dantu, Rodney Nielsen
Department of Computer Science and Engineering
University of North Texas
Denton, Texas
YassirHashem@my.unt.edu,{Takabi,Rodney.Nielsen,Ram.Dantu}@unt.edu

ABSTRACT

It has long been recognized that solutions to insider threat are mainly user-centric and several psychological and psychosocial models have been proposed. However, user behavior underlying these malicious acts is still not fully understood, motivating further investigation at the neuro-physiological level. In this work, we conduct a multi-modal study of how users' brain processes malicious and benign activities. In particular, we focus on using Electroencephalogram (EEG) signals that arise from the user's brain activities and eye tracking which can capture spontaneous responses that are unfiltered by the conscious mind. We conduct human study experiments to capture the Electroencephalogram (EEG) signals for a group of 25 participants while performing several computer-based activities in different scenarios. We analyze the EEG signals and the eye tracking data and extract features and evaluate our approach using several classifiers. The results show that our approach achieved an average accuracy of 99.77% in detecting the malicious insider using the EEG data of 256 channels (sensors) and average detection accuracy up to 95.64% using only five channels (sensors). The results show an average detection accuracy up to 83% using the eye movements and pupil behaviors data. In general, our results indicates that human Electroencephalogram (EEG) signals and eye tracking data can reveal valuable knowledge about user's malicious intent and can be used as an effective indicator in designing real-time insider threats monitoring and detection frameworks.

CCS CONCEPTS

• **Security and privacy → Intrusion detection systems**; *Biometrics*; • **Human-centered computing → Human computer interaction (HCI)**;

KEYWORDS

Electroencephalogram (EEG); Neuroscience; Eye tracking; Insider Threat

MIST'17, , October 30, 2017, Dallas, TX, USA.

ACM ISBN 978-1-4503-5177-5/17/10…$15.00
https://doi.org/10.1145/3139923.3139930

1 INTRODUCTION

The threat from malicious insiders is a complicated challenge for organizations and are considered the most damaging and costly threat [28]. The computer emergency response team CERT defines a malicious insider as a current or former employee who has or had authorized access to an organization's information systems and has intentionally used that access to influence the confidentiality, integrity, or availability of the organization's information systems [41]. A report produced by the security management company AlgoSec in 2013, found that the majority of the information security professionals view insider threat as their primary organizational risk [1]. In 2015, a federal cybersecurity survey of 200 federal IT managers showed that 76% of the participants are concerned about leaks from insider threats [42]. Furthermore, just last year a report from the Ponemon Institute studied cyber attacks cases for over 237 companies in six countries around the world found that insiders threat was the most expensive attack and cost companies an average of $167,890 annually and this cost is likely to increase in the future [28].

Insider threat problem has been extensively studied, and various detection approaches been proposed. These methods range from technical approaches such as process analysis, decoys, and honeypots, etc. to behavioral approaches based on psychological theories [15][16][19]. However, it still remains one of the most difficult security issues to combat.

It is recognized that solutions to insider threat are mainly user-centric and several psychological and psychosocial models have been proposed [15][45]. However, most of these approaches monitor the insider's voluntary activities on using the network or the organization's computer systems and resources, a skilled insider can always forge these activities and deceive the detection system. Some recent studies look at the psychophysiological metrics of the insiders and try to use them as threat indicators [2][17][18]. The neuro-physiological metrics such as electroencephalography (EEG), electrocardiogram (ECG), galvanic skin response (GSR), etc. are involuntarily generated, difficult if not impossible to mimic or change and can carry a wealth of knowledge about the user's physiological and mental states.

The human brain processes legitimate and malicious activities differently. So, by capturing these neural activities and user's brain state, we can develop methods to automatically separate malicious activities from benign behavior. The neuro-physiological methods can provide knowledge of user's brain state by accessing and recording neural activities. These neuro-physiological metrics are continuously available and can be measured automatically, so they can be used as a useful tool for studying malicious insider threats.

In this work, we pursue a comprehensive multi-modal study of how users' brain processes malicious and benign activities. In particular, we focus on using Electroencephalogram (EEG) signals that arise from the user's brain activities and eye tracking which can capture spontaneous responses that are unfiltered by the conscious mind. We perform experiments with 30 participants and capture their Electroencephalogram (EEG) signals and eye movements while they perform different tasks including both malicious and benign activities. Our goal is to access and record neural activities, and to retrieve and analyze information from brain state produced by neurocognitive processing.

Our Contributions: We report results of (to the best of our knowledge) the first study of users' neural response (EEG) and eye movement dynamics for insider threat detection. The main contributions of our work are as follows:

- We conduct a comprehensive multi-modal study of neurophysiological brain responses to determine a deeper underlying brain state and detect if a user is committing a malicious act.
- We utilize noninvasive neuro-physiological methods and tools including neuroimaging technique (EEG) and eye-tracking and gaze-tracking captured by an eye tracker.
- Our work advances and extends the understanding of neurocognitive processing with respect to malicious behavior. This can have significant effect on designing insider threat detection and mitigation approaches.

The rest of the paper is organized as follows. In section 2, we provide a brief background information about the Electroencephalogram (EEG) signal, the human eye and eye movements, and the related work. Section 3 describes our experimental design including the setup and tasks of the experiments. Section 4 presents our study procedure, and section 5 shows our data analysis. Section 6 presents the experimental results. And in section 7, we review the limitation and provide the discussion. Finally, section 8 discusses the future work and concludes the paper.

2 BACKGROUND INFORMATION

In this section, we briefly introduce the electroencephalography (EEG), EEG devices, the human visual system and eye tracking technologies to justify their applicability to the problem of insider threat detection and mitigation.

2.1 The Electroencephalography (EEG)

Electroencephalography (EEG) is a non-invasive method of measuring postsynaptic brain activity from the surface of the scalp. The human brain consists of billions of cells called neurons which use electricity to communicate with each other. The Electroencephalography (EEG) measures these electrical activities generated by the mass action of neurons within the cortex and midbrain structures using multiple electrodes placed on the scalp [27]. The electrical signals emanating from the brain are very small (of the order of microvolts). EEG records the continuous stream of activity that is always present in the brain. This activity can be characterized as patterns of oscillatory waveforms that have conventionally been subdivided in terms of their frequency into four main bands: delta (low frequency, 0.5-4 Hz; amplitude 20-200μV), theta (low frequency, 4-7 Hz; amplitude 20-100μV), alpha (dominant frequency, 8-13 Hz; amplitude 20-60μV) and beta (high frequency, 13-40 Hz; amplitude 2-20μV) [7].

The temporal resolution of EEG is superior to many other methods of brain imaging. While other methods may experience a delay on the order of seconds or minutes (e.g., fMRI - functional magnetic resonance imaging), EEG is able to depict changes within milliseconds. Because of its higher temporal resolution, EEG is often used to evaluate the time changes in brain activation across different brain regions and is also a good method for assessing cognitive states which are not visible to the observer's eye.

Electroencephalography (EEG) is commonly used in the medical domain for diagnosis of mental diseases, sleep disorders, and encephalopathy [31]. The traditional Electroencephalography (EEG) devices were expensive and difficult to use by people from outside the medical domain. However, EEG devices and technologies are growing rapidly and adoption of these devices is increasing. Although these devices were traditionally developed as communication tools, they have also been used for near real-time decoding of a person's neurocognitive state [49]. With the recent convergence of advances in consumer electronics, ubiquitous computing, and wearable sensor technologies, real-time monitoring of neurocognitive states can be studied in an objective, timely, and ecologically valid manner.

In recent years, several inexpensive consumer-grade EEG devices have been introduced by different companies such as NeuroSky [22] and Emotiv [20]. These devices are easy to use, offer different recording qualities and sampling rates, and allow increased flexibility and mobility over traditional devices. This opens the door for other domains such as the computer security domain to exploit the Electroencephalography (EEG) signals [6].

On the other hand, Electroencephalography (EEG) signals capture many aspects of the brain activities and physiological states of the user, many valuable features can be extracted from the frequency domain or the time domain of these signals and can reflect the conducts of unusual thoughts or behavior changes of the users. These benefits make it a suitable tool for detecting the malicious activities and identifying insider threats.

2.2 Human Eye and Eye Movements

In the human visual system, the eyes move to scan the visual scenes, the eyes' pupils control the light and pass it to the retina. The retina consists of light-sensitive cells located at the back of the eye that converts the light into electrochemical signals, the optical nerve transfer these signals to the visual cortex part of the brain. As a result of this process, human eyes frequently move to observe the objects. The current understanding of the human brain includes considerable knowledge about the connections between the retina and the brain regions which are responsible for generating eye movements. The eye movements can be categorized into two types: Saccades and Fixations. Saccades are rapid eye movements with duration range between 20ms to 100ms used to shift the line of vision from one position to another [5]. However, Fixations are slower eye movements compared to Saccades with duration around 100ms to over 500ms maintaining the visual gaze on a particular spot [40].

Eye tracking is the process of capturing a person's eye movements and measuring their positions. If the eye positions are calibrated with respect to an external display, then the process is called gaze tracking. The eye tracking can capture spontaneous responses that are unfiltered by the conscious mind.

The eye tracking devices can be categorized into two types: First, the eye-attached tracking technology which requires a direct contact with the eyes or the muscles around the eyes using a particular contact lens with a magnetic sensor to measure the eye movements. In other eye-attached technology, electrooculography (EOG) electrodes are placed around the eyes to measure the eye movements by recording the electrical signals recorded by these electrodes. Second, the optical eye tracking technology is non-invasive and does not require direct contact with the eyes. It can be built into glasses or other wearable devices or used as a video-based tracking device that has a unique camera with infrared light which tracks the eyes pupil's movements and size changes.

The first use of the eye tracking technology was in the medical domain. Nowadays, this technology has become more popular and widely employed in other fields such as advertising, gaming, etc. due to the advance in the video-based tracking devices. These devices can be implemented using a simple webcam or built-in laptop webcam with a simple software. A complete picture of the eye behavior can be obtained and used for various purposes. The computer security is one of these applications which has recently benefited from these technologies. Most of the previous work focuses on using eye movements for user authentication and identification [11][12][25].

2.3 Related Work

Designing efficient and scalable frameworks for monitoring and detecting the malicious insiders is a significant research interest nowadays. Many research studies have been investigating and analyzing the problem, and many approaches have been provided include implementing security awareness frameworks, segregation of duties and least privilege, anomaly detection and introduce decoys/honeypots to entrap insiders onto the network [37][33][46] [24]. For example, Thompson et al. present a content-based framework to detect insider anomalies in accessing documents and queries [33]. Salem et al. apply the machine learning techniques to identify the malicious intent in information gathering commands [37]. Kaghazgaran et al. proposed a model to consolidate honey permissions into role-based access control [24]. Also, Park et al. introduce a software-based decoy system to entrap malicious insiders [46]. Other approaches exploit the psychological behaviors of the insiders. For example, Greitzer et al. present a comprehensive view of psychological methods combined with a computational approach for detecting the insider [15]. Theoharidou et al. propose various criminology and related social science theories on the behaviors of insiders [45].

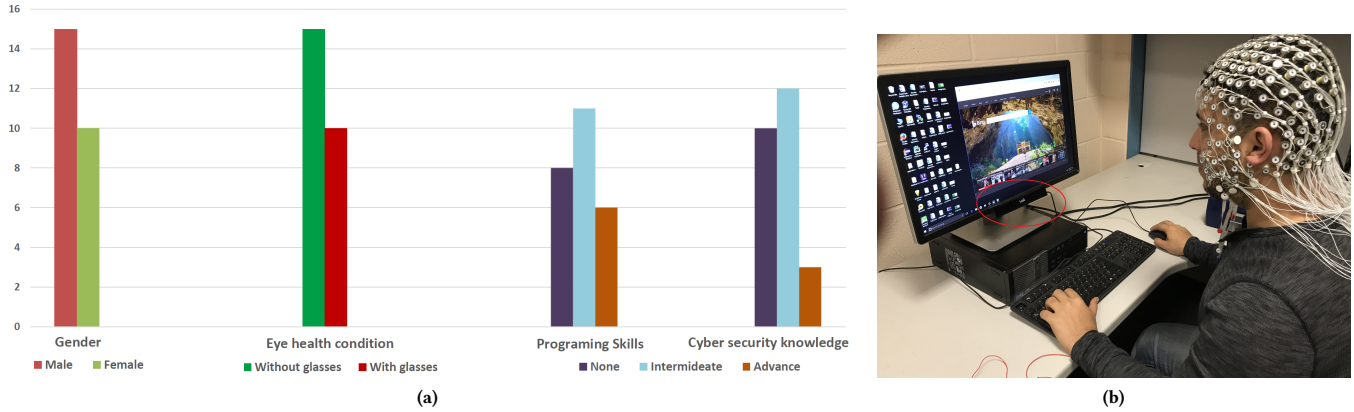
More recently, some studies start to investigate the possibility of using users' psychophysiological measures such as the Electrocardiogram (ECG), Electroencephalogram (EEG), Eye movements and pupil behaviors, voice, and skin conductivity in insider threat detection. Almehmadi et al. investigated the use of physiological signals as a measurement to detect insider threat where they monitor abnormal deviation rate of electrocardiogram (ECG), Galvanic Skin Response (GSR) and skin temperature [2]. On the eye movement dynamics field, Eberz et al. proposed an eye tracking biometric based approach to detect the malicious insider who temporarily gains physical access to a workstation of another employee or user [12]. Also, Neupane et al. conducted a three-dimensional study of phishing detection to detect the unintentional insiders based on Electroencephalogram (EEG) and eye gaze patterns [32].

On the other hand, the Electroencephalogram in computer science domain has been used mainly for emotion detection. For example, Wang et al. analyze the characteristics of EEG features to categorize the emotions and address the path of emotion changes with manifold learning [47]. However, very few researchers that focus on utilizing the Electroencephalogram (EEG) for the insider threat detection and mitigation. Recently, new study accomplished by Veritas company propose an insider threat monitoring system based on the electromagnetic signals (EEG) and functional near-infrared imaging (fNIRs) used to monitor both U.S. Army troops and contractors to detect any signs of disloyalty (malicious insiders) [39]. In our previous work, we have used user's psychophysiological signals to develop a real-time insider threat monitoring framework [17][18]. We used the Electroencephalogram (EEG) signals that arise from the user's brain activities, as well as the electrocardiogram (ECG) signals that arise from the user's heart activities to detect the malicious insiders.

In this paper, we extend our previous work by conducting a human study experiments include a larger number of participants and more complex activity tasks, and include the eye movement dynamics in our framework design. In addition, we are using more advanced recording device include 256 channels to cover the entire skull and record the electrocardiogram (ECG) signals from each part of the brain. We aim to deeply investigate the use of the EEG for the purpose of insider threat mitigation and detection. Also, we want to study each channel and identify which part of the brain can reflect the best knowledge and can provide better detection accuracy.

3 EXPERIMENTAL DESIGN

In this section, we first provide an overview of our design goals and then describe our experimental design to meet those goals. We describe our experiment environment including the Electroencephalography (EEG) recording device and the eye tracking device used in the experiments and procedures followed in the experiments. Our main goal in this experiment is to study malicious behavior using the electroencephalography (EEG) signals and eye movement dynamics. To do this, we record the electroencephalography (EEG) signals and eye movements for participants while they perform several activities, both benign and malicious. In general, there are two types of experiments that can be conducted for our purpose. The first is the controlled experiment where the participant reacts to visual stimuli displayed on the screen, and the device records his eye movements or brain reaction. In EEG studies, this is called event-related potential (ERP) experiments. The second type is the free experiment where there is no specific stimuli or event. In order to be as close as possible to the real-world insider threat scenarios we aim to address in this study, we choose the second type of experiment. We do not use any stimuli in the experiments, and instead



(a) (b)

Figure 1: (a) Participants information. (b) The experimental environment setup.

we focus on developing tasks that are close to real-world scenarios. Our study of malicious insider threats includes the following components:

Human subjects study: This research involves human subjects experiments to collect the Electroencephalogram (EEG) signals and the eye movements samples. We recruited a total of 30 participants to conduct the experiments. The experiment includes six distinct tasks that are a mix of regular computer-based activities such as data entry, browsing the Internet, using applications, etc. and malicious activities that are usually conducted by insiders such as unauthorized access to data, copying, modifying, or deleting the data, etc. Each task emulates a real-life scenario that is very similar to a typical work environment as described in section 3.3 and 3.4.

Data Acquisition: To record the participant's Electroencephalogram (EEG) signals during the experiment, we used Clinical Geodesic EEG System [21]. And for eye movements, we used a Tobii Pro X2-60 device [35].

Preprocessing the data: We filter and preprocess the EEG signals to remove any potential noise and artifacts that could be included in the recording.

Feature Extraction: We apply our feature extraction algorithms to analyze the EEG signals and the eye tracking data and obtain applicable features for malicious insider detection purpose.

Activity Classification: We use four different classification algorithms (Support Vector Machine (SVM) [10], k-nearest-neighbors (k-NN) [3], Random forests [9], Bagging predictors [8]) to evaluate our approach and detect the malicious activities.

3.1 Experiment Environment and Setup

The experiments were conducted in our lab room which was set up to keep the same environmental conditions for all tasks and all participants. We used a regular personal computer for conducting the experiments with Intel Core i5-4210U Processor, 6GB PC3 DDR3L SDRAM and Windows 10 Home operating system. For recording the EEG and eye tracking data, we used a Mac Pro computer with 3.7GHz Quad-Core Intel Xeon processor, 12GB DDR3 ECC memory and OS X El Capitan software.

To record the EEG signals, we use a medical grade device, Geodesic EEG System with the Geodesic Sensor Net (GSN) which include a total of 256 sensors (channels) that capture the EEG signals from all around the skull. Also, the device provides an excellent recording quality with a sampling rate of 1000 Hz [21]. The device has been widely used by the clinical and research community because of its ease of use, comfort, and ability to produce high-quality and high-resolution data.

To record the participant's eye movements during the experiment, we used a Tobii Pro X2-60 device, a screen-based eye tracker capturing gaze data at 60 Hz [35]. The device delivers accurate gaze position data within the entire experiment screen. Figure 1.b shows our experiments station setup include the eye tracking device and the Geodesic Sensor Net.

3.2 Experiment Procedure

The experiment was divided into six different tasks for a time period of 10 minutes per task. There were four benign activity tasks and two malicious activity tasks. In the following, we describe each of the six tasks in detail.

3.3 Benign Activities Scenarios

3.3.1 Task 1 : users perform benign daily activities. This task emulates the benign daily activities performed by most employees in any organization such as browsing the Internet, using computer applications or using an email account. In this task, the participating participant received through email an excel sheet containing names of students who participated in a previous survey and their associated information. The participant needed to use the browser to login to the database system and find out the students' names and update their missing data using the excel sheet. This task consisted of doing the following activities for a period of 10 minutes: 1) Login to their email account, find the email and download the excel sheet. 2) Open the browser and login to the database system using their own username and password (username and password are given to the participant before the experiment). 3) Browse through the files on the database system to find the students names and update their records. In this task, we did not require the participants to

finish all the students' record, and there was no pressure or stress introduced during the task.

3.3.2 Task 2: users perform benign daily activities under stress. In this task, we repeat the previous task with some changes to introduce stress to the participants in order to emulate the scenario where employees work under pressure or emotional stress. The reason behind this experiment is to differentiate between the regular work pressure, fatigue or stress and the malicious intent of the users. To do this, we conducted the experiment at the end of the working day, so the participants came to the lab after attending classes, exams or labs during the day causing them to have more mental workload compared to Task 1. The participants were also given twice the number of the records compared to the first task and asked to make sure to finish all the records during the 10 minutes experiment. In addition, we removed some of the students' names from the database to add more pressure as the participants were not able to find those names. The participants were told that there will be a special prize for the participant who finished his/ her report faster than the others adding more stress and time pressure to the experiment.

3.3.3 Task 3: users perform high mental workload activities. This task emulates the professional job activities when the employees perform some activity involving high mental interaction. We try to show that our approach covered all the possible activities. The participants were asked to complete a short coding project (Designing a calculator) which requires more mental workload compared to the benign daily activities in Task 1. The participants were allowed to choose any programming language they felt comfortable with (C++, Java, Python). They were also allowed to browse the Internet for help if needed. However, the participants were told that copying the code from the Internet was not allowed and they had to write their own code. This task consisted of doing the following activities for a period of 10 minutes: 1) Use the integrated development environment (IDE) for their choice of language to write the code. 2) Browse the Internet for extra help if needed. 3) Write the code and test the results. 4) Export the code and send by email to the examiner. The participants were encouraged to finish the code project. However, the task did not require them to complete the project and there was no pressure or stress introduced to the experiment.

3.3.4 Task 4: users perform high mental workload activities under stress. In this task, we repeated the previous task with some changes to introduce stress to the participants in order to emulate situations where employees work under pressure or emotional stress. To do this, we conducted the experiment at the end of the working day, so the participants came to the lab after attending classes, exams or labs during the day causing them to have more mental workload compared to Task 3. The participants were asked to repeat the same project but with another programing language. Participants were still able to browse the Internet for help. However, the participants had to complete the code and test it in 10 minutes. The participants were told that there will be a special prize for the participant who completed his/ her code faster than the others.

3.4 Malicious Activities Scenarios

3.4.1 Task 5: users perform remote access attack. This task emulates the malicious activities that could be performed by an insider. We used the remote access scenario where an insider accesses to another computer in the network which he is not authorized to access. The insider can steal the credential information using shoulder surfing and use it to login to the victim's device. So, in this task the participants were asked to remotely access the teaching assistant's computer and steal data related to the exams, quizzes, projects etc.

Participants were instructed to perform this task without the TA noticing and to incentivize them, they were told that they would receive extra reward if they could complete these tasks without leaving any trace. This task consisted of doing the following activities for a period of 10 minutes:1) Login to the teaching assistant's computer remotely. 2) Search for data related to the exams, quizzes, projects, grades, etc. 3) Type a report including the data they found on the teaching assistant's computer. 4) Close the files on the remote computer and exit without leaving any trace or making the account owner (teaching assistant in this case) notice the access. 5) Send the report by email to the examiner. For this task, we added a timer on the computer desktop showing the time remaining to complete the task.

3.4.2 Task 6: users perform SQL injections attack. In this task, we emulate the scenario of the script kiddie insider (an unskilled system user who uses codes or programs developed by others to attack computer systems and networks participants). More specifically, we used the scenario when an insider uses SQL injections to access to information he has no permission to access. In this task, the participants were asked to use SQL injection to bypass the authentication for the database system. Then update, delete and copy the student's information in the database. This task consisted of doing the following activities for a period of 10 minutes: 1) Use the browser to login to the database system. 2) Try to bypass the authentication system using the string SQL injection. 3) Access the database. 4) Change some information on the tables. 5) Delete some records. 6) Type a report containing the information modified or deleted. 7) Close the browser and clean any trace that might make the account owner notice the access. 8) Send the report by email to the examiner. The participants were told that successfully completing this task without leaving any trace will result in an extra reward. We also added a timer on the computer screen showing the time remaining to to complete the task.

4 STUDY PROCEDURE

4.1 Ethical Considerations

The experiments were conducted with the approval of Institutional Review Board (IRB) from the University of North Texas, and the participants were compensated $30 for one hour of their time. The participation was voluntary, and the participants were given the option to withdraw from the experiment at any time. We followed the standard best practices to protect the participants' data (prescreening, task responses, EEG and eye tracking data) collected during the experiments.

4.2 Recruitment and Study Participants

To recruit our experiment participants, we used a paper advertisement (flyers) posted and distributed in the University of North Texas. We recruited a total of 30 participants, we use data of 25 participants in our approach evaluation; the record of five participants was incomplete, and we decide to remove it from our evaluation process. Out of 25 participants, 15 were male, and 10 were female. the entire group of participants were between the age of 18 and 34 years old and were a graduate or undergraduate students at the University of North Texas. We used the following guidelines in our recruiting process:

(1) Include participants with different levels of programming and cybersecurity knowledge. As insider skills range from script kiddie (an unskilled user who uses codes or programs developed by others) to highly skilled insider, our participants vary in the levels of programming and cybersecurity knowledge from novice to intermediate and advanced.
(2) Include participants with prescription eye glasses to emulate real-world scenarios for typical work environment where some employees may wear eye glasses (10 of our participants had eye glasses and we made sure they wear their glasses during the experiments).
(3) Have a fair distribution of participants w.r.t gender, race, and age.

Figure 1.a shows details information of our participants' group.

4.3 Data Collection

The participants were first given a pre-screening form. The form included questions about user's health, education level, programming skills, cybersecurity knowledge, etc. After filling the form, the participants were briefed on the objectives of the study and given a written informed consent form to read and sign. The consent form included a precise information about experiment procedure and participant's right to participation.

Once the consent form was obtained, the participants were seated in a comfortable chair. The examiner then explained the task and what the participant was supposed to do step by step using a task script document located on the computer desktop. The participants were given five minutes to read the script before each task and to feel comfortable with the test environment.

Participants performed three tasks per session for a total of two sessions. The sessions were conducted on two different days and at various times of the day. The main reason is to test participants to different situations w.r.t mental overload. The first session was conducted at the early morning hours while the participant is still fresh and the second session was conducted at the end of the day when the participant is probably tired as a result of being overloaded with many daily activities.

To ensure recording a quality data we perform the following:

- For eye movements data collection, the participant was sitting 2 feet away from the computer screen, and a calibration process was carried out before each task to ensure the device capture the eye movements data with the best accuracy.
- For EEG data collection, we measure the circumference of participants head and use the right size Geodesic Sensor Net (GSN) to ensure the accuracy of the sensors locations. We have three different sizes of the GSN: small (54-56cm), medium (56-58cm), and large (58-61cm). After applying the right GSN, we verify the link quality of each sensor using the device software (Net Station Software).

Furthermore, To prevent skin irritation and infection, the Geodesic Sensor Nets were rinsed with warm water and soaked with special disinfection solution every time were used by the participants.

5 DATA ANALYSIS

5.1 EEG Data

The Geodesic EEG System is integrated with a software package (Net Station software) for signal acquisition, review, and analysis purposes [21]. The device records the EEG signals from 256 channels (sensors) with a sampling rate of 1000 Hz. Each one second contains 1000 raw data samples from each channel (sensor) saved in EGI's Metafile Format (MFF) which used by a specific medical software.

The Net Station software can be used to convert the output files to more popular format such as EDF, TXT and MAT formats. The software also includes many built in signal processing tools such as filtering, artifact removal, baseline correction, feature extraction, etc. However, most of these tools are event-related potential (ERP) data processing tools. Our experiment design is different and doesn't include specific events, so we had to implement our own algorithms to process the signals and extract the features. In addition, the software includes very specific feature extraction tools which are mostly used in the medical domain and doesn't provide flexibility in modifying these algorithms. For these reasons, we used the software for only filtering, removing the artifacts and converting the output files to TXT format. Then, we developed our own algorithms in Matlab to process the EEG signals and extract the features as described in section 5.4.

5.2 Eye Tracking Data

For eye tracking, we used a Tobii Pro X2-60 device which comes with Tobii Studio software that provides analysis and visualization of the recorded data [35]. Tobii Pro Studio used for stimuli presentation, recording, and analysis. However, it is mainly used for controlled experiments (stimulus based experiments) which record the eye movements while visual stimuli are presented to the participants. As our experiments are entirely free and participants can choose what to do for the duration of the task without involving any specific stimulus we couldn't use this software. However, we used the software to export the recorded raw data into a tab-separated value (TSV) file format, then we implemented our own algorithms to extract the eye movements and pupil features as described in section 5.5.

5.3 Preprocessing and Data Preparation

One of the essential steps in our data analysis is to preprocess and filter the acquired EEG signals. This step requires specific signal processing and filtering procedures. Electroencephalographic (EEG) signals, as we explained before, are low frequency signals ranging from 0.1 Hz to 60 Hz with very low signal intensity measured in microvolts (mV). Therefore, these signals will naturally include some noises that may corrupt their purity. There are two types of noises.

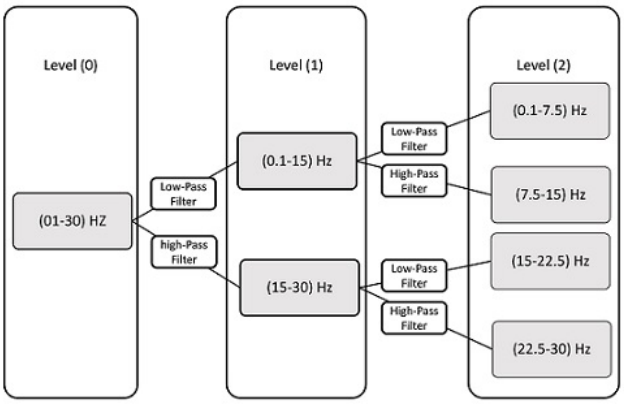


Figure 2: The wavelet packet decomposition(WPD) tree used to extract features from the EEG signals

First, the Electromyography (EMG) artifacts happen due to involuntary skeletal muscle movements around the EEG device electrodes. Second, the EOG (electrooculogram) artifacts are electrical noises generated as a result of eye blinking.

So, our first step is to remove these artifacts and remove any other noises that may influence our results. We used a low-pass filter to remove the higher frequency noises and high-pass filter to cutoff our lower frequency and select our frequency range from 0.1 Hz to 30 Hz, which include the EEG bands (Delta, Theta, Alpha, Beta).

5.4 EEG Data Feature Extraction

The features extraction component is a crucial part of our data analysis. In this part, we aim to extract useful information from the Electroencephalogram (EEG) data. As EEG is a signal and can be presented in time and frequency domains. A combination of frequency information features and time domain information features can be extracted from both domains and improve the classification performance of EEG signals [30]. There are many features extraction techniques that can be applied to the EEG signals. However, those extraction methods can obtain features from either the time or frequency domains. For example, Fast Fourier transform algorithm has been widely used in EEG signal processing and converts the signals from its original domain (time domain) to the frequency domain. However, this method only uses the frequency information and does not use the time domain information.

In other words, the wavelet transform algorithms have received substantial attention in the analysis of non-stationary signals (signal's statistical characteristics change with time) [26]. Wavelets are localized in both the time and frequency domains, and these characteristics of wavelets make it a useful tool for the purpose of feature extraction. In this work, we use wavelet packet decomposition (WPD) technique to extract our features set. In more details, the wavelet packet decomposes the originally recorded signals into a specific number of sub-bands using the wavelet function and generate a sub-band tree. Each level of the tree is composed by passing the previous approximation coefficients over high and low pass filters. Then, we take the energy of the wavelet coefficients for each sub-band.

Figure 2 shows our wavelet packet decomposition (WPD) feature extraction tree. We use ten seconds time frame (epoch) to extract our feature vector. Per each channel, we decompose the original signal to two levels using the high-pass and low-pass filters. The tree consists of seven nodes each one representing a specific EEG sub-band. We extract the energy feature of the wavelet coefficients for each sub-band from each channel and combine them in one feature vector.

5.5 Eye tracking data Feature Extraction

The eye tracking device captures the eye gaze locations on the screen (x,y) coordinates and produces a raw data at a sampling rate of 60 times per second including the saccade, fixation locations (x,y) and pupil diameter.

We analyze these raw samples to extract our features. We sample the eye tracking raw data into a ten second time frame (epoch), each time frame represents one feature vector. We extracted two types of features: the movements features which can be categorized as spatial features and temporal, and the pupil features.

We obtain a total of 38 movements features and 8 pupil features that include temporal features such as the saccade and fixation duration, the pairwise speed and acceleration. And spatial features such as the pairwise distance, the distance from the center of the screen, and the direction of saccades. We also consider the frequency of eye blinking and the saccades and fixations frequencies. For the pupil's data, we obtain the pupil diameter and apply statistic measures such as the minimal, maximal, mean, and standard deviation of the diameter.

We employ three feature selection algorithms to chose a group of best quality features. Features evaluation and selection techniques have been extensively studied in machine learning and considered an essential step to improve the classification process and achieve a good accuracy [48].

We use the *forward and backward greedy search algorithms,* which are hill-climbing heuristics algorithms designed to incrementally tune the feature set to improve the expected test set classification performance metric [23]. We also use the *information gain feature evaluation algorithm,* which has been widely used for features evaluation and selection by calculating the information gain for each feature with respect to the class [38].

$InfoGain(Class, feature) = H(Class) - H(Class \mid feature)$

Where H represents the entropy.

We employ each algorithm independently to our extracted feature set. Then, we obtain the results from each algorithm which represent the set of the best features, and combine the three sets into one final set of features as below:

Selected features = (Info Gain features) U (Forward Algorithm features) U (Backward Algorithm features).

By applying this method, we reduce our feature set from 46 to 17 features, and we ensure that we only include a high-quality feature in our approach.

5.6 Classification

To evaluate our approach, we use several classification algorithms. We only report the results for the following four classifiers as they provide the best performance among the other classifiers using our data set. Also, the SVM and k-nearest-neighbors classifiers have been used in previous EEG related work.

- Support Vector Machine (SVM) [10].
- K-nearest-neighbors (*K*-NN) [3].
- Random forests [9].
- Bagging predictors [8].

6 EXPERIMENTAL RESULTS

In this section, we describe our test setup and present the experimental results. We also discuss the performance fluctuation of each channel and each brain region and the differences in the classification accuracy while using a different number of channels. Furthermore, we will discuss in detail the training phase and the number of examples required to reach an acceptable detection accuracy. Then, we will examine how our framework can differentiate between the regular work pressure and stress and the malicious intent of the users. After completing the experiments for all participants, we organized the recorded signals and eye tracking data for each participant in two ways as the following:

- We label the feature vectors extracted from each participant by the task activity. The feature vectors extracted from the benign activities tasks (tasks 1, 2, 3, 4) have a label "0" (negative), and the feature vectors obtained from the malicious activity tasks (tasks 5, 6) have a label "1" (positive). This setup is used to evaluate our approach's capability in distinguishing the malicious activities from the benign activities.
- We only use four tasks in this setup by labeling the feature vectors extracted from the benign activities under stress (task 2, 4) as "0" (negative), and the feature vectors extracted from the malicious activities (tasks 5, 6) as "1" (positive). We only consider the malicious tasks and the benign tasks performed under stress to measure our approach's performance in differentiating between the malicious activities and the benign activities performed under stress.

We perform training and testing on the each participant's data. We split each participant's data into 70% tuning and training set, and 30% testing set by dividing the 10 minutes task time to seven minutes for training and three minutes for testing. In order to assure a good separation between the training and testing sets, we ignored 30 seconds time window between the training and testing time (last 15 seconds from the training minutes and the first 15 seconds from the testing minutes).

We use four measures to evaluate our approach, the classification accuracy (the percentage of correctly classified activities from all the activities), True Positives (the malicious activities are classified correctly), False Positives (the benign activities are misclassified as being malicious), and the F-measure (the geometric mean between the precision and recall of the classifiers' output).

Table 1: Average results of detecting malicious activities using 256 channels (six tasks).

Classifire	# participants	Accuracy	TP Rate	FP Rate	F-Measure
SVM	25	**99.77**	0.997	0.002	**0.998**
Random *F*	25	97.78	0.977	0.029	0.978
k-NN	25	97.93	0.979	0.027	0.979
Bagging	25	96.91	0.969	0.043	0.969

Table 2: Average results of detecting malicious activities using the eye tracking data (the sign * represents the participants who wore glasses during the experiments).

Classifier	# participants	Accuracy	TP Rate	FP Rate	F-Measure
SVM	25	79.23	0.79	0.36	0.79
Random *F*	25	**83.18**	0.83	0.25	**0.83**
k-NN	25	76.29	0.76	0.37	0.76
SVM	10*	76.20	0.76	0.37	0.75
Random *F*	10*	**78.54**	0.79	0.29	**0.78**
k-NN	10*	73.79	0.74	0.38	0.73
SVM	15	81.25	0.81	0.35	0.79
Random *F*	15	**86.27**	0.86	0.24	**0.86**
k-NN	15	77.95	0.78	0.37	0.76

6.1 Malicious Activities Detection

In this section, we show the performance of our approach in detecting malicious activities. We first run the classifiers on each participant's dataset individually using the entire seven minutes training data and calculate the average result for all the participants. We use the data on setup one, which contains data from all experiment tasks and evaluates the performance of the classifiers in detecting the malicious activities.

Table 1 presents the EEG data results of our four classifiers. As shown, all classifiers show a good average accuracy. However, the SVM classifiers outperformed the other three classifiers and achieved up to 99.77% average classification accuracy and 0.002 average false positive rate while the bagging classifiers show the lowest performance with an average classification accuracy of 96.91% and the highest false positive rate of 0.043.

Table 2 shows the result of our eye tracking data. As we can see, the average results over our entire group of participants (25 participants) indicate that the Random Forest classifier outperformed the other classifiers with an average classification accuracy of 83.18% and better average true positive rate, false positive rate, and F-measure.

However, the average results for the group of participants who were wearing glasses during the experiments show slightly lower detection accuracy of 78.54%. These results are expected as glasses can impact the recording quality and reflect the light. On the other hand, the average detection accuracy for participants who had healthy eyes and didn't wear eye glasses during the experiments is up to 86% when using the Random Forest classifier and average true positive rate of 0.86 and false positive rate of 0.24 while the average F-measure is 0.85.

Overall, the eye tracking data results show that Random Forest classifier provides the best detection accuracy for all cases.

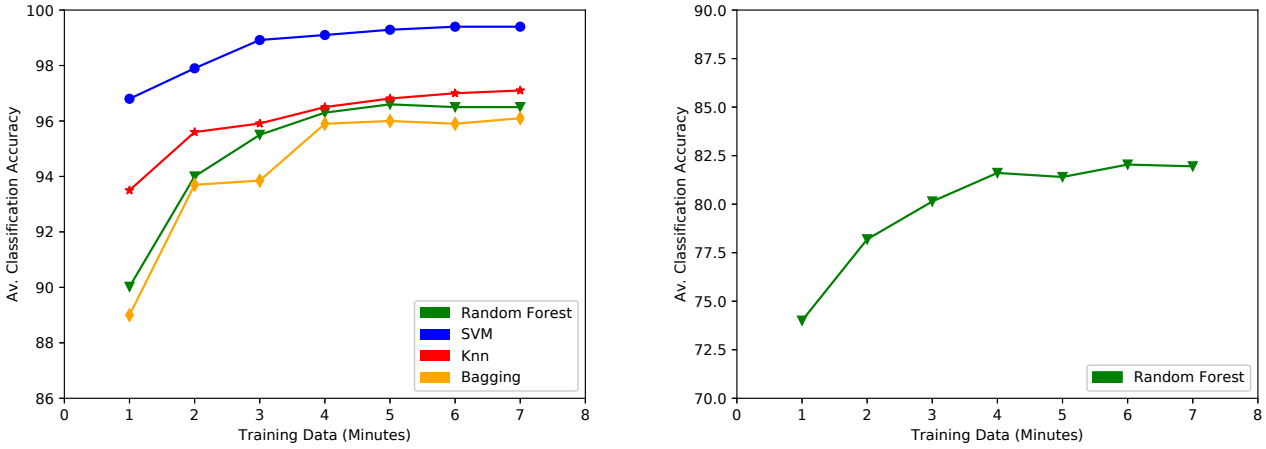


Figure 3: (a) Results of training with different amount of training data (EEG data). (b) Results of the eye tracking data for training the Random Forest classifier with different amount of training data .

Furthermore, the above results consider the training and testing performed on the same participant's data using seven minutes for training and three for testing. As the seven minutes can be a relatively long period of training time and may not be available in real-world settings, we investigate our classifiers' performance on training with less amount of time. We start by using only one minute of activities for training then we gradually increase the training data by one minute and record the performance of the classifiers. Figure 3.a shows our four classifiers average accuracy results using the EEG data for different amounts of training data. As shown, the average detection accuracy improved by increasing the training data (activities time). However, after minute five, the results are stable and show relatively similar performance among the four classifiers.

We repeat the same experiment using the eye tracking data. Figure 3.b shows the average accuracy results using the Random Forest classifier (best classifier) for different amounts of training data. The results indicate that, after we reach four minutes of training data, the detection accuracy remains the same. These results imply that we can decrease the amount of training time to five minutes in both the brain and eye tracking data and have relatively same classification performance.

6.2 Channels location and Brain regions

The brain is a complex and magnificent organ in the human body that contains around one hundred billion neurons to promote and control our perception and interaction with the world. Thoughts, feelings, behaviors, and plans are controlled by our brain. In neuroscience, the largest part of the brain is the cerebrum, which is associated with higher brain exercises such as thinking and actions [36][34]. The cerebrum consists of four regions (lobes) as shown in Figure 4: the frontal lobe, parietal lobe, occipital lobe, and temporal lobe [13][43][4]. Each lobe controls specific functions. For example, the frontal lobe constitutes two-thirds of the human brain and controls functions associated with problem solving, behavior, some emotion as well as the muscle movements and the physical reaction. The parietal lobe functions are associated with orientation, recognition, perception, and appreciation of form through

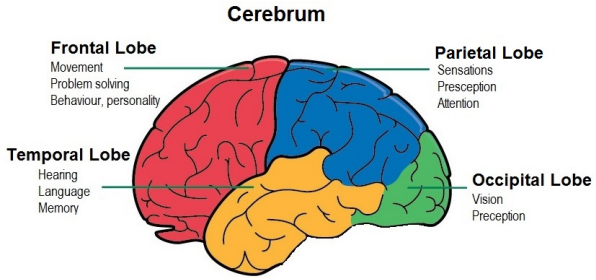


Figure 4: Human brain regions

Table 3: The top ten channels and their associated brain regions.

Channel No.	Accuracy	Brain Location
132	82.39	Frontal-Parietal Lobe
89	80.75	Parietal Lobe
185	80.51	Frontal-Parietal Lobe
81	80.48	Frontal-Parietal Lobe
79	79.67	Frontal-Parietal Lobe
17	79.62	Frontal-Parietal Lobe
198	79.38	Frontal Lobe
45	79.38	Frontal-Parietal Lobe
53	79.28	Frontal-Parietal Lobe
186	79.15	Frontal-Parietal Lobe

Table 4: The average detection accuracy for each region of the brain.

Brain Location	Average of Accuracy
Frontal-Parietal Lobe	76.31
Parietal Lobe	75.95
Frontal Lobe	75.58
Occipital Lobe	75.36
Temporal Lobe	74.57

Table 5: Average results for detecting malicious activities use different small groups of channels (EEG data)

Classifire	# Channels	Accuracy	TP Rate	FP Rate	F-Measure
SVM	1	79.58	0.796	0.370	0.760
Random F	1	82.39	0.824	0.236	0.823
k-NN	1	80.53	0.805	0.240	0.808
Bagging	1	83.11	0.831	0.244	0.826
SVM	2	85.88	0.858	0.194	0.848
Random F	2	89.31	0.893	0.136	0.893
k-NN	2	87.57	0.876	0.162	0.876
Bagging	2	88.89	0.889	0.140	0.889
SVM	3	87.77	0.878	0.174	0.871
Random F	3	92.12	0.921	0.100	0.921
k-NN	3	90.82	0.908	0.124	0.908
Bagging	3	90.51	0.905	0.118	0.906
SVM	4	89.99	0.900	0.138	0.899
Random F	4	93.51	0.935	0.086	0.935
k-NN	4	91.91	0.919	0.108	0.920
Bagging	4	91.58	0.916	0.103	0.917
SVM	5	92.49	0.925	0.0899	0.925
Random F	5	95.64	0.956	0.060	0.956
k-NN	5	94.85	0.948	0.0721	0.949
Bagging	5	93.31	0.933	0.084	0.933

touch (stereognosis). The occipital lobe is responsible for vision and reading functions, and the temporal lobe correlates with visual memories, speech and language, and some perception and recognition functions.

As insider attack involve different behaviors and activities associated with the insider's brain, we deeply investigate our results and identify if there is a correlation between the detection accuracy we have achieved and the brain regions. We first investigate each channel's location to find out which area of the brain the best channels belong. Then, we calculate the average accuracy for each region using the results from each channel in that area. To do that, we labeled our 256 channels to five brain regions based on the sensor's location on the skull. Frontal, parietal, temporal, and occipital lobe regions and we add to that the center region which is shared between the frontal and parietal lobes and we call it "Frontal-Parietal Lobe" region.

We run our classifiers using the data of each channel separately for the entire participant's group and sort the average detection accuracy from each channel. Table 3 presents our top ten channels, which show the best average detection accuracy. The first column shows the channels number based on the Geodesic Sensor Net (GSN) used on our recording. As shown, we can reach up to 82% average accuracy using only one channel (single sensor). However, all the ten best channels are located on the frontal and parietal lobes, as both lobes are associated with functionality that can be correlated to the insider practices and behavior, such as the fluctuation of the behaviors, emotional state, and attention.

To identify which region of the brain arise Electroencephalogram (EEG) signal that more effectively reflect the status of the insider mindset than the other regions, we calculate the average detection accuracy for each region using the accuracy of each channel located in that region. Table 4 shows the average accuracy result for all the participants by brain regions. We run the classifiers for each channel data; then we calculate the average for the group of channels in that particular region. As shown, the "Frontal-Parietal Lobe" region shows the best result followed by the "parietal lobe" and "frontal lobe" regions.

Furthermore, on the above results, we investigate each channel and each region performance in detecting the malicious insider. However, the accuracy when using a single channel was much lower when we use the entire group of channels (256 channels), and as using 256 channels in real life scenarios seems unrealistic, it's better to find the right trade-off between the detection accuracy and the applicability of the approach. To find the small group of channels that can provide decent detection accuracy, we adopt the best performance channels and generate a combination of a small number of channels to improve the detection accuracy. We start with using one channel (best channel) then combine the channel with other channels and measure the performance. We use four groups of channels: two channels group, three channels group, four channels group and five channels group. Table 5 presents the average results using the different groups of channels start with one channel to five channels group. As we can see, the average accuracy improves by increasing the number of channels four all the classifiers. By using a group of five channels only, we can reach an average detection accuracy of 95.64% using the random forest classifier. These results indicate that we can reduce the number of channels to five channels and still gain an excellent detection accuracy.

6.3 Distinguishing Malicious Activities from Benign Activities Performed Under Stress

One may argue that changes in neural activity might be due to emotional stress. To address this issue, we examine the capability of our approach in distinguishing between benign activities that are performed by users under emotional stress or high mental workload and the malicious activities of an insider. To do that, we use the second setup which contains four tasks. Task 2 and Task 4 (section 3.3) are benign activities performed under stressful conditions and tasks 5 and 6 which are the insider threat attack tasks.

We evaluate the performance of our classifiers using the data with this setup. We chose to use the feature vectors extracted from 5 channels as using the entire group of channels will always show relatively better results, so we want to make it slightly difficult for the classifiers by using less number of channels.

Table 6 presents the results of each classifier. As shown, the four classifiers are able to distinguish between the malicious activities and the benign stressful with about 90% average detection accuracy.

Table 6: Average results for detecting malicious activities from benign activities performed under stress (brain data)

Classifire	# Channels	Accuracy	TP Rate	FP Rate	F-Measure
SVM	5	89.53	0.895	0.102	0.894
Random *F*	5	**91.92**	0.919	0.081	**0.919**
k-NN	5	90.71	0.907	0.097	0.906
Bagging	5	90.03	0.900	0.104	0.900

Table 7: Average results for detecting malicious activities from activities performed under stress (eye tracking data)

Classifire	# participants	Accuracy	TP Rate	FP Rate	F-Measure
SVM	25	72.35	0.72	0.29	0.71
Random *F*	25	**78.39**	0.78	0.23	**0.78**
k-NN	25	69.38	0.69	0.32	0.69
SVM	10*	67.74	0.68	0.32	0.67
Random *F*	10*	**73.65**	0.74	0.26	**0.74**
k-NN	10*	67.46	0.67	0.32	0.67
SVM	15	75.42	0.75	0.27	0.74
Random *F*	15	**81.55**	0.82	0.21	**0.81**
k-NN	15	70.66	0.71	0.32	0.70

However, the random forest classifiers show the best result with 91.92% average detection accuracy and 0.081 false positive rate.

We repeat the same experiment with the eye tracking data. Table 7 lists the results of our classifiers. As illustrated, the best average detection accuracy using the entire participants' data (25 participants) is achieved using the Random Forest classifier and show up to 78.39% average detection accuracy. The accuracy increased by using the data of participants with healthy eyes (15 participants) and reach up to 81.55% using the Random Forest classifier. However, participants who were wearing eye glasses introduced the lower average detection accuracy of 73.65% for the reason we explained before.

These results clearly show that our study does not simply target the stress or emotional symptoms but can differentiate between the malicious activities and benign activities even when they involving emotion or stress.

7 DISCUSSION AND LIMITATIONS

The goal of our work is to propose a new insider threat detection approach based on the neuro-physiological perspectives of the user. We specifically focused on the neuro-physiological brain responses and the eye movements and pupil behaviors of the insiders. As these neuro-physiological measures generated involuntarily and can't change or mimic, it can provide a substantial assist in detecting the malicious insiders. Current approaches depend on user behaviors and practices can always be fabricated by well-skilled insiders. Our work lays out the necessary foundation to establish a new generation of insider threat detection mechanisms that doesn't depend only on a machine (technical detection approaches) or a user voluntarily behavior, instead it can go deep on the neuro-physiological aspect of the user, and learn from the real-time neural and eye movements data whether a user is acting maliciously.

Our results indicate that both the Electroencephalogram (EEG) signals and the eye movements and pupil behaviors carry out a good resolution on detecting the malicious activities. However, our approach can easily be combined with other technical and non-technical insider threat detection methods and frameworks and increase their accuracy and performance. Computer-based behaviors when a user interacts with computer peripherals (e.g., mouse; keyboard) also can be integrated with our approach as they are correlated with the neural response and can change in patterns based on the insider brain neurocognitive processes.

A common drawback of our approach is the cost and the availability of the hardware setup. However, with the advances in the wearable and sensor technologies and many of off-the-shelf low-cost EEG devices and eye-tracking systems, this technical limitation can be addressed. Also, many new implementations of eye tracking systems have been proposed that does not require a complicated hardware and can achieve good accuracy close to the original systems[14][29][44].

As we conducted human research experiments to evaluate our approach, we were very cautious in choosing the participants in term of gender, age, education level, and the cybersecurity knowledge. We did our best to have diverse participants that can represent the real world workplace environment. However, it would be valuable to include participants with less education and computer skills.

On the other hand, our main challenge was the experiment scenarios, precisely the malicious scenarios. Emulating the real world insider threat scenario is a very complicated task as it is associated with the psychological and behavioral aspects of the users. We tried to simulate the real world workplace environment in our experimental environment and test the participants in conditions that are similar to the real world insider attack scenarios. It is unrealistic to incorporate all the insider attack scenarios due to the nature of lab environment and the time constraint. However, we chose two attacks that involve the network and the application level and mostly used by insiders in practice. It is possible that what we are actually discriminating between is the specific task the participant is performing, rather than whether that task is malicious. To address this issue with statistical significance, more data needs to be collected from more tasks and tested based on tasks not involved in the training.

8 CONCLUSION AND FUTURE WORK

The insider threats have become a growing challenge in the cybersecurity domain, and many studies have focused on mitigating such threats. In this work, we proposed a new insider threat detection and mitigation approach. We conducted human subject experiments with 25 participants and captured their EEG signals and eye movements while they performed several computer-based activities for both malicious and benign scenarios. We preprocessed, analyzed and extracted features from the data then evaluated our approach using four different classifiers. Our results show that our approach achieved an average accuracy of up to 99% in detecting the malicious insiders using the EEG data. We also achieved an average detection accuracy of up to 83% using the eye movements and pupil behavior data. Furthermore, we investigated the performance of our approach using a small group of EEG channels, and the results show an average detection accuracy up to 95% using

only five channels (sensors). We also inspected our approach's capability in differentiating between the malicious activities and benign activities performed under stress. The results show about 92% average detection accuracy using the EEG data and 78% using the eye tracking data.

For future work, we plan to integrate the computer-based behaviors when a user interacts with computer peripherals (e.g., mouse; keyboard) into our multi-modal framework to efficiently monitor and detect the insider threat activities and improves the detection accuracy.

REFERENCES

[1] AlgoSec. 2014. AlgoSec Survey: State of Network Security 2014. (2014). Retrieved August 22, 2017 from http://www.algosec.com.

[2] Abdulaziz Almehmadi and Khalil El-Khatib. 2014. On the possibility of insider threat detection using physiological signal monitoring. In *Proceedings of the 7th International Conference on Security of Information and Networks*. ACM, 223.

[3] Naomi S Altman. 1992. An introduction to kernel and nearest-neighbor nonparametric regression. *The American Statistician* 46, 3 (1992), 175–185.

[4] Claude J Bajada, Hamied A Haroon, Hojjatollah Azadbakht, Geoff JM Parker, Matthew A Lambon Ralph, and Lauren L Cloutman. 2016. The tract terminations in the temporal lobe: Their location and associated functions. *Cortex* (2016).

[5] Robert Baloh, Andrew Sills, Warren Kumley, and Vicente Honrubia. 1975. Quantitative measurement of saccade amplitude, duration, and velocity. *Neurology* 25, 11 (1975), 1065–1065.

[6] Benjamin Blankertz, Michael Tangermann, Carmen Vidaurre, Siamac Fazli, Claudia Sannelli, Stefan Haufe, Cecilia Maeder, Lenny Ramsey, Irene Sturm, Gabriel Curio, et al. 2010. The Berlin brain–computer interface: non-medical uses of BCI technology. *Frontiers in neuroscience* 4 (2010).

[7] Warrent T Blume. 1999. Atlas of pediatric electroencephalography. (1999).

[8] Leo Breiman. 1996. Bagging predictors. *Machine learning* 24, 2 (1996), 123–140.

[9] Leo Breiman. 2001. Random forests. *Machine learning* 45, 1 (2001), 5–32.

[10] Corinna Cortes and Vladimir Vapnik. 1995. Support-vector networks. *Machine learning* 20, 3 (1995), 273–297.

[11] Alexander De Luca, Martin Denzel, and Heinrich Hussmann. 2009. Look into my eyes!: Can you guess my password?. In *Proceedings of the 5th Symposium on Usable Privacy and Security*. ACM, 7.

[12] Simon Eberz, Kasper Bonne Rasmussen, Vincent Lenders, and Ivan Martinovic. 2015. Preventing Lunchtime Attacks: Fighting Insider Threats With Eye Movement Biometrics.. In *Proceedings 2015 Network and Distributed System Security Symposium (NDSS)*.

[13] Leonardo Fogassi, Pier Francesco Ferrari, Benno Gesierich, Stefano Rozzi, Fabian Chersi, and Giacomo Rizzolatti. 2005. Parietal lobe: from action organization to intention understanding. *Science* 308, 5722 (2005), 662–667.

[14] Jose Gómez-Poveda and Elena Gaudioso. 2016. Evaluation of temporal stability of eye tracking algorithms using webcams. *Expert Systems with Applications* 64 (2016), 69–83.

[15] Frank L Greitzer and Deborah A Frincke. 2010. Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation. In *Insider Threats in Cyber Security*. Springer, 85–113.

[16] Frank L Greitzer, Lars J Kangas, Christine F Noonan, Angela C Dalton, and Ryan E Hohimer. 2012. Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats. *System Science (HICSS), 2012 45th Hawaii International Conference on* (2012), 2392–2401.

[17] Yassir Hashem, Hassan Takabi, Mohammad GhasemiGol, and Ram Dantu. 2015. Towards Insider Threat Detection Using Psychophysiological Signals. In *Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats*. ACM, 71–74.

[18] Yassir Hashem, Hassan Takabi, Mohammad GhasemiGol, and Ram Dantu. 2016. Inside the Mind of the Insider: Towards Insider Threat Detection Using Psychophysiological Signals. *Journal of Internet Services and Information Security (JISIS)* 6, 1 (2016), 20–36.

[19] Jeffrey Hunker and Christian W Probst. 2011. Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques. *JoWUA* 2, 1 (2011), 4–27.

[20] Emotiv Inc. 2017. Emotive System. (2017). Retrieved August 22, 2017 from http://www.emotiv.com.

[21] Electrical Geodesics Inc. 2017. Clinical Geodesic EEG System 400. (2017). Retrieved August 22, 2017 from http://www.egi.com.

[22] NeuroSky Inc. 2017. NeuroSky System. (2017). Retrieved August 22, 2017 from http://www.neurosky.com.

[23] Anil Jain and Douglas Zongker. 1997. Feature selection: Evaluation, application, and small sample performance. *IEEE transactions on pattern analysis and machine intelligence* 19, 2 (1997), 153–158.

[24] Parisa Kaghazgaran and Hassan Takabi. 2015. Toward an Insider Threat Detection Framework Using Honey Permissions. *Journal of Internet Services and Information Security (JISIS)* 5, 3 (2015), 19–36.

[25] Oleg V Komogortsev and Ioannis Rigas. 2015. BioEye 2015: Competition on biometrics via eye movements. In *Biometrics Theory, Applications and Systems (BTAS), 2015 IEEE 7th International Conference on*. IEEE, 1–8.

[26] Zhancheng Li, Minfen Shen, and Patch Beadle. 2004. Classification of EEG signals under different brain functional states using RBF neural network. In *International Symposium on Neural Networks*. Springer, 356–361.

[27] Gregory A Light, Lisa E Williams, Falk Minow, Joyce Sprock, Anthony Rissling, Richard Sharp, Neal R Swerdlow, and David L Braff. 2010. Electroencephalography (EEG) and event-related potentials (ERPs) with human participants. *Current Protocols in Neuroscience* (2010), 6–25.

[28] Ponemon Institute LLC. 2016. Cost of Cyber Crime 2016: Reducing the Risk of Business Innovation. (2016). Retrieved August 22, 2017 from https://saas.hpe.com/en-us/marketing/cyber-crime-risk-to-business-innovation.

[29] Osama Mazhar, Taimoor Ali Shah, Muhammad Ahmed Khan, and Sameed Tehami. 2015. A real-time webcam based Eye Ball Tracking System using MATLAB. In *Design and Technology in Electronic Packaging (SIITME), 2015 IEEE 21st International Symposium for*. IEEE, 139–142.

[30] Brett D Mensh, Justin Werfel, and H Sebastian Seung. 2004. BCI competition 2003-data set Ia: combining gamma-band power with slow cortical potentials to improve single-trial classification of electroencephalographic signals. *IEEE Transactions on Biomedical Engineering* 51, 6 (2004), 1052–1056.

[31] National Institutes of Health National Library of Medicine. 2012. electroencephalogram (EEG). (2012). Retrieved August 22, 2017 from http://www.nlm.nih.gov/medlineplus/ency/article/003931.htm.

[32] Ajaya Neupane, Md Lutfor Rahman, Nitesh Saxena, and Leanne Hirshfield. 2015. A Multi-Modal Neuro-Physiological Study of Phishing Detection and Malware Warnings. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 479–491.

[33] Younghee Park and Salvatore J Stolfo. 2012. Software decoys for insider threat. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*. ACM, 93–94.

[34] Michael I Posner and Steven E Petersen. 1990. The attention system of the human brain. *Annual review of neuroscience* 13, 1 (1990), 25–42.

[35] Tobii pro group. 2017. Tobii Pro X2-60 eye tracker. (2017). Retrieved August 22, 2017 from http://www.tobiipro.com/product-listing/tobii-pro-x2-60/.

[36] Per E Roland, Pere E Roland, and Per E Roland. 1993. *Brain activation*. Wiley-Liss New York.

[37] M Ben Salem and Salvatore J Stolfo. 2009. Masquerade attack detection using a search-behavior modeling approach. *Columbia University, Computer Science Department, Technical Report CUCS-027-09* (2009).

[38] Steven L Salzberg. 1994. C4. 5: Programs for machine learning by j. ross quinlan. morgan kaufmann publishers, inc., 1993. *Machine Learning* 16, 3 (1994), 235–240.

[39] Veritas Scientific. 2013. handshakes test and technologies. (2013). Retrieved August 22, 2017 from http://veritas.blueleveragemedia.com/products/handshake/.

[40] Sara C Sereno and Keith Rayner. 2003. Measuring word recognition in reading: eye movements and event-related potentials. *Trends in cognitive sciences* 7, 11 (2003), 489–493.

[41] George Silowash, Dawn Cappelli, Andrew Moore, Randall Trzeciak, Timothy J Shimeall, and Lori Flynn. 2012. *Common sense guide to mitigating insider threats 4th edition*. Technical Report. DTIC Document.

[42] SolarWinds. 2015. SolarWinds Survey Investigates Insider Threats to Federal Cybersecurity. (2015). Retrieved August 22, 2017 from http://www.solarwinds.com/company/newsroom/press_releases/threats_to_federal_cybersecurity.aspx.

[43] Donald T Stuss and Robert T Knight. 2002. *Principles of frontal lobe function*. Oxford University Press.

[44] Kun Ha Suh, Yun-Jung Kim, Yoonkyoung Kim, Daejune Ko, and Eui Chul Lee. 2015. Monocular Eye Tracking System Using Webcam and Zoom Lens. In *Advanced Multimedia and Ubiquitous Engineering*. Springer, 135–141.

[45] Marianthi Theoharidou, Spyros Kokolakis, Maria Karyda, and Evangelos Kiountouzis. 2005. The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security* 24, 6 (2005), 472–484.

[46] Paul Thompson. 2004. Weak models for insider threat detection. *International Society for Optics and Photonics,Defense and Security* (2004), 40–48.

[47] Xiao-Wei Wang, Dan Nie, and Bao-Liang Lu. 2014. Emotional state classification from EEG data using machine learning approach. *Neurocomputing* 129 (2014), 94–106.

[48] Bing Xue, Mengjie Zhang, Will N Browne, and Xin Yao. 2016. A survey on evolutionary computation approaches to feature selection. *IEEE Transactions on Evolutionary Computation* 20, 4 (2016), 606–626.

[49] Thorsten O Zander and Christian Kothe. 2011. Towards passive brain–computer interfaces: applying brain–computer interface technology to human–machine systems in general. *Journal of neural engineering* 8, 2 (2011), 025005.