

Disease Detector: A Disease Inference Attack Using Brainwave Signals Associated with Body Postures

Anuradha Mandal

Independent Researcher

ORCID: 0000-0001-7331-0542

Nitesh Saxena

Texas A&M University, College Station

ORCID: 0000-0001-6083-104X

Abstract—Consumer-grade brain computer interface, i.e., EEG headsets are getting popular in our daily life activities. These devices are low-cost, light-weight in design and powerful enough to interact with a computing device effectively. In medical-grade use, EEG signal helps to detect different brain disease, e.g., sleep disorder, Epilepsy, Parkinson’s disease, Alzheimer’s disease. In consumer-grade use, EEG signal helps to communicate with the computing system in an error-free way. The high density brain imaging techniques and the easy integration features of EEG headsets introduce serious privacy attack to end-users. In this paper, we introduce Disease Detector, an eavesdropping attack which infers information about brain disease from EEG signal collected during daily life activities, such as stationary activities (e.g., desk work, idle sitting), light ambulatory activities (e.g., stairs up and down, walking), and intense ambulatory activities (e.g., jogging, running). In this attack, we utilize a low-cost and light-weight consumer-grade EEG headset to integrate with a smartphone/smartwatch/computer using Bluetooth connection and collect data passively without user intervention. We show that how an attacker can infer user’s private health conditions (i.e., Epilepsy) from uncontrolled EEG signal and use it for unknown malicious purposes (e.g., targeted advertisement, trigger disease symptoms with flashing strobe lights, high frequency sounds etc.). We evaluate the attack with spectral analysis and machine learning. Our machine learning results show accuracy of 82% on stationary activities, 94% on light ambulatory activities and 83% on intense ambulatory activities in identifying an epileptic patient from a healthy person.

Our work shows that, it is indeed feasible for an attacker to learn about serious health condition by analyzing EEG signal collected from a low-end EEG headset. We believe our work serves to raise awareness to a potentially hard-to address threat arising from consumer-grade EEG headset and provides insights to security researchers to consider robust security measurements to protect users’ private sensitive information (e.g., health condition).

Index Terms—Side-channel attacks, Security & privacy, Wearable Security

I. INTRODUCTION

Brain computer interface (BCI) is a computing system which collects brainwaves, and analyzes the brainwaves to generated input from thoughts to interacts with a computing device. In general, BCI establishes a direct pathway between brain’s electrical activity and a computing system [1]–[3] with help of electrodes attached to the scalp. In BCI, Electroencephalography (EEG) is a non-invasive method to record electrogram (EGM) of electrical activity of human brain with electrode/sensor attached to scalp. Due to high resolution imaging of EEG and easy use of dry electrodes, EEG has

gained popularity in gaming and entertainment industry. With EEG integration in 3D games, players can interact with the virtual reaty environment easily and can achieve more realistic feeling [4]. Moreover, EEG has been implemented as an implant to human-scalp by Neuralink recently [5]–[8]. Thus, people with this implant will carry the EEG sensor in their body all the time. While these implementations of EEG in daily life activities provide users more efficiency in decision making (implant EEG), more flexibility and realistic feeling in virtual gaming environment (wearable EEG), but it also brings serious privacy threats. The existing BCI in consumer-grade use is light-weight in design and user-friendly, which provides high resolution brain signals. It is easy to collect the EEG signals via Bluetooth without user intervention. Moreover, the system does not require additional permission when an app collects the data from user once the EEG device is paired with a designated computing device. Such easy integration and easy use makes the EEG signals available through out the computing device and applications being used on the device. Such deployment of BCI can bring unknown threats to the user.

Evidence of un-told information reveal from brain. Researches have found that neuro-muscular signals can be classified using advanced machine learning models, which can reveal untold words and predict sentences with higher accuracy [9], detect left/right handedness [10], [11]. While the research efforts in this area are going to help disabled people in functioning properly, but EEG being deployed in consumer-grade use opens the door of exposing un-told information to adversaries. There are some high resolution EEG headsets available in the market (e.g., Neurosky Mindwave Mobile [12], Emotive Eloc [13], NextMind [14]) for consumer-grade use, e.g., neuro-games, meditations training etc. These devices can communicate with the computing system silently and without asking for user-intervention while being used by an application installed in the computing device. Such user-friendly design of consumer-grade EEG headsets may leak private sensitive information, e.g., brain-disease or disability information to a malicious parties which could bring dangerous, even life threatening situation to the victim.

Implications of private-sensitive information exposure. There are evidence of cyber attack targeting people’s health condition, i.e., epilepsy syndrome, by showing flashing lights

or strobe lights to trigger epilepsy syndrome [15]. Strobe light at frequency range of 15-25 Hz in dance floor has been known for potential cause of giving seizures [16]. A news has stated the fact that using strobe light in dance festival has enough warning and requires preservative measurements before using it [17]. A recent cyber attack was introduced targeting the Epileptic Foundation on Twitter. On Twitter the hackers sent images of flashing strobe lights to the Epileptic Foundation's Twitter's page to launch several attacks [18]. Another news about a cyber attack stated that a GIF strobed violently across a journalist's computer screen with flashing a red, yellow and blue geometric pattern behind the words "You deserve a seizure for your posts." gave the journalist seizure [19]. Since EEG signals provide high resolution brain images as a form of epoch, it could be possible to identify some brain disease or physical disabilities from basic body movements with attacker's pre-trained machine learning model. If such information gets exposed to the attacker, then a targeted person with medical condition can get seriously ill or killed from cyber attack.

Analyzing exposed information capabilities. With the evidence of cyber attacks and the state-of-art consumer-grade EEG use, in this paper, we investigate a cyber threat associated with people's medical condition, which could be identified from EEG signals collected during daily life activities. By answering three key questions, we aim to contribute in better understanding the topic of how EEG use in daily life activities could expose private sensitive disease information and its implications: First, What is the capability of low-end EEG signal in carrying more information than the designated purpose? Second, Does current deployment of consumer-grade EEG headset connect and transmit data to the computing system with users' consent? Third, When would the more-than-needed information be dangerous and how it can cause serious harm to the end-users?

To answer these questions, we need to address several factors related to the currently deployed EEG technology in consumer-grade use. The EEG headset requires Bluetooth connection to get paired with the computing device and once it is connected, it transmits data continuously without asking permission from the user. Currently available EEG headsets have good data sampling rate to measure the brain activity according to the required task, i.e., Neurosky Mindwave Mobile has sampling rate of 512 Hz [12], Emotive Epoc has sampling rate of 256 Hz [13]. With the high density EEG data and the quality of the signal provide application developers to build various types of applications. These EEG devices provide the raw EEG signals along with their calculated EEG metrics, which contains original signal components of EEG. Thus, accurately inferring information from EEG signal collected from low-end devices could provide potential capability to an attacker to exploit it for personal gain. Some previous works in BCI attack showed that learning information from human-cognitive perspective is possible. Martinovic et al. [20] designed a side-channel attack to learn about bank information, home location.

Frank et al. [21] designed an attack to detect subliminal brain activity (detecting known face) which was performed in less than 13.3 milliseconds. In Peep, Neupane et al. detected typed each digit/character of PIN (4-digits), password (6-characters) by eavesdropping on victim's brainwaves while typing [22]. All these attacks provide evidence that an attacker could design a strong attack scenario to infer private sensitive information correctly from people's thought and later use it maliciously. In the light of the progressive brainwave technology, we leverage a novel approach to design an attack, which uses one channel EEG electrode's data from forehead area and utilizes some basic body movements to infer if the person/headset-wearer has a medical condition.

Our Contribution and Novelty Claim: To justify the security and privacy of currently deployed brainwave technology in daily life, in this paper, we introduce an attack, called *Disease Detector*, which can infer private sensitive medical condition from brainwave signals. In particular, it can identify an epileptic patient from a healthy person based on the neural fingerprint created during walking, standing, sitting etc. postures. Our key contributions are as follows,

- We design and develop an attack called, *Disease Detector*, which can infer disease information from brainwave signals collected during different postures made in day-to-day life activities and we study *Disease Detector* against a low-cost and light-weight consumer-grade EEG headset.
- We validate the *Disease Detector* attack using spectral analysis and machine learning from brainwave signals related to different types of daily life activities.

II. BACKGROUND & RELATED WORK

A. Background

Electroencephalography (EEG). Electroencephalography (EEG) is an electrophysiological monitoring method to record electrical activity of the brain using small electrodes placed on the scalp using. Typical EEG is noninvasive method using the electrodes placed along the scalp with or without sensor foam and synapse conductive electrode cream (depending on the EEG devices). There are invasive electrodes sometimes being used, as in electrocorticography, sometimes called intracranial EEG. For the brain activity measurements, EEG method measures the voltage fluctuations from ionic current within the neurons of the brain. At the beginning, the EEG signal investigated the potential fluctuations time locked to an event, such as "Pressing a button". The latter analysis could observe the neural oscillations or brainwave from EEG signal in frequency domain [23].

Brainwaves (Neural Oscillations). Neural oscillations or brainwaves are rhythmic or repetitive patterns of neural activity in the central nervous system. Neural tissue can generate oscillatory activity in many ways; driven either by mechanisms within individual neurons or by interactions between neurons. These signal properties can be extracted from neural recordings using time-frequency analysis. In large-scale oscillations,

amplitude changes are considered to result from changes in synchronization within a neural ensemble, also referred to as local synchronization [24]. Neural oscillations and synchronization have been linked to many cognitive functions, i.e., information transfer, perception, motor control and memory. The first discovered and best-known frequency band is alpha activity (8–12 Hz) [25] that can be detected from the occipital lobe during relaxed wakefulness and which increases when the eyes are closed [26]. Other frequency bands are: delta (1–4 Hz) [27], theta (4–8 Hz) [28], beta (13–30 Hz) [29], gamma (30–40 Hz) [30] frequency bands. We used these EEG frequency bands in spectral analysis to illustrate the differences in average band power in controlled group vs. healthy group and in machine learning feature engineering.

B. Related Work

Existing Attack Studies using Consumer-Grade EEG. Mandal et al. demonstrated in the paper that on how brainwave signals can leak private sensitive information without users' intervention [31]. In this work, different existing brainwave attacks and possible attack scenarios have been presented with reasonable accuracy which raises concern about unprotected BCI in consumer-grade use and research direction towards security of BCI technology. Martinovic et al. [20] designed a side-channel attack scenario to get users' private sensitive information. In this attack, they used different calibration phases, for example, they showed different banks' logos to infer bank information, asked participant to memorize a random 4-digit PIN to infer PIN code from brainwave etc. Later, during the attack scenario they showed different images of digits, credit cards logos associated with showed banks' logo during calibration phase, location highlighted map to infer home location of the participants. These attacks showed success rate of 30% location identification, 20% in PIN detection and 30% in bank information identification which all are better than random guessing. Frank et al. [21] designed an attack to detect subliminal brain activity which was performed for less than 13.3 milliseconds. In this attack scenario visual probing was tested and the classifier showed accuracy of 21% in identifying brain activity brain activity related to known face that the user subliminally recognizes, unknown face and a plain video sequence without any subliminal stimulation. Peep [22] was designed by Neupane et al. to detect typed PIN, password by passively eavesdropping on victim's neural signal. Four different attack scenarios were demonstrated in this paper: Virtual keyboard PIN, virtual ATM PIN, physical numeric keypad PIN entry and physical keyboard password entry using data types (4-digit pin vs. 6-character password) which showed accuracy of 43%, 33%, 46% and 35% respectively. Another work by Neupane et al. showed brain can leak age group and alcoholism by analyzing neural pattern [32].

Recognizing Brain Disease and Unstable Postures using EEG. In medical-grade use, EEG is being used to determine different brain diseases, i.e., sleep disorder, dementia, Parkinson's disease, Alzheimer's disease (AD), epilepsy. Dogun et

al. performed a study using EEG on 12 AD patients and 11 healthy people to detect Alzheimer's disease (AD) and developed an automated detection model using directed graph for local texture feature extraction. In that study, a weighted k-nearest neighbor (KNN) classifier was used for binary classification of controlled vs. healthy using both leave-one subject-out (LOSO) which obtained 92.01% [33]. Zu et al. used a deep recurrent neural network (RNN) on EEG signal collected from 20 patients with Parkinson's disease (PD) and 20 healthy people [34]. The proposed RNN architecture was equipped with LSTM units, which can automatically detect PD using EEG signals with a precision, sensitivity, and specificity of 88.31%, 84.84%, and 91.81%, respectively. Savadkoobi et al. studied brain's electrical activity from different brain-regions to detect the state of epileptic seizure. The data was collected from five healthy participants and five epileptic patients in seizures-free condition. The study used EEG signal to capture the electrical activity of brain and recorded signal from 100 EEG channels with sampling rate of 173.61 Hz. The features selection was done using time domain, frequency domain and time-frequency domain using Butterworth filter, Fourier Transform and Wavelet Transform respectively. The machine learning classification reached accuracy of 100% and 99.5% using SVM and KNN classifiers respectively, for detection of epileptic seizure group from healthy group [35]. Cortes et al. studied a VR sickness while the user is wearing 64-channel EEG headset, and a VR headset and walks in the virtual environment. In this experiment, the VR sickness was induced by gradually increasing the translation gain beyond the user's detection threshold. From the behavioral and cognitive measurements, the study showed significant difference in postural stability in between two groups [36]. The discussed literature in identifying brain disease using EEG proves that EEG signal has significant strength in identifying people's brain disease.

III. THREAT MODEL

In *Disease Detector* attack, attacker has access to the EEG signal from the headset and does not require any additional permission during data collection since the headset is paired with the computing system with Bluetooth. The ease and efficient design of consumer-grade EEG integration made the user experience smooth and reliable. The attacker takes advantage of this smooth system and eavesdrops on victim's brainwave signals silently.

In this attack scenario, the victim was wearing a comfortable EEG headset for meditation training or entertainment purpose (e.g., playing 3D games in virtual platform). The victim takes a break during the meditation training or from the game, and did not turn off the headset. The running headset transmit EEG data to victim's computing system. The victim may have browsed some web page to read some news or browsing social media for a quick check up, and a malicious java-script enabled web page with EEG scanning capabilities can collect victim's brainwaves, which can draw this attack.

Type of Attacker. The attacker could be a malicious application which was installed during the meditation training/gaming

break or a java-script enabled web page which has EEG scanning capabilities. Since, already paired EEG device does not require any additional permission to collect data from the victim's head, thus, the victim is unaware of the data collection/leakage by the unauthorized application or web page. The victim may have been walking or sitting or taking stairs to go somewhere while the malicious actor is collecting data silently. Since, the EEG headset used in this attack has 512 Hz sampling rate, thus, the attacker has 512 data points in each seconds which is very good density data to analyze and find something in few seconds.

Knowledge of Attacker. To run the attack, the attacker has capability to hack user's computing system secretly. The attacker is also capable of building java-script with EEG scan enabled. For EEG data analysis, the attacker has basic knowledge of analyzing EEG bands and metrics using basic statistical analysis and off the shelf machine learning. The attacker can extract features from raw EEG when the EEG device given bands and metrics are unavailable.

Intuition of Attacker. In this attack, the attacker's intuition is to learning victim's health condition based on the body posture, i.e., desk working, running, jogging, idle sitting etc. Using body postures, our attacker can learn if the person has any serious health condition, such as epilepsy. Such disease identification of victim, based on EEG recording related to different postures can lead to future serious attack, such as, attacker can target the victim with strobe light attack from web page or social media or applications, use health condition for selling products, create discomfort by increasing noise and unknown malicious ways.

Practicality of Attack. Neuro-based 3D games, meditation training using EEG headsets, real-life behavioral study, i.e., driving distraction detection using EEG headset, attention monitoring of students and workers etc. are main source of EEG use in practical life. Moreover, now brain-computer interface (BCI) has been successfully appeared as implant, i.e., Neuralink [6], [8], which will be always with human body. In Section II-A, we presented existing work on medical grade to use EEG signal to detect brain disease, unstable postures. With this background study and existing EEG deployment in daily life, could introduce serious attack as *Disease Detector*. Moreover, the EEG provides high density brain imaging data, which carries more-than-designated purpose information. With or without stimulus, the unauthorized access of EEG signal from low-end EEG headset can introduce serious security and privacy attack like *Disease Detector*.

IV. DESIGN OF DISEASE DETECTOR

In this section, we discuss about the design of the *Disease Detector*, features and analysis methodologies for the attack evaluation.

A. Attack Engine

According to the threat model described in Section III, the attacker has access to the raw EEG signal and no other media

or component during the attack time. The attacker has data of controlled and healthy groups of people doing different types of daily life activities, i.e., desk working, running, jogging, idle sitting etc. We start with the raw EEG signal to design an appropriate attack engine for our *Disease Detector* attack.

The attacker extract the EEG bands with approximate spectral boundaries described in Section II-A using band-pass filtering method in Matlab's signal processing toolbox. Each of the bands has different functional characteristics to identify a neural oscillation from brainwaves. Thus in this attach, we are considering all five EEG bands: Delta, Theta, Alpha, Beta and Gamma to generalize the analysis. After the EEG band filtering, the attacker try to distinguish the controlled group from healthy group using spectral analysis, i.e., frequency domain analysis. To achieve the goal, the attacker tries to differentiate the controlled group or the victim's health condition by comparing the EEG signal components with healthy people's EEG signal. The attacker does this spectral analysis on different category tasks performed by the victim in a day. Once, the spectral analysis shows some lights on distinguishing the signal pattern of the controlled group from healthy group of people, then the attacker start analyzing the EEG signal with machine leaning and correctly identify the controlled group from healthy people. For machine learning, the attacker extract features to train and test the machine learning model for classification. In the below section, we discuss more about the feature extraction techniques to be used in the attack evaluation and the details of machine learning models to classify the controlled group from healthy group.

B. Feature Engineering

We evaluate our *Disease Detector* using frequency domain analysis and machine learning. For machine learning evaluation, we need features to feed the models and to classify the designated classes. From the raw EEG signal, we extract different features of the signal to correctly identify the components of EEG signal and use them in the machine learning classification.

Band Power Calculation. We first extract the five EEG bands: Delta, Theta, Alpha, Beta and Gamma from the raw EEG signal. We apply band pass filtering to extract each EEG bands of different frequency described in Section II-A. Afterwards, by integrating periodogram power spectral density estimates of each EEG band signal over its frequency range, we calculated band power as frequency domain features [37]. Finally, we recorded average power of each EEG band of each session to use it as feature vector.

Discrete Wavelet Packet Transform (DWPT): Since EEG signals are time-varying, non-stationary signals containing different frequency elements at different times, time-frequency domain analysis is a more suitable method to characterize EEG signals due to capturing sufficient information on non-stationary signals, both in the time and frequency domain. In this work, discrete wavelet packet transform (DWPT) method was chosen to extract time-frequency domain features, which

provides optimal time-frequency resolution of EEG signals in all the EEG frequency bands by eliminating the requirement of signal as stationary [38]. Like Band Power Calculation, we considered both, raw signal and EEG bands given by EEG device in order to extract final features based on DWPT. We used the Daubechies family (db8) as the mother wavelet for the transform. The irregular shape and compact nature of db8 help in analyzing signals with discontinuities and sharp changes such as EEG signals. Instead of using all the coefficients at each decomposition level, we extracted the information from the wavelet coefficients only at the levels corresponding to frequency bands mentioned in Band Power Calculation. The means of absolute values of coefficients and average power of relevant levels were used as features. We have 10 features (delta coefficient mean, delta coefficient power, theta coefficient mean, theta coefficient power, alpha coefficient mean, alpha coefficient power, beta coefficient mean, beta coefficient power, gamma coefficient mean, gamma coefficient power etc.) for each session. Table I contains the list of all features (i.e., EEG band power and DWPT features) used in our machine learning models [38]. Figure IX represents the 7 level decomposition of EEG signal using discrete wavelet packet transform (DWPT).

TABLE I
BAND POWER AND DISCRETE WAVELET PACKET TRANSFORM BASED FEATURES

Band Power	Delta band power Theta band power Alpha band power Beta band power Gamma band power
DWPT Features	Delta coefficient (DWPT) mean Delta coefficient (DWPT) power Theta coefficient (DWPT) mean Theta coefficient (DWPT) power Alpha coefficient (DWPT) mean Alpha coefficient (DWPT) power Beta coefficient (DWPT) mean Beta coefficient (DWPT) power Gamma coefficient (DWPT) mean Gamma coefficient (DWPT) power

C. Methodology of Spectral Analysis

Frequency domain analysis is very important for signal processing and analysis to capture the patterns by distinguishing events or features in different repetition periods. The EEG data collected from the EEG headset is in time domain, which cannot capture all features of signal components required for frequency domain analysis. Power spectrum or power spectral density is one of the most popular feature extraction methods in frequency domain analysis, which represents the relative contribution of each individual frequency component to the total power of the signal [38]. Further, we extracted frequency domain features by calculating average band power of each signal across different EEG bands (delta, theta, alpha, beta and gamma) for different ambulatory activities, such as, stationary activities (desk work), light ambulatory activity (walking) and intense ambulatory activity (jogging). Further, we extracted frequency domain features by calculating average

band power of each signal across different EEG bands for different postures. The average band power was computed by integrating the periodogram power spectral density estimates across frequency ranges for each band [37].

Since, different types of body postures may create different results in between two groups, thus we have performed the spectral analysis on three different types of works to distinguish the control group from the healthy group. We also illustrate the difference found in spectral analysis of two different groups. The details of the spectral analysis in differentiating the controlled group (epileptic person) from the healthy group (healthy person) are in Section V-A.

D. Machine Learning Models

In the machine learning evaluation, we target different types of daily life activities to detect the disease information from the EEG signal. And we focus on the frontal left area of the brain, which is, in general, responsible for significant cognitive functionality. The dataset we used in the attack evaluation, is based on the Neurosky Mindwave EEG data, which has one EEG sensor attached to the FP1 position of the brain (according to 10-20 EEG sensor placement system). Since we are targeting different daily life activities to detect the disease. Thus, based on the body posture and intensity of the body movement, we name the activities with different identifiers, i.e., stationary activities, light ambulatory activities and intense ambulatory activities. We call desk work, idle sitting, laying, sitting as stationary activities, stairs up and down, walking as light ambulatory activities and, running, jogging as intense ambulatory activities. For better understanding and ease of discussion, we call machine learning models with stationary activities, light ambulatory activities and intense ambulatory activities as *stationary-model*, *light-ambulatory-model* and *intense-ambulatory-model* respectively. We discuss the details of machine learning models and their performances in Section V-B.

E. Dataset Description

For our *Disease Detector* attack, we used a public dataset consisting of brainwave signals collected by a portable EEG headset for different types of daily living activities. In this dataset, Neurosky Mindwave Mobile EEG headset was used in this attack. This device is low cost, portable, and easy to use. The headset's EEG electrode is placed on the sensor arm, resting on the forehead above the eye (FP1 position) (Figure X). The dataset consists of raw EEG signal (sampling rate: 512 Hz). The dataset has EEG raw signal recording of three different daily life activities of two groups of people: healthy people and epileptic patients. As daily life activities, stationary activities, light ambulatory activities and intense ambulatory activities were considered. To record EEG signal from stationary activities of healthy individuals, desk work, idle sitting, laying, sitting, standing, watching TV were considered and for epileptic patients, desk work, idle sitting, laying, sitting were considered as stationary activities. Next, cooking, stairs up and down, walking were considered as light ambulatory activities

of healthy individuals, while cooking was eliminated for epileptic patients. Lastly, intense ambulatory activities include: jogging, running, jumping for healthy individuals and: jogging, running for epileptic patients. Since couple of activities are not available for epileptic patients, thus for our attack validation, we considered common activities from each type of activities. For example, we considered desk work, idle sitting, laying, sitting as stationary activities for both healthy and epileptic people, while considered stairs up and down, walking as light ambulatory activities for both groups and similarly jogging, running as common activity for healthy and epileptic people [39].

V. ATTACK EVALUATION

A. Spectral Analysis

In this section, we discuss about spectral analysis on EEG bands extracted from the raw EEG signal collected by Neurosky EEG headset for different types of tasks of two different groups of people (i.e., healthy and epileptic groups).

Since, different types body postures may create different results in between two groups, thus we have performed the spectral analysis on three different types on works to test and distinguish the control group (epileptic) from healthy group. First, we calculated the average band power of five EEG bands (i.e., Delta, Theta, Alpha, Beta and Gamma) for different body postures or daily life activities, e.g., desk-work, sitting, laying, walking, stairs, walking, jogging and running, to check if there is any difference in average band power among activities of one randomly chosen healthy person and one randomly chosen epileptic person. The result of the average band power of different activities of two different people of two different groups is presented in Table II. From the result we can see that the average band power of all activities across all EEG bands for the healthy and epileptic person are different. Specially, the average band power of Delta EEG band of healthy and epileptic person is significantly different in activities: stairs (30.67 dB in healthy and 10.37 dB in epileptic person, laying (7.13 dB in healthy and -3.76 in epileptic person), walking (30.34 dB in healthy and 2.36 dB in epileptic person) and jogging (31.41 dB in healthy and 10.76 dB in epileptic person). Also, jogging (an intense activity) has similar difference in between two groups among all five EEG bands. The average band power of the healthy person in Delta EEG band is 31.41 dB, while the epileptic person's average Delta EEG band power is 10.76 dB. Similarly, the average band power of Theta is 7.05 dB for healthy and is -3.59 dB for epileptic person, the average band power of Alpha is 3.32 dB for healthy and is -7.31 dB for epileptic person, the average band power of Beta is 1.84 dB for healthy and is -6.04 dB for epileptic person and the average band power of Gamma is -10.98 dB for healthy and is -15.74 dB for epileptic person. All other activities have slight difference in between two groups, but from the results, it is clear that the jogging activity created the most differentiable results in identifying an epileptic person from a healthy person.

After observing interesting findings from the average band power calculation, we try to illustrate the power spectral

density of a randomly picked healthy person and a randomly picked epileptic person for three different types of activities, i.e., stationary activity, light ambulatory activity and intense ambulatory activity. From several activities in each categories, we select desk-work as stationary activity, walking as light ambulatory activity and jogging as intense ambulatory activity for illustrations. Since EEG band Delta and Theta are more effective in measuring unconscious and sleep conditions, thus for visualizing the active state of mind while performing some tasks in conscious state of brain, we choose Alpha, Beta and Gamma EEG bands. The Figure 1 illustrates the difference in power spectral density in between healthy and epileptic person. Similarly, Figure 2 and Figure 3 illustrate the difference of power spectral density (EEG bands: Alpha, Beta and Gamma) of a healthy person and an epileptic patient from light ambulatory activity, e.g., walking and intense ambulatory activity, e.g., jogging respectively. The illustrated Figures 1, 2 and 3, clearly shows the differences in spectral powers in EEG bands for each chosen activities in between two groups, i.e., healthy and epileptic. Across all illustration, the epileptic patient has more EEG band power/power spectral density than the healthy person. In the Figures (2 and 3) and in the Table II, it is clearly visible that the epileptic person's EEG bands have significantly more band power and power spectral density in walking and jogging than the healthy person. The Figure 1 shows that all three illustrated bands' power spectral densities are easily differentiable in between two groups of people for desk-work.

The spectral analysis we performed and presented in this section represents that an epileptic patient could be differentiate from spectral analysis of EEG signals collected during any types of body postures made in daily life activities. But the difference might be more identifiable from ambulatory activities, since the walking and jogging in power spectral density showed significant difference in band power (presented in Table II) and also showed clear difference in Figures 2 and 3.

B. Machine Learning Evaluation Metrics

To classify victim's health condition (e.g., epileptic patient) from brainwaves collected for body postures made in daily life activities, we applied traditional machine learning classifiers on the extracted features (Section IV-B). We used 10-fold cross-validation test to estimate and validate our classifiers and run classifiers on train-test (90% - 10%) dataset. We applied the classifiers on all three machine learning models, i.e., *stationary-model*, *light-ambulatory-model* and *intense-ambulatory-model*.

We calculated false positive (FP), false negative (FN), precision (Prec), recall (Rec), and F-measure (FM) to measure the performances of machine learning classifiers. TP denotes number of correctly classified classes, TN denotes the number of times instances belong to the control class is rejected, FP represents number of incorrectly classified instances and FN represents incorrectly identified wrong classes. Afterward, we calculated precision, recall and F-measure. Precision is the

TABLE II
 AVERAGE BAND POWER (dB) OF DIFFERENT EEG BANDS FOR DIFFERENT ACTIVITIES OF TWO RANDOM USERS (ONE HEALTHY PERSON (H) AND ONE EPILEPTIC PATIENT (E))

EEG Bands	Delta		Theta		Alpha		Beta		Gamma	
Activities	H	E	H	E	H	E	H	E	H	E
Desk-Work	-7.89	-6.47	-12.25	-18.34	-18.30	-21.64	-16.13	-21.55	-21.84	-27.52
Sitting	-7.26	9.64	-13.42	-18.52	-21.00	-22.63	-22.45	-20.83	-29.32	-26.75
Laying	7.13	-3.76	-18.69	-14.94	-22.72	-22.58	-23.77	-23.55	-28.98	-29.07
Stairs	30.67	10.37	-8.77	-4.55	-13.99	-11.24	-12.89	-12.55	-21.95	-20.75
Walking	30.34	2.36	-5.19	-15.97	-8.34	-20.49	-9.98	-18.57	-22.37	-23.79
Jogging	31.41	10.76	7.05	-3.59	3.32	-7.31	1.84	-6.04	-10.98	-15.74
Running	20.22	23.29	0.34	2.72	-0.48	2.14	-0.36	2.22	-12.73	-10.93

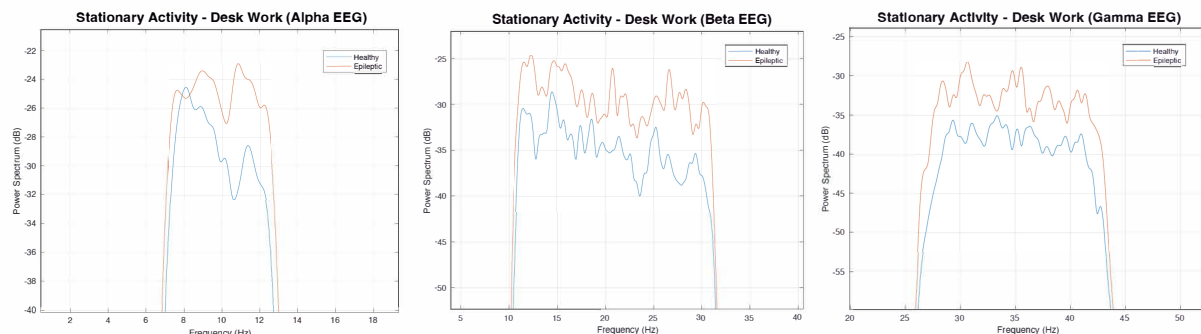


Fig. 1. Power Spectral Density of Stationary Activity (Desk Work) of Alpha EEG Band of Two Random Users (Healthy Person and Epileptic Patient)

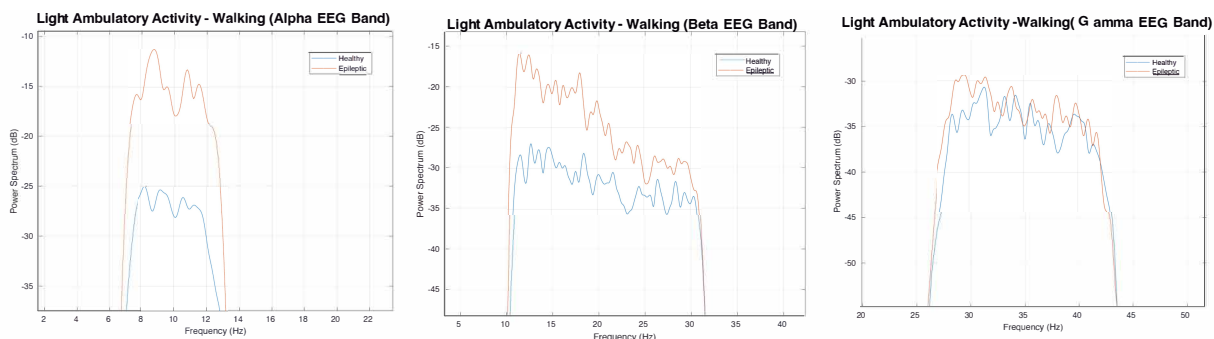


Fig. 2. Power Spectral Density of Light Ambulatory Activity (Walking) of Beta EEG Band of Two Random Users (Healthy Person and Epileptic Patient)

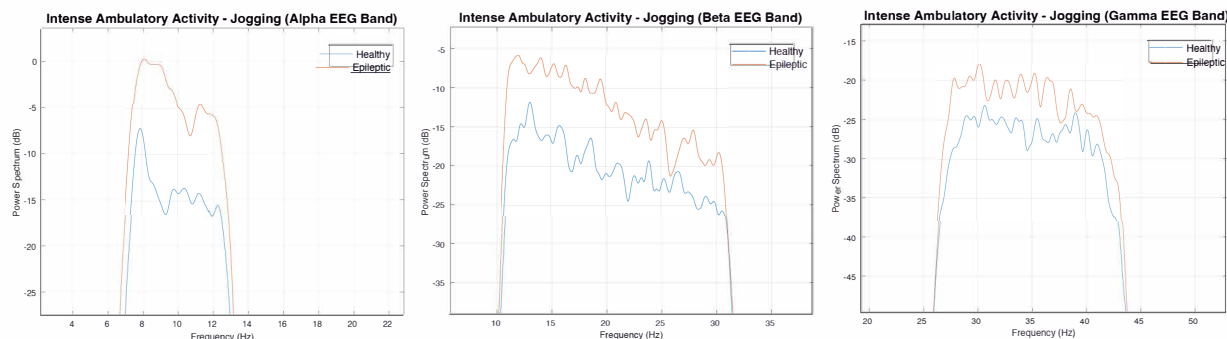


Fig. 3. Power Spectral Density of Intense Ambulatory Activity (Jogging) of Gamma EEG Band of Two Random Users (Healthy Person and Epileptic Patient)

accuracy of the system in rejecting instances belonging to the control classes. Recall is the accuracy of the system in accepting instances belonging to the healthy/epileptic classes.

Low recall leads to high rejection of positive instances, hence unusable, and low precision leads to high acceptance of negative instances, hence insecure. So, we compute F-measure

as the harmonic mean of the precision and recall of the test. It depicts the balance between precision and recall. High F-measure represents a good classification system.

Using traditional machine learning classifiers, we classify the epochs associated with the classes of machine learning models: *stationary-model*, *light-ambulatory-model* and *intense-ambulatory-model*. Once the epoch classification is done, we applied max-pool calculation on the identified or classified epochs to classify the associated class. For example, in disease classification using the *stationary-model*, we classified the EEG epochs first and then we applied max-pool calculation to identify which class was classified mostly in the epoch classification and then recognize the class (epileptic or healthy) with the maximum result of epoch classification. Similarly, we performed the classification using *light-ambulatory-model* and *intense-ambulatory-model*.

C. Performance of Machine Learning Classifications

We aggregated all features (band power and DWPT features) presented in Table I and applied off the shelf machine learning classifiers. Since we have three different types of activities, i.e., stationary activities, light ambulatory activities and intense ambulatory activities, thus we applied the traditional machine learning classifiers on all three models described in Section IV-D representing the three different types of activities.

In Table III, we presented the results of machine learning classifiers of *stationary-model* in identifying epileptic patient from healthy people from aggregated features of different types of stationary activities, e.g., desk work, idle sitting, laying, sitting patterns of all participants. Similarly, we presented the results of machine learning classification of classifying epileptic patient from healthy person from *light-ambulatory-model* and *intense-ambulatory-model* in Table IV and Table V respectively.

We performed 10-fold cross validation on all three machine learning models, i.e., *stationary-model*, *light-ambulatory-model* and *intense-ambulatory-model*. Afterwards, we ran the traditional machine learning classifiers on the 90%-10% train-test split dataset.

From result of *stationary-model* presented in Table III, we can see that machine learning classifiers showed accuracy between 71% to 82% in identifying epileptic patient from healthy group of people, which is higher than random guess (50% for two class classifier). The performance of *light-ambulatory-model* is presented in the Table IV. The performance of *light-ambulatory-model* in disease classification based on four light ambulatory activities' (i.e., stairs up and down, walking) is between 80% to 95%, which is also higher than 2-class random guessing (50%). We presented the result of *intense-ambulatory-model* is presented in Table V. The results show that our attack model in identifying person's health condition based on the brainwave signals achieved accuracy up to 84% which is also better than random guess. For all three models, i.e., *stationary-model* and *intense-ambulatory-model*, random forest classifier achieved the highest accuracy in identifying

the epileptic person from healthy person, while IBK classifier achieved highest accuracy in *light-ambulatory-model*.

From machine learning classification, it is clear that the presence of epilepsy is easily identifiable from neural pattern collected during daily life activities (e.g., sitting, desk-working, running, jogging) which validates our threat model (Section III).

VI. RESULTS AND DISCUSSION

In this section, we present our overall finding from the spectral analysis and machine learning classification. According to our attack model, we try to identify a serious health condition, i.e., epilepsy from some daily life activities. We start with spectral analysis (Sec. V-A) to show the presence of difference of EEG band power in between healthy group vs epileptic group. Afterwards, we validate our *Disease Detector* attack with machine learning (Sec. V-B) classification. The dataset has several numbers of tasks in each category. To keep the consistency of our analysis, we select similar tasks for each group of people and balance our data for analysis.

In spectral analysis (Sec. V-A), we calculated the average band power of five EEG bands, i.e., delta, theta, alpha, beta and gamma and overall result is presented in Table II for all participants. To visually illustrate the difference between a random epileptic patient and a healthy person, we plot the average band power in graphs.

In machine learning classification, we extracted features from the raw EEG signal collected from FP1 positioned electrode. As features, we calculated the band power and Discrete Wavelet Packet Transform (DWPT) in each type of activity (i.e., stationary, light ambulatory and intense ambulatory activities) for all EEG bands (i.e., delta, theta, alpha, beta and gamma). The detailed discussion about feature engineering is presented in section IV-B. We evaluate the machine learning classification for controlled class and healthy class using aggregated features from EEG band power and DWPT for stationary activity, light ambulatory activity and intense ambulatory activity.

We discuss the summary of the findings from spectral analysis and machine learning classification in the below sections,

Evidence of Disease from Stationary Activity. In our analysis, stationary activities include desk-work, laying, sitting. We calculated EEG band power across EEG bands (i.e., alpha, beta, gamma) and illustrated the difference in between two groups using of a stationary activity, i.e., desk-work in Figure 1. From the figure, it is clear that an epileptic patient utilized higher cognitive power than a healthy person. Our machine learning model, i.e., *stationary-model* showed the similar success in identifying an epileptic patient from the healthy group with accuracy of 82% in random forest classifier. The findings from the spectral analysis and machine learning classification, it is clear that private sensitive disease information can be identified from stationary activities which is very likely to happen in a real-world scenario when people work on computer or sitting idle with the EEG headset on.

TABLE III
PERFORMANCE OF *stationary-model* IN INFERRING DISEASE FROM STATIONARY ACTIVITIES

stationary-model	10-fold cross-validation						80%-20% train-test model					
	Classifiers	TPR	FPR	Prec	Rec	FM	Acc(%)	TPR	FPR	Prec	Rec	FM
RT	0.719	0.281	0.719	0.719	0.719	71.89	0.717	0.283	0.717	0.717	0.716	71.65
RF	0.821	0.179	0.825	0.821	0.821	82.09	0.819	0.181	0.819	0.819	0.819	81.86
IBK	0.790	0.210	0.790	0.790	0.789	78.95	0.791	0.209	0.791	0.791	0.791	79.06

TABLE IV
PERFORMANCE OF *light-intense-model* IN INFERRING DISEASE FROM LIGHT AMBULATORY ACTIVITIES

light-intense-model	10-fold cross-validation						80%-20% train-test model					
	Classifiers	TPR	FPR	Prec	Rec	FM	Acc(%)	TPR	FPR	Prec	Rec	FM
RF	0.908	0.092	0.908	0.908	0.908	90.81	0.912	0.088	0.912	0.912	0.912	91.16
RT	0.842	0.158	0.842	0.842	0.842	84.25	0.841	0.158	0.842	0.841	0.841	84.09
LMT	0.814	0.186	0.814	0.654	0.814	81.40	0.808	0.191	0.809	0.808	0.808	80.83
IBK	0.950	0.050	0.950	0.950	0.950	95.01	0.946	0.054	0.946	0.946	0.946	94.61

TABLE V
PERFORMANCE OF *intense-intense-model* IN INFERRING DISEASE FROM INTENSE AMBULATORY ACTIVITIES

intense-intense-model	10-fold cross-validation						80%-20% train-test model					
	Classifiers	TPR	FPR	Prec	Rec	FM	Acc(%)	TPR	FPR	Prec	Rec	FM
RF	0.834	0.166	0.834	0.834	0.834	83.40	0.836	0.164	0.836	0.836	0.836	83.62
RF	0.706	0.294	0.706	0.706	0.706	70.57	0.729	0.217	0.729	0.729	0.729	72.89
IBK	0.785	0.215	0.785	0.785	0.785	78.46	0.785	0.215	0.785	0.785	0.785	78.47

Evidence of Disease from Light Ambulatory Activity. Similar to the stationary activities, we considered light ambulatory works, such as, stairs up-down, walking to identify an epileptic patient from healthy group. Our spectral analysis showed that there are visible difference in power spectral density of brain activities of an epileptic patient and a healthy individual while walking. From the Figure 2, we can see that the epileptic patient has higher spectral density while waling than the healthy person and the difference is mostly visible in EEG band Alpha and Beta. In machine learning, we considered all light ambulatory activities to extract features for our model and the *light-ambulatory-model* reached accuracy of 94% on IBK in identifying the epileptic patient from the healthy group. So, from the spectral analysis and machine learning classification, it is clear that identifying the disease information from light body posture related brain activity is easily possible with consumer-grade EEG headset.

Evidence of Disease from Intense Ambulatory Activity. The motivation of *Disease Detector* is to successfully identify private sensitive disease information from consumer-grade EEG headset while victim wears it for gaming purpose or forget to turn it off after use. To validate our threat scenario, we also considered intense ambulatory activities, such as, jogging, running. We believe EEG signal related to such activities also provide enough evidence of epilepsy. With the given dataset, we run spectral analysis on EEG signal collected during jogging and found that difference of spectral density in healthy person and epileptic patient is visible as illustrated in Figure 3. Similar to stationary activities and light ambulatory activities, we performed machine learning on intense ambulatory activities as well. From Table V, we can see that random forest classifier reached accuracy of 83% in identifying an epileptic patient from healthy group of people in *intense-ambulatory-model*. The results from spectral analysis and machine learning

classification, it is clear that from running and jogging, we can identify the disease information by analyzing EEG signal easily with traditional machine learning.

From the analysis from stationary activity (e.g., Desk Work), light intense activity (e.g., Walking) and intense stationary activity (e.g., Jogging), it is clear that identification on an epileptic patient from a healthy person is possible using EEG signal collected from a low-grade EEG headset. This insight is important to design strong and secured brain-computer interface for consumer-grade use, otherwise serious health injuries can be occurred by hackers to mass population in future.

VII. DISCUSSION AND FURTHER RESEARCH INSIGHT

A. Possible Defensive Mechanism

In this section, we discuss about possible defense mechanism to protect brainwave signals from being exposed to malicious parities. **Existing Defense Solutions:** One of the possible mitigation strategies of *Disease Detector* attack could be, adding a security layer on the EEG signal like BCI Anonymizer [40]. BCI Anonymizer pre-processes the neural signals before it gets release to the computing system and it allows to hide private sensitive information from the EEG. Another possible defense to the *Disease Detector* attack could be the implementation of Privacy-Preserving Cryptographic Protocols [41] in BCI. The Privacy-Preserving Cryptographic Protocol is designed to hide individual's EEG signal from being revealed from the outside.

Access Permission Model: One potential reason that opens up the threat of private data leakage through brainwave signals is the unfiltered access to raw EEG signal by the application. Any application can freely access and utilize the raw EEG signal using Bluetooth for their own purpose leading to the privacy leakage through brainwaves. Therefore, one potential counter-

measure towards brainwave attacks could be implementation of an access control mechanism or a permission model that limits or restricts the access of raw EEG signals to the third party applications. In access permission model, the BCI will analyze raw EEG signals to detect any specific event and provides only the features or the information corresponding to that events rather than the raw EEG. In particular, the access permission model will prevent the exposition of raw EEG signal to malicious third-party applications. This approach requires the EEG vendors to design a restricted API that would allow access to only certain features or information of EEG signal, e.g., allowing only visual stimuli related signals for a visual task, rather than the whole raw EEG signal.

A permission model similar to the ones in Android or iOS can also be implemented on the BCI devices that requires the third-party application to obtain the user's permission to access the EEG signal. Such permission model can reduce the threat of privacy leakage through EEG signal. Such users' behavior towards the security model has already been demonstrated in user-centered security literature such as the study in [42], [43], allowing the adversary to successfully launch various attacks.

System Noise: A potential approach to mitigate brainwave threats could be automatically insert noise to the EEG signal to obfuscate the original signals as was introduced in Slogger [44]. Shrestha et al. introduced Slogger as a defense mechanism against motion-based touchstroke leakage based on sensory noise generated automatically by the system. Slogger utilizes the Android's ADB (Android Debugging Bridge) functionality to sniff and inject sensory noise to various inertial sensors for defeating the sensor-based keystroke logging attacks. It transparently inserts the noise in the background as the user provides sensitive touch input in order to obfuscate the original sensor measurements. In the similar fashion, raw brain signals can be sniffed and neural noise can be injected transparently in the background to obfuscate the original raw brain signals. Such noise can be injected to the raw brain signal either before making it available to the legitimate application or only at the time when the user is performing sensitive act (e.g., typing passwords or PINs).

Detect Active Tasks: Since BCI is designed to interact with the computing system using brain commands. To detect the exact brain command, the BCI uses different features extraction methods (e.g., time frequency analysis, frequency domain analysis etc.) to extract features and machine learning and deep learning techniques to finally identify the command from neural signal. Based on BCI working methodology, it is also possible to determine if a person is playing a game, taking a nap or talking over phone. Once the activity is detected from the device-end and it is found that no active application is not using the EEG headset, then the headset should be immediate turned off and terminate the Bluetooth connection to save unnecessary data transferring.

B. Study Strength and Weakness

Our *Disease Detector* attack has several strengths, such as, light-weight design of consumer-grade EEG headset makes it

possible to forget removing of the headset (attached with head-band or cap) from head while implant like BCI implementation makes it possible to keep BCI always with body. Moreover, EEG headsets use Bluetooth connection to transmit data and they do not need any user intervention or permission to make a connection with computing system. Such zero-permission BCI use in consumer-grade purpose can definitely attract malicious users to exploit the system's security hole. Another strength of this attack is, we used raw EEG signals (which do not require any manufacture's key to decrypt EEG metrics) and extracted features from it for attack analysis which makes the attack scenario powerful. We balance the data according to the machine learning models (e.g., stationary activity, light ambulatory activity and intense ambulatory activity).

Our attack model has certain limitation as well. Since the EEG dataset we used was based on training purpose, thus in real life scenario postures can be different during walking, standing or playing a 3D game. But we believe the body postures we considered in this paper, are sufficient in validating the risk introduced in *Disease Detector*.

C. Future Research Direction

In future, we will include more realistic attack scenario where the user will either play a 3D game wearing a EEG mounted AR/VR headset instead of body movement in training sessions. Moreover, we will perform the experiment with combination of different EEG devices; train model in lab environment with one type of EEG headset and test the machine learning model with different EEG headset's data. This type of attack design will give more accurate measurements of the real life attack scenarios.

VIII. CONCLUDING REMARKS

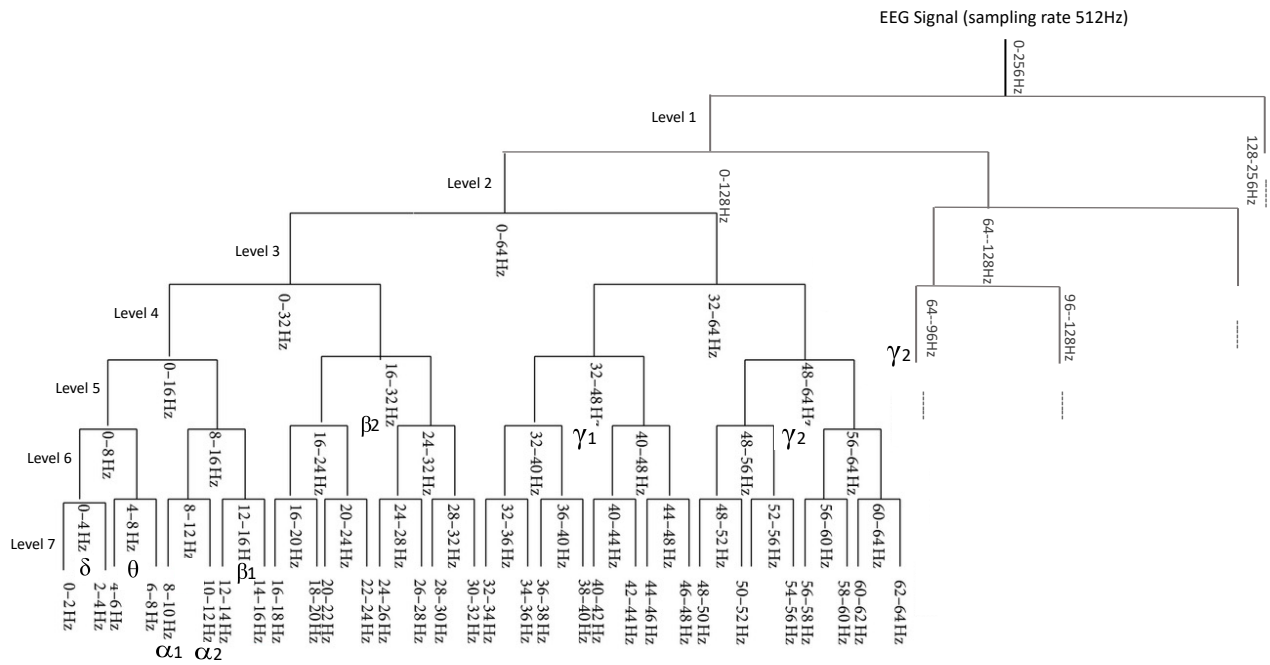
In this paper, we designed an attack on EEG headset by utilizing a publicly available EEG dataset to demonstrate that private sensitive disease information, i.e., epilepsy is possible by analyzing brainwaves. This attack can be launched against any consumer-grade EEG headset which are available on market and can communicate with computing system (computer or smartphone or smartwatch) without any user-intervention. We evaluated the attack using spectral analysis and traditional machine learning classifications. We illustrated the difference of brain activities in different types of body postures (stationary activity, light ambulatory activity and intense ambulatory activity). Finally, we validated our attack model with machine learning classification and found that traditional classifiers could identify the disease information with minimal feature engineering from three different types of body activities. *Disease Detector* showed highest success rate in random forest classifier (82%) with stationary activities, highest success rate of 94% in IBK with light ambulatory activities and highest success rate of 83% in random forest with intense ambulatory activities. The future work can focus on more sophisticated ways of attack scenario in which the attacker will have more measurements to consider to launch a successful attack.

REFERENCES

- [1] F. Nijboer, A. Furdea, I. Gunst, J. Mellinger, D. J. McFarland, N. Birbaumer, and A. Kübler, "An auditory brain-computer interface (bci)," *Journal of neuroscience methods*, no. 1, pp. 43–50, 2008.
- [2] S. Gao, Y. Wang, X. Gao, and B. Hong, "Visual and auditory brain-computer interfaces," *IEEE Transactions on Biomedical Engineering*, no. 5, pp. 1436–1447, 2014.
- [3] M. Sugı, Y. Hagimoto, I. Nambu, A. Gonzalez, Y. Takei, S. Yano, H. Hokari, and Y. Wada, "Improving the performance of an auditory brain-computer interface using virtual sound sources by shortening stimulus onset asynchrony," *Frontiers in neuroscience*, p. 108, 2018.
- [4] K. Sumi, K. Yabuki, T. J. Tiam-Lee, A. N. Belkacem, Q. Ferre, S. Hirai, and T. Endo, "A cooperative game using the p300 eeg-based brain-computer interface," in *Assistive and Rehabilitation Engineering*, Y. Rybarczyk, Ed. Rijeka: IntechOpen, 2019, ch. 10. [Online]. Available: <https://doi.org/10.5772/intechopen.84621>
- [5] "Scientists are using brain-computer connections to restore a lost sense of touch," 2020, <https://www.zdnet.com/article/scientists-are-using-brain-computer-connections-to-restore-a-lost-sense-of-touch>.
- [6] "Neuralink," 2020, <https://neuralink.com/>.
- [7] "Neuralink human test," 2020, <https://www.cnet.com/news/elon-musk-neuralink-works-monkeys-human-test-brain-computer-interface-in-2020>.
- [8] "Neuralink," 2024, <https://www.scientificamerican.com/article/elon-musk-neuralink-has-implanted-its-first-chip-in-a-human-brain-whats-next>.
- [9] V. P. Oikonomou, S. Nikolopoulos, P. Petrantonakis, and I. Kompatsiaris, "Sparse kernel machines for motor imagery eeg classification," in *2018 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. IEEE, 2018, pp. 207–210.
- [10] A. Dey, S. Bhattacharjee, and D. Samanta, "Recognition of motor imagery left and right hand movement using eeg," in *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. IEEE, 2016, pp. 426–430.
- [11] N. T. M. Huong, H. Q. Linh *et al.*, "Classification of left/right hand movement eeg signals using event related potentials and advanced features," in *International Conference on the Development of Biomedical Engineering in Vietnam*. Springer, 2017, pp. 209–215.
- [12] "Neurosky," 2024, <https://store.neurosky.com/>.
- [13] EMOTIV, "Neurotech for the Global Community," <https://www.emotiv.com/>, 2020, [Accessed: 11/19/2021].
- [14] "Nextmind visual eeg headsets," <https://www.next-mind.com/technology>, 2020, [Accessed: 11/19/2021].
- [15] "Photosensitivity and seizures," 2022, <https://www.epilepsy.com/what-is-epilepsy/seizure-triggers/photosensitivity>.
- [16] "Strobing stage lights could up risk of epileptic seizures," 2019, <https://www.reuters.com/article/us-health-strobe-lights-epilepsy-idUSKCN1TK30X>.
- [17] "Strobe lighting at dance music cyberattack," 2009, <https://www.bmj.com/company/newsroom/strobe-lighting-at-dance-music-festivals-linked-to-tripling-in-epileptic-fit-risk/>.
- [18] "Epilepsy foundation was targeted in mass strobe cyberattack," 2009, <https://www.nytimes.com/2019/12/16/us/strobe-attack-epilepsy.html>.
- [19] "A tweet gave a journalist a seizure," 2009, <https://www.nytimes.com/2019/12/16/us/strobe-attack-epilepsy.html>.
- [20] I. Martinovic, D. Davies, M. Frank, D. Perito, T. Ros, and D. Song, "On the feasibility of side-channel attacks with brain-computer interfaces," in *21st {USENIX} Security Symposium ({USENIX} Security 12)*, 2012, pp. 143–158.
- [21] M. Frank, T. Hwu, S. Jain, R. T. Knight, I. Martinovic, P. Mittal, D. Perito, I. Sluganovic, and D. Song, "Using eeg-based bci devices to subliminally probe for private information," in *Proceedings of the 2017 on Workshop on Privacy in the Electronic Society*, 2017, pp. 133–136.
- [22] A. Neupane, M. L. Rahman, and N. Saxena, "Peep: Passively eavesdropping private input via brainwave signals," in *Financial Cryptography*, 2017.
- [23] "Electroencephalography (eeg)," 2019, <https://en.wikipedia.org/wiki/Electroencephalography>.
- [24] "Neural oscillation," 2024, https://en.wikipedia.org/wiki/Neural_oscillation.
- [25] "Alpha wave," 2024, https://en.wikipedia.org/wiki/Alpha_wave.
- [26] W. Nan, F. Wan, Q. Tang, C. M. Wong, B. Wang, and A. Rosa, "Eyes-closed resting eeg predicts the learning of alpha down-regulation in neurofeedback training," *Frontiers in psychology*, vol. 9, p. 1607, 2018.
- [27] "Delta wave," 2024, https://en.wikipedia.org/wiki/Delta_wave.
- [28] "Theta wave," 2024, https://en.wikipedia.org/wiki/Theta_wave.
- [29] "Beta wave," 2024, https://en.wikipedia.org/wiki/Beta_wave.
- [30] "Gamma wave," 2024, https://en.wikipedia.org/wiki/Gamma_wave.
- [31] A. Mandal and N. Saxena, "Sok: Your mind tells a lot about you: On the privacy leakage via brainwave devices," in *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 175–187. [Online]. Available: <https://doi.org/10.1145/3507657.3528541>
- [32] A. Neupane, K. Satvat, M. Hosseini, and N. Saxena, "Brain hemorrhage: When brainwaves leak sensitive medical conditions and personal information," in *2019 17th International Conference on Privacy, Security and Trust (PST)*, 2019, pp. 1–10.
- [33] S. Dogan, M. Baygin, B. Tasci, H. W. Loh, P. D. Barua, T. Tuncer, R.-S. Tan, and U. R. Acharya, "Primate brain pattern-based automated alzheimer's disease detection model using eeg signals," *Cognitive Neurodynamics*, vol. 17, no. 3, pp. 647–659, 2023.
- [34] S. Xu, Z. Wang, J. Sun, Z. Zhang, Z. Wu, T. Yang, G. Xue, and C. Cheng, "Using a deep recurrent neural network with eeg signal to detect parkinson's disease," *Annals of translational medicine*, vol. 8, no. 14, 2020.
- [35] M. Savadkoobi, T. Oladunni, and L. Thompson, "A machine learning approach to epileptic seizure prediction using electroencephalogram (eeg) signal," *Biocybernetics and Biomedical Engineering*, vol. 40, no. 3, pp. 1328–1341, 2020. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0208521620300851>
- [36] C. A. T. Cortes, C.-T. Lin, T.-T. N. Do, and H.-T. Chen, "An eeg-based experiment on vr sickness and postural instability while walking in virtual environments," in *2023 IEEE Conference Virtual Reality and 3D User Interfaces (VR)*. IEEE, 2023, pp. 94–104.
- [37] "Matlab bandpower," 2022, <https://www.mathworks.com/help/signal/ref/bandpower.html>.
- [38] M. K. Wali, M. Murugappan, and B. Ahmmad, "Wavelet packet transform based driver distraction level classification using eeg," *Mathematical Problems in Engineering*, vol. 2013, 2013.
- [39] S. Zia and A. Nawaz Khan, "Activities of daily livings using a portable eeg headset," 2021. [Online]. Available: <https://dx.doi.org/10.21227/mtwx-p951>
- [40] H. J. Chizeck and T. Bonaci, "Brain-computer interface anonymizer," Aug. 14 2014, uS Patent App. 14/174,818.
- [41] A. Agarwal, R. Dowsley, N. D. McKinney, D. Wu, C.-T. Lin, M. De Cock, and A. C. Nascimento, "Protecting privacy of users in brain-computer interface applications," *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, vol. 27, no. 8, pp. 1546–1555, 2019.
- [42] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," in *Proceedings of the eighth symposium on usable privacy and security*. ACM, 2012, p. 3.
- [43] J. Sunshine, S. Egelman, H. Almuhammedi, N. Atri, and L. F. Cranor, "Crying wolf: An empirical study of ssl warning effectiveness," in *USENIX security symposium*, 2009, pp. 399–416.
- [44] P. Shrestha, M. Mohamed, and N. Saxena, "Slogger: Smashing motion-based touchstroke logging with transparent system noise," in *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. ACM, 2016, pp. 67–77.
- [45] "Eeg 10-20 system," 2024, [https://en.wikipedia.org/wiki/10-20_system_\(EEG\)](https://en.wikipedia.org/wiki/10-20_system_(EEG)).

APPENDIX

IX. SEVEN LEVEL EEG SIGNAL DECOMPOSITION USING DISCRETE WAVELET PACKET TRANSFORM (DWPT)



X. EEG 10-20 SYSTEM [45] (NEUROSKY MINDWAVE MOBILE SENSOR PLACEMENT POSITION IS HIGHLIGHTED)

