Politechnika Wrocławska

FIELD OF SCIENCE: **Engineering and technology**

DISCIPLINE OF SCIENCE: Information and communication technology

DOCTORAL DISSERTATION

Applications of Simplified Brain-Computer Interfaces in Cybersecurity and Emotion Recognition

mgr inż. Rafał Chałupnik

Supervisor:
dr hab. inż. Ireneusz Jóźwiak, prof. PWr

Assistant supervisor:
dr inż. Michał Kędziora

Keywords: EEG, BCI, interface, cybersecurity, emotion, stress, recognition, dataset, classifier, research, machine learning, ml.net

WROCŁAW 2024

Contents

For the people who, directly or not, have contributed to making this work possible and to whom I dedicate this dissertation:

For my parents, who made this dissertation possible and supported me in my career as a programmer.

For my grandmother, who was the highest motivation of all in this study.

For my fiancée, Kinga, who has provided moral support and humanistic point of view.

For my dearest friends, Katarzyna, Milena, Michał, and Jerzy, for their overwhelming support.

For my thesis supervisors, prof. Jóźwiak and dr. Kędziora, for their time and support.

Abstract

The main purpose of the thesis is to present the original solution to the scientific problem of exploring the applications of simplified brain-computer interfaces in cybersecurity and emotion recognition, especially in terms of evaluating the potential of such interfaces within the field of stress detection and subject recognition. It has been done by building stress detection and subject recognition classifiers based on the data provided by the Neurosky MindWave Mobile 2 interface and evaluating the results, with cybersecurity applications in mind, and what the metrics of such classifiers are. Considering the participation of human participants, the research has been approved by the Committee for Research Ethics.

Two classifiers have been built to evaluate the possibilities of using a simplified EEG interface for stress detection in a reproducible manner, by fine-tuning the parameters of the model, exploring the preprocessing approaches, and evaluating the classifier by its metrics and the improvement ratios for all available EEG bands, along with the Attention and Meditation features, to define the impact of a specific feature on the performance of the model.

The classifier built upon the "Stress" dataset achieved the F1 score of 0.921606 with precision of 0.857198 and recall of 0.996541, while the classifier built upon the "Login" dataset achieved the F1 score of 0.945356 with precision of 0.901603 and recall of 0.993748. The analysis of the confusion matrices produced by both models indicates that it is possible to use simplified EEG interfaces in stress detection, as both models tend to skew the results into false-positive area, which in terms of cybersecurity makes it more desirable than skewing into false-negative predictions.

Two other classifiers have been built to evaluate the possibilities of using the simplified EEG interface for subject recognition. Contrary to the stress detection recognition study, these two classifiers were, respectively, binary model calculated for every subject based on the Fast Tree classifier, compared to the one-for-all multi-class model based on the LightGBM classifier. The methodology used to develop these classifiers was similar to that in the stress detection study.

Both classifiers have been evaluated by calculating their metrics and improvement ratios for all included features. The binary classifier achieved the F1 score of 0.927333 with accuracy of 0.984822, while the multi-class model achieved the macro accuracy of 0.929150 and micro accuracy of 0.929454. Such measure values indicate that it may be more viable to create a model per subject in commercial setup, as the system would not have to relearn every subject when there is a new subject joining the group of users.

Streszczenie

Głównym celem rozprawy jest zaprezentowanie oryginalnego rozwiązania problem naukowego, jakim jest zbadanie zastosowań uproszczonych interfejsów mózg-komputer w cyberbezpieczeństwie i rozpoznawaniu emocji, a w szczególności ewaluacja wspomnianych interfejsów w zakresie detekcji stresu i rozpoznawania osób. Zostało to osiągnięte poprzez zbudowanie klasyfikatorów do detekcji stresu i rozpoznawania emocji bazując na danych pochodzących z interfejsu Neurosky MindWave Mobile 2 oraz ewaluację wyników, mając na celu cyberbezpieczeństwo. Ze względu na uczestnictwo ludzi, wszystkie przeprowadzone badania uzyskały pozytywną opinię Komisji ds. Etyki Badań Naukowych.

W celu zbadania możliwości detekcji stresu dwa klasyfikatory zostały zbudowane w sposób pozwalający na odtworzenie tego procesu, poprzez dobranie optymalnych parametrów modelu, eksplorację dostępnych metod przetwarzania wstępnego oraz ewaluację metryk klasyfikatora oraz współczynników poprawy dla wszystkich dostępnych pasm EEG, wraz z metrykami Uwagi oraz Rozluźnienia, mając na celu określenie wpływu każdego elementu wejściowego na wyniki opracowanego modelu.

Klasyfikator zbudowany na danych ze zbioru "Stres" osiągnął wartość F1 na poziomie 0.921606 z precyzją 0.857198 i kompletnością 0.996541, natomiast klasyfikator zbudowany na danych ze zbioru "Login" osiągnął wartość F1 na poziomie 0.945356 z precyzją 0.901603 i kompletnością 0.993748. Analiza macierzy błędów obu modeli wskazuje na możliwość wykorzystania uproszczonych interfejsów EEG w detekcji stresu ze względu na tendencję obu modeli do przekłamania w stronę wyników fałszywie dodatnich, co w temacie cyberbezpieczeństwa jest bardziej pożądane niż przekłamanie w stronę wyników fałszywie ujemnych.

Dodatkowe dwa klasyfikatory zostały zbudowane w celu zbadania możliwości rozpoznawania osób. W przeciwieństwie do badań rozpoznawania stresu, wspomniane dwa klasyfikatory bazowały odpowiednio na binarnym modelu Fast Tree oraz wieloklasowym modelu jeden-na-wszystkich LightGBM. Metodologia wykorzystana do budowy tych klasyfikatorów była podobna do badań rozpoznawania stresu.

Obydwa klasyfikatory zostały zbadane za pomocą obliczenia ich metryk oraz współczynników poprawy dla wszystkich dostępnych wartości wejściowych. Klasyfikator binarny osiągnął wartość F1 na poziomie 0.927333 z precyzją 0.984822, natomiast klasyfikator wieloklasowy osiągnął dokładność makro 0.929150 oraz mikro 0.929454. Wartości te wskazują na model binarny jako bardziej praktyczny w rozwiązaniu komercyjny, z racji braku konieczności ponownego uczenia klasyfikatora za każdym dołączeniem nowego użytkownika.

1. Introduction

This chapter is a comprehensive overview of the subject of the thesis, along with the scope, goal, and structure of the thesis. The main goal is to explore the feasibility of simplified and commercially available EEG interfaces in terms of cybersecurity and emotion recognition. The main benefit of this approach is to fill the gap between the existing state-of-the-art research on medical-grade EEG interfaces and practical, accessible applications of the EEG interfaces available on the market.

1.1. Subject Overview

The human brain is one of the most complex parts of our bodies, responsible for congitive function, sensory processing, motor control, memory, and much more[35]. For decades, it has been the subject of various research. One of the groundbreaking tools that gives us insight into the human brain and its activity is electroencephalography (EEG)[51], a technique that records electrical fluctuations along the scalp of the subject that are an effect of neurons firing within the brain[25]. The history of EEG goes back to the early 20th century; a German psychiatrist, Hans Berger, first recorded the electrical activity of the human brain in 1924[47]. His work has become the foundation for EEG development as the useful tool it is today, both in clinical and scientific fields. The traditional EEG interface is a non-invasive device that allows one to measure brain activity through a range of electrodes placed on the scalp of the patient, covering various areas of the brain[49]. Within preset frequency, the device captures the ongoing electrical activity, providing the software with the raw signal data that can be later analyzed, providing valuable insight into our brains. Although currently the use cases of EEG are much more diverse, they evolved over the decades from the very first recording by Berger. In a clinical setting, EEG is a valuable tool in the diagnosis and monitoring of a variety of neurological disorders, such as epilepsy[32], sleep disorders[63], and brain injuries, helping to detect abnormalities in electrical patterns that may indicate seizures. Outside of clinical applications, EEG is researched in cognitive neuroscience[16] to study brain functions related to perception, attention, motor skills, and memory. In addition, advances in EEG technology have been made for it to be used in brain-computer interfaces (BCI)[38], enhancing communication between humans and computers, which could especially help people with severe motor or mental disabilities. The versatility of EEG is also presented in other use cases, including understanding the stages and disorders of sleep, or neurofeedback therapy[43]. As more extensive research is performed, the applications may expand as well, possibly introducing EEG to fields that have never been before.

EEG is already used in a variety of use cases, as described above. However, traditional full-scale EEG interfaces are usually prohibitively expensive and complex, significantly limiting their adoption in commercial applications beyond the medical and scientific field.

It is difficult to use such a device in a daily routine as a smartphone when it requires extensive setup, specialized personnel, and environment, which makes it horrendously impractical. However, the technological advancements since day one of EEG research have led to the development of simplified, wearable EEG devices. Although they cannot be compared with traditional medical interfaces in terms of data quality and number of channels, they address the limitations associated with their traditional counterparts.

The simplified interfaces are designed from scratch to be more user-friendly and affordable at the cost of medical-grade quality data, however, innovations such as dry electrodes, wireless connectivity, and compact form factors make them a more viable solution for daily usage in any commercial applications, such as BCI devices, security measures, or continuous and unobtrusive monitoring of brain activity. The sole factors of affordability and simplicity have the potential to extend the use of EEG devices far beyond traditional medical applications. The simplified interfaces could easily be used to continuously monitor stress, anxiety, and other psychological states, providing useful information to individuals, doctors, and healthcare providers. The aforementioned brain-computer interfaces could also be deployed more universally, as devices are simpler and cheaper, allowing people, especially those in special need, to explore the new possibilities of controlling computers, smartphones, and other devices that could significantly improve their comfort of life. Beyond the domain of clinical-like application and quality of life, the possibilities of simplified EEG devices extend to other areas, such as education, allowing one to monitor cognitive load and attention, optimizing the learning process and experience. In the fitness area, those interfaces could be used to track mental states to improve performance during training and recovery afterwards. Lastly, within the entertainment area, such devices look promising in immersive and interactive movies, games, and other activities, by possibly adapting the content to the current state of the one's brain activity.

The extensive research on EEG has outstandingly advanced humanity's understanding of brain activity and gave us incredible insight on how our brains work. However, following the recent enrollment of simplified EEG interfaces, there is a significant gap in the literature. The traditional interfaces, given their history, although complex and expensive, have been a main focus of numerous experiments performed within the last century. The fact that simplified interfaces are becoming more popular suggests a need for revisiting the already performed research and re-evaluate it, now with the simplified devices. This could bring a significant insight to the field, either reassuring the position of the new interfaces or discarding them as not viable. Although existing research could be repeated, the idea that some of the research topics may have been declined due to the impracticality of traditional EEG interfaces seems to be justified. In addition to evaluating newer interfaces with older research, there is a domain of research that probably has not yet been explored at all or a fraction of it has. One of those areas is cybersecurity - given the traditional interfaces would be irrationally impractical to, for example, confirm someone's identity, it seems natural to evaluate the new simplified devices within the prospect of deploying them to a wider audience, potentially allowing people to authenticate and log into the popular services in a practical, possibly more secure way.

1.2. Goal and Scope of the Thesis

The main goal of the thesis is to explore the applications of simplified EEG interfaces within the field of cybersecurity and emotion recognition. This thesis addresses the research question of whether it is feasible to develop classifiers for stress detection and subject recognition using data from simplified EEG interfaces and what performance metrics can be achieved. The real-world goal is to make it possible to integrate such classifiers into already existing security protocols and biometric identification systems, thus improving their security. By meticulously examining the performance metrics of these classifiers, this study seeks to evaluate the practicality and reliability of simplified EEG interfaces in the scenarios mentioned above. The thesis not only addresses the technical challenges posed by the development of such classifiers but also covers the development of two proprietary datasets to make the development of those classifiers possible, as no viable dataset of required data is publicly accessible at the moment. The research employs a rigorous and deterministic approach within its experimental procedures to ensure that the results achieved are fully reproducible. In the end, every developed classifier is validated through the metrics described later within the thesis. Ultimately, the goal of this thesis is to contribute to the expanding body of knowledge about EEG technology, demonstrating how these simplified interfaces can be used effectively beyond traditional medical settings. This work aims to revolutionize various aspects of daily life by extending the utility of simplified EEG interfaces, thereby enhancing their accessibility and applicability in diverse real-world contexts, where no EEG device could be considered before due to the impracticality and high cost of older traditional versions.

1.3. Structure of the Thesis

The rest of the thesis is organized into eight chapters. Chapter 2 contains the theoretical framework describing topics related to the research conducted, such as EEG technology, machine learning, algorithms, and metrics, establishing a robust basis for the subsequent practical work. Chapter 3 provides the review of the current state of the art, datasets, highlighting key advances, and gaps in the existing literature. This chapter sets the stage for the research by offering a thorough understanding of the fundamental concepts and the context in which this study is situated. Chapter 4 describes the methodology and details the approach taken in planning the research process, including data collection from subjects, experimental design, and execution. This chapter also describes the specific techniques and tools used for data acquisition and pre-processing, ensuring that the experimental setup is both rigorous and replicable. Chapters 5 to 8 focus on developing models to address the research questions using the ML.NET library. They involve the implementation of various machine learning algorithms, the tuning of the parameters, and the evaluation of the performance of the model. These chapters provide a step-by-step account of the model-building process, from initial data exploration to final validation of results. Chapter 9 synthesizes the conclusions drawn from each experiment, extracting meaningful insights and discussing their significance in the broader context of EEG research.

This chapter also suggests potential directions for future research, proposes new avenues for further exploration, and highlights areas where further investigation is needed. By offering a comprehensive summary of the research results and their implications, this chapter aims to contribute to the ongoing discourse in the field.

2. Theoretical Framework

The following chapter explains the theoretical aspects used to perform the research required in this dissertation. First, the area of electroencephalography (EEG) is covered, along with traditional medical-grade interfaces, as well as simplified, more affordable counterparts. Afterwards, the technical aspects are explained, starting with the Simple Moving Average algorithm used to smooth out the noises present within signal, the ML.NET library and the classifiers it offers, as well as the metrics that can be used to assess the created models and compare them with each other.

2.1. EEG and Interfaces

Electroencephalography (EEG) is a method of recording voltage fluctuations between neurons in the subject's brain (shown in Figure 2.1) by utilizing the metal electrodes distributed over the subject's scalp (shown in Figure 2.2). Despite the fact that EEG is a fairly safe imaging technique due to not requiring any invasive action, its cost, complexity, and availability may be a considerable impediment in the way of successfully using them in commercial solutions.

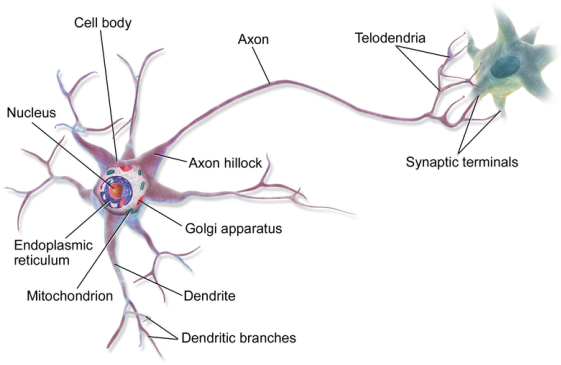


Figure 2.1: Neuron structure

Source: commons.wikimedia.org
(BruceBlaus - access date: 16 Jul 2024)

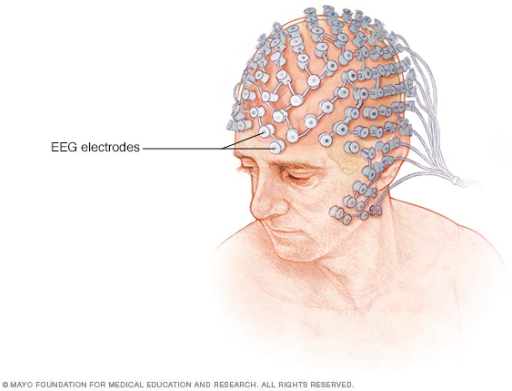


Figure 2.2: Traditional EEG interface

Source: mayoclinic.org
(access date: 16 Jul 2024)

The state of the art research shows that each part of the brain seems to be responsible for specific functions[14]. The traditional interface utilizes electrodes placed on the scalp of the subject, recording data from specific local channels presented in Table 2.1 and Figure 2.3.

Table 2.1: Brain Regions, Channels, and Functions

Region	Channels	Functions
Frontal Lobe	F*	Memory, concentration, emotions
Parietal Lobe	P*	Problem Solving, attention, grammar, sense of touch
Temporal Lobe	T*	Memory, face recognition, hearing, word recognition
Occipital Lobe	O*	Reading, vision
Cerebellum	-	Motor control, balance
Sensorimotor Cortex	C*	Attention, mental processing, fine motor control

Source: [14]

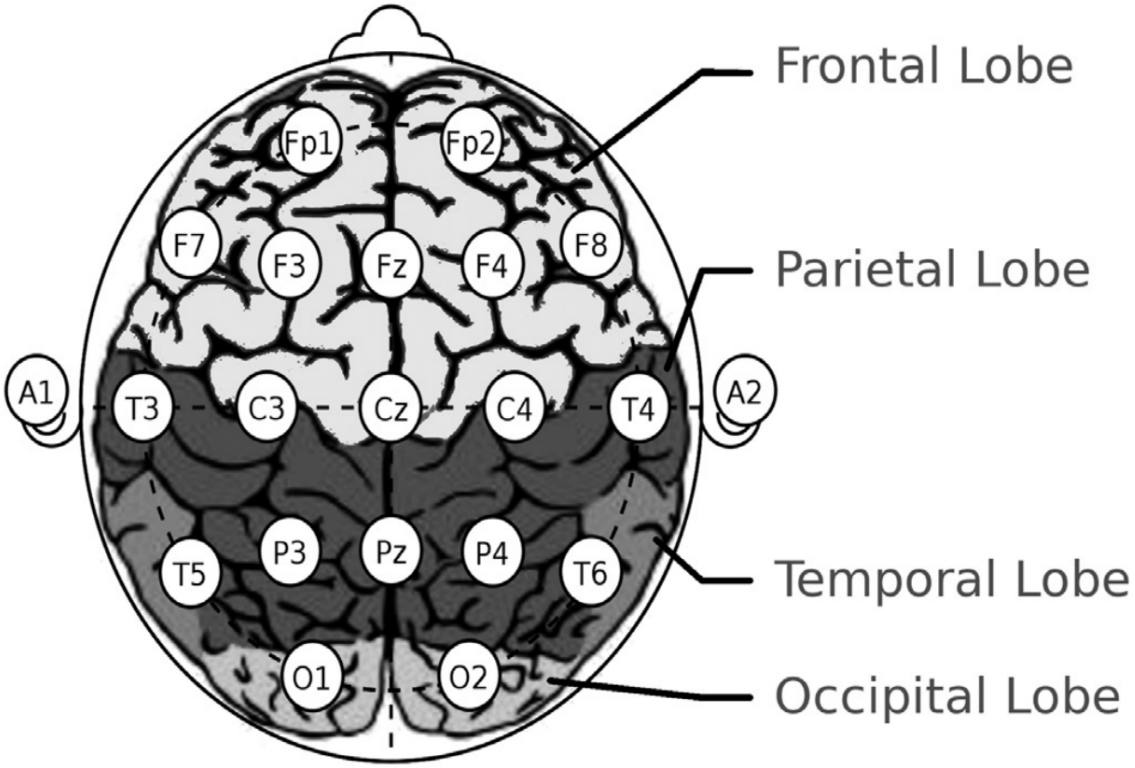


Figure 2.3: EEG Local Channels

Source: [14]

EEG output can be divided into bands defined by their frequency, location, and characteristic behavior. Table 2.2 presents the EEG bands along with the characteristic frequencies. Delta waves are dominant especially in the deep sleep state. They are useful for the detection of diseases and disorders, such as Parkinson's disease, diabetes, and insulin resistance. Theta waves are commonly observed in the front part of the brain. Their activity can be especially observed in idle states, such as hypnosis or light dream phase. They can also be observed within the inhibition of elicited responses, where the subject tries to suppress the reaction to some stimuli.

Alpha waves are mostly associated when the subject is not exposed to visual stimuli (for example, has closed eyes), relaxation state, and suppressed cognitive function[55]. Beta waves are observed to be correlated with one's cognitive activity, especially prominent in the deep concentration state. They can be used to determine whether the subject is calm, intense, or stressed[56]. Gamma waves are especially prominent in cross-modal sensory processing, i.e. when the stimuli are affecting more than one of the subject's senses (e.g. audiovisual stimulation). [39][41]. They are also associated with short-term memory usage, such as matching objects, sounds, or sensations.

Table 2.2: EEG bands and frequencies

Band	Frequency
Delta	1 - 4 Hz
Theta	4 - 8 Hz
Alpha	8 Hz - 12 Hz
Beta	12 - 25 Hz
Gamma	25 - 40 Hz

For some time now, an increasing number of simplified and wearable EEG devices have been available on the market. The main factors of affordability and simplicity, at least compared to the full-scale, medical-grade counterparts, make them an interesting choice to conduct research and expand the current state of the art by both revisiting already published research with such simplified interfaces to evaluate their viability and conducting research topics that have been discarded in the past due to impracticality of traditional EEG interfaces. An example of such a simplified EEG interface is MindWave Mobile 2, produced by the NeuroSky company, which features only one electrode placed above the left eyebrow[7]. The device picture is presented in Figure 2.4. This is the device that will be used throughout this thesis. For the latter purpose, cybersecurity and biometrics are a plausible choice to experiment with newly available hardware.

Figure 2.4: NeuroSky Mindwave Mobile 2

Source: researchgate.net
(access date: 16 Jul 2024)

Figure 2.5: Emotiv MN8

Source: emotiv.com
(access date: 16 Jul 2024)

2.2. Simple Moving Average Algorithm

In cases where the input signal is considered to be noisy, it may be useful to introduce some technique to smooth out the signal and remove the noise that could negatively impact the classifier. One way of performing such a transformation is the Simple Moving Average algorithm[24] - a statistical tool widely employed in time series analysis to smooth out the short-term fluctuations in favor of long-term trends. The core idea is to apply the moving window throughout the signal and calculate the average value of the signal. To achieve it, two parameters must be defined for the algorithm: *windowsize*, which defines how many samples will consitute to one averaged one, and *stepsize*, which will define how many original samples the moving window need to skip to calculate new value. The intuitive visualization of the algorithm is presented in Figure 2.6.

Figure 2.6: Visualization of Simple Moving Average algorithm

Source: optionalpha.com (access date: 29 Aug 2024)

Due to its simplicity and ease of implementation, the Simple Moving Average algorithm is widely used in a variety of domains, such as finance and economics, e.g. for stock price analysis, providing insights into the trends on the market by averaging past prices within a predefined window, thus focusing on the long-term trends instead of the short-term price fluctuations. Within the scientific context, one of the prime goals the algorithm is used for is to filter out the noise from the datasets, improving the quality of the samples and reducing the amount of random variations within the samples. Despite its advantages, the choice of its parameters (window and step size) is critical, as too small window size may not sufficiently filter the noise, while too large window may obscure the trends that were smaller than it. Fine-tuning the parameters of the Simple Moving Algorithm is crucial in this matter.

For example, let us consider the original signal presented in Figure 2.7. After applying the Simple Moving Average algorithm with window size of 4 and step size of 2, the signal will be smoothed out as presented in Figure 2.8.

$$\lambda = [4, 9, 6, 5, 2, 1, 3, 10, 8, 7] \tag{2.1}$$

$$\lambda - example\, signal\, vector$$

Figure 2.7: Signal before applying Simple Moving Average algorithm

$$\begin{aligned} \lambda\prime &= [\frac{\sum_1^w \lambda_n}{w}, \frac{\sum_{s+1}^{s+1+w} \lambda_n}{w}, \frac{\sum_{2s+1}^{2s+1+w} \lambda_n}{w}, ...] \\ &= [\frac{4+9+6+5}{4}, \frac{6+5+2+1}{4}, \frac{2+1+3+10}{4}, \frac{3+10+8+7}{4}] \\ &= [6, 3.5, 4, 7] \end{aligned} \tag{2.2}$$

$$\lambda\prime - signal\, vector\, after\, SMA\, algorithm$$

$$\lambda_n - n - th\, element\, of\, the\, original\, signal\, vector$$

$$w - window\, size$$

$$s - step\, size$$

Figure 2.8: Signal after applying Simple Moving Average algorithm

2.3. ML.NET Library

ML.NET is a free, open source, and cross-platform machine learning framework[4] for the building of ML models that allows one to effortlessly construct, evaluate, and use machine learning models in .NET projects. AutoML is the set of tools within the ML.NET library[3] that allows one to quickly and practically discover the models that perform the best for any given dataset by automatically detecting the input data schema, selecting model parameters, and running each model in a time box window to quickly assert which model would suit the dataset the best. ML.NET also provides the user with a handy "wizard" tool that allows setting up the session via an intuitive user interface, as shown in Figure 2.9. For the datasets that were created within this thesis, AutoML recommended FastTree classifier for binary model[18], and LightGBM classifier for multi-class model. Those are the models that will be explored later on.

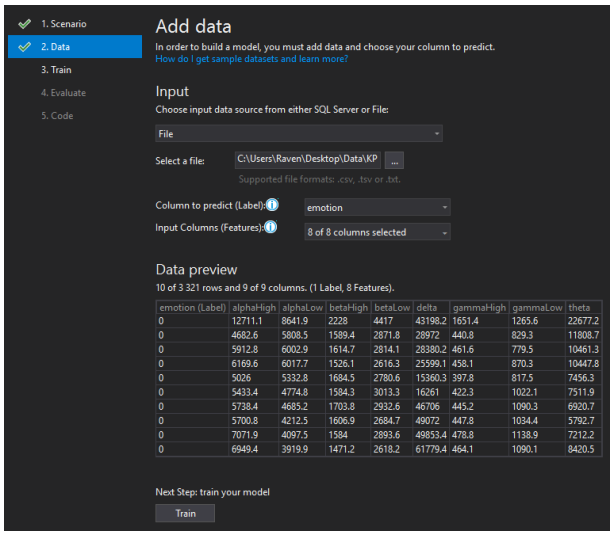


Figure 2.9: AutoML wizard tool

Source: own

Fast Tree Binary Trainer (which for the sake of brevity will be referred to as "Fast Tree" classifier later on) uses the optimized implementation of MART (Multiple Additive Regression Trees) gradient-boosting algorithm. In the learning phase, every decision tree is built via a step-by-step approach, using a predefined loss function to measure the error in every step. The core idea of the MART algorithm is to combine a set of weak models with a stronger model rather than to build a simple optimized one. The algorithm produces new decision trees sequentially by reducing existing residuals. This sequential approach is a type of functional gradient descent[30]. The most important parameters of this classifier from the perspective of this thesis are the number of trees and the learning rate; these are the parameters that will be explored and optimized later on.

Light GBM Multiclass Trainer (which for the sake of brevity will be referred to as "LightGBM" classifier later on) is an implementation of the gradient boosting framework utilizing tree-based learning algorithms [2]. The major advantages of this trainer are faster training and higher efficiency, lower memory usage, better accuracy, support of parallel and distributed learning (even on GPU), and capacity of handling large datasets. The most important parameters of this classifier from the perspective of this thesis are the number of iterations of the algorithm and the learning rate; these are the parameters that will be explored and optimized later on.

Cross-validation is a technique to assess how the classifier results would scale to the independent data set. Although cross-validation can refer to numerous approaches, such as the "leave-p-out" or "k-fold" methods, the experiments within this thesis will utilize the "leave-one-out" variant. Leave-one-out cross-validation is a specific case of the "leave-p-out" method, where the dataset is split into N folds. Then, in each of N iterations, the nth fold takes the role of the test data set, while the rest of the folds act as the training dataset. The validation results are then combined in the end. This method is the acceptable way of reusing data for training and testing purposes without maximizing the chances of a classifier overfitting[53]. The general flow of cross-validation is presented in Figure 2.10.

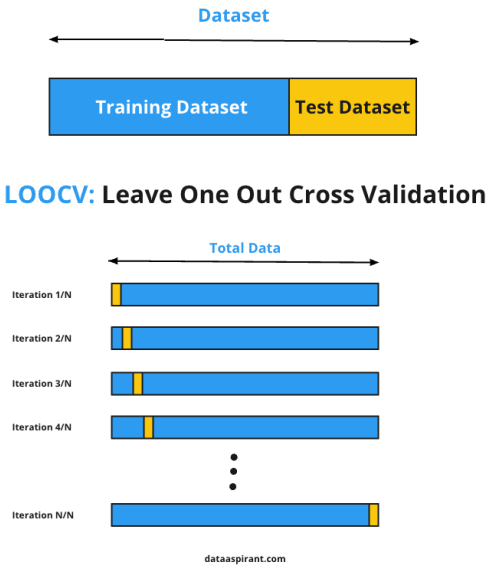


Figure 2.10: Leave-One-Out Cross-Validation

Source: dataaspirant.com (access date: 28 Aug 2024)

2.4. Metrics Used for Classifier Evaluation

A confusion matrix is a useful tool in the evaluation of classification models within the domain of machine learning and statistical classification. Using a specific table layout, it gives insight into the performance of an algorithm, typically a supervised learning one. The matrix is structured with rows representing the true labels and columns representing the predicted labels - each cell in the matrix contains the count of instances that correspond to the actual and predicted labels. The primary diagonal of the matrix, where the actual and predicted labels are the same, presents the number of samples classified correctly; these values are called, respectively, true positives (TP) and true negatives (TN). The off-diagonal represents the samples classified incorrectly, named false positives (FP) and false negatives (FN), displaying the divergence from the true labels. The confusion matrix is essential for deriving many more metrics described in the following, such as precision, recall, F1 score, and accuracy. The analysis of the matrix can be particularly useful in unbalanced datasets, where the sole analysis of singular metrics may be misleading. Examples of binary and multiclass confusion matrices are presented, respectively, in Tables 2.3 and 2.4.

Table 2.3: Example confusion matrix for binary model

		Predicted		
		Positive	Negative	Recall
Truth	Positive	98	74	0.5698
	Negative	9	85	0.9043
	Precision	0.9159	0.5346	

Table 2.4: Example confusion matrix for multi-class model

		Predicted			
		A	B	C	Recall
Truth	A	62	3	55	0.5167
	B	2	89	34	0.7120
	C	4	68	66	0.4783
	Precision	0.9112	0.5563	0.4258	

Precision is defined as the ratio of true positive predictions to the sum of true positive and false positive predictions. It indicates the proportion of correctly identified positive instances out of all predicted positive instances. A high precision value is usually an indicator of the lower rate of samples classified as false positives, which may be crucial in use cases such as medical diagnostics or fraud detection. In an unbalanced dataset where there are only few positive samples, a classifier may easily achieve a high precision value. Intuitively, when the dataset is unbalanced in the other way, a low precision value may prevail. Recall, also known as sensitivity, is one of the other fundamental metrics that indicates the ratio of correctly identified positive samples to all factually positive instances. A recall value of 1 means that all positive samples within the dataset have been correctly classified by the model, while a value of 0 indicates that none of them have been correctly identified. In an unbalanced dataset where there are only few positive samples, a classifier may easily achieve a high recall value by overpredicting the positive label, thus increasing the chance of false positive result. Intuitively, when the dataset is unbalanced in another way, a low precision value may prevail, indicating that the model is underpredicting the positive label. Both metrics are calculated as presented in Figure 2.11. Those two metrics and the correlation between them are intuitively described in Figure 2.12.

$$p = \frac{tp}{tp + fp} \tag{2.3}$$

$p - precision$

$tp - number\,of\,true\,positives$

$fp - number\,of\,false\,positives$

(a) Precision formula in binary model

$$r = \frac{tp}{tp + fn} \tag{2.4}$$

$r - recall$

$tp - number\,of\,true\,positives$

$fn - number\,of\,false\,negatives$

(b) Recall formula in binary model

Figure 2.11: Precision and recall formulas

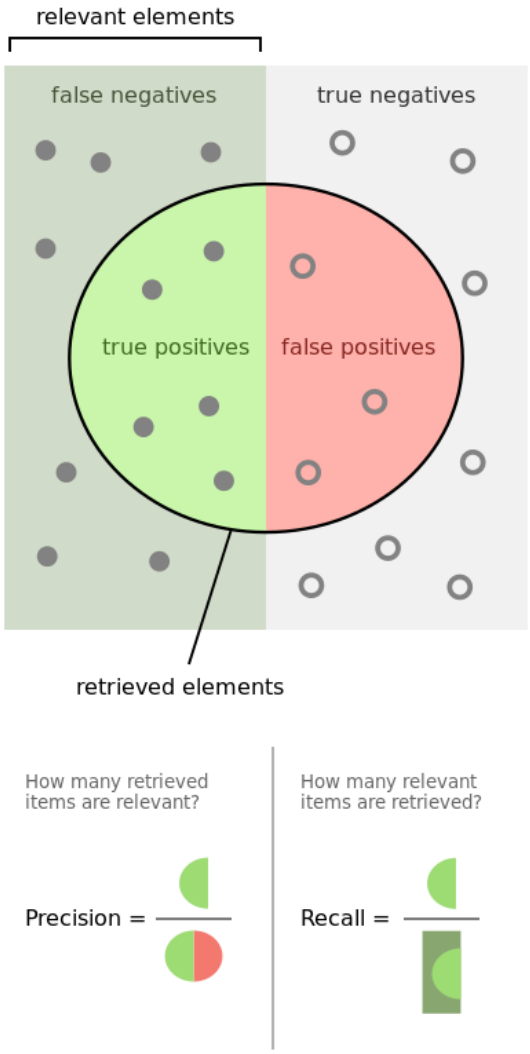


Figure 2.12: Precision and recall

Source: commons.wikimedia.org (Walber - access date: 28 Aug 2024)

Accuracy is defined as the ratio of correctly classified items to the overall number of samples. While it is a straightforward measure tempting to be used as a sole metric for comparison with other classifiers due to the dependency on all values from the confusion metrix, its reliability can be severely compromised in imbalanced datasets. For example, when the dataset contains one dominant label, a model can achieve high accuracy by focusing on this label and neglecting the rest, misleadingly indicating good classifier performance[22]. In addition, noisy data and outliers can skew the metrics, lowering the efficiency of the classifier. While accuracy is a useful metric, it cannot be used for model comparison on its own - a better idea is to compare other metrics as well. The accuracy value is calculated as presented in Figure 2.13. For multi-class models evaluation, the ML.NET library uses macro- and micro-accuracy measures. Micro accuracy is an average metric of the input that all classes have, defined as the fraction of correctly predicted items. This measure does not account for the membership of the class, which means that every tuple of the item and class has the same weight to the metric[5].

$$a = \frac{tp + tn}{tp + fp + tn + fn} \tag{2.5}$$

$$a - accuracy$$

$$tp - number\,of\,true\,positives$$

$$fp - number\,of\,false\,positives$$

$$tn - number\,of\,true\,negatives$$

$$fn - number\,of\,false\,negatives$$

Figure 2.13: Accuracy formula in binary model

Macro accuracy, on the other hand, is defined as the average of accuracy for each predicted class. Similarly to micro accuracy, every class has the equal weight to the metric, regardless of balance (i.e. how many items each class contains) of the dataset[5]. F1 score is one of the F-measures, specifically the harmonic mean of precision and recall of the classifier[62]. It is calculated as presented in Figure 2.14. Combining both precision and recall of the classifier makes it possible to compare models by using only one metric. The value of the metric ranges from 0 to 1, where the value of 1 indicates perfect precision and recall, while 0 indicates the worst possible performance. Within unbalanced datasets, the F1 score can experience some instability and unintuitive behavior; if one of the labels outnumbers another, the classifier may achieve high accuracy by predicting mainly the dominating label, yet the F1 score can be significantly lower due to poor recall of the other label.

$$F_1 = \frac{2}{p^{-1} + r^{-1}} = 2\frac{pr}{p + r} \tag{2.6}$$

$$F_1 - F1\,score$$

$$p - precision$$

$$r - recall$$

Figure 2.14: F1 score formula

In the ML.NET library, the entropy measure is provided for the test-set in binary classifier, based on the ratio of positive and negative instances in the test set[5]. It is calculated as presented in Figure 2.15. It measures the unpredictability of the distribution of the dataset. The ML.NET library uses the entropy measure to evaluate the purity of splits in decision tree classifiers, where a lower value indicates a more homogeneous set of samples, thus improving the accuracy of the predictions. Within the unbalanced datasets, entropy can vary significantly - its value will be low if there is a dominant label, indicating the high predictability of the dataset. Intuitively, if the distribution of data sets labels is more or less equal, the entropy value will be higher, indicating more uncertainty in making a prediction.

$$e = -plog_2(p) - (1-p)log_2(1-p) \tag{2.7}$$

$$e - entropy$$

$$p - proportion\, of\, the\, positive\, class\, in\, test\, set$$

Figure 2.15: Entropy formula

Logarithmic loss in the ML.NET library measures the model's performance while taking into account the divergence of predicted probabilities from the true class label. Contrary to other metrics, the lower log-loss value, the better the classifier - the perfect model predicting a probability of 1 for the true class would have the log-loss value of 0. It is calculated as presented in Figure 2.16. When the probabilities of classifier predictions are close to boundary values of 0 and 1, the metric can achieve an outstanding value due to the nature of logarithmic function near those boundaries. For example, a model predicting the probability of 0.01 will be marked with a higher penalty than the model predicting the probability of 0.99. The focus on probability instead of raw predictions makes the logarithmic loss a measure that ensures that the evaluated classifiers not only predict the correct labels, but also focuses on the probabilities.

$$l = -\frac{1}{m}\sum i = 1^m ln(p_i) \tag{2.8}$$

$$l - log\, loss$$

$$m - number\, of\, items\, in\, test\, set$$

$$p_i - probability\, returned\, by\, classifier$$

Figure 2.16: Logarithmic loss formula

$$Q_\lambda = \frac{\mu_\lambda}{\mu_{\neg\lambda}} = \frac{\frac{\sum^M \lambda_m}{M}}{\frac{\sum^N \neg\lambda_n}{N}} \tag{2.9}$$

$$Q_\lambda - improvement\, ratio$$

$$\mu_\lambda - average\, of\, metric\, in\, classifiers\, containing\, the\, feature$$

$$\mu_{\neg\lambda} - average\, of\, metric\, in\, classifiers\, not\, containing\, the\, feature$$

$$\lambda_m : metric\, of\, the\, classifier\, containing\, the\, feature$$

$$\lambda_n : metric\, of\, the\, classifier\, not\, containing\, the\, feature$$

Figure 2.17: Improvement ratio formula

To designate the importance of each tested feature, it is possible to calculate the improvement ratio for the metric by calculating the ratio of the average metric in classifiers containing the feature to the average metric in classifiers not containing the feature. This value can be calculated for every metric of the classifier, although it may be counterintuitive with the "the lower, the better" metrics. The improvement ratio is calculated as presented in Figure 2.17.

3. Related Works

Electroencephalography (EEG) is a method of recording electrical activity between neurons in the subject's brain. The procedure itself is quite safe, considering that it does not require any invasive action, just placing the electrodes on the scalp of the subject. Recently, an increasing number of simplified and wearable EEG devices are available on the market. Top companies, such as NeuroSky[1] or Emotiv[50], are developing and researching EEG interfaces that are more suitable for everyday commercial use. Given such a fact, along with the interesting characteristics of the EEG, it is an interesting topic to research the possible gains in terms of cybersecurity and biometrics. There is an important distinction between the identification and authentication processes. Identification means that one subject is recognized from the others, that is, their identity is claimed. Authentication means confirming that this identity claim is indeed real and true. Given that there is a system that can successfully authenticate the subject based on EEG readings, it could either replace the traditional username/password authentication approach or support it by being the second authentication factor. Multifactor authentication is an already established and widely adopted process where the user is authenticated via at least two of the factors: something that the user knows (e.g., username/password), something that the user has (e.g., a hardware token or dedicated smartphone app), or something that the user is (biometrics: fingerprint, retinal scan, etc.). Given that, it is worth exploring related works on the subject to extract the valuable information available and to avoid committing the mistakes that already have been done.

Numerous EEG datasets are available to create and train classifiers. They have been summarized in the following. It is worth mentioning that building classifiers on these datasets will be sufficient as long as the experiment does not require recording the EEG signals manually, e.g. while testing a particular EEG device. Goldberger et al.[33] in their work have created one of the most popular datasets that is available publicly, the Physionet motor movement/imagery dataset. It includes records from over 100 volunteers performing various tasks involving motor movement and imagery. The EEG records were recorded from 64 channels sampled at 160Hz. As the dataset provides both baselines of the subjects (e.g., EEG recordings without doing anything), along with having a lot of subjects and sampling channels, it gained the attention of many researchers. The BCI competition datasets were collected by the cooperation of universities and laboratories (Graz University of Technology, University of Tübingen, and Berlin BCI Group, to name a few). Dataset IIIa consists of the records coming from 62 channels sampled at 250Hz while the subjects imagined the movement of body parts (hands, feet, and tongue) according to a cue. It was used by various researches, including Bao et al.[12] among others. Dataset IIa, on the other hand, consists of recordings from 9 subjects, 22 EEG channels, and 3 EOG channels sampled at 250Hz.

Figure 3.1: Distribution of different EEG acquisition protocols in the EEG authentication. Source: [15]

Subjects similarly imagined the movement of both hands, legs, and tongue. It has also been used in numerous papers, e.g., by Lawhern et al.[45]. The Australian EEG database dataset is a result of an 11-year study on EEG recordings of 40 patients at John Hunter Hospital in Australia[37]. The recording was made on a subject who had open, then closed eyes for about 20 minutes. 23 electrodes were used, sampled at 167 Hz. The DEAP dataset[42] is probably the most famous dataset in emotion detection research. However, it was also used in authentication studies[26]. The samples were collected from 32 subjects, using 32 channels sampled at 512Hz. Each subject was presented with 40 one-minute videos that were supposed to invoke emotions such as pride, joy, satisfaction, hope, sadness, and fear.

There are numerous EEG data acquisition protocols; most of them are different from each other due to the stimuli used. They are summarized in the following sections. The distribution of these protocols in the related works is presented in Figure 3.1. Recording resting states is the most popular protocol[15]. The subject is asked to relax, sit in a chair in a quiet, non-disturbing environment for the recording to begin. There are two variants: both eyes open (named "REO") and both eyes closed (named "REC"). Depending on whether the eyes are open or closed, the most efficient EEG channels are those placed in the central region for REO and the parietal region for REC. Moreover, such a protocol is the easiest to implement because the subject does not have any sophisticated instructions to follow. However, it is crucial to have an environment that does not disturb the subject. Visual stimuli, also known as the "Visual Evoked Potential" (VEP), are another acquisition protocol. As the name suggests, they cover a wide range of visual stimuli, such as reading unconnected texts[34], a sequence of pictures that is displayed for a few seconds, or responding to a picture by concentrating or pressing a button. "Rapid Serial Visual Presentation" (RSVP) is yet another protocol in which the sequence of pictures is shown with a high rate (2-10Hz) to minimize the training duration.

Acoustic stimulus is a protocol in which the subject is listening to music or a special tone, however, it is not as common as VEP[15]. Kaur et al.[40] played four different genres of music to subjects that induce different emotions in response. Subjects were asked to provide their preferences for music to use it as a personal identification mechanism. Mental tasks are the protocol in which subjects are asked to imagine some body movements or perform some mental activities. Some studies show that the process of imagining the body movement leads to better results than the similar physical one[15], since physical movement does not interfere with EEG recording. Chuang et al.[23] asked subjects to silently sing a favorite song, count numbers in mind, or concentrate on a desired thought. Compared to visual stimuli, mental task protocols may not need special devices for stimulation, but they still need some simple equipment to initialize the task. There are also works that combine the aforementioned protocols. For example, the subjects are watching short music videos that induce different emotional states. Of course, more combinations are allowed both in count and complexity.

As in various other classifiers, the input EEG signal may be preprocessed prior to feature extraction to enhance the quality of the signal and reduce the noise present. Pre-processing is commonly performed within the three domains: frequency, spatial, and time. As mentioned in the "Theoretical Framework" chapter, the EEG signal frequencies range from 1 to 40 Hz. The band filter is commonly used to split the raw signal from the interface into lower and higher frequencies, classified into the aforementioned bands. To achieve that, a variety of filters may be used, such as the "Butterworth" anti-aliasing filter[10], "Chebyshev" filter with the sharper cut-off frequency[20], and the "Notch" filter that keeps the higher frequency below 50 to 60 Hz to remove artifacts from the power line [27]. Along with categorization of the data, some of them may be dropped before feature extraction; for example, some of the bands may be excluded from the classifier after all. In terms of spatial domain filtering, which is especially applicable when an interface with a large number of electrodes is used[14], the commonly used filters are the Common Average Referencing filter subjecting the signal from each electrode to the mean of all[46], the Independent Component Analysis filter intended to remove artifacts caused by stimuli such as eye and muscle movement[11], and the Laplacian filter that enhances local activities compared to diffused ones[44]. Finally, in the time domain, commonly used filters are Ensemble Averaging that requires multiple recordings in the same setup to reduce noise[31] and Baseline Removal that requires the recording of the rest state before presenting the stimuli [19].

Walaa et al. [9] developed the classifier for EEG-based identification and authentication and demonstrated its potential for high-security applications. Traditional biometric modalities, such as fingerprints and facial recognition, are susceptible to spoofing, whereas EEG signals offer a more secure alternative due to their complexity and sensitivity to mental states1. Existing EEG-based recognition methods often rely on extensive channels and long recording durations, which limit their practicality. However, recent studies have introduced lightweight convolutional neural network (CNN) models that address these limitations. A notable contribution is the development of a robust EEG-based recognition system utilizing a lightweight CNN model with a minimal number of learnable parameters.

This system achieves high accuracy with only two EEG channels and a recording length of 5 seconds, making it feasible for real-life security applications. The system was validated using benchmark datasets from the public domain, achieving a rank-1 identification accuracy of 99% and an equal error rate (EER) of 0.187%. These results underscore the efficacy of EEG signals for both identification and authentication tasks, highlighting their potential for integration into high-level security systems. While their work is promising, achieving more than satisfying results and overall indicating the possibility of using EEG in authentication processes, it uses already-existing datasets created by using the traditional interfaces.

Cheng et al. [21] explore a biometric authentication system that integrates electroencephalography (EEG) along with eye movement data to improve security against shoulder-surfing attacks. The interface employs 64 electrodes to capture brain activity, providing a high-resolution signal that is crucial for accurate user identification. The study demonstrates that combining EEG data with eye movement patterns significantly improves the robustness and reliability of the authentication process. The results indicate that the hybrid approach not only enhances security, but also maintains user convenience. The system's accuracy in distinguishing between legitimate users and impostors is markedly higher compared to traditional methods, reaching the average accuracy of 84.36%. This is attributed to the unique and complex nature of EEG signals, which are difficult to replicate or spoof. The research highlights the potential of hybrid BCI systems in developing secure and user-friendly authentication mechanisms, paving the way for future advancements in biometric security technologies. While this research is promising, it uses the interface with 64 electrodes, along with additional eye tracking.

Hernández et al. [36] investigated the use of biometric authentication systems based on EEG, emphasizing the development of a proprietary dataset using the Emotiv Epoc+ headset with 18 electrodes. The dataset comprises EEG signals from 39 volunteers, collected under controlled conditions. The study explores both one-class and multi-class classifiers for user authentication, introducing Isolation Forest and Local Outlier Factor models as new tools for this purpose. The authors compare these models with traditional multi-class models like Support Vector Machines, Random Forest, and k-Nearest Neighbors. The results indicate that while the multi-class models generally achieve higher accuracy, one-class models like IF and LOF are more practical in scenarios where data from impostors are unavailable. The study highlights the importance of high-frequency EEG components, particularly gamma waves, in achieving effective authentication. The authors also propose a hybrid system that combines one-class and multi-class models, which improves the performance of one-class models by leveraging multi-class algorithms. The metrics used to evaluate the models include precision, recall, F1 score, accuracy, and false positive rate (FPR). The study finds that the hybrid system achieves a precision of 91.1%, a recall of 75.3%, and an accuracy of 82.3%, demonstrating a balanced trade-off between security and usability. The research underscores the potential of EEG-based biometric systems for secure and user-friendly authentication, paving the way for future studies to incorporate additional biometric features and deep learning techniques. Although the authors developed their own dataset on somehow simplified interface and the results indicate that EEG could definitely be used for authentication purposes, it is still worth considering evaluating the 1 electrode interface.

Stergiadis et al. [61] present the EEG-based user authentication system that addresses the limitations of conventional biometric methods. The authors developed their own dataset using the EGI Geodesic EEG System (GES) 300 interface, which includes 128 electrodes distributed across the scalp. This setup ensures high-quality EEG recordings, essential for accurate biometric authentication. The study focuses on extracting power spectral features from three central electrodes (Fz, Cz, Pz) across all EEG bands. The authors highlight the advantages of EEG-based authentication, such as its resistance to spoofing. The mean accuracy of the system of 95. 6% demonstrates its potential for real-time applications and the general possibility of using EEG within authentication models. The study also compares various classification algorithms and emphasizes the importance of selecting the optimal algorithm for each individual user. This personalized approach improves the reliability and efficiency of the system.

4. Methodology

The following chapter explains the methodology used to perform the research required in this thesis. First, the interface is described in a more technical manner, such as the frequency of sampling, the interpretation of provided data units, and the structure of the software responsible for retrieving raw data from the interface and storing it securely in a local file. Next, two datasets have been described that have been created for the purpose of this thesis. Each of them describes the statistics of the research group, the setup of the data gathering station, along with the descriptions of the steps a subject had to follow throughout the procedure. Afterwards, the general flow of the experiment has been presented, with the high-level steps required to properly train and evaluate the classifier. Lastly, it is strictly correlated with the proposed testing framework, allowing quick algorithm implementation swaps without the need to adjust the existing codebase.

4.1. Working with the Interface

To collect the EEG data from the subject and save them in a file, software was needed to connect to the ThinkGear firmware provided by the vendor, transform the data into the desired format, and then write it out to the file that can later be included in the dataset. NeuroSky ThinkGear software is responsible for maintaining the Bluetooth connection between the device and the machine running the software, while exposing the technology- and device-agnostic API for developers to consume the data. The simplified flow of the data collection application is presented in Figure 4.1.

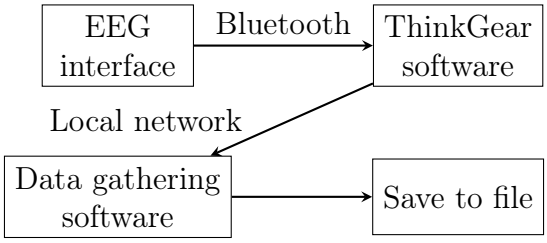


Figure 4.1: Data gathering connection diagram

The core of the MindWave Mobile 2 interface is the application-specific integrated circuit (ASIC) chip, specially designed for the purpose of EEG data processing. The ThinkGear AM (TGAM) chip collects the data from the sensor placed right above the left eyebrow, while using the ear clip as a reference to filter out any noise generated by either the environment (like electrical/electronic devices, background noise, etc.)[8] or the subject's own body.

While the TGAM chip produces the raw output EEG data at the measurement frequency of 512 Hz, the developer is presented with the already processed information at 1 Hz, such as:

- divide the raw data by frequency into well-known bands (alpha, beta, gamma, delta, and theta),
- define signal strength and quality,
- provide three eSense measures developed by NeuroSky: Attention, Meditation and EyeBlink detection.

ThinkGear software, which allows the developer to access data from the NeuroSky MindWave Mobile 2 device, provides the data using its own proprietary units[6] that indicate the relative amplitudes of the individual EEG bands. The TGAM chip applies the set of transforming and rescaling operations to the original voltage measurements, which are volts squared per Hz - see Figure 4.2. According to the vendor, there is no simple linear correlation between raw and processed units, and therefore they encourage the unit to be labeled $ASIC\_EEG\_POWER$.

$$ASIC\_EEG\_POWER = \frac{V^2}{Hz} \tag{4.1}$$

Figure 4.2: TGAM proprietary measurement unit

The EEG data collected from the TGAM chip consists of eight measures[13]:

- Delta (1 - 4 Hz)
- Theta (4 - 8 Hz)
- Low alpha (8 - 10 Hz)
- High Alpha (10 - 12 Hz)
- Low beta (12 - 17 Hz)
- High Beta (17 - 25 Hz)
- Low gamma (25 - 40 Hz)
- High gamma (40 - 50 Hz)

Both datasets described in the following sections consist of the same set of the following features, sampled at 1 Hz from the vendor interface.

- EEG bands:
  - Alpha (low + high)
  - Beta (low + high)
  - Gamma (low + high)
  - Delta
  - Theta
- eSense data:
  - Attention
  - Meditation

4.2. Datasets Developed for Experiments

Given the relatively young age of the simplified EEG interfaces, no viable public datasets could be found that would fit the experiment; thus the need for data gathering. To collect the required data, a station was assembled that would consist of specific stress-inducing stimuli required for the experiment, the monitor screen to expose the subject to audiovisual stimuli, and the Neurosky Mindwave Mobile 2 EEG interface to record the EEG data. The flow of the data gathering session is presented in Figure 4.3.

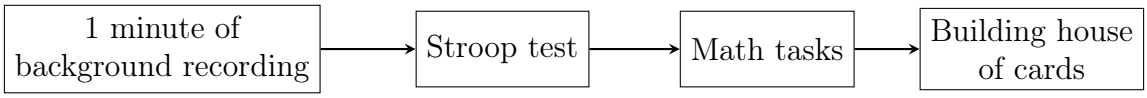


Figure 4.3: "Stress" dataset data gathering flow

The experiment begins with a 1-minute recording of the subject in the resting state, without prior exposure to stress stimuli. After that, three sessions are begun that were designed to induce stress in the subject in a humane way. In the first session, the subject was asked to perform the "Stroop test"[52], which presents the subject with a word representing some color, displayed in a different color. The subject is required to pick the "meant" color, not the displayed one, from the set of colors underneath. Figure 4.4 presents the application used. To increase the likelihood of stressing the subject, everyone was told to achieve the highest possible score.

Figure 4.4: Stroop test

Source: memorize.link (access date: 30 Aug 2024)

In the second session, the subject was presented with a series of 10 math equations to solve, ranging from the most basic ones (involving addition and subtraction), to more complex ones (several multiplication, division, and expontentation operations). The difficulty of the tasks has been kept within the scope presented, to not exclude any of the subjects due to their mathematical skills. This approach seems warranted, as the dataset have been built with the stress data in mind, not correctly solving the tasks. In the third session, to expand the research on stress detection to movement as well, subjects were asked to stack the highest possible stack of cards. Given that this is the exercise that requires focus and fine motor skills, it should be a relevant addition to the "Stress" dataset. The dataset is based on data collected in 2023 from 23 subjects (5 women, 18 men), aged 18 to 49 years. The data set is collectively 100,000 seconds long in terms of recording and consists of the features described above.

To collect the data required for the "Login" dataset, a station was assembled that would present the subject with the set of specific scenarios required for the particular experiment, the monitor screen and headphones to expose the subject to audio stimuli, and the Neurosky Mindwave Mobile 2 EEG interface to record the EEG data. The flow of the data gathering session is presented in Figure 4.5.

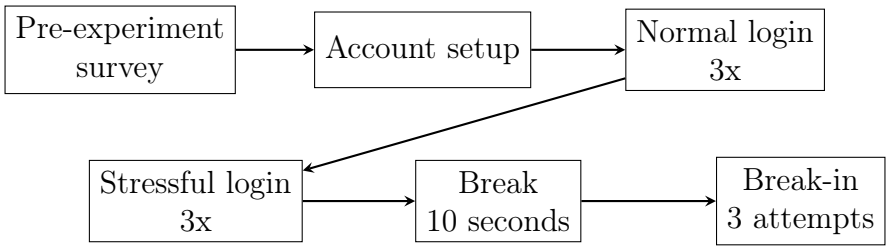


Figure 4.5: "Login" dataset data gathering flow

In the beginning, the subject is presented with the pre-experiment survey collecting the data such as age and sex. No data that could possibly identify the subject later in the dataset has been collected. Figure 4.6 presents the survey phase of the application. After that, the EEG recording begins.

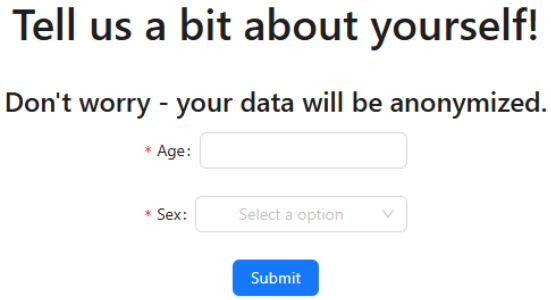


Figure 4.6: "Login" dataset - survey

Source: own

In the next phase, the subject is presented with the screen requiring them to set up an account within the test system. They are asked to do it as it would be any normal service they log into every day. Afterwards, the subject is asked to perform the normal log-on action three times in a row. The registration and log-in screens are presented respectively by Figures 4.7 and 4.8.

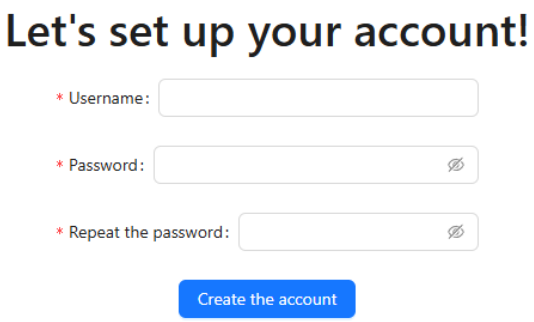


Figure 4.7: "Login" dataset - account setup

Source: own

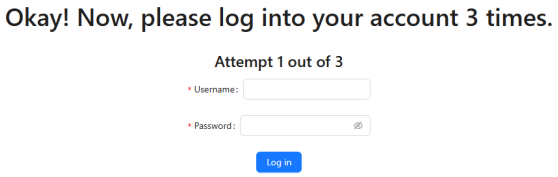


Figure 4.8: "Login" dataset - account setup

Source: own

After successful log-on actions, another three are required from the subject. This time, they are meant to induce stress within the subject. The first one is performed with the presence of audio stimuli, which is playing two tones simultaneously, respectively, at 853 Hz and 960 Hz[48]. These frequencies are not chosen at random, but chosen on purpose - the original idea has been borrowed from the Emergency Alert System in the USA, where the sound of the "attention signal" has been defined as exactly those two frequencies due to their unpleasantness. The next stress-inducing log-on action is accompanied by three quickly disappearing popups displayed after 500 milliseconds after loading the page, in intervals of 250 milliseconds. The last log-on action is meant to be a placebo stimulus, because the subject now expects some stress-inducing situation, while nothing actually happens. Afterwards, the subject is allowed to rest for 10 seconds. As for the last phase of data collection, the subject is asked to perform a break-in to someone else's account. It is important to keep in mind that this is a test setup, so no illegal action is performed here - the subject is not actually breaking in anywhere. There are three attempts here, with two first being rejected, and the last one accepted, regardless of the input data. The "Login" dataset" is based on data collected in 2024 from 27 subjects (9 women, 18 men), aged 22 to 49 years. The data set is collectively 4,000 seconds long in terms of recording and consists of the same features as the "Stress" dataset.

The development of the aforementioned datasets required the participation of human subjects willingly and knowingly attending the experimental procedure. To underscore the ethical manners and compliance of the methodology with established standards, the research has received the approval of the Committee for Research Ethics, thus validating the integrity and ethical principles of data collection processes, minimizing the potential risks to the subjects, and guaranteeing the privacy of the data for all stakeholders. The opinion of the Committee for Research Ethics has been attached as Appendix A. Submitting such a request for opinion requires a number of attachments, such as the request itself, containing the details necessary for the Committee to reach a decision (Appendix B); the description of the research, including the legal and ethical aspects (Appendix C); consent form presented to the subject outlining the details of the experiment, along with notices of data privacy and the possibility to exit the study at all times (Appendix D); the safety and regulations certificate from the interface vendor (Appendix E).

4.3. General Experiment Flow and Testing Framwork

Although different experiments may differ from each other, the common part between them is the flow of the experiment, as presented in Figure 4.9. Every experiment needs to be based on some dataset; in this instance, the "Stress" and "Login" datasets will be used. After that, pre-processing will be applied, as a method of input filtering or data transformation, such as frequency filters, signal smoothers, etc. Afterwards, the feature extraction begins, with the purpose of transforming the samples into feature vectors with labels. This set of feature-label tuples will later be used to train the chosen classifier model. In the end, the classifier results will need to be validated. The classifier metrics, such as F1 score, accuracy, precision, recall, log loss, confusion matrices, etc, will be used to assess the classifier, along with the comparison between the developed models.

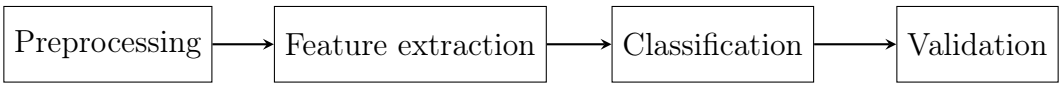


Figure 4.9: General experiment flow

To make it easier to test the variations of the classifier, a custom testing framework has been developed. The general flow explained above has already been implemented in a reusable way, leaving only to the user the possibility to specify fragments to test, which consists of preprocessors - fragments of code that transform the input data before it has the features extracted; feature extractors - fragments of code that transform data into classifier-acceptable data points; and classifiers - fragments of code that represent ML.NET classifier models to explore. To describe it formally, the singular experiment consists is a tuple of sets and the framework will run all possible combinations of the fragments specified above and collect the results, as presented in Figure 4.10.

$$E = \{P, F, C\} \tag{4.2}$$

$$E - experiment$$

$$P - set\,of\,preprocessors$$

$$F - set\,of\,feature\,extractors$$

$$C - set\,of\,classifiers$$

(a) Experiment formula

$$R = \forall p \in P, \forall f \in F, \forall c \in C, e(p, f, c) \tag{4.3}$$

$$R - experiment\,run$$

$$P - set\,of\,preprocessors$$

$$F - set\,of\,feature\,extractors$$

$$C - set\,of\,classifiers$$

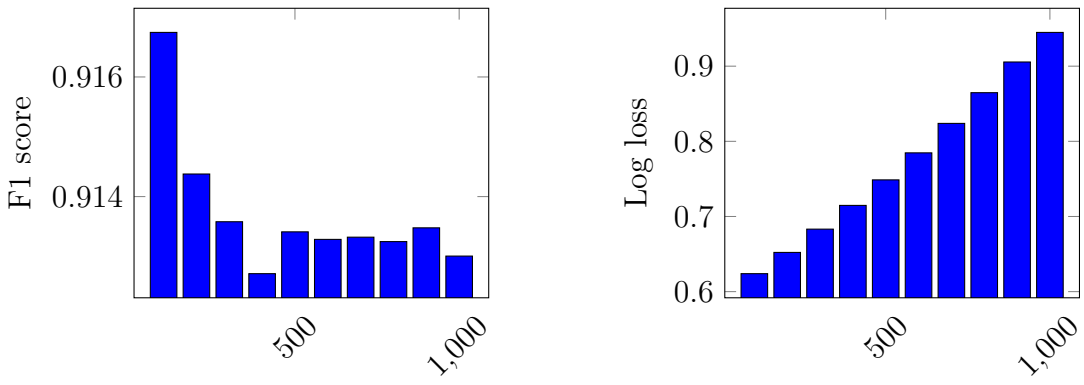
$$e - experiment\,execution\,function$$

(b) Experiment run formula

Figure 4.10: Experiment formulas

5. Stress Detection Classifier Based on "Stress" Dataset

The classifier built in this chapter uses the "Stress" dataset described above. Given that a full brute-force approach would take a long time without guaranteeing error-proof code, this chapter describes the step-by-step approach taken to fine-tune the parameters of the classifier. First, the impact of number of trees is explored within the Fast Tree classifier to locate the optimal value. A similar approach is used for the learning rate. Afterwards, within the parameters defined in the previous steps, the improvement ratio is calculated for all EEG bands, along with the Attention and Meditation measures, to determine the importance of the features used to build the classifier. Next, the preprocessing approach is defined. Firstly, the poor signal level preprocessor is evaluated to determine how dismissal of samples with this metric being less than or equal to the predetermined value will impact the performance of the classifier. It is followed by applying the Simple Moving Average algorithm preprocessor and evaluating its impact on the classifier relative to the size of the window and the step of the algorithm. Finally, the classifier is evaluated with the metrics provided by the ML.NET library, as well as the improvement ratios of the features used to build it. At the end of the chapter, conclusions are drawn from the final results.



(a) F1 score

(b) Log loss

Figure 5.1: Finding optimal number of trees

5.1. Finding Optimal Parameters of Fast Tree Classifier

To find the optimal number of trees, 10 tests have been run, respectively, from 100 to 1000 trees with a step of 100. The results have been presented in Table 5.1 and Figure 5.1. Log loss seems to be linearly correlated with the number of trees, throughout values from 0.623914 to 0.944914, so it is not suitable to determine which number of trees is the best for this problem. However, the F1 score metric seems to be helpful here. The smallest tested number of trees of 100 seems to be the best suited value for the classifier, however, not by a high margin, having the lowest value of 0.913580 and the highest value of 0.916745. Given that this is the best result achieved within this experiment run, it will be used throughout the rest of the steps within this experiment.

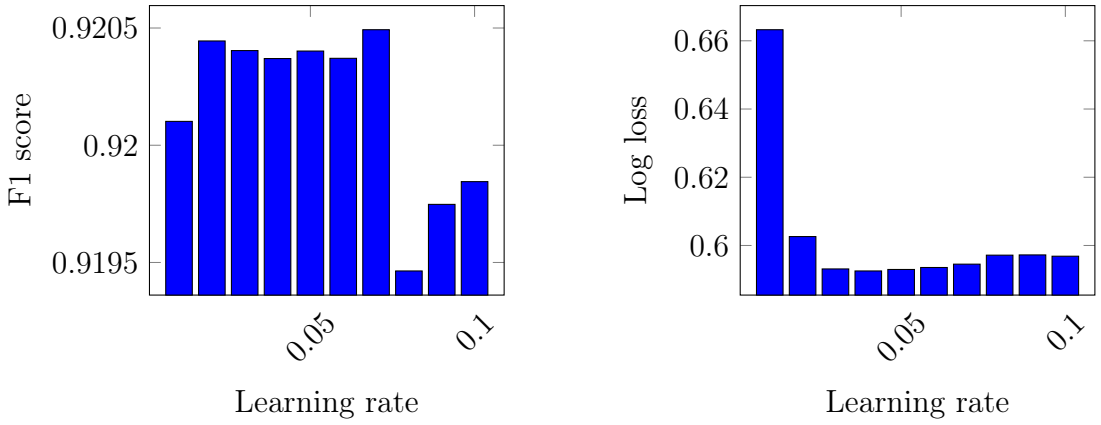
Table 5.1: Finding optimal number of trees

# Trees	F1 score	Log loss
100	0.916745	0.623914
200	0.914378	0.652181
300	0.913580	0.683166
400	0.912712	0.714742
500	0.913411	0.748701
600	0.913285	0.784658
700	0.913322	0.823859
800	0.913248	0.864724
900	0.913478	0.905565
1000	0.913006	0.944914

To find the optimal learning rate, 10 tests have been run, respectively, from a learning rate of 0.01 to 0.1 with a step of 0.01. The results have been presented in Table 5.2 and Figure 5.2. Log loss strongly indicates that the learning rate of 0.01 is the worst possible within the tested range, throughout values from 0.592529 to 0.663249. However, the F1 score metric, together with the log loss score, indicates that the best suited learning rate value for the classifier lies between 0.02 and 0.04, but again not by a high margin, having the lowest value of 0.919464 and the highest value of 0.920493. Given that these are the best results achieved within this experiment run, the learning rate of 0.02 will be used throughout the rest of the steps within this experiment.

Table 5.2: Finding optimal learning rate

Learning rate	F1 score	Log loss
0.01	0.920102	0.663249
0.02	0.920445	0.602610
0.03	0.920404	0.593121
0.04	0.920370	0.592529
0.05	0.920402	0.592965
0.06	0.920371	0.593543
0.07	0.920493	0.594525
0.08	0.919464	0.597160
0.09	0.919748	0.597231
0.10	0.919845	0.596852



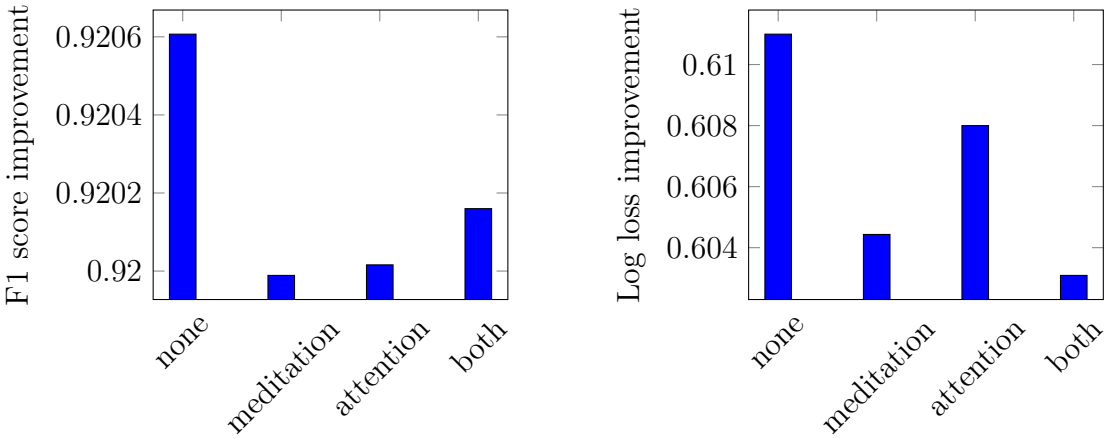
(a) F1 score

(b) Log loss

Figure 5.2: Finding optimal learning rate

5.2. Finding Improvement Ratios of EEG Bands, Attention, and Meditation Measures

To calculate the improvement ratio of Attention and Meditation measures, as described above, ratios of respectively F1 scores and log losses have been calculated. The results have been presented in Table 5.3 and Figure 5.3. The results for both F1 score and log loss metrics seem to indicate that the Attention and Meditation measures do not have measurable impact on the classifier - while the F1 score indicates that the classifier might perform worse with those features included, ranging from 0.919989 to 0.920607, the log loss metric indicates otherwise, ranging from 0.603092 to 0.610997. Given that the Attention and Meditation measures seem to be virtually ineffective within this experiment run, they will not be used throughout the rest of the steps within this experiment.



(a) F1 score

(b) Log loss

Figure 5.3: Finding Attention/Meditation improvement ratios

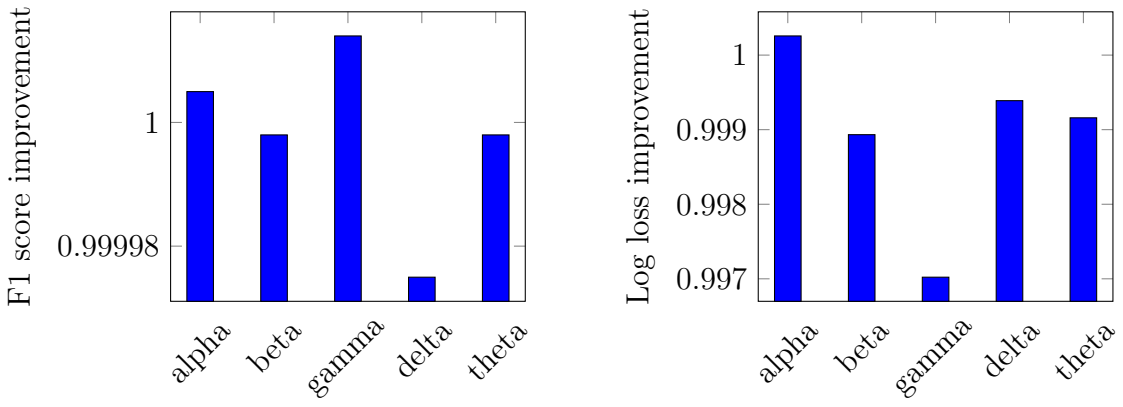
Table 5.3: Finding Attention/Meditation improvement ratios

Attention included	Meditation included	F1 score	Log loss
No	No	0.920607	0.610997
No	Yes	0.919989	0.604434
Yes	No	0.920016	0.608001
Yes	Yes	0.920160	0.603092

To calculate the improvement ratio of EEG bands, as described above, ratios of respectively F1 scores and log losses have been calculated. To simplify the experiment, five whole bands have been used (alpha, beta, gamma, delta, theta), without distinction to the high/low classification that are specific to MindWave interface. The results have been presented in Table 5.4 and Figure 5.4. The results for both F1 score and log loss metrics seem to indicate that within a margin of error, there are no dominating EEG bands in this experiment run - while the F1 score, ranging from 0.999975 to 1.000014, may indicate the gamma band as the most important one and the delta band as the least important, the log loss metric, ranging from 0.997002 to 1.000257, seems to agree regarding the gamma band being the best one, but indicates alpha as the worst one. Given that none of the EEG bands seem to be significantly more important than the others within this experiment run, none of them will be dropped throughout the rest of the steps within this experiment.

Table 5.4: Finding EEG bands improvement ratios

Band	F1 score improvement	Log loss improvement
Alpha	1.000005	1.000257
Beta	0.999998	0.998933
Gamma	1.000014	0.997022
Delta	0.999975	0.999389
Theta	0.999998	0.999159



(a) F1 score

(b) Log loss

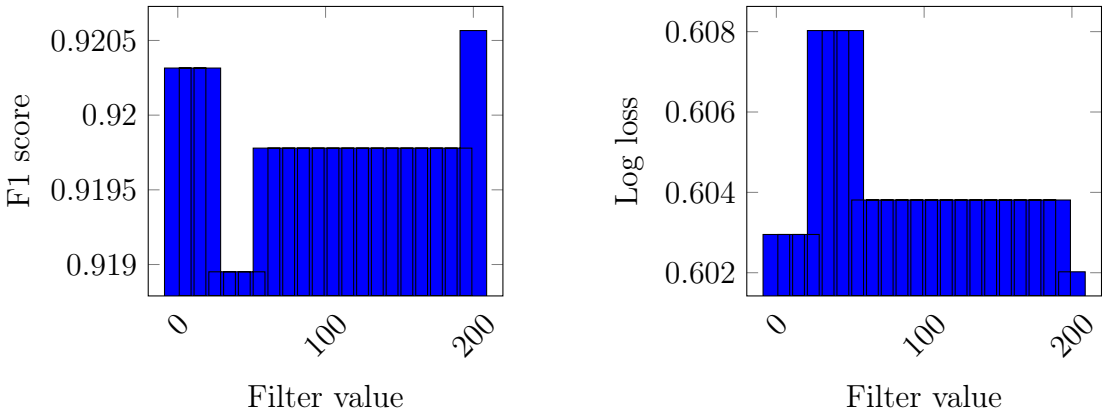
Figure 5.4: Finding EEG bands improvement ratios

5.3. Finding Optimal Preprocessors Parameters

To find the optimal poor signal level filter threshold, 21 tests have been run, respectively, from a value of 0 to 200 with a step of 100. The results have been presented in Table 5.5 and Figure 5.5. The results for both the F1 score and the log loss metrics seem to consistingly indicate the threshold of the poor signal level filter of 20 is the best suited for this classifier while retaining most of the samples. While both of the measures seem not to be linearly correlated with the filter value, both classifiers seem to perform the best with the filter value of 200, with the F1 score and log loss respectively of 0.920566 and 0.602023, thus accepting all samples, these measures are not significantly lower for the filter value of 20, with the same metrics being the value respectively of 0.920315 and 0.602952. Given that the best filter value, while retaining most samples, is the value of 20, it will be used throughout the rest of the steps within this experiment.

Table 5.5: Finding optimal poor signal level filter

Worst acceptable level	F1 score	Log loss
0..20	0.920315	0.602952
30..50	0.918951	0.608027
60..190	0.919779	0.603810
200	0.920566	0.602023



(a) F1 score

(b) Log loss

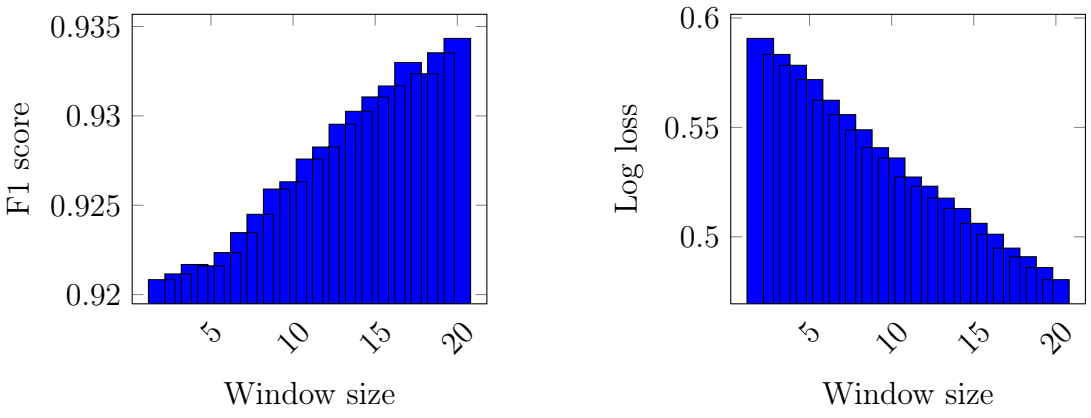
Figure 5.5: Finding optimal poor signal level filter

To find the optimal window size for the Simple Moving Average algorithm, 19 tests have been run, respectively, from a value of 2 to 20 with a step of 1. The results have been presented in Table 5.6 and Figure 5.7. The results for both the F1 score and the log loss metrics seem to improve linearly in relation to the window size of the algorithm, the F1 score metric ranging from 0.920835 to 0.934331 and the log loss metric ranging from 0.480417 to 0.590632. While higher values of window size may benefit the performance of the classifier, practical reason dictates that there should be a reasonable limit for the window size. Given that reasoning, the window size of 5 will be used throughout the rest of the steps within this experiment.

Window size	F1 score	Log loss
2	0.920835	0.590632
3	0.921156	0.583311
4	0.921685	0.578372
5	0.921606	0.571823
6	0.922349	0.562396
7	0.923465	0.555819
8	0.924491	0.548891
9	0.925905	0.540694
10	0.926308	0.536013

Window size	F1 score	Log loss
11	0.927584	0.527309
12	0.928255	0.523116
13	0.929530	0.517665
14	0.930253	0.512938
15	0.931057	0.506151
16	0.931669	0.501174
17	0.932986	0.494834
18	0.932356	0.490890
19	0.933527	0.485972
20	0.934331	0.480417

Figure 5.6: Finding optimal Simple Moving Average window size



(a) F1 score

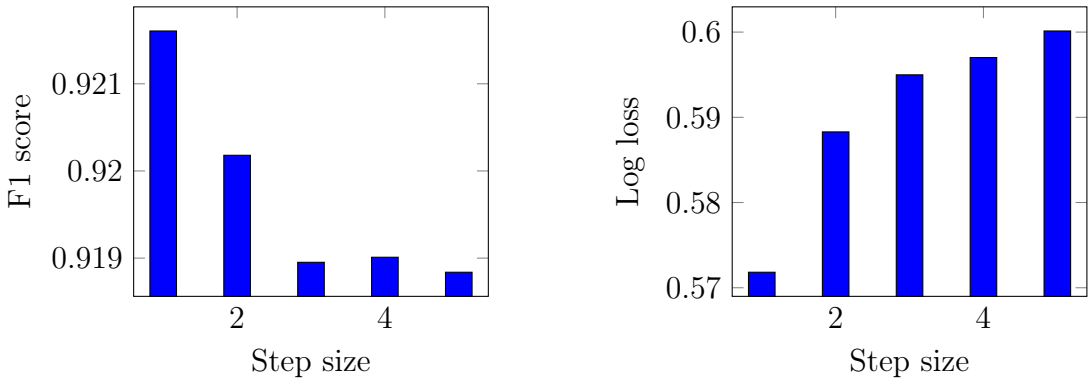
(b) Log loss

Figure 5.7: Finding optimal Simple Moving Average window size

To find the optimal step size for the Simple Moving Average algorithm, 5 tests have been run, respectively, from a value of 1 to 5 with a step of 1. The results have been presented in Table 5.6 and Figure 5.8. The results for both the F1 score and the log loss metrics seem to indicate an inverse linear correlation between the efficiency of the classifier and the step size of the Simple Moving Average algorithm. This is not unexpected, as the larger step size effectively limits the number of samples which the classifier can use. In this case, both the F1 score metric ranging from 0.918838 to 0.921606 and the log loss metric ranging from 0.571823 to 0.600131 suggest that the step value of 1 is the best suited in this classifier. Given that the step value of 1 seems to have the best outcome for the classifier, it will be used throughout the rest of the steps within this experiment.

Table 5.6: Finding optimal Simple Moving Average step size

Step size	F1 score	Log loss
1	0.921606	0.571823
2	0.920180	0.588288
3	0.918952	0.594984
4	0.919010	0.597011
5	0.918838	0.600131



(a) F1 score

(b) Log loss

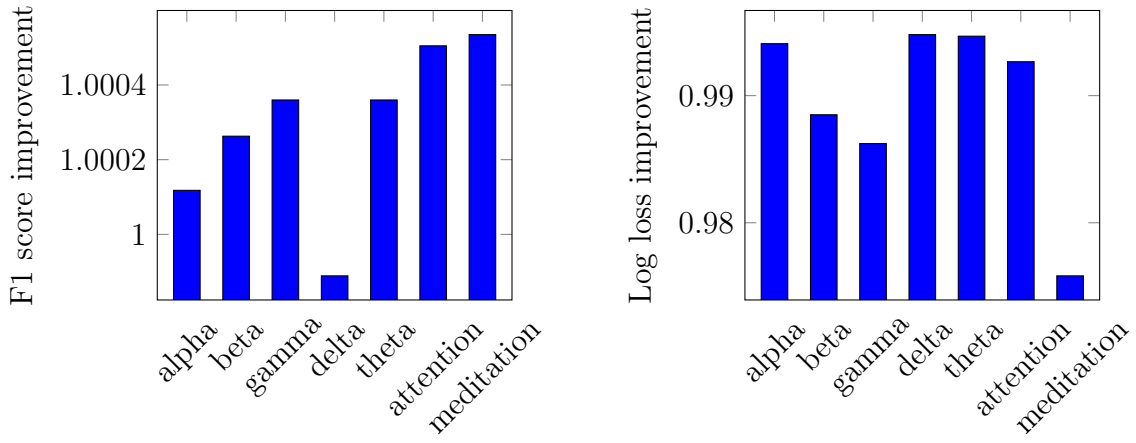
Figure 5.8: Finding optimal Simple Moving Average step size

5.4. Evaluating the Classifier

To finally evaluate the classifier, the ratios of, respectively, F1 scores and log losses have been calculated. The results have been presented in Table 5.7 and Figure 5.9. It seems that introducing the used preprocessing steps made the Attention and Meditation features more important within the classifier, while the delta band is still the least improving feature. The improvement of F1 score metric ranges between 0.999889 and 1.000535, while the improvement of log loss metric ranges between 0.975825 and 0.994802. Although the differences are not by a large margin, they still bring important insights to the classifier.

Table 5.7: Finding features improvement ratios

Feature	F1 score	Log loss
Alpha	1.000118	0.994089
Beta	1.000263	0.988497
Gamma	1.000360	0.986231
Delta	0.999889	0.994802
Theta	1.000360	0.994678
Attention	1.000505	0.992669
Meditation	1.000535	0.975825



(a) F1 score

(b) Log loss

Figure 5.9: Finding features improvement ratios

The final classifier metrics are presented in Table 5.8. The confusion matrix is presented by Table 5.9. Reaching the F1 score of 0.921606 is a satisfactory result of this classifier. While the classification is not perfect, the brief analysis of confusion matrix indicates that while taking wrong predictions, the classifier tends towards the false positive error rather than the false negative one, having precision and recall respectively of 0.857198 and 0.996541. Taking into account the topic of this thesis and potential cybersecurity applications, it is better for the classifier to falsely mark the subject as stressed and potentially deny access to sensitive data or systems than to grant such access by mistake.

Table 5.8: Stress detection classifier metrics

Metric	Value
F1 Score	0.921606
Log loss	0.571824
Entropy	0.602991

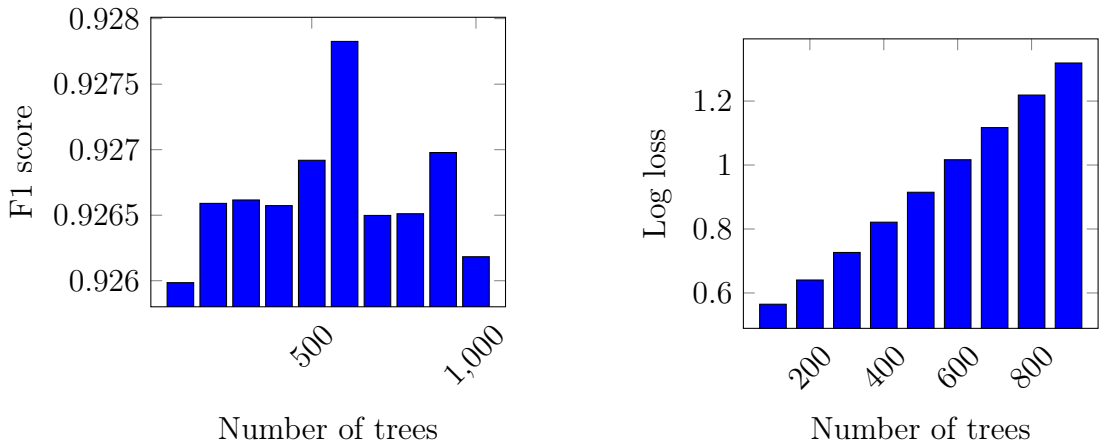
Table 5.9: Stress detection classifier confusion matrix

		Predicted		
		Positive	Negative	Recall
Truth	Positive	8932	31	0.996541
	Negative	1488	62	0.040000
	Precision	0.857198	0.666667	

The classifier built in this chapter has been using the "Stress" dataset described above and has been fine-tuned to evaluate the best possible performance. First, the model parameters have been evaluated and it has been determined that the best parameters are 100 trees and the learning rate of 0.02. Subsequently, the improvement ratios of the EEG bands and the Attention and Meditation features were calculated. It has been made clear that no feature has significantly improved the classifier. For the preprocessing part, the poor signal level filter value has been set to 20. Applying the Simple Moving Average algorithm preprocessor to the data revealed intuitive insight of the changes in the parameters. While increasing the window size almost linearly improves the classifier performance, having more data in the domain of time within one sample and removing potential noise, increasing the step size linearly decreases the classifier performance, having fewer samples to train and validate the classifier on. The results of the classifier evaluation, with an F1 score of 0.921606, are satisfactory. The brief analysis of confusion matrix indicates that the classifier tends towards the false-positive error rather than the false-negative one, having precision and recall, respectively, of 0.857198 and 0.996541. Given the topic of this thesis and potential cybersecurity applications, it is better for the classifier to return the false positive prediction rather than the false negative one.

6. Stress Detection Classifier Based on "Login" Dataset

The classifier built in this chapter uses the "Login" dataset described above. Similarly to the stress detection research, the full brute-force approach would take a long time without guaranteeing error-proof code, so this chapter describes the step-by-step approach taken to fine-tune the parameters of the classifier. First, the impact of number of trees is explored within the Fast Tree classifier to locate the optimal value. A similar approach is used for the learning rate. Afterwards, within the parameters defined in the previous steps, the improvement ratio is calculated for all EEG bands, along with the Attention and Meditation measures, to determine the importance of the features used to build the classifier. Next, the preprocessing approach is defined. Firstly, the poor signal level preprocessor is evaluated to determine how dismissal of samples with this metric being less than or equal to the predetermined value will impact the performance of the classifier. It is followed by applying the Simple Moving Average algorithm preprocessor and evaluating its impact on the classifier relative to the size of the window and the step of the algorithm. Finally, the classifier is evaluated with the metrics provided by the ML.NET library, as well as the improvement ratios of the features used to build it. At the end of the chapter, conclusions are drawn from the final results.



(a) F1 score

(b) Log loss

Figure 6.1: Finding optimal number of trees

6.1. Finding Optimal Parameters of Fast Tree Classifier

To find the optimal number of trees, 10 tests have been run, respectively, from 100 to 1000 trees with a step of 100. The results have been presented in Table 6.1 and Figure 6.1. Log loss seems to be linearly correlated with the number of trees, throughout values from 0.564788 to ∞, so it is not suitable to determine which number of trees is the best for this problem. However, the F1 score metric seems to be helpful here. The number of trees of 600 seems to be the best suited value for the classifier, however, not by a high margin, having the lowest value of 0.925985 and the highest value of 0.927826. Given that this is the best result achieved within this experiment run, it will be used throughout the rest of the steps within this experiment.

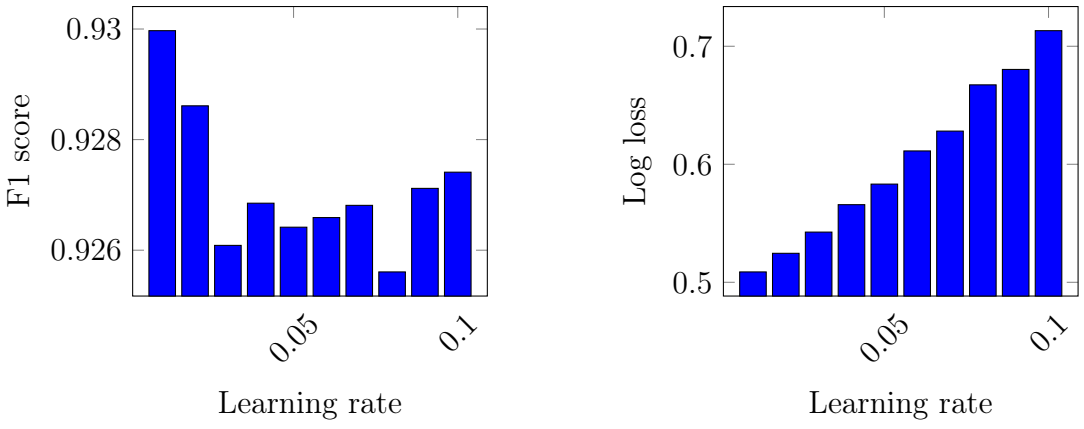
Table 6.1: Finding optimal number of trees

# Trees	F1 score	Log loss
100	0.925985	0.564788
200	0.926590	0.640544
300	0.926616	0.726638
400	0.926573	0.821302
500	0.926919	0.914894
600	0.927826	1.016553
700	0.926498	1.117044
800	0.926511	1.218775
900	0.926978	1.319055
1000	0.926183	∞

To find the optimal number of trees, 10 tests have been run, respectively, from a learning rate of 0.01 to 0.1 with a step of 0.01. The results have been presented in Table 6.2 and Figure 6.2. Log loss still seems to be linear, ranging from 0.508777 to 0.713199. However, the F1 metric seems to be helpful, ranging from 0.925607 to 0.929970, indicating that the best value is the lowest tested. Exploring the lower order of magnitude could be beneficial in this case. To explore the lower order of magnitude, 10 tests have been run, respectively, from a learning rate of 0.001 to 0.01 with a step of 0.001. The results have been presented in Table 6.3 and Figure 6.3. The log loss metric has yielded results within the range between 0.505253 and 0.692421. The significantly higher value in the left range of the tested values indicates that the correct order of magnitude has been explored. The F1 score, which ranges from 0.928317 to 0.931559, indicates that the best learning rate within this experiment run is between 0.005 and 0.007. Given the results of those two trials, the learning rate of 0.006 will be used throughout the rest of the steps within this experiment.

Table 6.2: Finding optimal learning rate

Learning rate	F1 score	Log loss
0.01	0.929970	0.508777
0.02	0.928611	0.524553
0.03	0.926087	0.542531
0.04	0.926850	0.565760
0.05	0.926416	0.583194
0.06	0.926590	0.611297
0.07	0.926811	0.628111
0.08	0.925607	0.667290
0.09	0.927118	0.680355
0.10	0.927411	0.713199



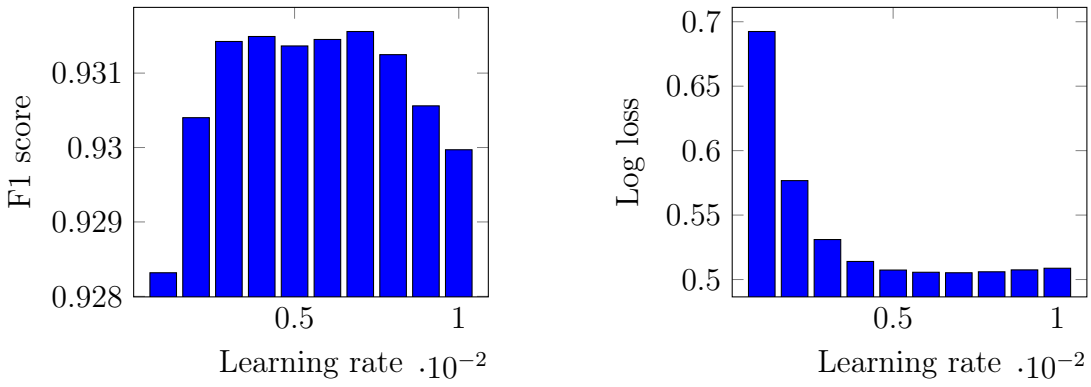
(a) F1 score

(b) Log loss

Figure 6.2: Finding optimal learning rate

Table 6.3: Finding optimal learning rate

Learning rate	F1 score	Log loss
0.001	0.928317	0.692421
0.002	0.930401	0.576734
0.003	0.931425	0.531021
0.004	0.931492	0.514018
0.005	0.931365	0.507350
0.006	0.931452	0.505634
0.007	0.931559	0.505253
0.008	0.931248	0.505999
0.009	0.930560	0.507481
0.010	0.929970	0.508757

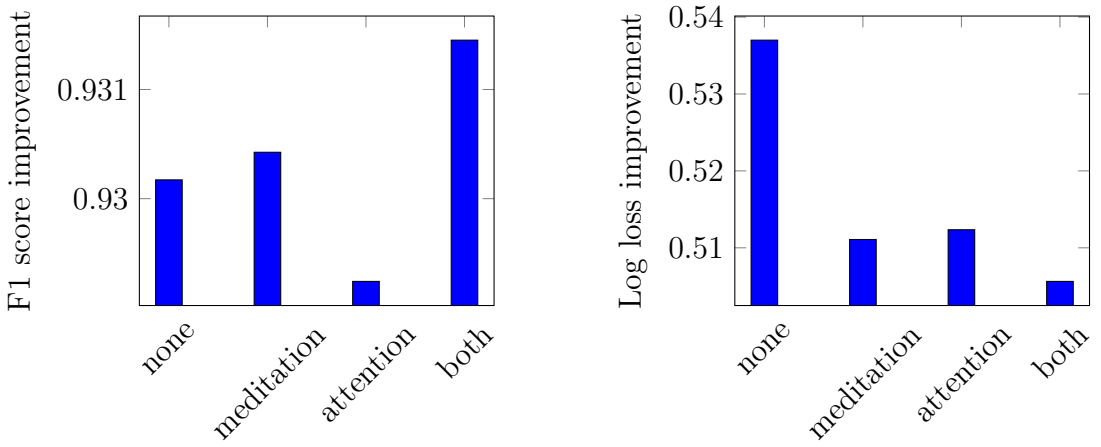


(a) F1 score (b) Log loss

Figure 6.3: Finding optimal learning rate

6.2. Finding Improvement Ratios of EEG Bands, Attention, and Meditation Measures

To calculate the improvement ratio of Attention and Meditation measures, as described above, ratios of respectively F1 scores and log losses have been calculated. The results have been presented in Table 6.4 and Figure 6.4. The results for both F1 score and log loss metrics seem to indicate that the Attention and Meditation measures do not have realistic impact on the classifier - while the F1 score indicates that the classifier might perform better with those features included, ranging from 0.929242 to 0.931452, and the log loss metric indicates the same, ranging from 0.536998 to 0.536998, the difference made is not of a big impact. Given that the Attention and Meditation measures seem to be virtually ineffective within this experiment run, they will not be used throughout the rest of the steps within this experiment.



(a) F1 score (b) Log loss

Figure 6.4: Finding Attention/Meditation improvement ratios

Table 6.4: Finding Attention/Meditation improvement ratios

Attention included	Meditation included	F1 score	Log loss
No	No	0.930172	0.536998
No	Yes	0.930425	0.511083
Yes	No	0.929242	0.512351
Yes	Yes	0.931452	0.505634

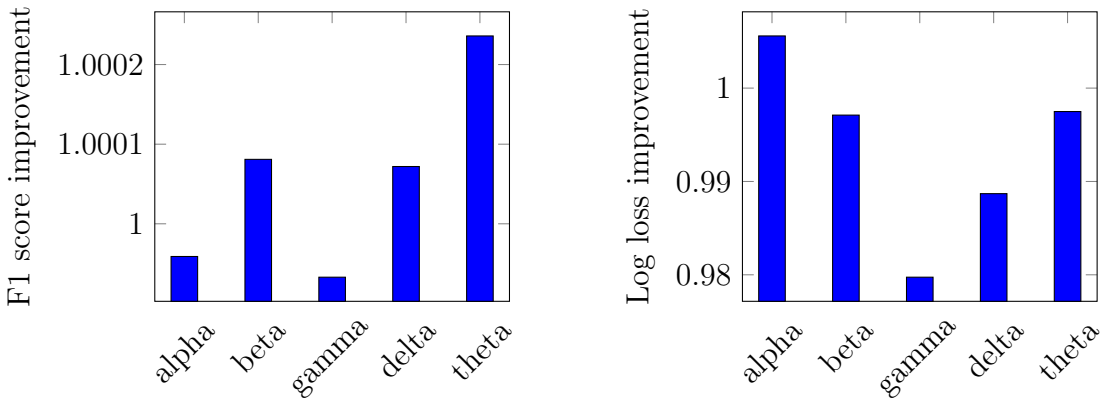
To calculate the improvement ratio of EEG bands, as described above, ratios of respectively F1 scores and log losses have been calculated. Similarly to previous experiments, to simplify the process, five whole bands have been used (alpha, beta, gamma, delta, theta), without distinction to the high/low classification that are specific to MindWave interface. The results have been presented in Table 6.5 and Figure 6.5.

The results for both F1 score and log loss metrics seem to indicate that within a margin of error, there are no dominating EEG bands in this experiment run - while the F1 score, ranging from 0.999933 to 1.000236, may indicate the theta band as the most important one and the gamma band as the least important, the log loss metric, ranging from 0.979745 to 1.005588, seems to agree regarding the alpha band being the best one, but indicates gamma as the worst one.

Given that none of the EEG bands seem to be significantly more important than the others within this experiment run, none of them will be dropped throughout the rest of the steps within this experiment.

Table 6.5: Finding EEG bands improvement ratios

Band	F1 score improvement	Log loss improvement
Alpha	0.999959	1.005588
Beta	1.000081	0.997108
Gamma	0.999933	0.979745
Delta	1.000072	0.988693
Theta	1.000236	0.997489



(a) F1 score

(b) Log loss

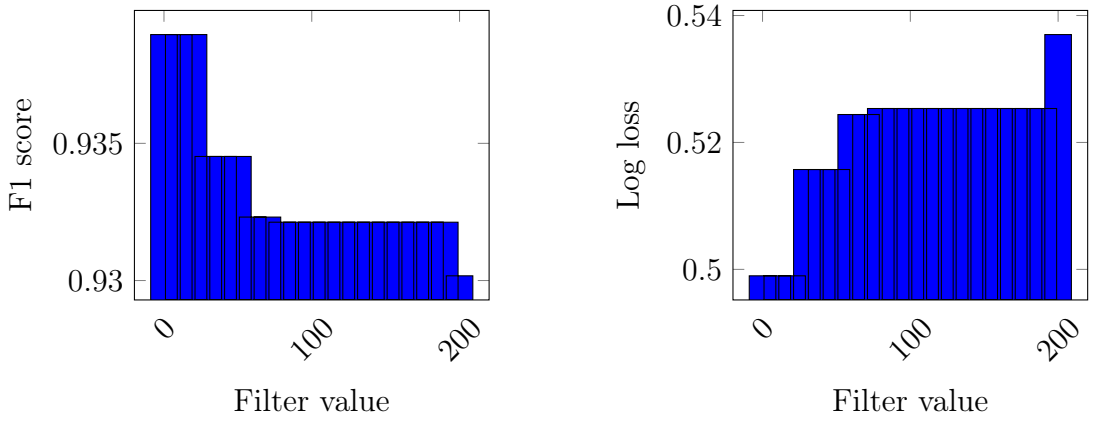
Figure 6.5: Finding EEG bands improvement ratios

6.3. Finding Optimal Preprocessors Parameters

To find the optimal poor signal level filter threshold, 21 tests have been run, respectively, from a value of 0 to 200 with a step of 100. The results have been presented in Table 6.6 and Figure 6.6. The results for both the F1 score and the log loss metrics seem to consistingly indicate the threshold of the poor signal level filter of 20 is the best suited for this classifier while retaining most of the samples. While both of the measures seem not to be linearly correlated with the filter value, both classifiers seem to perform the best with the filter value of 20, with the F1 score and log loss respectively of 0.930172 and 0.938964, thus accepting all samples, these measures are not significantly lower for the filter value of 20, with the same metrics being the value respectively of 0.498983 and 0.536998. Given that the best filter value, while retaining most samples, is the value of 20, it will be used throughout the rest of the steps within this experiment.

Table 6.6: Finding optimal poor signal level filter

Worst acceptable level	F1 score	Log loss
0..20	0.938964	0.498983
30..50	0.934522	0.515733
60..70	0.932313	0.524400
80..190	0.932126	0.525348
200	0.930172	0.536998



(a) F1 score

(b) Log loss

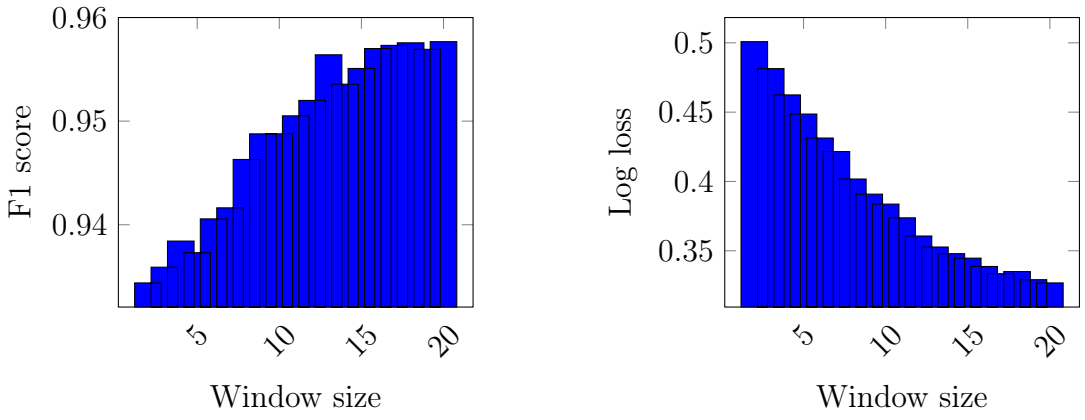
Figure 6.6: Finding optimal poor signal level filter

To find the optimal window size for the Simple Moving Average algorithm, 19 tests have been run, respectively, from a value of 2 to 20 with a step of 1. The results have been presented in Table 6.7 and Figure 6.8. The results for both the F1 score and the log loss metrics seem to improve linearly in relation to the window size of the algorithm, the F1 score metric ranging from 0.934388 to 0.957666 and the log loss metric ranging from 0.326809 to 0.500844. While higher values of window size may benefit the performance of the classifier, practical reason dictates that there should be a reasonable limit for the window size. Given that reasoning, the window size of 5 will be used throughout the rest of the steps within this experiment.

Window size	F1 score	Log loss
2	0.934388	0.500844
3	0.935906	0.481396
4	0.938425	0.462433
5	0.937304	0.448629
6	0.940566	0.431338
7	0.941632	0.421574
8	0.946301	0.401764
9	0.948770	0.390852
10	0.948775	0.383666

Window size	F1 score	Log loss
11	0.950510	0.373755
12	0.951998	0.360644
13	0.956399	0.352709
14	0.953562	0.347907
15	0.955081	0.344675
16	0.957003	0.338670
17	0.957308	0.333460
18	0.957556	0.335006
19	0.956925	0.329131
20	0.957666	0.326809

Figure 6.7: Finding optimal Simple Moving Average window size



(a) F1 score

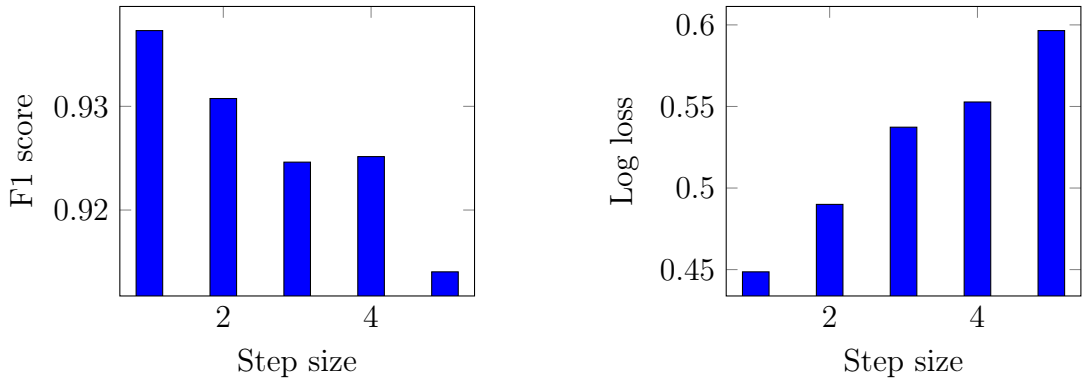
(b) Log loss

Figure 6.8: Finding optimal Simple Moving Average window size

To find the optimal step size for the Simple Moving Average algorithm, 5 tests have been run, respectively, from a value of 1 to 5 with a step of 1. The results have been presented in Table 6.7 and Figure 6.9. The results for both the F1 score and the log loss metrics seem to indicate an inverse linear correlation between the efficiency of the classifier and the step size of the Simple Moving Average algorithm. This is not unexpected, as the larger step size effectively limits the number of samples which the classifier can use. In this case, both the F1 score metric ranging from 0.914040 to 0.937304 and the log loss metric ranging from 0.448629 to 0.596507 suggest that the step value of 1 is the best suited in this classifier. Given that the step value of 1 seems to have the best outcome for the classifier, it will be used throughout the rest of the steps within this experiment.

Table 6.7: Finding optimal Simple Moving Average step size

Step size	F1 score	Log loss
1	0.937304	0.448629
2	0.930753	0.489975
3	0.924619	0.537296
4	0.925153	0.552745
5	0.914040	0.596507



(a) F1 score

(b) Log loss

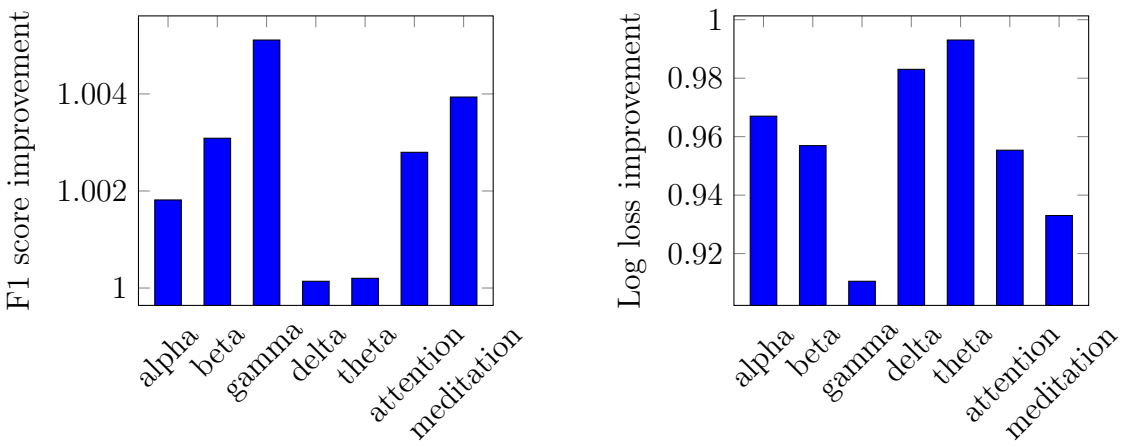
Figure 6.9: Finding optimal Simple Moving Average step size

6.4. Evaluating the Classifier

To finally evaluate the classifier, the ratios of, respectively, F1 scores and log losses have been calculated. The results have been presented in Table 6.8 and Figure 6.10. It seems that introducing the used preprocessing steps made the Attention and Meditation features more important within the classifier, while the delta and theta bands are the least improving features. The improvement of the F1 score metric ranges between 1.000139 and 1.005111, while the improvement of the log loss metric ranges between 0.910533 and 0.993065. Although the differences are not by a large margin, they still bring important insights to the classifier.

Table 6.8: Finding features improvement ratios

Feature	F1 score	Log loss
Alpha	1.001815	0.967010
Beta	1.003087	0.956933
Gamma	1.005111	0.910533
Delta	1.000139	0.983035
Theta	1.000200	0.993065
Attention	1.002797	0.955370
Meditation	1.003936	0.933027



(a) F1 score

(b) Log loss

Figure 6.10: Finding features improvement ratios

The final classifier metrics are presented in Table 6.9. The confusion matrix is presented by Table 6.10. Reaching the F1 score of 0.945356 is a satisfactory result of this classifier, beating the metrics of the classifier built upon the "Stress" dataset. While the classification is not perfect, the brief analysis of confusion matrix also indicates that while taking wrong predictions, the classifier tends towards the false positive error rather than the false negative one, having precision and recall, respectively, of 0.901603 and 0.993748. Taking into account the topic of this thesis and potential cybersecurity applications, it is better for the classifier to falsely mark the subject as stressed and potentially deny access to sensitive data or systems than to grant such access by mistake.

Table 6.9: Stress detection classifier metrics

Metric	Value
F1 Score	0.945356
Log loss	0.401116
Entropy	0.550409

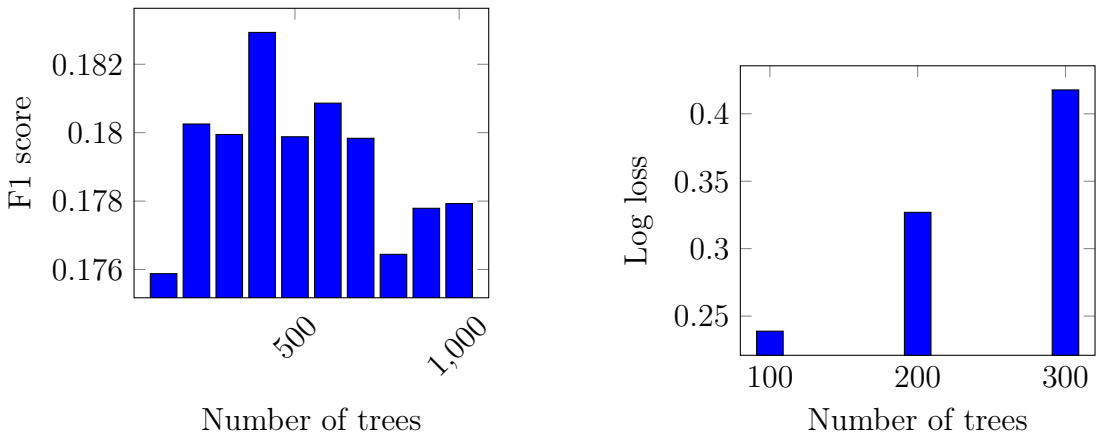
Table 6.10: Stress detection classifier confusion matrix

		Predicted		
		Positive	Negative	Recall
Truth	Positive	3656	23	0.993748
	Negative	399	139	0.258364
	Precision	0.901603	0.858025	

The classifier built in this chapter has been using the "Login" dataset described above and has been fine-tuned to evaluate the best possible performance. First, the model parameters have been evaluated and it has been determined that the best parameters are 600 trees and the learning rate of 0.006. Subsequently, the improvement ratios of the EEG bands and the Attention and Meditation features were calculated. It has been made clear that no feature has significantly improved the classifier. Even with small difference, the alpha, beta and gamma bands seem to be more important bands than delta and theta, which makes it consistent with earlier work[17]. For the preprocessing part, the poor signal level filter value has been set to 20. Applying the Simple Moving Average algorithm preprocessor to the data revealed intuitive insight of the changes in the parameters. While increasing the window size almost linearly improves the classifier performance, having more data in the domain of time within one sample and removing potential noise, increasing the step size linearly decreases the classifier performance, having fewer samples to train and validate the classifier on. The results of the classifier evaluation, with an F1 score of 0.945356, are satisfactory and better than the classifier built upon the "Stress" dataset. The brief analysis of confusion matrix indicates that the classifier tends towards the false-positive error rather than the false-negative one, having precision and recall, respectively, of 0.901603 and 0.993748. Given the topic of this thesis and potential cybersecurity applications, it is better for the classifier to return the false positive prediction rather than the false negative one.

7. Binary Subject Recognition Classifier

The classifier built in this chapter uses the "Login" dataset described above. Similarly to the previous experiments, the full brute-force approach would take a long time without guaranteeing error-proof code, so this chapter describes the step-by-step approach taken to fine-tune the parameters of the classifier. First, the impact of number of trees is explored within the Fast Tree classifier to locate the optimal value. A similar approach is used for the learning rate. Afterwards, within the parameters defined in the previous steps, the improvement ratio is calculated for all EEG bands, along with the Attention and Meditation measures, to determine the importance of the features used to build the classifier. Next, the preprocessing approach is defined. Firstly, the poor signal level preprocessor is evaluated to determine how dismissal of samples with this metric being less than or equal to the predetermined value will impact the performance of the classifier. It is followed by applying the Simple Moving Average algorithm preprocessor and evaluating its impact on the classifier relative to the window size of the algorithm. Finally, the classifier is evaluated with the metrics provided by the ML.NET library, as well as the improvement ratios of the features used to build it. At the end of the chapter, conclusions are drawn from the final results.



(a) F1 score

(b) Log loss

Figure 7.1: Finding optimal number of trees

7.1. Finding Optimal Parameters of Fast Tree Classifier

To find the optimal number of trees, 10 tests have been run, respectively, from 100 to 1000 trees with a step of 100. The results have been presented in Table 7.1 and Figure 7.1. Within this classifier, log loss seems to be difficult to use; while ranging from 0.238800 to 0.417722 up to 300 trees, it reaches infinity on 400 trees. The F1 score, which ranges from 0.175879 to 0.182931, looks significantly worse than within the previously developed classifiers. Although the results are not promising, the classifier reached the best performance with 400 trees. Given that this is the best result achieved within this experiment run, it will be used throughout the rest of the steps within this experiment.

Table 7.1: Finding optimal number of trees

# Trees	F1 score	Log loss
100	0.175879	0.238800
200	0.180254	0.326927
300	0.179947	0.417722
400	0.182931	∞
500	0.179881	∞
600	0.180864	∞
700	0.179836	∞
800	0.176444	∞
900	0.177790	∞
1000	0.177928	∞

To find the optimal number of trees, 10 tests have been run, respectively, from a learning rate of 0.1 to 1.0 with a step of 0.1. The results have been presented in Table 7.2 and Figure 7.2. The classifier yielded the only useful log loss value of 0.322200 for a 0.1 learning rate. However, the F1 score metric, ranging from 0.147878 to 0.182931, indicates that classifier performance improves with the decrease of learning rate, stopping at 0.2 learning rate with the best F1 score. Given that these are the best results achieved within this experiment run, the learning rate of 0.2 will be used throughout the rest of the steps within this experiment.

Table 7.2: Finding optimal learning rate

Learning rate	F1 score	Log loss
0.1	0.180210	0.322200
0.2	0.182931	∞
0.3	0.179573	∞
0.4	0.177856	∞
0.5	0.173158	∞
0.6	0.171878	∞
0.7	0.168612	∞
0.8	0.158827	∞
0.9	0.150649	∞
1.0	0.147878	∞

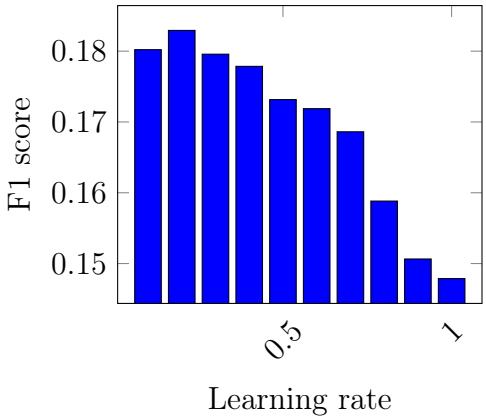


Figure 7.2: Finding optimal learning rate (F1 score)

7.2. Finding Improvement Ratios of EEG Bands, Attention, and Meditation Measures

To calculate the improvement ratio of Attention and Meditation measures, as described above, ratios of respectively F1 scores and log losses have been calculated. The results have been presented in Table 7.3 and Figure 7.3. The results for the F1 score, ranging from 0.068570 to 0.182931, seem to indicate that Attention and Meditation indeed have the measurable impact on the classifier. Given that the Attention and Meditation measures seem to be effective within this experiment run, they will be used throughout the rest of the steps within this experiment.

Table 7.3: Finding Attention/Meditation improvement ratios

Attention included	Meditation included	F1 score	Log loss
No	No	0.068570	∞
No	Yes	0.126090	∞
Yes	No	0.117635	∞
Yes	Yes	0.182931	∞

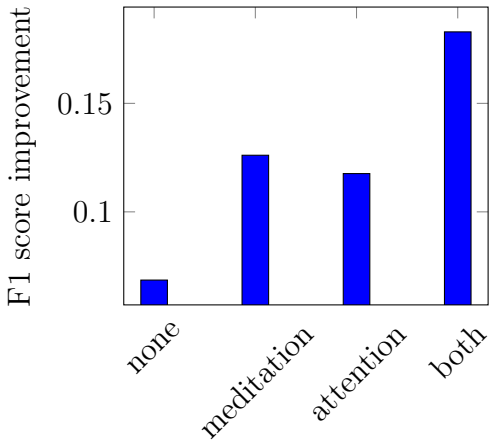


Figure 7.3: Finding Attention/Meditation improvement ratios (F1 score)

To calculate the improvement ratio of the EEG bands, as described above, the ratios of the F1 scores have been calculated. To simplify the experiment, five whole bands have been used (alpha, beta, gamma, delta, theta), without distinction to the high/low classification that are specific to MindWave interface. The results have been presented in Table 7.4 and Figure 7.4. The improvement results of the F1 score, ranging from 0.992984 to 1.422657, strongly indicate the dominance of the gamma EEG band. Regardless of the gamma EEG band being dominant in the classifier, none of the other bands will be dropped throughout the rest of the steps within this experiment.

Table 7.4: Finding EEG bands improvement ratios

Band	F1 score improvement
Alpha	0.992984
Beta	1.102444
Gamma	1.422657
Delta	1.090385
Theta	0.997525

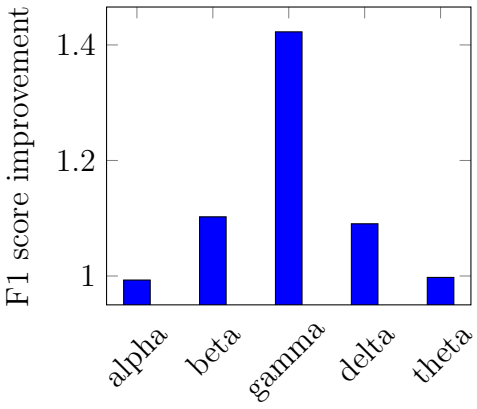


Figure 7.4: Finding EEG bands improvement ratios (F1 score)

7.3. Finding Optimal Preprocessors Parameters

To find the optimal window size for the Simple Moving Average algorithm, 19 tests have been run, respectively, from a value of 2 to 20 with a step of 1. The results have been presented in Table 7.5 and Figure 7.6. The results for the F1 score metric, ranging from 0.295870 to 0.930051, indicate that the classifier performance improves along with the window size of the Simple Moving Average algorithm. Although higher values of window size may benefit the performance of the classifier, practical reason dictates that there should be a reasonable limit for the window size. Given that reasoning, the window size of 20 will be used throughout the rest of the steps within this experiment, without checking extended range of possible values.

Window size	F1 score
2	0.295870
3	0.421824
4	0.547763
5	0.632653
6	0.704027
7	0.756741
8	0.788955
9	0.821150
10	0.846271

Window size	F1 score
11	0.859182
12	0.872131
13	0.889224
14	0.900655
15	0.908559
16	0.916218
17	0.921740
18	0.923466
19	0.928390
20	0.930051

Figure 7.5: Finding optimal Simple Moving Average window size

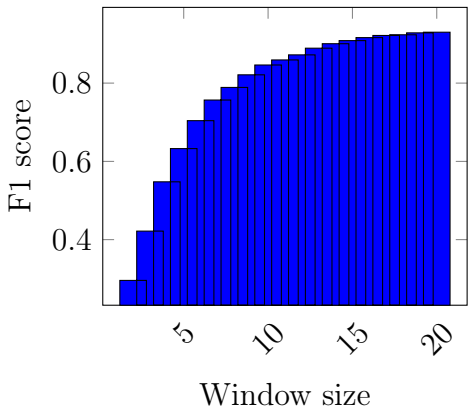


Figure 7.6: Finding optimal Simple Moving Average window size (F1 score)

7.4. Evaluating the Classifier

To finally evaluate the classifier, the F1 score ratios have been calculated. The results have been presented in Table 7.5 and Figure 7.7. It seems that introducing the used preprocessing steps made the Attention and Meditation features more important within the classifier, while the delta and theta bands are the least improving features. The improvement of the F1 score metric ranges between 1.087870 and 1.287013. The differences have a larger margin than in the previously developed classifier and bring important insights into the classifier.

Table 7.5: Finding features improvement ratios

Feature	F1 score
Alpha	1.210912
Beta	1.238773
Gamma	1.287013
Delta	1.087870
Theta	1.091508
Attention	1.156059
Meditation	1.150487

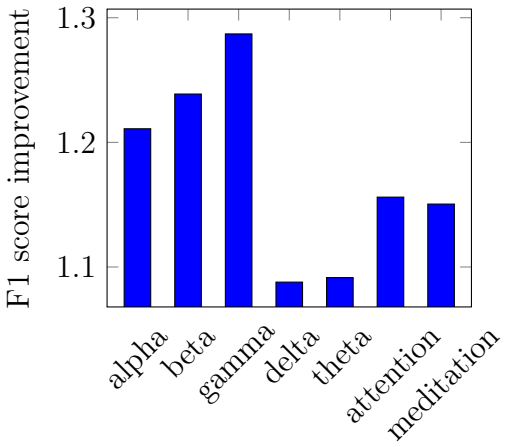


Figure 7.7: Finding features improvement ratios (F1 score)

The final classifier metrics are presented in Table 7.6. The confusion matrix is presented by Table 7.7. Reaching the F1 score of 0.927333 is a satisfactory result of this classifier, being similar to the metrics of the classifiers built previously. The brief analysis of confusion matrix indicates that while taking wrong predictions, the classifier no longer tends towards the false positive error rather than the false negative one, having precision and recall, respectively, of 0.867618 and 0.696472. Taking into account the topic of this thesis and potential cybersecurity applications, the classifier is more likely to make a false-negative prediction. To allow comparison with multi-class model described afterwards, the accuracy measure has been calculated from the confusion matrix in Figure 7.8.

Table 7.6: Stress detection classifier metrics

Metric	Value
F1 Score	0.927333
Log loss	0.178655
Entropy	0.225432

Table 7.7: Subject recognition classifier confusion matrix

		Predicted		
		Positive	Negative	Recall
Truth	Positive	373002	162557	0.696472
	Negative	56913	13867621	0.995913
	Precision	0.867618	0.988414	

$$
\begin{aligned}
a &= \frac{tp + tn}{tp + fp + tn + fn} \\
&= \frac{373002 + 13867621}{373002 + 56913 + 13867621 + 162557} \\
&= \frac{14240623}{14460093} \\
&= 0.984822
\end{aligned}
\tag{7.1}
$$

$$tp - number\,of\,true\,positives$$

$$fp - number\,of\,false\,positives$$

$$tn - number\,of\,true\,negatives$$

$$fn - number\,of\,false\,negatives$$

Figure 7.8: Accuracy of the binary subject recognition classifier

The classifier built in this chapter has been using the "Login" dataset described above and has been fine-tuned to evaluate the best possible performance. First, the model parameters have been evaluated and it has been determined that the best parameters are 400 trees and the learning rate of 0.2. Subsequently, the improvement ratios of the EEG bands and the Attention and Meditation features were calculated. It has been made clear that gamma EEG band improved the classifier the most. Even with a small difference, the alpha and beta bands seem to be the more important bands than delta and theta, which is consistent with earlier work[17]. For the preprocessing part, the Simple Moving Average algorithm preprocessor applied to the data revealed intuitive insight of the changes in the parameters, as increasing the window size also improves the classifier performance, having more data in the domain of time within one sample and removing potential noise. Unfortunately, there was not enough data in the data set to explore the poor signal level filter and step size for the Simple Moving Average algorithm. The results of the classifier evaluation, with an F1 score of 0.927333 and an accuracy of 0.984822, are satisfactory. The brief analysis of confusion matrix indicates that the classifier may tend towards the false-negative error with higher probability than the previously developed classifiers, having precision and recall, respectively, of 0.867618 and 0.696472. Given the topic of this thesis and potential cybersecurity applications, unfortunately, the classifier is more likely to make the false-negative prediction.

8. Multi-class Subject Recognition Classifier

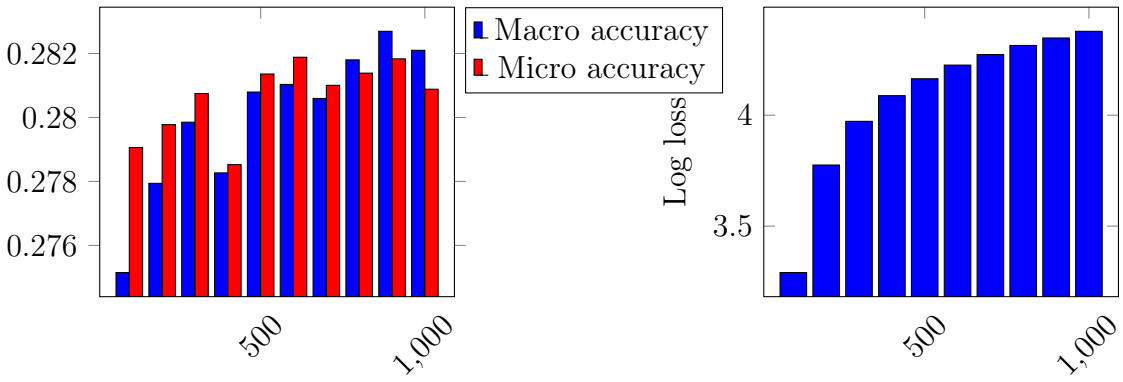
The classifier built in this chapter uses the "Login" dataset described above. Contrary to the previous experiments, this classifier is a multi-class model, requiring a slightly different approach and evaluating different metrics. However, a similar characteristic is that the full brute-force approach would take a long time without guaranteeing error-proof code, so this chapter describes the step-by-step approach used to fine-tune the classifier parameters. First, the impact of number of iterations is explored within the LightGBM classifier to locate the optimal value. A similar approach is used for the learning rate. Afterwards, within the parameters defined in the previous steps, the improvement ratio is calculated for all EEG bands, along with the Attention and Meditation measures, to determine the importance of the features used to build the classifier. Next, the preprocessing approach is defined. Firstly, the poor signal level preprocessor is evaluated to determine how dismissal of samples with this metric being less than or equal to the predetermined value will impact the performance of the classifier. It is followed by applying the Simple Moving Average algorithm preprocessor and evaluating its impact on the classifier relative to the size of the window and the step of the algorithm. Finally, the classifier is evaluated with the metrics provided by the ML.NET library, as well as the improvement ratios of the features used to build it. At the end of the chapter, conclusions are drawn from the final results.

Table 8.1: Finding optimal number of iterations

# Iterations	Macro accuracy	Micro accuracy	Log loss
100	0.275150	0.279059	3.290677
200	0.277940	0.279775	3.775411
300	0.279851	0.280748	3.972300
400	0.278266	0.278524	4.088000
500	0.280794	0.281358	4.164211
600	0.281033	0.281882	4.225815
700	0.280593	0.281004	4.273329
800	0.281800	0.281385	4.314268
900	0.282693	0.281832	4.347961
1000	0.282099	0.280883	4.378086

8.1. Finding Optimal Parameters of LightGBM Classifier

To find the optimal number of iterations, 10 tests have been run, respectively, from 100 to 1000 iterations with a step of 100. The results have been presented in Table 8.1 and Figure 8.1. Within this classifier, log loss, ranging from 3.290677 to 4.378086, seems to be increasing along with the number of iterations, thus not being helpful in determining the best number of iterations. Macro and micro accuracy measures, ranging respectively from 0.275150 to 0.282693 and from 0.278524 to 0.281882 , favor the higher number of iterations. However, given that the processing time grows almost linearly with the number of iterations, a reasonable value needs to be chosen. Given that the differences in accuracy measures are not of high margin, the number of iterations of 300 will be used throughout the rest of the steps within this experiment.



(a) Accuracy

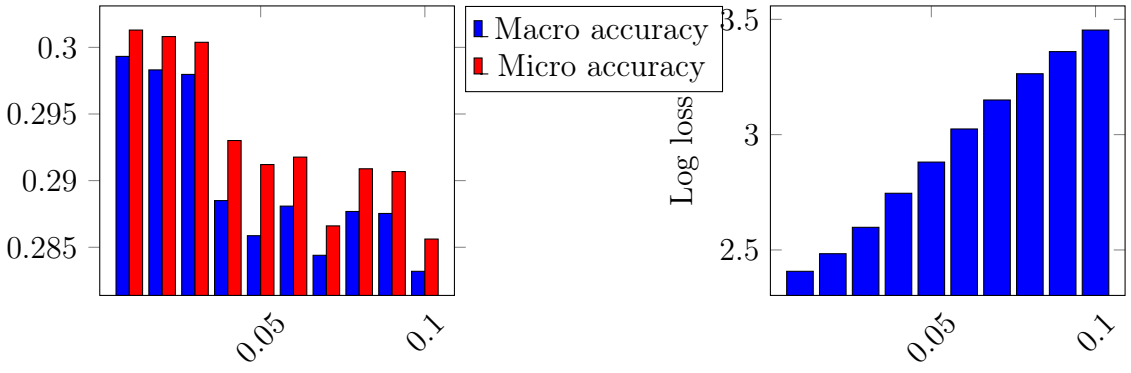
(b) Log loss

Figure 8.1: Finding optimal number of iterations

To find the optimal learning rate, 10 tests have been run, respectively, from a learning rate of 0.01 to 0.01 with a step of 0.01. The results have been presented in Table 8.2 and Figure 8.2. Within this classifier, log loss seems to grow linearly with the learning rate, ranging from 2.407454 to 3.453484. The macro and micro accuracy measures, ranging respectively from 0.283197 to 0.299322 and from 0.285617 to 0.301298, indicate the best classifier performance with the smallest learning rate. Exploring the lower order of magnitude could be beneficial in this case. To explore the lower order of magnitude, 10 tests have been run, respectively, from a learning rate of 0.001 to 0.01 with a step of 0.001. The results have been presented in Table 8.3 and Figure 8.3. The log loss measure, ranging from 2.407454 to 3.453484, starts to be useful within this experiment run, indicating the higher loss within the lowest tested learning rates, consistent with macro- and micro-accuracy measures, ranging respectively from 0.270710 to 0.299322 and from 0.279033 to 0.301298. All metrics together seem to show that the best learning rate in this scenario is 0.01. Further experiments will be conducted with this value.

Table 8.2: Finding optimal learning rate

Learning rate	Macro accuracy	Micro accuracy	Log loss
0.01	0.299322	0.301298	2.407454
0.02	0.298308	0.300808	2.483696
0.03	0.297970	0.300380	2.598158
0.04	0.288502	0.293009	2.745824
0.05	0.285868	0.291206	2.881024
0.06	0.288088	0.291765	3.024592
0.07	0.284399	0.286604	3.150235
0.08	0.287686	0.290889	3.264041
0.09	0.287537	0.290678	3.359978
0.10	0.283197	0.285617	3.453484



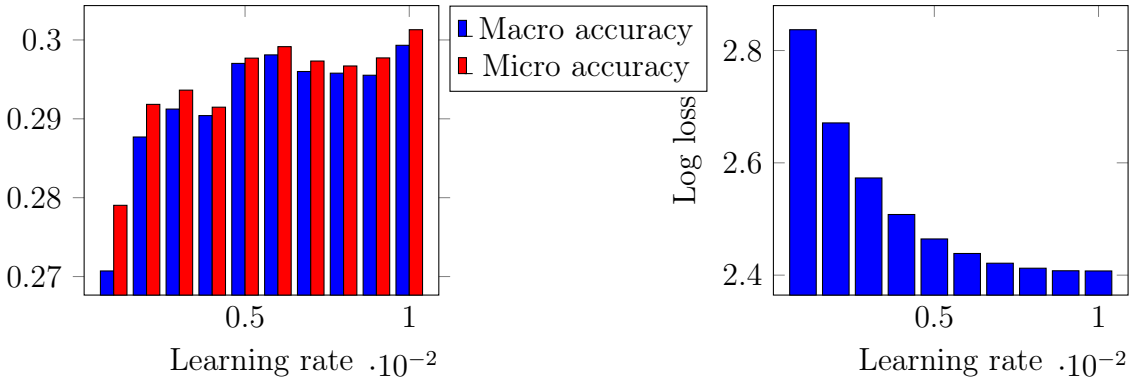
(a) Accuracy

(b) Log loss

Figure 8.2: Finding optimal learning rate

Table 8.3: Finding optimal learning rate

Learning rate	Macro accuracy	Micro accuracy	Log loss
0.001	0.270710	0.279033	2.837064
0.002	0.287695	0.291832	2.671082
0.003	0.291237	0.293637	2.573057
0.004	0.290408	0.291475	2.507983
0.005	0.297026	0.297693	2.464454
0.006	0.298106	0.299150	2.438563
0.007	0.296000	0.297326	2.421246
0.008	0.295788	0.296700	2.412345
0.009	0.295526	0.297722	2.407782
0.010	0.299322	0.301298	2.407454



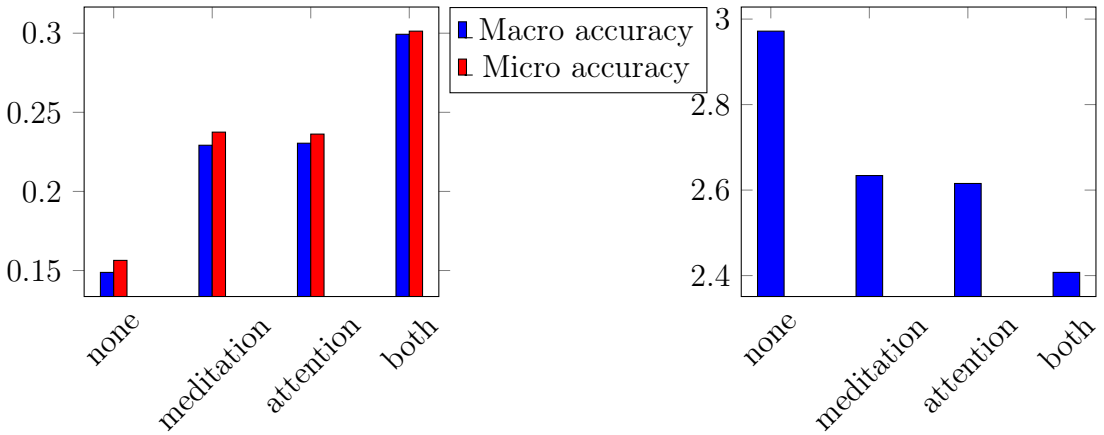
(a) Accuracy

(b) Log loss

Figure 8.3: Finding optimal learning rate

8.2. Finding Improvement Ratios of EEG Bands, Attention, and Meditation Measures

To calculate the improvement ratio of the Attention and Meditation measures, as described above, the ratios of all measures have been calculated. The results have been presented in Table 8.4 and Figure 8.4. The results of all of the measures: macro accuracy, ranging from 0.148814 to 0.299322; micro accuracy, ranging from 0.156410 to 0.301298; and log loss, ranging from 2.407454 to 2.971764; strongly indicate that the Attention and Meditation features indeed have the measurable impact on the classifier. The Attention and Meditation measures seem to be actually helpful in this classifier, and thus will be included in the further experiments.



(a) Accuracy

(b) Log loss

Figure 8.4: Finding Attention/Meditation improvement ratios

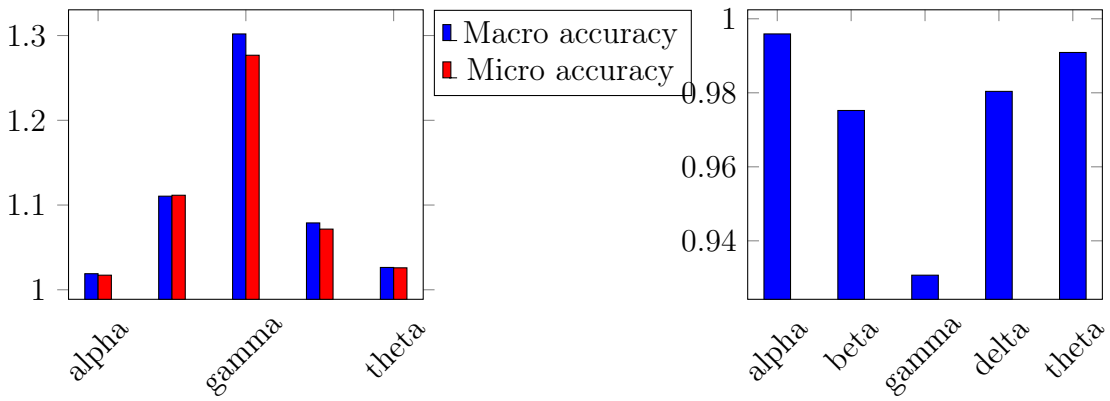
Table 8.4: Finding Attention/Meditation improvement ratios

Attention	Meditation	Macro accuracy	Micro accuracy	Log loss
False	False	0.148814	0.156410	2.971764
False	True	0.229188	0.237468	2.634001
True	False	0.230468	0.236229	2.615459
True	True	0.299322	0.301298	2.407454

To calculate the improvement ratio of the EEG bands, as described above, the ratio of all measures has been calculated. To simplify the experiment, five whole bands have been used (alpha, beta, gamma, delta, theta), without distinction to the high/low classification that are specific to MindWave interface. The results have been presented in Table 8.5 and Figure 8.5. The improvement ratios of all measures: macro accuracy, ranging from 1.018970 to 1.301907; micro accuracy, ranging from 1.017225 to 1.276775; and log loss, ranging from 0.930719 to 0.995911; strongly indicate the gamma EEG band as dominant and the alpha band as least improving. An interesting correlation can be observed, as the gamma band was also among the most important features in the previous classifier. Regardless of the gamma EEG band being dominant in the classifier, none of the other bands will be dropped throughout the rest of the steps within this experiment.

Table 8.5: Finding EEG bands improvement ratios

Band	Macro accuracy	Micro accuracy	Log loss
Alpha	1.018970	1.017225	0.995911
Beta	1.110455	1.111552	0.975223
Gamma	1.301907	1.276775	0.930719
Delta	1.078893	1.071601	0.980386
Theta	1.026352	1.025912	0.990897



(a) Accuracy

(b) Log loss

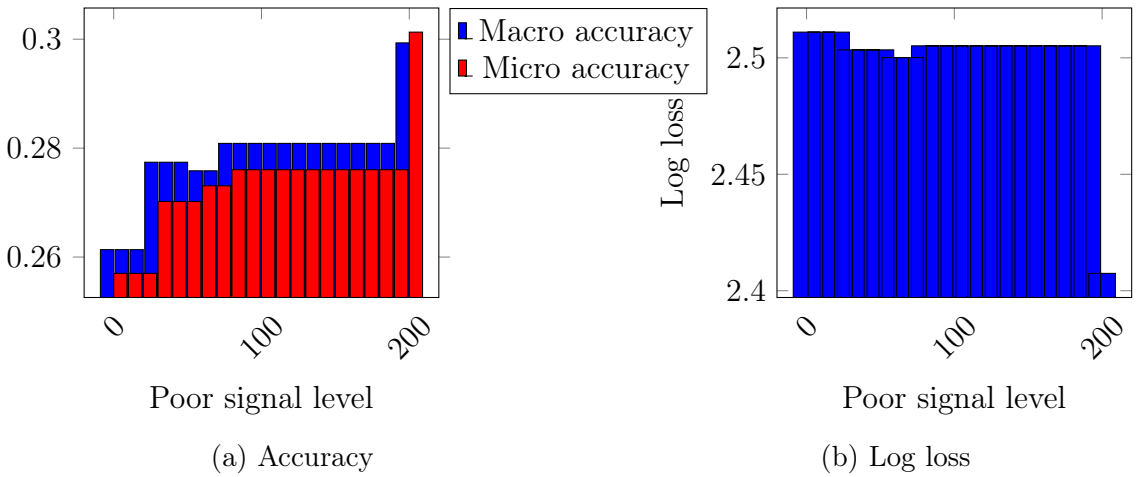
Figure 8.5: Finding EEG bands improvement ratios

8.3. Finding Optimal Preprocessors Parameters

To find the optimal poor signal level filter threshold, 21 tests have been run, respectively, from a value of 0 to 200 with a step of 100. The results have been presented in Table 8.6 and Figure 8.6. The results of all metrics: macro accuracy, ranging from 0.261358 to 0.299322; micro accuracy, ranging from 0.257003 to 0.301298; and log loss, ranging from 2.407454 to 2.511040; seem to indicate no classifier performance improvement along with restrictiveness of the poor signal level filter. Given that the best filter value, while retaining most samples, is the value of 200, using a poor level signal filter may not be warranted in this classifier and will not be used throughout the rest of the steps within this experiment.

Table 8.6: Finding optimal poor signal level filter

Worst acceptable level	Macro accuracy	Micro accuracy	Log loss
0..20	0.261358	0.257003	2.511040
30..50	0.277411	0.270201	2.503422
60..70	0.275834	0.273088	2.500117
80..190	0.280869	0.276034	2.505149
200	0.299322	0.301298	2.407454



(a) Accuracy

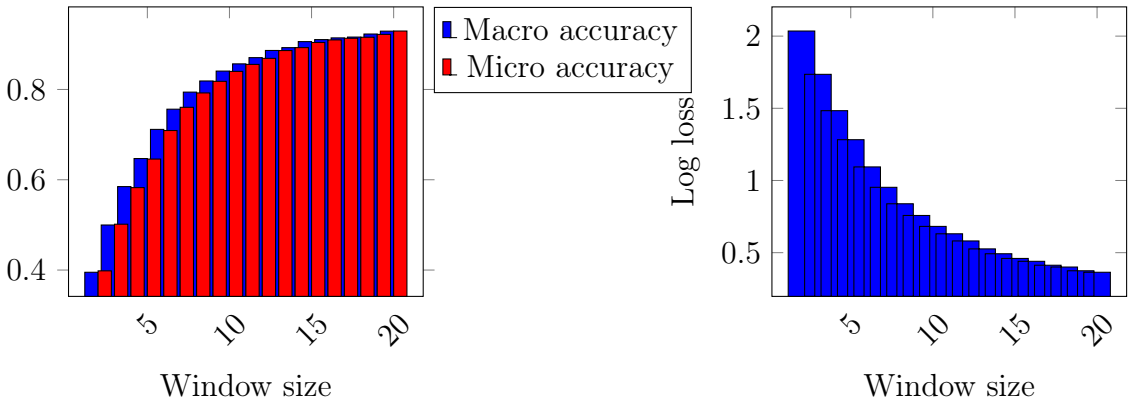
(b) Log loss

Figure 8.6: Finding optimal poor signal level filter

To find the optimal window size for the Simple Moving Average algorithm, 19 tests have been run, respectively, from a value of 2 to 20 with a step of 1. The results have been presented in Table 8.7 and Figure 8.7. The results for all of the metrics: macro accuracy, ranging from 0.395102 to 0.929150; micro accuracy, ranging from 0.398246 to 0.929453; and log loss, ranging from 0.364307 to 2.035322; seem to improve along with the window size of the Simple Moving Average algorithm. Although higher values of window size may benefit the performance of the classifier, practical reason dictates that there should be a reasonable limit for the window size. Given that reasoning, the window size of 20 will be used throughout the rest of the steps within this experiment, without checking extended range of possible values.

Table 8.7: Finding optimal Simple Moving Average window size

Window size	Macro accuracy	Micro accuracy	Log loss
2	0.395102	0.398246	2.035322
3	0.499794	0.501536	1.735300
4	0.584854	0.582611	1.483580
5	0.646965	0.645821	1.282528
6	0.711561	0.709050	1.093982
7	0.756321	0.760478	0.952696
8	0.794135	0.792310	0.838758
9	0.818804	0.818001	0.757710
10	0.840717	0.840026	0.681960
11	0.856697	0.855515	0.630811
12	0.870485	0.868892	0.581237
13	0.886395	0.886173	0.526200
14	0.892619	0.892704	0.492559
15	0.905986	0.904065	0.460060
16	0.910468	0.909777	0.440138
17	0.914232	0.913396	0.413030
18	0.916051	0.915673	0.400550
19	0.922816	0.921958	0.374644
20	0.929150	0.929453	0.364307



(a) Accuracy

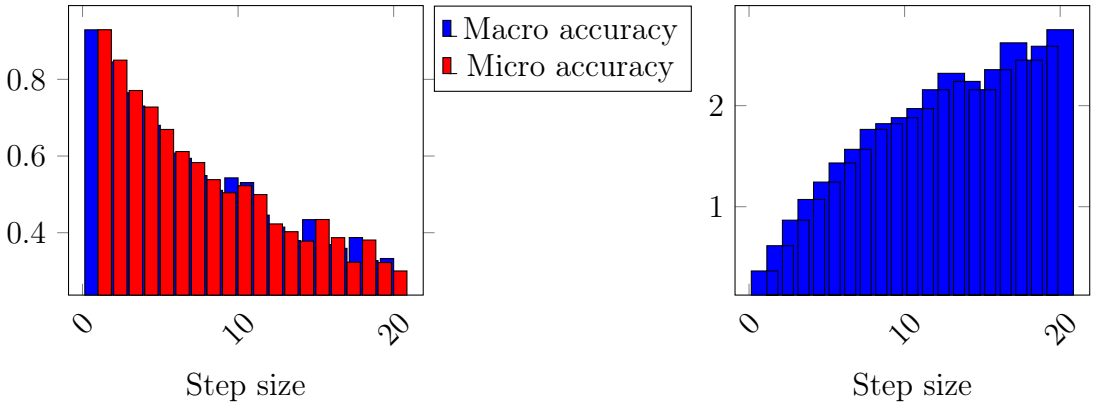
(b) Log loss

Figure 8.7: Finding optimal Simple Moving Average window size

To find the optimal step size for the Simple Moving Average algorithm, 20 tests have been run, respectively, from a value of 1 to 20 with a step of 1. The results have been presented in Table 8.8 and Figure 8.8. The results for all metrics: macro accuracy, ranging from 0.327106 to 0.929150; micro accuracy, ranging from 0.300237 to 0.929453; and log loss, ranging from 0.364307 to 2.751214; seem to indicate an inverse linear correlation between the efficiency of the classifier and the step size of the Simple Moving Average algorithm. This is not unexpected, as the larger step size effectively limits the number of samples which the classifier can use. In this case, all metrics suggest that the step value of 1 is the best suited in this classifier. Given that the step value of 1 seems to have the best outcome for the classifier, it will be used throughout the rest of the steps within this experiment.

Table 8.8: Finding optimal Simple Moving Average step size

Step size	Macro accuracy	Micro accuracy	Log loss
1	0.929150	0.929453	0.364307
2	0.845421	0.850069	0.614096
3	0.764927	0.770895	0.866870
4	0.730392	0.727758	1.071665
5	0.680138	0.669350	1.243780
6	0.607671	0.611723	1.432725
7	0.594035	0.582923	1.567695
8	0.549060	0.538404	1.764976
9	0.510485	0.504177	1.821368
10	0.543018	0.522546	1.880632
11	0.530766	0.499585	1.970681
12	0.445809	0.422917	2.157311
13	0.414622	0.402648	2.319753
14	0.379477	0.378084	2.239907
15	0.434032	0.434486	2.157635
16	0.369080	0.387063	2.356020
17	0.359244	0.323238	2.621151
18	0.387341	0.380912	2.450045
19	0.327106	0.322091	2.587622
20	0.332727	0.300237	2.751214



(a) Accuracy

(b) Log loss

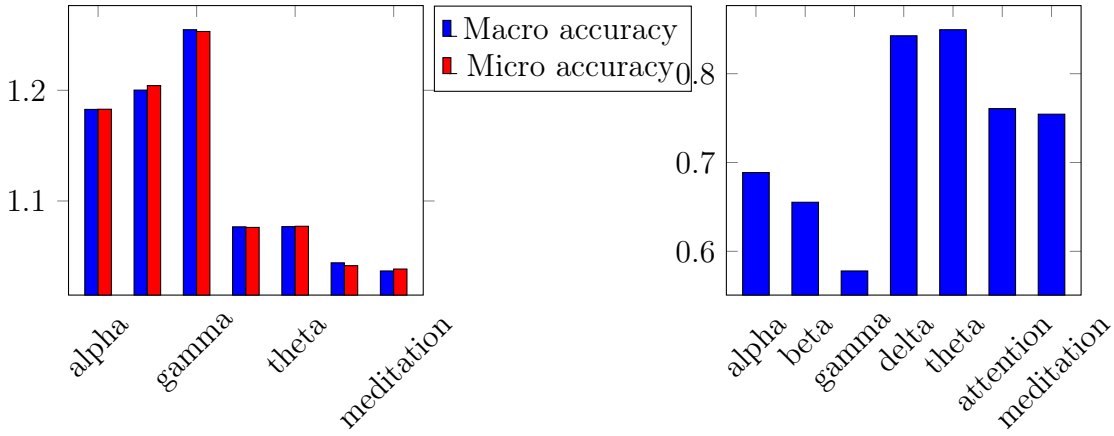
Figure 8.8: Finding optimal Simple Moving Average step size

8.4. Evaluating the Classifier

To finally evaluate the classifier, the ratios of all metrics have been calculated. The results have been presented in Table 8.9 and Figure 8.9. It seems that introducing the used preprocessing steps made the Attention and Meditation features less important within the classifier, while the delta and theta bands became improving features. The improvement of all metrics: macro accuracy, ranging from 1.036777 to 1.254743; micro accuracy, ranging from 1.038507 to 1.253139; and log loss, ranging from 0.577915 to 0.760693; indicates the vast importance of alpha, beta, and gamma EEG bands, bringing important insights into the classifier, as those bands are also among the most important features in emotion recognition research.

Table 8.9: Finding features improvement ratios

Feature	Macro accuracy	Micro accuracy	Log loss
Alpha	1.182739	1.182899	0.688734
Beta	1.200190	1.204240	0.655263
Gamma	1.254743	1.253139	0.577915
Delta	1.076644	1.076114	0.842695
Theta	1.076832	1.077163	0.849521
Attention	1.044127	1.041553	0.760693
Meditation	1.036777	1.038507	0.754411



(a) Accuracy

(b) Log loss

Figure 8.9: Finding features improvement ratios

The final classifier metrics are presented in Table 8.10. Reaching the macro and micro accuracy scores of respectively 0.929150 and 0.929454 is a satisfactory result of this classifier, being similar to the metrics of the classifiers built previously. Analysis of confusion matrix would not be efficient in this case, having almost 30 classes.

Table 8.10: Multi-class subject recognition classifier metrics

Metric	Value
Macro accuracy	0.929150
Micro accuracy	0.929454
Log loss	0.887535

The classifier built in this chapter has been using the "Login" dataset described above and has been fine-tuned to evaluate the best possible performance. First, the model parameters have been evaluated and it has been determined that the best parameters are 300 iterations and the learning rate of 0.01. Subsequently, the improvement ratios of the EEG bands and the Attention and Meditation features were calculated. It has been made clear that gamma EEG band improved the classifier the most. Even with small difference, the alpha and beta bands seem to be more important bands than delta and theta, which makes it consistent with earlier work[17]. For the preprocessing part, the poor signal level filter value has been set to 200. Applying the Simple Moving Average algorithm preprocessor to the data revealed intuitive insight of the changes in the parameters. While increasing the window size almost linearly improves the classifier performance, having more data in the domain of time within one sample and removing potential noise, increasing the step size linearly decreases the classifier performance, having fewer samples to train and validate the classifier on. The results of the classifier evaluation, with the macro accuracy of 0.929150 and micro accuracy of 0.929454, are satisfactory. Analysis of confusion matrix would not be efficient in this case, having almost 30 classes.

9. Summary and Future Work

The main purpose of this thesis was to present the original solution to the scientific problem of exploring the applications of simplified brain-computer interfaces in cybersecurity and emotion recognition, especially in terms of evaluating the potential of such interfaces within the field of stress detection and subject recognition. Given that simplified EEG interfaces seem to have more customer-friendly potential than traditional ones because of their simplicity and low cost, it has been done by building stress detection and subject recognition classifiers based on the data provided by the Neurosky MindWave Mobile 2 interface and evaluating the results, with cybersecurity applications in mind, and what are the metrics of such classifiers. Considering the participation of human participants, the research has been approved by the Committee for Research Ethics.

There were two Fast Tree classifiers built to evaluate the possibilities of using a simplified EEG interface for stress detection, built respectively on "Stress" and "Login" datasets. To fine-tune such classifiers, first, the model parameters have been evaluated to determine the best values for both the number of trees and the learning rates of the classifiers. The improvement ratios have been calculated for all available EEG bands, along with the attention and meditation features, to define the impact of a specific feature on the performance of the model. The preprocessing part of the experiment included the poor signal level filter and the Simple Moving Average algorithm. First, the poor signal level filter was evaluated to determine the best threshold value for the classifier performance. Second, the window and step sizes for the Simple Moving Average algorithm have been evaluated in a similar manner. In the end, both classifiers have been evaluated by calculating their metrics and improvement ratios for all the included features. Although the performance of both models has been quite similar and overall satisfactory, that stress seems to be detectable in all EEG bands, the model built upon the "Login" dataset performed slightly better than the "Stress" one. The classifier built upon the "Stress" dataset achieved the F1 score of 0.921606 with precision of 0.857198 and recall of 0.996541, while the classifier built upon the "Login" dataset achieved the F1 score of 0.945356 with precision of 0.901603 and recall of 0.993748. Regarding the improvement ratios of the F1 score and the Log loss metrics, although the difference is subtle, the "Login" dataset classifier shows that the alpha, beta, and gamma bands appear to be the most impactful, which is consistent with earlier work[17]. The analysis of the confusion matrices produced by both models indicates that it is possible to use simplified EEG interfaces in stress detection. Within inaccurate predictions, both models tend to skew the results into false-positive area, which in terms of cybersecurity makes it more desirable than skewing into false-negative predictions.

To address the second research question, two classifiers have been built to evaluate the possibilities of using the simplified EEG interface for subject recognition; both of them have been built on the "Login" dataset. Contrary to the stress detection recognition study, these two classifiers were, respectively, binary model calculated for every subject based on the Fast Tree classifier, compared to the one-for-all multi-class model based on the LightGBM classifier. To fine-tune these classifiers, first, the model parameters have been evaluated to determine the best values for both the number of trees and the learning rate for the Fast Tree classifier, along with the number of iterations and the learning rate for the LightGBM classifier. The improvement ratios have been calculated for all available EEG bands, along with the attention and meditation features, to define the impact of a specific feature on the performance of the model. The preprocessing part of the experiment included the poor signal level filter and the Simple Moving Average algorithm. Similarly, the poor signal level filter was evaluated to determine the best threshold value for classifier performance. After that, the window and step sizes for the Simple Moving Average algorithm have been evaluated in a similar manner. In the end, both classifiers have been evaluated by calculating their metrics and improvement ratios for all the included features. Although it is challenging to compare the binary and multi-class models, the metrics of both seem to be satisfactory. The binary classifier achieved the F1 score of 0.927333 with accuracy of 0.984822, while the multi-class model achieved the macro accuracy of 0.929150 and micro accuracy of 0.929454. Such measure values indicate that it may be more viable to create a model per subject in commercial setup, especially that it has the advantage of making the setup process for the new user more streamlined, as the system would not have to re-learn every subject when there is new subject joining the group of users. Regarding the improvement ratios of the metrics, both the binary and multi-class models strongly indicate the importance of alpha, beta, and gamma EEG bands (especially gamma in the multi-class model), which is also consistent with earlier work[17].

The research presented in this thesis has addressed the initial research questions, demonstrating the feasibility of constructing stress detection and subject recognition classifiers using data from simplified EEG interfaces. The metrics obtained, as summarized in the preceding sections, validate the potential of these classifiers. However, this study opens several avenues for future research. One significant recommendation for future work is the anonymization and public dissemination of the datasets used in this study. Making these datasets available on platforms such as GitHub would enable other researchers to replicate and extend the findings presented here, fostering a collaborative environment for further advancements in this field. Such transparency and accessibility are crucial for the validation and refinement of the classifiers developed. Moreover, the domain of simplified EEG interfaces remains rich in unexplored potential. Future research could investigate the optimization of these interfaces for practical applications, particularly in the realm of cybersecurity. The integration of EEG-based stress detection systems in cybersecurity protocols could revolutionize the way digital security is approached, providing real-time monitoring and response mechanisms based on physiological data. In conclusion, while this thesis has made significant strides in demonstrating the capabilities of simplified EEG interfaces for stress detection and subject recognition, it also highlights the vast landscape of opportunities that lie ahead. Continued research and collaboration in this area is essential to fully realize the potential of these technologies, paving the way for innovative applications that improve both scientific understanding and practical utility in cybersecurity and beyond.

Bibliography

[1] EEG Headsets and the Rise of Passthoughts. http://neurosky.com/2017/02/eeg-headsets-and-the-rise-of-passthoughts/. Accessed: 2020-06-08.

[2] LightGBM documentation website. https://lightgbm.readthedocs.io/en/latest/index.html. Accessed: 2024-08-28.

[3] ML.NET official documentation. https://docs.microsoft.com/en-us/dotnet/api/microsoft.ml.automl. Accessed: 2024-08-28.

[4] ML.NET official webpage. https://dotnet.microsoft.com/apps/machinelearning-ai/ml-dotnet. Accessed: 2024-08-28.

[5] ML.NET official webpage. https://learn.microsoft.com/en-us/dotnet/machine-learning/resources/metrics. Accessed: 2024-08-28.

[6] NeuroSky EEG Band Power values meaning. http://support.neurosky.com/kb/development-2/eeg-band-power-values-units-amplitudes-and-meaning. Accessed: 2020-06-14.

[7] NeuroSky MindWave Mobile 2 official product page. https://store.neurosky.com/pages/mindwave. Accessed: 2020-06-08.

[8] NeuroSky ThinkGear chip technical specifications. http://neurosky.com/biosensors/eeg-sensor/. Accessed: 2024-09-02.

[9] Alsumari, W., Hussain, M., Alshehri, L., and Aboalsamh, H. A. Eeg-based person identification and authentication using deep convolutional neural network. *Axioms 12*, 1 (2023).

[10] Alyasseri, Z. A. A., Khader, A. T., Al-Betar, M. A., Papa, J. P., and Alomari, O. a. Eeg-based person authentication using multi-objective flower pollination algorithm. In *2018 IEEE Congress on Evolutionary Computation (CEC)* (2018), pp. 1–8.

[11] Arnau-Gonzalez, P., Katsigiannis, S., Ramzan, N., Tolson, D., and Arevalillo-Herrez, M. Es1d: A deep network for eeg-based subject identification. In *2017 IEEE 17th International Conference on Bioinformatics and Bioengineering (BIBE)* (2017), pp. 81–85.

[12] Bao, X., Wang, J., and Hu, J. Method of individual identification based on electroencephalogram analysis. In *2009 International Conference on New Trends in Information and Service Science* (2009), pp. 390–393.

[13] Białas, K., Kedziora, M., Chałupnik, R., and Song, H. H. Multifactor authentication system using simplified eeg brain–computer interface. *IEEE Transactions on Human-Machine Systems 52*, 5 (2022), 867–876.

[14] Bidgoly, A. J., Bidgoly, H. J., and Arezoumand, Z. A survey on methods and challenges in eeg based authentication. *Computers & Security 93* (2020), 101788.

[15] Bidgoly, A. J., Bidgoly, H. J., and Arezoumand, Z. A survey on methods and challenges in eeg based authentication. *Computers & Security 93* (2020), 101788.

[16] Buzzell, G. A., Morales, S., Valadez, E. A., Hunnius, S., and Fox, N. A. Maximizing the potential of eeg as a developmental neuroscience tool. *Developmental Cognitive Neuroscience 60* (2023), 101201.

[17] Chalupnik, R., Bialas, K., Majewska, Z., and Kedziora, M. Using simplified eeg-based brain computer interface and decision tree classifier for emotions detection. In *International Conference on Advanced Information Networking and Applications* (2022), Springer, pp. 306–316.

[18] Chałupnik, R., Białas, K., Jozwiak, I., and Kedziora, M. Acquiring and processing data using simplified eeg-based brain-computer interface for the purpose of detecting emotions.

[19] Chen, J., Mao, Z., Yao, W., and Huang, Y. Eeg-based biometric identification with convolutional neural network. *Multimedia Tools and Applications 79* (2020), 10655–10675.

[20] Chen, Y., Atnafu, A. D., Schlattner, I., Weldtsadik, W. T., Roh, M.-C., Kim, H. J., Lee, S.-W., Blankertz, B., and Fazli, S. A high-security eeg-based login system with rsvp stimuli and dry electrodes. *IEEE Transactions on Information Forensics and Security 11*, 12 (2016), 2635–2647.

[21] Cheng, S., Wang, J., Sheng, D., and Chen, Y. Identification with your mind: A hybrid bci-based authentication approach for anti-shoulder-surfing attacks using eeg and eye movement data. *IEEE Transactions on Instrumentation and Measurement 72* (2023), 1–14.

[22] Chicco, D., and Jurman, G. The advantages of the matthews correlation coefficient (mcc) over f1 score and accuracy in binary classification evaluation. *BMC genomics 21* (2020), 1–13.

[23] Chuang, J., Nguyen, H., Wang, C., and Johnson, B. I think, therefore i am: Usability and security of authentication using brainwaves. In *International conference on financial cryptography and data security* (2013), Springer, pp. 1–16.

[24] Clapham, C., Nicholson, J., and Nicholson, J. *The Concise Oxford Dictionary of Mathematics*. Oxford Paperback Reference. OUP Oxford, 2014.

[25] da Silva, F. L. *EEG: Origin and Measurement*. Springer International Publishing, Cham, 2022, pp. 23–48.

[26] DelPozo-Banos, M., Travieso, C. M., Weidemann, C. T., and Alonso, J. B. Eeg biometric identification: a thorough exploration of the time-frequency domain. *Journal of neural engineering 12*, 5 (2015), 056019.

[27] DelPozo-Banos, M., Travieso, C. M., Weidemann, C. T., and Alonso, J. B. Eeg biometric identification: a thorough exploration of the time-frequency domain. *Journal of neural engineering 12*, 5 (2015), 056019.

[28] Ekman, P. What scientists who study emotion agree about. *Perspectives on Psychological Science 11*, 1 (2016), 31–34.

[29] Ekman, P., and Cordaro, D. What is meant by calling emotions basic. *Emotion Review 3*, 4 (2011), 364–370.

[30] Elbisy, M. S., and Elbisy, A. M. Prediction of significant wave height by artificial neural networks and multiple additive regression trees. *Ocean Engineering 230* (2021), 109077.

[31] Frank, D., Mabrey, J., and Yoshigoe, K. Personalizable neurological user authentication framework. In *2017 International Conference on Computing, Networking and Communications (ICNC)* (2017), pp. 932–936.

[32] Gallotto, S., and Seeck, M. Eeg biomarker candidates for the identification of epilepsy. *Clinical Neurophysiology Practice 8* (2023), 32–41.

[33] Goldberger, A. L., Amaral, L. A., Glass, L., Hausdorff, J. M., Ivanov, P. C., Mark, R. G., Mietus, J. E., Moody, G. B., Peng, C.-K., and Stanley, H. E. Physiobank, physiotoolkit, and physionet: components of a new research resource for complex physiologic signals. *circulation 101*, 23 (2000), e215–e220.

[34] Gui, Q., Jin, Z., and Xu, W. Exploring eeg-based biometrics for user identification and authentication. In *2014 IEEE Signal Processing in Medicine and Biology Symposium (SPMB)* (2014), IEEE, pp. 1–6.

[35] Hall, J. E. *Guyton and Hall Textbook of Medical Physiology, Jordanian Edition E-Book.* Elsevier Health Sciences, 2016.

[36] Hernández-Álvarez, L., Barbierato, E., Caputo, S., Mucchi, L., and Hernández Encinas, L. Eeg authentication system based on one- and multi-class machine learning classifiers. *Sensors 23*, 1 (2023).

[37] Hunter, D. M., Smith, R. L. L., Hyslop, W., Rosso, O., Gerlach, R., Rostas, J. A. P., Williams, D., and Henskens, F. The australian eeg database. *Clinical EEG and Neuroscience 36*, 2 (2005), 76–81.

[38] Janapati, R., Dalal, V., and Sengupta, R. Advances in modern eeg-bci signal processing: A review. *Materials Today: Proceedings 80* (2023), 2563–2566.

[39] Kanayama, N., Sato, A., and Ohira, H. Crossmodal effect with rubber hand illusion and gamma-band activity. *Psychophysiology 44*, 3 (2007), 392–402.

[40] Kaur, B., Singh, D., and Roy, P. P. A novel framework of eeg-based user identification by analyzing music-listening behavior. *Multimedia tools and applications 76*, 24 (2017), 25581–25602.

[41] Kisley, M., and Cornwell, Z. Gamma and beta neural activity evoked during a sensory gating paradigm: Effects of auditory, somatosensory and cross-modal stimulation. *Clinical neurophysiology : official journal of the International Federation of Clinical Neurophysiology 117* (12 2006), 2549–63.

[42] Koelstra, S., Muhl, C., Soleymani, M., Lee, J.-S., Yazdani, A., Ebrahimi, T., Pun, T., Nijholt, A., and Patras, I. Deap: A database for emotion analysis; using physiological signals. *IEEE transactions on affective computing 3*, 1 (2011), 18–31.

[43] Kopańska, M., Banaś-Ząbczyk, A., Łagowska, A., Kuduk, B., and Szczygielski, J. Changes in eeg recordings in covid-19 patients as a basis for more accurate qeeg diagnostics and eeg neurofeedback therapy: A systematic review. *Journal of clinical medicine 10*, 6 (2021), 1300.

[44] Kostilek, M., and Stastny, J. Eeg biometric identification: Repeatability and influence of movement-related eeg. *2012 International Conference on Applied Electronics* (2012), 147–150.

[45] Lawhern, V. J., Solon, A. J., Waytowich, N. R., Gordon, S. M., Hung, C. P., and Lance, B. J. Eegnet: a compact convolutional neural network for eeg-based brain–computer interfaces. *Journal of neural engineering 15*, 5 (2018), 056013.

[46] Maiorana, E., and Campisi, P. Longitudinal evaluation of eeg-based biometric recognition. *IEEE Transactions on Information Forensics and Security 13*, 5 (2018), 1123–1138.

[47] Mecarelli, O. *Past, Present and Future of the EEG.* 06 2019, pp. 3–8.

[48] Mitchell, H., Johnson, J., and LaForce, S. Wireless emergency alerts: An accessibility study. In *ISCRAM* (2010).

[49] Montoya-Martínez, J., Vanthornhout, J., Bertrand, A., and Francart, T. Effect of number and placement of eeg electrodes on measurement of neural tracking of speech. *Plos one 16*, 2 (2021), e0246769.

[50] Moore, S. K. "brainprint" biometric id hits 100% accuracy [news]. *IEEE Spectrum 53*, 6 (2016), 14–14.

[51] Moran, A. *Sport and exercise psychology: A critical introduction.* Routledge, 2013.

[52] Mueller, V., Richer, R., Henrich, L., Berger, L., Gelardi, A., Jaeger, K. M., Eskofier, B. M., and Rohleder, N. The stroop competition: a social-evaluative stroop test for acute stress induction. In *2022 IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)* (2022), IEEE, pp. 1–4.

[53] Ng, A. Y., et al. Preventing" overfitting" of cross-validation data. In *ICML* (1997), vol. 97, Citeseer, pp. 245–253.

[54] Nie, D., Wang, X.-W., Shi, L.-C., and Lu, B.-L. Eeg-based emotion recognition during watching movies. In *2011 5th international IEEE/EMBS conference on neural engineering* (2011), IEEE, pp. 667–670.

[55] Niedermeyer, E. Alpha rhythms as physiological and abnormal phenomena. *International Journal of Psychophysiology 26*, 1 (1997), 31 – 49.

[56] Niedermeyer, E. *Electroencephalography : basic principles, clinical applications, and related fields*. Lippincott Williams & Wilkins, Philadelphia, 2005.

[57] Opitz, J. A Closer Look at Classification Evaluation Metrics and a Critical Reflection of Common Evaluation Practice. *Transactions of the Association for Computational Linguistics 12* (06 2024), 820–836.

[58] Osgood, C., Suci, G., and Tenenbaum, P. *The Measurement of meaning*. University of Illinois Press, 1957.

[59] Schacter, D. L. *Psychology*. New York, NY : Worth Publishers, 2011.

[60] Shiota, M. N. Ekman's theory of basic emotions. *The SAGE Encyclopedia of Theory in Psychology* (2016).

[61] Stergiadis, C., Kostaridou, V.-D., Veloudis, S., Kazis, D., and Klados, M. A. A personalized user authentication system based on eeg signals. *Sensors 22*, 18 (2022).

[62] Taha, A. A., and Hanbury, A. Metrics for evaluating 3d medical image segmentation: analysis, selection, and tool. *BMC medical imaging 15* (2015), 1–28.

[63] Zhang, X., Zhang, X., Huang, Q., Lv, Y., and Chen, F. A review of automated sleep stage based on eeg signals. *Biocybernetics and Biomedical Engineering 44*, 3 (2024), 651–673.

List of Figures

List of Tables

Appendices

Zał. nr. 2 do ZW 9/2022
Załącznik nr 2 do Regulaminu Komisji ds. Etyki Badań Naukowych

OPINIA KOMISJI DS. ETYKI BADAŃ NAUKOWYCH POLITECHNIKI WROCŁAWSKIEJ nr O-24-41 z dnia 16.07.2024 r.

dotycząca wniosku nr W-24-41 o wydanie opinii w sprawie aspektów etyczno-deontologicznych projektu badań naukowych z udziałem człowieka:

Nazwa projektu badawczego

Badanie zastosowań uproszczonych interfejsówEEG w cyberbezpieczeństwie, detekcji stresu oraz rozpoznawania emocji

Kierownik badania

Imię i nazwisko: Michał Kędziora
Stopień/ tytuł naukowy: dr inż.
Jednostka organizacyjna: Katedra Informatyki Stosowanej, Wydział Informatyki i Telekomunikacji, Politechnika Wrocławska

Po zapoznaniu się z przedłożoną dokumentacją dotyczącą wyżej wymienionego projektu badawczego Komisja ds. Etyki Badań Naukowych Politechniki Wrocławskiej wydaje:

☒ **POZYTYWNĄ OPINIĘ** o zgodności aspektów etyczno-deontologicznych projektu badań naukowych z udziałem człowieka.

☐ NEGATYWNĄ OPINIĘ o zgodności aspektów etyczno-deontologicznych projektu badań naukowych z udziałem człowieka, stanowiącą przesłankę do wstrzymania realizacji projektu.

☐ WARUNKOWO POZYTYWNĄ OPINIĘ o zgodności aspektów etyczno-deontologicznych projektu badań naukowych z udziałem człowieka. Projekt może być realizowany po warunkiem wprowadzenia przez Wnioskodawcę wskazanych poniżej zaleceń Komisji.

Zalecenie:

1. W dokumentacji projektu należy uaktualnić datę rozpoczęcia projektu.

Podpisane elektronicznie przez Jacek Bronisław Cichoń (Certyfikat kwalifikowany) w dniu 2024-07-16.

Podpis przewodniczącego Komisji ds. Etyki Badań Naukowych Politechniki Wrocławskiej

.....

Politechnika Wrocławska
Komisja ds. Etyki Badań Naukowych
Wybrzeże Wyspiańskiego 27,
50-370 Wrocław
T: + 48 71 340 78 20
+ 48 71 320 20 47
komisja.etyki@pwr.edu.pl
www.pwr.edu.pl
www.nauka.pwr.edu.pl
REGON: 000001614
NIP: 896-000-58-51
Nr konta:
37 1090 2402 0000 0006 1000 0434

Zał. nr 1 do ZW 9/2022

Załącznik nr 1 do Regulaminu Komisji ds. Etyki Badań Naukowych

Nr wniosku: ..... *(wypełnia Komisja)*
Data złożenia wniosku: .....

WNIOSEK
o wydanie opinii w sprawie aspektów etyczno-deontologicznych projektu badań naukowych z udziałem człowieka

1. Nazwa projektu badawczego:

Badanie zastosowań uproszczonych interfejsów EEG w cyberbezpieczeństwie, detekcji stresu oraz rozpoznawaniu emocji.

2. Wnioskujący

dr. inż Michał Kędziora

3. Jednostka organizacyjna:

Katedra Informatyki Stosowanej (K45W04N)

4. Kierownik jednostki organizacyjnej:

prof. dr hab. inż. Ngoc Thanh Nguyen

5. Kierownik tematu badawczego/promotor:

dr hab. inż. Ireneusz Jóźwiak, ireneusz.jozwiak@pwr.edu.pl
dr inż. Michał Kędziora, michal.kedziora@pwr.edu.pl

6. Członkowie zespołu badawczego ze wskazaniem osoby odpowiedzialnej za gromadzenie i przechowywanie dokumentacji badania:

dr inż. Michał Kędziora – osoba odpowiedzialna za gromadzenie i przechowywanie dokumentacji badania, opiekun koła naukowego
mgr inż. Katarzyna Białas – doktorantka PWr, asystent opiekuna naukowego
mgr inż. Rafał Chałupnik – doktorant PWr

7. Temat badań:

Tematem badań jest zastosowanie uproszczonych interfejsów EEG w zakresie cyberbezpieczeństwa (w szczególności uwierzytelniania wieloskładnikowego), detekcji stresu oraz rozpoznawania emocji.

8. Miejsce prowadzenia badań:

Sale dydaktyczne lub laboratoryjne Politechniki Wrocławskiej z zachowaniem regulaminów.

9. Data rozpoczęcia badań:

01.07.2024

10. Okres badań:

01.07.2024 – 30.12.2024

11. Informacje o badaniach, z uwzględnieniem aspektów prawno-etycznych i roli człowieka w ich podmiocie (jako załącznik do wniosku - max 500 słów).

12. Wzór informacji dla uczestnika badania (jako załącznik do wniosku- opracowuje kierownik projektu).

13. Wzór zgody na udział w badaniu (załącznik nr 1 lub nr 2). Zgoda powinna zawierać:

1) miejsce na czytelne wpisanie imienia i nazwiska osoby badanej;
2) świadomą dobrowolną zgodę uczestnika badania na udział w eksperymencie;
3) potwierdzenie możliwości zadawania pytań prowadzącemu eksperyment lub badanie i otrzymania odpowiedzi na te pytania;
4) informację o możliwości odstąpienia od udziału w eksperymencie lub badaniu w każdym jego stadium;
5) miejscowość i datę;
6) podpis badanego

14. W przypadku, gdyby zachodziła możliwość identyfikacji osoby biorącej udział w eksperymencie, uczestnik badania powinien wyrazić również zgodę na ujawnienie tego faktu.

Kierownik
Katedry Informatyki Stosowanej
prof. dr hab. inż. Ngoc-Thanh Nguyen
(1)

....

podpis kierownika jednostki organizacyjnej *podpis wnioskującego*

Załączniki:

1. Załącznik nr 1- informacje o badaniu
2. Załącznik nr 2- Zgoda na udział w badaniach
3. Załącznik nr 3- EU_Declaration_of_Conformity_BrainAccess_Kits.pdf – Deklaracja zgodności opaski EEG

Informacja o badaniach, z uwzględnieniem aspektów prawno-etycznych.

„Badanie zastosowań uproszczonych interfejsów EEG w cyberbezpieczeństwie, detekcji stresu oraz rozpoznawaniu emocji."

Jak będzie wyglądało badanie?

Badanie rozpoczyna się od założenia i uruchomienia urządzenia EEG na głowę osoby badanej. Po uruchomieniu aplikacji, osoba badana wpisuje w aplikacji informacje o wieku oraz płci, a także oświadczenia o historii epilepsji, nadużywania alkoholu, papierosów oraz substancji psychoaktywnych. Inne dane nie są wymagane, wobec tego zbierane dane nie spełniają definicji danych osobowych w myśl przepisów RODO. Osoba badana informowana jest o przebiegu badania.

Następnie prezentowany jest ekran utworzenia „konta" w aplikacji. Konto to nie jest nigdzie przechowywane w sposób permanentny – istnieje tylko do potrzeb przeprowadzenia badania. Po założeniu konta osoba badana proszona jest o trzykrotne zalogowanie się do systemu.

Następnie osoba badana proszona jest o trzykrotne zalogowanie się do systemu, gdzie każdemu z tych zalogowań towarzyszyć będzie inny bodziec stresowy:

- dźwiękowy; emisja jednocześnie dwóch dźwięków o częstotliwości odpowiednio X oraz Y Hz,
- wizualny; szybkie wyświetlanie powiadomień typu „pop-up",
- placebo; osoba badana spodziewa się bodźca stresowego, który nie występuje.

Po 10-sekundowej przerwie, osoba badana proszona jest o trzykrotne „włamanie się" na konto innego użytkownika.

Badanie polega na bezinwazyjnym i bezpiecznym dla badanego pomiarze aktywności mózgu, bez bezpośredniej ingerencji w działanie mózgu. Wykorzystywane urządzenie nie jest sprzętem medycznym, a pozyskane pomiary fal mózgowych nie będą danymi o charakterze medycznym.

Jak te dane będą wykorzystywane?

Dane zostaną wykorzystane do stworzenia klasyfikatora, który umożliwi wykorzystanie interfejsu EEG do uwierzytelniania wieloskładnikowego oraz detekcji stresu i rozpoznawania emocji.

Co będzie rezultatem końcowym?

Rezultatem końcowym będzie klasyfikator, który umożliwi uwierzytelnianie wieloskładnikowe z detekcją stresu.

Aspekty prawno-etyczne:

Liczba osób, która będzie brała udział w badaniu to ok. 30 osób pełnoletnich, w tym studenci Politechniki Wrocławskiej. Dane pozyskane przy użyciu interfejsu EEG będą anonimowe i w

żaden sposób nie będą powiązane z osobami z których zostały pozyskane. Dane zostaną wykorzystane do porównania działania wybranych modeli do klasyfikacji tych danych oraz stworzenia modeli klasyfikatorów.
Przed wykonaniem badania, każdy z badanych otrzyma formularz informacyjny dotyczący przebiegu czynności i doświadczeń użytkownika podczas badań.
Zespół badawczy na bieżąco monitoruje stan badanych oraz dopełnia wszelkich starań, aby osoby badane były informowane, że w każdym momencie badanie może zostać przez nich przerwane. Czas badania będzie wynosił około 5 minut.

Zebranie od uczestników danych, będzie wykonane na podstawie świadomej, dobrowolnej i jednoznacznej zgody, informując ówcześnie uczestników o celach przetwarzania tych danych. Zebrane dane osobowe, płeć i przedział wiekowy oraz zapis fal EEG, będą przechowywane w sposób bezpieczny i poufny. Podjęte zostaną odpowiednie środki techniczne i organizacyjne, aby zapewnić ochronę danych przed dostępem osób nieuprawnionych. Po zebraniu danych, niezwłocznie podjęte zostaną natychmiastowe działania w celu anonimizacji danych, tak aby nie można ich było zidentyfikować. Zanonimizowane dane będą przetwarzane w celu analizy i wykorzystania ich do celów naukowych, takich jak prowadzenie nad nimi badań, analizowanie wyników i wnioskowanie. Przetwarzanie danych będzie odbywać się zgodnie z zasadą ograniczenia celu, co oznacza, że dane będą przetwarzane tylko w zakresie niezbędnym do osiągnięcia określonych celów naukowych. Po zakończeniu okresu retencji, dane osobowe zostaną usunięte.

Administrator danych osobowych jest odpowiedzialny za zapewnienie odpowiednich środków ochrony danych, takich jak zabezpieczenia techniczne i organizacyjne, które minimalizują ryzyko nieautoryzowanego dostępu, utraty czy uszkodzenia danych.

Interfejs EEG:

Urządzeniem, które będzie wykorzystywane w badaniach będzie **Neurosky Mindwave Mobile 2.** Posiada ono jedną elektrodę sucho-stykową, do której wykorzystania nie jest potrzebny żel przewodzący. Komunikacja z urządzeniem odbywa się za pomocą łączności bezprzewodowej Bluetooth.

Biorąc pod uwagę Stany Zjednoczone jako rodzimy rynek dla tego interfejsu, spełnia ono wymagania stawiane przez agencję Federal Communications Commission (FCC) (załącznik nr 3 do wniosku).

Szersze informacje o wykorzystywanym sprzęcie można znaleźć pod adresem producenta: https://store.neurosky.com/pages/mindwave

Fachowa dezynfekcja sprzętu wykorzystanego do badań:

Naszym głównym celem jest zapewnienie higienicznych warunków badań oraz minimalizacja ryzyka zakażenia dla naszych uczestników.
W celu skutecznej dezynfekcji opaski EEG, będziemy przestrzegać następujących procedur:

- Wybór odpowiednich środków dezynfekcyjnych: Wykorzystamy tylko te środki dezynfekcyjne, które są skuteczne przeciwko szerokiemu spektrum drobnoustrojów, w tym wirusom, bakteriom i grzybom.

- Przygotowanie przed dezynfekcją: Przed przystąpieniem do procesu dezynfekcji, dokładnie oczyścimy interfejs EEG z widocznych zanieczyszczeń, takich jak kurz czy ślady makijażu, za pomocą miękkiej ściereczki.
- Na miękką ściereczkę lub chusteczkę do dezynfekcji naniesiemy odpowiednią ilość środka dezynfekcyjnego i dokładnie wyczyścimy wszystkie powierzchnie opaski EEG. Skupimy się na dezynfekcji pasków mocujących, elektrod oraz innych obszarów, które mogą mieć kontakt z ciałem osoby badanej.
- Czas kontaktu środka dezynfekcyjnego: Upewnimy się, że środek dezynfekcyjny będzie miał wystarczający czas kontaktu z powierzchnią opaski, zgodnie z zaleceniami producenta, aby zapewnić skuteczną dezynfekcję.
- Wietrzenie i suszenie: Po oczyszczeniu opaski EEG, zostawimy ją na odpowiednim podłożu, aby naturalnie wyschła. Przed ponownym użyciem upewnimy się, że opaska jest w pełni sucha i przygotowana dla kolejnego uczestnika badania.

Nasze procedury dezynfekcji zostaną przeprowadzone z najwyższą starannością i zgodnie z aktualnymi standardami higienicznymi. Będziemy również stale monitorować i aktualizować nasze procedury, aby spełniały wszelkie obowiązujące przepisy związane z ochroną danych osobowych oraz zabezpieczeniem uczestników naszych badań.

Zał. nr 1a do ZW 158/2021

Załącznik nr 1 do Wniosku o wydanie opinii w sprawie aspektów etyczno-deontologicznych projektu badań naukowych z udziałem człowieka

…….....
miejscowość, data

…….....
Nr identyfikacyjny
(wypełnia opiekun badania)

ZGODA NA UDZIAŁ W BADANIACH

Imię i nazwisko osoby badanej:.....

Wiek: .....
Płeć: .....
Jestem osobą praworęczną / leworęczną. (właściwe podkreślić).

Niniejszym oświadczam, że zostałem/am* szczegółowo poinformowany/a* o sposobie przeprowadzenia badań i moim w nich udziale.

Rozumiem, na czym polegają badania i do czego potrzebna jest moja zgoda. Oświadczam, że otrzymałem/am* wyczerpujące, satysfakcjonujące mnie odpowiedzi na zadane pytania, dotyczące tego badania.

Zostałem/am* poinformowany/a*, że mogę odmówić uczestnictwa w badaniach w każdym momencie realizacji projektu badawczego.

Wyrażam opartą na przedstawionych mi informacjach zgodę na uczestnictwo w badaniach.

.....
podpis osoby badanej

KLAUZULA INFORMACYJNA DOTYCZĄCA PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 13 i 14 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE L.2016.119.1 z dnia 04.05.2016 r. – dalej: „Rozporządzenie" lub „RODO"), informujemy, że:

1) Administratorem Danych Osobowych jest Politechnika Wrocławska z siedzibą we Wrocławiu, ul. Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, strona internetowa: www.pwr.edu.pl). Z administratorem danych osobowych można kontaktować się za pomocą formularza kontaktowego na stronie: http://pwr.edu.pl/kontakt. W sprawach dotyczących przetwarzania danych osobowych czy skorzystania z praw dotyczących przetwarzania danych osobowych można się też zwracać bezpośrednio do **kierownika badania** - w tym na jego adres elektroniczny **dr inż. Michał Kędziora – michal.kedziora@pwr.edu.pl**
2) Podstawą przetwarzania będzie art. 6 ust. 1 lit. a RODO.
3) Twoje dane osobowe będą przetwarzane:
   a) przez 5 lat - na potrzeby rachunkowości oraz ze względów podatkowych, okres liczony jest od końca roku kalendarzowego, w którym powstał obowiązek podatkowy;
   b) do czasu wniesienia sprzeciwu lub cofnięcia zgody na przetwarzanie danych osobowych, jeśli Twoje dane przetwarzaliśmy na takiej podstawie.
4) Jednak co do zasady Twoje dane przetwarzane będą przez minimalnie niezbędny okres: przeprowadzania badań naukowych, a następnie będą anonimizowane, przechowywane przez okres niezbędny do rozliczenia grantu, po ukończeniu badań chronione przez pracownika uczelni.
5) W imieniu Administratora dane osobowe przetwarzać będą upoważnieni pracownicy - członkowie zespołu badawczego. Ponadto Administrator udostępni dane osobowe podmiotom, które wybrał do przetwarzania danych osobowych, które przetwarzają dane osobowe w związku z wykonywaniem powierzonego im zadania (np. obsługa IT, przechowywanie danych itp.). Zespół badawczy nie będzie używał usług związanych z transferem danych poza obszar Unii Europejskiej.
6) Przysługują Ci następujące prawa związane z przetwarzaniem danych osobowych:
   a) prawo do wniesienia sprzeciwu wobec przetwarzania danych w celach marketingowych lub badania jakości i satysfakcji – jako że przetwarzamy Twoje dane na podstawie prawnie uzasadnionego interesu,
   b) prawo do wniesienia sprzeciwu wobec przetwarzania danych ze względu na szczególną sytuację – w przypadkach, kiedy przetwarzamy Twoje dane na podstawie naszego prawnie uzasadnionego interesu w celach innych niż w punkcie powyżej,
   c) prawo żądania sprostowania Twoich danych osobowych,
   d) prawo żądania usunięcia Twoich danych osobowych, tylko w sytuacji jeśli nie będziemy zobligowani przepisami prawa do ich przetwarzania,
   e) prawo żądania ograniczenia przetwarzania Twoich danych osobowych,
   f) prawo do przenoszenia Twoich danych osobowych, tj. prawo otrzymania od nas Twoich danych osobowych, w ustrukturyzowanym, powszechnie używanym formacie informatycznym nadającym się do odczytu maszynowego. Możesz przesłać te dane innemu administratorowi danych lub zażądać, abyśmy przesłali Twoje dane do innego administratora. Jednakże zrobimy to tylko jeśli takie przesłanie jest technicznie możliwe.
   g) dostępu do Twoich danych osobowych,

Aby skorzystać z powyższych praw, skontaktować się należy z kierownikiem badania lub wyznaczonym inspektorem ochrony danych. Natomiast do organu nadzorczego zajmującego się ochroną danych osobowych, tj. Prezesa Urzędu Ochrony Danych Osobowych można zwrócić się ze skargą w razie uznania, że przetwarzanie Twoich danych osobowych narusza postanowienia RODO.

7) Zebrane dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, oraz nie podlegają profilowaniu.
8) Podanie danych osobowych jest dobrowolne lecz niezbędne do wzięcia udziału w badaniach.
9) Osoby, których dane dotyczą mają prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem. Wycofanie zgody na przetwarzanie danych osobowych można przekazać tą samą drogą jaką ją udzielono przy czym Administrator danych zastrzega sobie możliwość przeprowadzenia dalszych czynności w celu upewnienia się co do tożsamości osoby wycofującej zgodę.
10) Administrator danych wyznaczył Inspektora Ochrony Danych (adres e-mail: iod@pwr.edu.pl)

FORMULARZ ŚWIADOMEJ ZGODY NA UDZIAŁ W BADANIU

Aplikacji do wykrywania kłamstw z wykorzystaniem interfejsu mózg-komputer oraz algorytmów sztucznej inteligencji

temat badania

Ja niżej podpisana/y ..... oświadczam, że zostałam/em poinformowana/y przez ..... o celu powyższego badania, czasie trwania, sposobie jego przeprowadzenia, oczekiwanych korzyściach, ewentualnym ryzyku i zagrożeniach, wszelkich niedogodnościach związanych z uczestniczeniem w tym badaniu oraz o moich prawach i obowiązkach.

Przeczytałam/em też i zrozumiałam treść Formularza Informacyjnego dla Uczestnika badania. Poinformowano mnie, że dodatkowe pytania dotyczące badania mogę kierować bezpośrednio do osoby prowadzącej badania i że uzyskam na nie wyczerpującą odpowiedź.

Oświadczam, że wszelkie podane przeze mnie informacje są zgodne z prawdą i zapewniam, że będę informowała/ł na bieżąco o wszelkich zmianach w stanie mojego zdrowia.

Jestem świadoma/y przysługującego mi prawa do odstąpienia od udziału w badaniu na każdym jego etapie, bez podania przyczyny. Wiem również, że skorzystanie z tego prawa nie wpłynie na dalszy przebieg mojego badania. Otrzymałam/em do rąk własnych Formularz Informacyjny dla Uczestnika badania oraz Oświadczenie dotyczące zgody na udział w badaniu z klauzulą informacyjną o przetwarzaniu moich danych osobowych.

Niniejszym wyrażam pełną, świadomą i dobrowolną zgodę na udział w tym badaniu oraz na anonimowe przetwarzanie i na publikację wyników moich badań (w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz przyjmuję przedstawione mi warunki.

.....
imię i nazwisko uczestnika badania (drukowanymi literami)

…….....
miejscowość , data, czytelny podpis uczestnika badania

Oświadczenie osoby odbierającej ZGODĘ NA UDZIAŁ W BADANIACH

Ja niżej podpisana/y wyjaśniłam/em osobie biorącej udział w badaniu szczegóły proponowanego badania, zgodnie z opisem w Formularzu Informacyjnym. Zanim podjęte zostały jakiekolwiek procedury omówiłam/em z osobą biorą udział w badaniu jej/jego udział w całym programie badawczym informując o celu i charakterze badania oraz o korzyściach i zagrożeniach wynikających z udziału w tym badaniu. Poinformowałem także o przysługujących jej/jemu prawach wynikających z RODO. Przekazałam/em do rąk własnych Formularz Informacyjny, Formularz Świadomej Zgody na udział w badaniu oraz klauzulę informacyjną dot. ochrony danych osobowych.

….....
imię i nazwisko badacza (drukowanymi literami)

…….....
miejscowość , data, czytelny podpis badacza

**niepotrzebne skreślić*

Formularz Informacyjny dla Uczestnika badania

Informacje o badaniu:

- Badany wchodzi do pomieszczenia, w którym przeprowadzamy badanie.
- Po zajęciu wskazanego miejsca, na głowę osoby badanej zostanie założona uprzednio zdezynfekowana opaska do badania EEG.
- Następnie osobie badanej zostanie przedstawiona aplikacja do zbierania danych (znajdująca się na laptopie).
- Badanie rozpoczyna się od wpisania przez uczestnika wieku oraz płci w aplikacji.
- Utworzenie konta użytkownika w aplikacji
- Rozpoczęcie właściwego badania, które składa się z 3 bloków:
    - Trzykrotne zalogowanie się na swoje konto
    - Trzykrotne zalogowanie się na konto przy obecności bodźców stresowych
    - Trzykrotne włamanie się na konto innej osoby
- Badanie trwa około 5 minut, a przez cały czas przy osobie badanej będzie znajdować się osoba je przeprowadzająca.
- Osoba badana może w dowolnej chwili i bez podania przyczyny zrezygnować z udziału w badaniu.

Safety and Regulations

Operating Conditions

- Operating temperature: 0-35C
- Headset: 1.5V / 95mA maximum average current

Safety

- Batteries should not be exposed to excessive heat such as sunshine, fire, or similar conditions.

ISO/IEC

ISO/IEC Guide 37 [17].

- No naked flame sources, such as lighted candles, should be placed on the apparatus;
- Battery disposal: This product requires the use of an AAA battery. AAA batteries commonly available in the market contains hazardous waste and should be properly disposed of. Contact your local government for disposal or recycling practices in your area.

FCC

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.