National College of Ireland

Integrating Tensor-Based Data Representation and CNN to Detect and Mitigate Noise-Based Attacks on EEG Signals in BCI Systems

MSc Research Project
Cybersecurity

Arun Edathil Veedu
Student ID: x22197931

School of Computing
National College of Ireland

Supervisor: Eugene Mclaughlin

National College of Ireland

National College of Ireland

Project Submission Sheet

Student Name: ……Arun Edathil Veedu…….

Student ID: ……x22197931……

Programme: ……Cybersecurity…… **Year:** …2023-2024……

Module: ……MSc Research Practicum……

Lecturer: ……Eugene Mclaughlin……

Submission Due Date:
……12/08/2024……

Project Title: Integrating Tensor-Based Data Representation and CNN Model to Detect and Mitigate Noise-Based Data Manipulation Attacks on EEG Signals in BCI Systems

Word Count: ……7285……

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature: ……Arun Edathil Veedu……

Date: ……12/08/2024……

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**
5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

AI Acknowledgement Supplement

Cybersecurity

Integrating Tensor-Based Data Representation with CNN Model to Detect and Mitigate Noise-Based Data Manipulation Attacks on EE Signals in BCI Systems

Your Name/Student Number	Course	Date
Arun Edathil Veedu	MSc Cybersecurity	12/08/2024

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click here.

AI Acknowledgment

This section acknowledges the AI tools that were utilised in the process of completing this assignment.

Tool Name	Brief Description	Link to tool
NIL	NIL	NIL
NIL	NIL	NIL

Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used**.

NIL	
NIL	
NIL	NIL

Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

Additional Evidence:

NIL

Additional Evidence:

NIL

Integrating Tensor-Based Data Representation and CNN Model to Detect and Mitigate Noise-Based Attacks on EEG Signal in BCI Systems

Arun Edathil Veedu
X22197931

Abstract

This research report represents a novel framework to integrate Tensor-Based Data encryption and Convolutional Neural Network Algorithms to enhance the detection and mitigation of noise-based data manipulation attacks on electroencephalography (EEG) signals within Brain-Computer Interface (BCI) systems. BCI is an evolving technology where several fields, such as the healthcare industry, entertainment, research, etc., rely on this to assist individuals who have mental or motion disorders. So, this situation necessitates robust security measures against various vulnerabilities, especially noise-based attacks that can compromise the integrity of neural data. This study identifies the gaps in existing detection and mitigation strategies for protecting EEG data from specific types of attacks. The primary research question analyses the impact of noise-based data manipulation attacks and develops an effective model for the integration of machine learning algorithms, such as the Convolutional Neural Network algorithm, with Tensor-Based Data Representation techniques. The primary objective of the proposed model is to produce a comprehensive solution for detecting and mitigating noise-based attacks. This model succeeded on implementing Tensor-Based Encryption and evaluating its effectiveness by simulating three types of ciphertext attacks. Two out of three attacks were failures, and one of them was partially successful. Additionally, the proposed model with CNN showed 97.4025% of detection rate, which is a higher detection rate in a complex brain related signal. However, more advanced version of tensors should be implemented with help of various libraries to prevent all types of ciphertext attacks and integrate advanced ML algorithm with more accuracy in detection.

1 Introduction

A Brain-Computer Interface (BCI) is a technology that connects brain activities in a human brain and external electronic devices (De Venuto, Annese, & Mezzina, 2018). This technology is used by applications in various fields, such as medical rehabilitation, entertainment, and communication for people who have movement disabilities. In general terms, a BCI is a computer-based system that records brain signals, then analyses them, converts them into commands or actions then sends them to an output device to perform a desired action (Shih, et al., 2012) In the past the main goal of the BCI technology was to replace or restore movement functions for the people who have disabilities such as amyotrophic lateral sclerosis, cerebral palsy, stroke, or spinal cord injury (Shih, et al., 2012). This technology has witnessed an evolution from an electroencephalography-based spelling and single-neuron-based device

control to electroencephalographic, intracortical, electrocorticographic, and other signals for increasingly complex control of cursors, robotic arms, prostheses, wheelchairs, and other devices. Additionally, a recent experiment conducted by the Neuralink Corp., owned by Elon Musk, successfully implanted a highly advanced BCI chip into a human brain. He was able to move computer cursors and play chess without any physical interaction but with only his thoughts.

As this technology evolves, the need for a strong and robust security measures becomes more critical (Maiseli, et al., 2023). Previous research has highlighted the importance of addressing these vulnerabilities, but most of these existing mitigation strategies fail to properly understand the unique characteristics of EEG data and its transmission and the specific nature of noise-based attacks (Bernal, et al., 2020). This paper seeks to fill this gap by exploring how Machine Learning techniques can be effectively integrated with Tensor-Based Data Representation techniques to improve the detection and mitigation of noise-based data manipulation attacks in EEG data transmission in a BCI framework.

By addressing the vulnerabilities and mitigation strategies associated with noise-based attacks, this study aims to develop a resilient and adaptable solution that can fortify and protect sensitive neural data from malicious activities. The integration of a powerful machine learning algorithms such as isolation forest or convolutional neural network algorithm with Tensor-Based Data Representation techniques offers a promising approach to enhance the detection and mitigation of these attacks. This will ultimately increase the trust in BCI technologies and facilitate their broader adoption.

1.1 RESEARCH QUESTIONS AND OBJECTIVES

The main research question to help the study is: **What are the impacts of noise-based data manipulation attacks and how can Tensor-Based Data Representation techniques be effectively integrated with Machine Learning Algorithms to detect and mitigate the attacks in EEG (Electroencephalogram) data transmission in a Brain Computer Interface System?**

To address this question, the following objectives have been established:

1. Analyse the impact of noise-based data manipulation attacks such as fake p300 signal insertion techniques on EEG data transmission in BCI systems.
2. Investigate existing Machine Learning algorithms and Tensor-Based Data Representation techniques applicable to EEG data.
3. Develop a framework that integrates appropriate Machine Learning algorithms with Tensor-Based Data Representation techniques for improved detection and mitigation of various attacks.
4. Evaluate the effectiveness of the proposed model through various testing and compare it with existing methods.

These objectives will help the research process, allowing for a systematic study of the problem and the development of innovative solutions.

While the goal of this research is to provide valuable insights and solutions, it is important to find out its limitations. Most of the EEG data are complex due to the variations in individual brain activities. This complexity poses challenges in developing universally applicable models. Additionally, the scope of this study is mainly focused on noise-based attacks, and other types of cyber threats may not be addressed comprehensively. Furthermore, the simulated data generated for training purposes may not completely analyse the complexities of real-world situations, which could affect the generalizability of the findings.

The motivation behind this research arises from the increasing reliance on BCI systems in critical applications, where the integrity of EEG data is paramount. As BCI technology became more important in various domains, the potential consequence of noise-based attacks grew more dangerous. Experts such as (Bernal, et al., 2020) pointed out the critical need for improved security measures to fortify against these vulnerabilities. The current impact of noise-based data manipulation attacks is significant, as they can lead to unauthorised access to confidential neural data. By accessing the sensitive data, they can manipulate it to change the BCI outputs, and ultimately, loss of control over devices.

While several approaches have been proposed to enhance the security of BCI systems, most of them focus on traditional cybersecurity measures that may not be effective against noise-based attacks. These existing sloutions most of the time overlook unique characteristics of EEG data and the specific vulnerabilities related to the technologies. Additionally, there were not enough studies are conducted recently, which means the scope of mitigating various attacks are not explored properly. Due to this reason, traditional anomaly detection methods may struggle to classify the signals as normal and anomaly (Pujari, 2024). The primary intention of this paper is to fill this gap by integrating the ability of Machine Learning techniques to study from complex data patterns and the capacity of Tensor-Based Data Representation techniques to represent multi-dimentional data to address the challenges posed by noise-based attacks.

1.2 REPORT OUTLINE

This report is systematically structured to guide the reader through the research process.

1. **Literature Review / Related Works**: Overview of existing research papers related to noise-based attacks on EEG data transmission, the role of machine learning and tensor-based data representation in BCI security. It will also highlight gaps in the literature related to the proposed solution.
2. **Methodology**: Proposed model design, data collection methods, and other techniques such as data analysis used for the study will be described in detail. Additionally, the section will describe how the objective of the study will be met and the specific tests that will be conducted to evaluate the proposed solution.
3. **Design Specifications**: Technical specifications and requirements for the proposed solution, including hardware and software specifications necessary for the implementation.
4. **Implementation**: Steps taken to develop and implement the proposed framework. It will also include the challenges encountered during the process.

5. **Evaluation**: Results and findings of the tests conducted to evaluate the effectiveness of the proposed model in classifying and mitigating the threats.
6. **Discussion**: The results of the tests will be discussed in this session, and the comparisons to existing literature and potential applications of the findings. Additionally, this session will address the limitations of the study, and assumptions made during the study.
7. **Conclusion and future work**: Summarize the key findings, give brief discussion of the limitations, and proposed directions for future research.

2 Literature Review

Various research studies have shown that BCI technology is hackable (Pugh, et al., 2018) (Enrique Tomás, et al., 2021) (Shaukat, et al., 2020), irrespective of the devices (e.g., EEG Headsets, ECOG, BCI implants (Pugh, et al., 2018), neural patterns (e.g., P300, technology related to movements), and applications (e.g., wheelchair) (Enrique Tomás, et al., 2021). Some of the machine learning algorithms such as Support Vector Machines, Decision trees, and random forests, are vulnerable to various cyber attacks (Shaukat, et al., 2020). In the specific case of manipulation of data using noise-based signals, cyber-attacks can lead to a substantial decrease of up to 74% in the AUC (Area Under the Curve) metric, with the exact reduction depending on familiarity of the attacker with the user's data (Enrique Tomás, et al., 2021).

Method	Solution	Application	Reference
Supervision	Navigation Unit (Camera, laser odometry)	P300-based navigation system	(Escolano, et al., 2012)
	Navigation unit (wheel encoders, proximity sensors, RGBD sensors)	P300-driven wheelchair	(Alimi, et al., 2015)
Authentication	RFID technology	Bidirectional BCI	(Ajrawi, et al., 2021)
	Near-field Communication	User framework	(Zou, et al., 2016)
	Facial recognition	IoT framework	(Mauricio, et al., 2020)
	Brain print biometric authentication	P300-speller	(Rathi, et al., 2020)
		BCI framework	(Borkotoky, et al., 2008)
Encryption	BCI anonymizer	BCI framework	(Bonaci, et al., 2014)
	Tensor-based data representation	EEG data	(Rahman, et al., 2019)
	Chaotic encryption	EEG data	(Iatropoulos, et al., 2021)
	Randomization	BCI framework	(Takabi, et al., 2016)
Cyber-attack identification software	User-specific action profile	User-framework	(Sasko, et al., n.d.)
	User-specific EEG data	EEG data	(Gui, et al., 2016)
		P300 BCI	(Belkacem, 2020)

Table 1. State-of-the-art cybersecurity framework of BCI systems.

Table 1 is a summary of existing cybersecurity solutions to improve the security of neural interface (Bernal, et al., 2020). These proposed methods employ multiple approaches to

supervise the BCI systems (Escolano, Antelis, & Minguez, 2012) (Iatropoulos, et al., 2021), authenticate users (Takabi, Bhalotiya , & Alohaly, 2016), encrypt the data, and ultimately detect cyber threats.

2.1 Noise-based attack on BCI systems

A study of noise-based cyber attacks (Enrique Tomás, et al., 2021) during EEG data transmission in a BCI environment shows that there are mainly two types of noise-based attacks: additive noise attacks and replacement attacks. Additive attack injects noise (synthetic data containing malicious behaviour) directly into EEG signal by keeping the form of original data. Replacement attack, however, substitute the segments of original signals with the noise. This can generate false signals and send them as malicious commands to the output device and changing the course of desired action.

This paper demonstrates that an attacker can manipulate EEG signals to create malicious P300 responses, which leads to incorrect interpretations by the BCI system. These types of attacks do require advanced knowledge on BCI technology, making it easily accessible and more dangerous threat. The noise-based data manipulation attack involves understanding the characteristics of P300 wave. This helps the attacker to optimize the noise injection process by analysing parameters that define P300 response, which increases the chance of a successful attack. Furthermore, the effectiveness of these attacks can vary based on the parameter of the BCI system, such as the threshold set to detect P300 signals. This variability indicates the need of a strong anomaly detection mechanism that can adapt to various attack environments and strategies.

The literature (Enrique Tomás, et al., 2021), explains the impact of noise-based cyber-attacks in a BCI system. This study analyses four different types of noise-based cyber-attacks during the critical stages of BCI framework: the acquisition phase (where EEG signals are collected) and the processing phase (where these signals are interpreted). This paper states that the attacks are significantly influenced by attacker's knowledge. An attacker with minimum knowledge affects acquisition phase by 1% and processing phase by 4%. An attacker with extensive knowledge can impact the acquisition phase 22% and processing phase by 74%. This points out the importance of implementing more robust mechanisms to detect and mitigate cyber-attacks based on the severity of attacks.

Detecting noise-based attack is challenging due to the non-stationary nature of EEG signals and the skills of an attacker to mimic movements and actions. Traditional filtering techniques are weak in distinguish between legitimate signal variations and manipulated variations. However, another study (Mezzina, et al., 2021) stated that they have successfully applied Brain Hacking Recognizer algorithm to detect fake P300 based on median filter. They achieved 99.996% of success rate in detecting fake P300 signals using the algorithm. However, their focus was only on detecting median filter based P300 signals. In this study, the objective is to detect all noise-based data manipulation attacks and integrate the detection technique with a strong data representation and encryption mechanism.

These papers on noise-based attacks indicate that there are gaps in research. Important one is the lack of comprehensive attack taxonomy that encompasses various attack vectors, their methodologies, and potential impact on various BCI applications. Limitations on empirical studies that assess the effectiveness of various noise-based attack types across different BCI systems is another disadvantage. The ability to adapt the detection capabilities based on the dynamic nature of EEG signals is, however, not effective as of the current scenarios. Additionally, there are limited exploration of various machine learning algorithms designed specifically to detect noise-based attacks.

2.2 Machine Learning for Anomaly Detection in EEG transmission

According to (Mufti, et al., 2021), Convolutional Neural Network (CNN) algorithm excels at identifying spatial and temporal patterns in EEG signals, making it more suitable for anoamaly detection tasks. CNN architecture consists of multiple convolutional layers and pooling layers at the bottom. This help reduce dimentiality of the data while preserving essential features. The paper (Wang, et al., 2021) describes another mahcine learning algorithm called Recurrent Neural Algorithm. RNNs are designed to capture temporal dependenceis, making them suited for when the order of data should not be altered.

CNNs are oftn trained on labaled dataset to identify patterns associated with normal and anomalous signals. This model has the capacity to acquire knowledge from raw EEG data, which eliminates the need for extensive feature engineering, which can be time-consuming and subjective. The study by (Mufti, et al., 2021) emphasizes that CNNs can effectively classify EEG signals by leveraging their spatial correlations across multiple channels. Meanwhile, RNNs analyse sequences of data by maintaining a hidden state that carries information across time stamps. This unique characterstic allow RNNs to model temporal dynamics of EEG signals effectively. The study by (Mufti, et al., 2021) suggests that RNNs can be useful in detecting anomalies that manifest over time, such as sudden spikes or shifts in brain activity.

Eventhough the model has significantly higher accuracy rate compared to traditional methods, the requirement of large labaled datasets for training is disadvantage of using CNN algorithm. Additionally, the model proposed in (Mufti, et al., 2021) has 88% accuracy and this resaerch aims to achieve improved accuracy.

2.3 Tensor-Based Data Representation

Tensor-Based Data representation is a powerful technique for analysing and evaluating EEG signals in BCI systems (Rahman, et al., 2019) . Tensors are mathematical objects that convert scalars, vectors, and matrices to higher dimensions. In EEG data, tensors are used to represent multi-channel recordings over time, capturing spatial, temporal, and spectral information simultaneously. According to the study by (Rahman, et al., 2019), tensor decomposition techniques, such as CANDECOMP/PARAFAC (CP) and Tucker decomposition can effectively extract better features from EEG data, enhancing the analysis of brain signal patterns. The study by (Zhang, et al., 2021) highlights that tensor decomposition can improve

EEG signal processing power by effectively isolating noise and artifacts from original neural signals. This is useful in BCI systems, where data integrity is critical for accurate interpretation.

Tensor decomposition process includes breaking down a multi-dimensional array (tensor) into simpler, interpretable components. This feature allows to identify latent structures in the data that may be indicative of anomalies or any other specific state. For example, CP decomposition can be used to sperate the EEG signals into its constituent factors, which give a clear idea of how different brain regions interact during various tasks.

Eventhough, the tensor-based methods are powerful in improving detection accuracy and noise resilience in multi-channel EEG systems, these methods can be computationally intensive, and they require significant processing power and memory resources.This can pose challenges for real-time applications. Integration of tensor with mahcine learning or deep learning techniques will be more effective in detecting and mitigating cyber attacks on BCI systems. The mentioned previous papers only propose tensor as a standalone technique.

These factors indicate the critical gap to be addressed to implement more robust cybersecure BCI frameworks in real-time scenarios. As such, this paper proposes an innovative method that use a resource-efficient, reproducible, and adaptable data representation and encryption technique integrated with more advanced machine learning algorithm to detect cyber-attacks that can happen in an EEG data transmission.

3 Research Methodology

This research focuses on a systematic approach to investigate the security and integrity of EEG signal transmission in a Brain Computer Interface System, particularly against noise-based data manipulation attacks. A thorough review of related papers was conducted as a part of methodology for the enhancement and critical analysis of the proposed model. The papers were selected based on the fact that they have same contents or have the motivation to address the implementation of the current solution. Most of the literature reviewed highlighted resourceful contents and research areas that had methodologies similar to the current study, and most of them are based on machine learning and deep learning technologies. These papers provided a base for the proposed model to develop as well as a foundation for further progress.

3.1 Data Selection

The main objective of this research is to develop a method to detect and mitigate noise-based cyber-attacks on EEG data transmission in a BCI environment. To achieve this, it is essential to acquire data from various sources with specific features. Typically, an EEG dataset should have multiple channels such as Time, Trigger, and Electrode Data. Time is for timestamp of each sample, usually in milliseconds, trigger is a column of event markers that indicate specific events during the recording, and electrode data columns represent data from individual electrodes (e.g., Fp1, Fp2, etc.).

Two types of datasets are considered for this study: dataset from other resources such as internet and dataset from a BCI device. A BCI device (Macrotellect Brainlink Lite v2.0) is used

to collect real-time data for this project to implement the model in real-time. However, the device is a basic BCI headset which only produces a limited number of brain signals such as eye movements, blinking, and eyebrow movements. To train the model in a complex environment, a large dataset is required from other sources.

3.2 Dataset Extraction and Loading

One of the main objectives of this research is to implement various machine learning algorithms on recorded and collected EEG datasets. EEG (Electroencephalogram) is a non-invasive BCI technology used to record the electrical activity of a brain (Bernal, et al., 2020). This technology is mainly used in clinical and research fields due to its ability to provide real-time information about brain function.

There are two types of data are collected: data from BCI device (Macrotellect Brainlink Lite v2.0), which is a basic BCI device consisting of three electrodes. The recording session lasted for 10 minutes with the user performing basic tasks such as blinking eyes, eye movements, and eyebrow movements. The data stream was divided into epochs tied to specific actions or triggers. Each epoch was defined with a time window of -200ms to 800ms.
Another set of data were collected from Kaggle (NIKOLAS, 2021), which contains the recording of 14 individuals performing a motor imagery task. This dataset contains EEG recordings collected using emotive epoch and a BCI headset with 14 individuals (AF3, F7, F3, FC5, T7, P7, O1, O2, P8, T8, FC6, F4, F8, AF4). This dataset consists of short-term continuous EEG recordings of each individuals performing multiple motor imagery tasks. The task given to each individual were to imagine moving their left or right hand without actual movement.

3.3 Data pre-processing and labelling

Various data pre-processing methods were used to ensure stability and reliability of datasets. Primary process did for the pre-processing of the data was to load the data into Jupyter notebook with pandas Data frame format. This helps to analyse and simulate manipulate data using various tools and libraries. This data frame was used to inspect and analyse different EEG channels, event markers, and any other information important for the analysis.

The data frame contains 32 columns with different EEG channels and an unnamed column at the end. It is found that the unnamed column has 8064 missing values. It is confirmed that there are no missing values by checking the output. Each channel showed zero missing values.

Standardization and normalization were one of the main pre-processing techniques used in this research. Normalization enabled all of the features to contribute equally to the analysis by transforming the data to a common scale. Min-max scaling is used for the normalization. The datasets needed to be labelled for the classification of normal signals and manipulated signals.

3.4 Feature Selection

The data frame of the collected data has total of 32 columns and 5 rows representing various electrodes. There are two types of feature engineering are used for this dataset: Manual feature engineering and Automated feature extraction using Principal Component Analysis (PCA).

3.4.1 Manual Feature Engineering

There are three types of manual feature extractions are used: Total, Mean, and Standard deviation.

1. **Total:** Features are calculated manually as the sum of all electrode values for each observation. The total value provided a single metric that reflects the overall brain activity across all electrodes. It is used to identify general trends in brain activity.

2. **Mean:** This feature is used to represent the average value of the electrode readings for each observation. It offered a normalized view of data, which allowed comparisons between different observations. It also helped to understand central tendency of the EEG signals.
3. **Standard Deviation:** Standard deviation is used to quantify the variability of the electrode readings for each observation. It indicated how much the signals deviated from the mean. It helps to understand the stability or fluctuations in brain activity.

3.4.2 Automated Feature Extraction Using PCA

The principal component analysis technique transforms the raw features into a new set of unrelated instances called Principal Components. The PCA variance is calculated to find the component which has majority of the variance. This component represents the most significant underlying pattern in the EEG data.

This process generated new features, labelled as ‘pca_1’, pca_2’, ‘pca_3’, and ‘pca_4’. These labels represent major principal columns.

3.5 Implementing Machine Learning and Deep Learning Algorithms

The pre-processed data was then divided into training and testing using selected features and implemented machine learning and deep learning techniques such as isolation forest algorithm and convolutional neural network algorithm (CNN). Several evaluation techniques were employed to verify which algorithm is best suited to detect cyber-attacks.

3.6 Implementing Tensor-Based Data representation

A 3D tensor is created using TensorFlow, which is a powerful library for machine learning and deep learning. Tensors support arithmetic operations such as addition, multiplication, and matrix multiplication. Various operations in tensor creation are element-wise addition, element-wise multiplication, matrix multiplication, reduction operations, finding maximum values and SoftMax function

4 Design Specification

A laptop with a Windows 11 Home edition Operating System was used to perform the proposed model. Latest version of Python and Anaconda Navigator with Jupyter Notebook were installed for this research.

System Specifications:

- CPU: AMD Ryzen 7 4800H with Radeaon Graphics.
- 16 GB DDR4 RAM
- External GPU Nvidea RTX 3050 with 4GB RAM.
- 1TB SSD storage.

BCI hardware used for the research:

- Mactrotellect Brainlink Lite v2.0 headset: This a BCI hardware which is used to record and analyse brain signal. This device is designed by Epihunter for absence seizure detection, but it can also be used for meditation, concentration training, and research purposes.

Software used:

- 64-bit Windows 11 Home editions.
- Anaconda Navigator with Jupyter Notebook.
- Python 3.12 64-Bit
- EEG recorder (Android)

EEG recorder is an Android application which is used to record EEG signals directly from the brain using a BCI device. It has a simple user interface, and the recorder signals can be converted into .csv file, which is useful for the analysis of collected data in Jupyter Notebook.

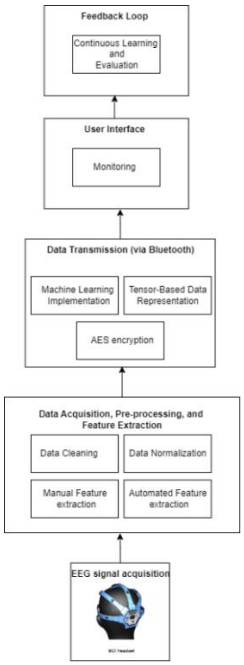


Figure 1. Architecture Diagram of Proposed model in a real-time environment

The EEG data is collected from the brain using a BCI device and applied multiple data pre-processing and feature extraction techniques. The proposed model is implemented and transmitted via Bluetooth technology to an output device. Continuous monitoring and evaluation can be performed in a feedback loop.

5 Implementation

Multiple tools and libraries were used for the entire processing of the model. They include data pre-processing, feature selection, training, and testing the model. All the tools and libraries are discussed in this section below.

5.1 Dataset Preparation

Two types of datasets were used for this research: Data recorded using a BCI device, and a complex dataset collected from Kaggle. Both of the datasets have the same characteristics but with different complexity. The real-time data is basic, having limited number of activities recorded while, the Kaggle dataset have more complex activities recorded from multiple number of individuals. The primary goal of this project is to mix synthetic or attack data with the original data. For this, a synthetic data with custom characteristics were made using the Jupyter Notebook.

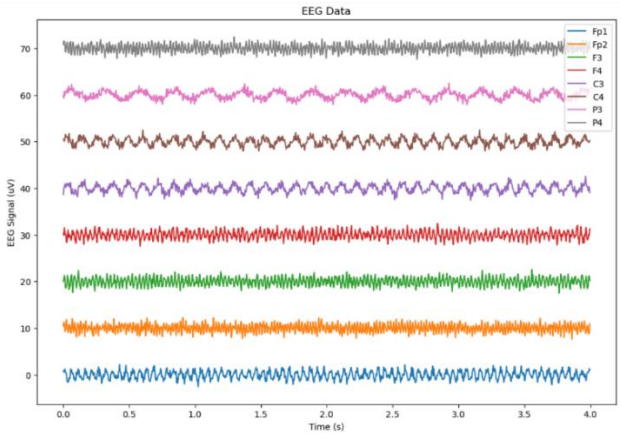


Figure 2. Original EEG data

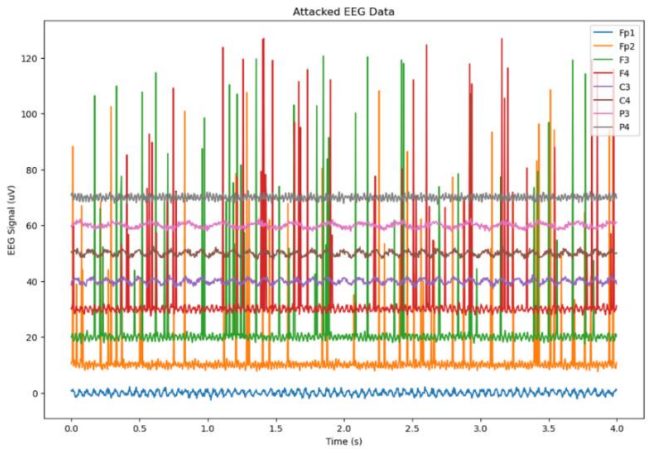


Figure 3. EEG data after signal manipulation.

Three types of attacks were simulated for the project they are: spike, shift, and scaling.

- **Spike attack** introduces sudden, large deviations or spikes in the EEG signal. In this model, random values between 20 and 100 microvolts (uV) were added to the selected samples in the channel. Three channels were randomly selected to simulate the attacks.

$$y[i] = x[i] + \text{spike}$$

where $y[i]$ is the altered EEG data, $x[i]$ is the original data, and the spike is a random value from a uniform distribution.

- **Shift attack** applied a constant shift to the EEG signal, altering its baseline. A random constant value between 10 and 50 uV was added to the selected samples.

$$Y[i] = x[i] + \text{shift value}$$

where shift value is a constant added to all selected samples.

- **Scaling attack** scaled the amplitude of the EEG signal, effectively amplifying or reducing the signals. A random scaling factor between 1.5 and 3.0 is multiplied by the selected samples.

$$Y[i] = x[i] \text{ X scaling factor}$$

where the scaling factor is a random multiplier applied to the selected samples.

The same attack method was used for the two datasets because they both have the same characteristics.

5.2 Feature Selection

Principal components are calculated by generating the standardized data and insert into the eigenvectors that map to only those principal axes with the highest eigenvalues.

5.2.1 Manual Feature Engineering

There are three types of manual features were added: Total, Mean, and Standard Deviation.

1. Total: Total is the sum of all electrode values for each observation.

$$\overline{\text{Total}_i} = \frac{1}{n}\sum_{j=1}^{n} x_{ij}$$

where x_{ij} is the value of the j th electrode for the I th observation, and n is the total number of electrodes.

2. Mean: Mean is the average value of all electrode readings for each observation.

$$\text{mean}_i = \frac{1}{n}\sum_{j=1}^{n} x_{ij}$$

3. Standard Deviation: It quantifies the variability of the electrode readings for each observation.

$$\text{std}_i = \sqrt{\frac{1}{n}\sum_{j=1}^{n}\left(x_{ij} - \text{mean}_i\right)^2]}$$

5.2.2 Automated Feature Engineering Using PCA

Principal Component Analysis (PCA) is used to reduce dimensionality of the datasets without losing as much variance as possible. It converts the original feature into a new coordinate system where the axes or principal components correspond to the directions of maximum variance. Multiple steps were taken to apply PCA.

5.2.2.1 Standardization

The data is standardized to make sure that each feature is distributed equally for the analysis. It is the process of cantering the data (subtracting the mean) and scaling.

$$z_{ij} = \frac{x_{ij} - \text{mean}(x_j)}{\text{std}(x_j)}$$

where z_{ij} is the standardized value of the j th feature for the i th observation.

5.2.2.2 Covariance Matrix

Calculating the covariance matrix of the normalized data is the first step of applying PCA.

$$C = \frac{1}{m-1} Z^T Z$$

Where C is covariance matrix, Z is the matrix of standardized data, and m is the number of observations.

5.2.2.3 Eigenvalues and Eigenvectors

Second step of applying PCA is to compute eigenvalues and eigenvectors of the covariance matrix. The eigenvalue is the amount of variance captured by each principal component and eigenvectors represent the directions of these components.

$$\det(C - \lambda I) = 0$$

where λ is the eigenvalues and I is the identity matrix.

5.2.2.4 Principal Components

Principal components are obtained by projecting standardized data onto eigenvectors corresponding to the largest eigenvalues.

$$PC_i = Z \cdot v_i$$

Where PC_i is the I th principal component, Z is the standardized data matrix, and v_i is the eigenvector corresponding to the i th largest eigenvalue.

After finding and applying the PCA, top feature is selected based on variance. It helps to identify the most informative feature for further analysis.

Top Features = sort(var(df),descending)[:k]

5.3 Dataset Training and Testing

The objective of the model is to train the train dataset and test it with both normal datasets and manipulated datasets. For this process, the model then divided the datasets as X_train and y_train for normal dataset and X_test and y_test for manipulated datasets, where X represents the dataset without the target variable and y denotes the label that characterise the manipulated data.

5.4 Machine Learning and Deep Learning Implementation

There are mainly two algorithms used for testing the modified datasets: Isolation Forest Algorithm and Convolutional Neural Network Algorithm. Both algorithms were used for both recorded and collected datasets. Accuracy, Precision, and Recall values are calculated for the assessment and comparison of the effectiveness of these algorithms.

The machine learning algorithms used for this model was CNN. CNN consists of several layers. Each layer is meant for reducing information parameters by using the feature extraction characteristics from particular layers. The layers of CNN are:

1. **First Convolutional Layer:** This layer has 32 kernels with size 3 to the input data using Rectified Linear Unit (ReLU) activation function. Then the layer extracts local

features from the EEG signals, such as spikes or patterns. They can be used for classifications.

2. **Max Pooling Layer:** It reduces the dimensionality of the features by acquiring maximum value from each pool of size 2. It helps to retain the most important features and reduce computational complexity at the same time to prevent overfitting.

3. **Second Convolutional Layer:** This layer is similar to the first convolutional layer but with 64 kernels and extracts more complex features from the pooled data.

4. **Second Max Pooling Layer:** This layer further reduces the dimensionality of the feature maps and simplify the representation of the data while preserving important features.

5.5 Tensor-Based Data Representation and Encryption

For this model, a 3D tensor is created using TensorFlow. The dimensions are 2,3, and 4. 2 is the first dimension and include number of slices or matrices. 3 is the second dimension with number of rows in each slice. 4 is the third dimension with number of columns in each row. This structure allowed the tensor to be visualized as a stack of two matrices, each matrix containing 3 rows and 4 columns.

A tensor can be represented as $T_{j1\ldots j}^{i1\ldots ip}$

Where 'I' is the contravariant indices, j is covariant indices, p is the number of contravariant indices, q is the number of covariant indices.

Key operations of the process are:

1. **Element-wise Addition:**

$$C_{j_1\ldots j_q}^{i_1\ldots i_p} = A_{j_1\ldots j_q}^{i_1\ldots i_p} + B_{j_1\ldots j_q}^{i_1\ldots i_p}$$

Where A and B are two tensors with the same shape

2. **Contraction:**

$$C_{j_1\ldots j_q}^{i_1\ldots i_{p-1}} = A_{j_1\ldots j_q}^{i_1\ldots i_p} B_{i_p}$$

Contraction reduces the rank of a tensor by adding one contravariant and one covariant index.

3. **Tensor product:**

$$C_{j_1 \dots j_q}^{i_1 \dots i_p} = A_{i_1 \dots i_p} \otimes B_{j_1 \dots j_q}$$

After implementing tensors AES encryption is implemented and three types of cryptographic attacks were simulated for the evaluation of the effectiveness of the model, they are: know-plaintext attacks, cyphertext-only attack, and chosen-plaintext attack.

6 Evaluation

The performance of Isolation Forest and CNN algorithms were evaluated to find out the effectiveness of detecting anomalies in the EEG signals. Additionally, to evaluate tensor-based encryption, three major ciphertext attacks were simulated. This model is evaluated on the basis on accuracy, precision, and the confusion matrix metrics i.e., True positives (TP), True negatives (TN), False Positives (FP) & False Negatives (FN). These metrics give an exhaustive knowledge of how well the acquired model is able to differentiate normal EEG signals and fused versions.

The Confusion Matrix Components are explained below:

1. **True Positives (TP):** The model correctly predicts normal data or class.
2. **True Negatives (TN):** The model correctly predicts manipulated data.
3. **False Positives (FP):** The number of samples falsely predicted as manipulated data, but it is normal data.
4. **False Negative (FN):** The number of samples falsely predicted as normal when it is manipulated.

Evaluation Metrics are explained below:

Here, **TP: True Positive TN: True Negative FP: False Positive FN: False Negative.**

1. **Accuracy:** It helps to measure the overall accuracy of the predictions. Accuracy is the ratio of true positives and true negatives to the total number of instances.

Accuracy = TP + TN / TP + TN + FN + FP.

2. **Precision:** Precision is the ratio of correctly predicted positive observations to the total predicted positive observations.

Precision = TP / TP + FP,

3. **Recall**: It is the proportion of all true predictions (both normal and anomaly classes) overall predictions.

Recall = TP / TP + FN

6.1 Case Study 1: Isolation Forest with recorded EEG signals

The training dataset (manipulated dataset) of recorded EEG signals was used to train the model using Isolation Forest algorithms. After that both normal dataset and manipulated dataset were used to test the Isolation Forest model. The performance of the Isolation Forest model was not enough to detect the anomalies properly.

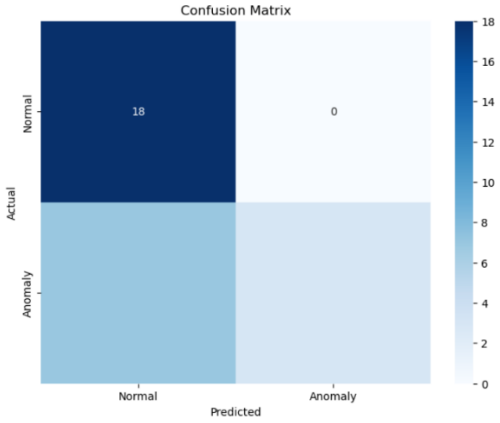


Figure 4. Confusion Matrix

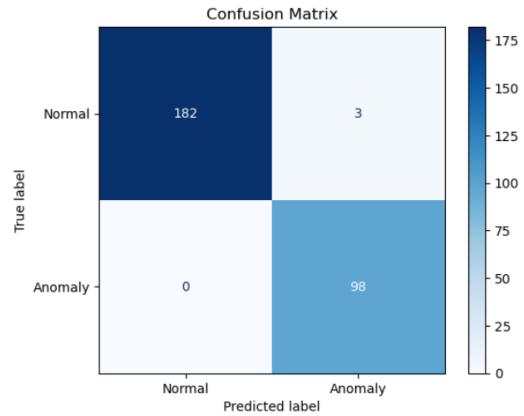
	precision	recall	f1-score	support
0	0.72	1.00	0.84	18
1	1.00	0.30	0.46	10
accuracy			0.75	28
macro avg	0.86	0.65	0.65	28
weighted avg	0.82	0.75	0.70	28

Figure 5. Classification report

Here, a total of 28 samples were analysed. There are two classes of data: Class 0 for normal data and Class 1 for anomalous or manipulated data. In this model, True Positive (TP) is 3, which means 3 instances were correctly predicted as anomalies or manipulated. True Negative (TN) is 18, which indicates that 18 samples were correctly predicted as normal data. False Positive (FP) is 0, which shows that 0 instances were incorrectly predicted as anomalies when they were normal. False Negative (FN) is 7, which means that 7 samples were incorrectly detected as normal when those samples were anomalies. These statistics indicate that this model struggles to identify anomalies from the anomaly class, as it has only 30%.

6.2 Case Study 2: CNN model with recorded EEG Signals.

The training dataset (manipulated dataset) of recorded EEG signals was used to train the model using CNN algorithm. After that both normal dataset and manipulated dataset were used to test the CNN model. The performance of the model was excellent with 98% of accuracy.



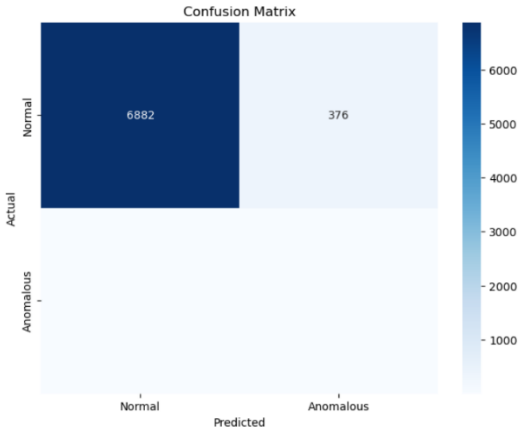
	precision	recall	f1-score	support
Normal	1.00	0.98	0.99	185
Anomaly	0.97	1.00	0.98	98
accuracy			0.99	283
macro avg	0.99	0.99	0.99	283
weighted avg	0.99	0.99	0.99	283

Figure 6. Confusion Matrix **Figure 7. Classification report**

Here, a total of 283 samples were analysed. In this model, the True Positive (TP) is 98, which means 98 instances were correctly predicted as anomalies or manipulated. True Negative (TN) is 182, which indicates 182 samples were correctly predicted as normal data. False Positive (FP) is 3, which shows that 3 instances were incorrectly predicted as anomalies when they were normal. False Negative (FN) is 0, which means that no instances were incorrectly predicted as normal when those instances were actually anomalies. These statistics suggest that the performance of the model is excellent, having a 100% detection rate of data manipulation attacks.

6.3 Case Study 3: Isolation Forest model with Collected Dataset.

The training dataset (manipulated dataset) of recorded EEG signals was used to train the model using Isolation Forest algorithms. After that both normal dataset and manipulated dataset were used to test the Isolation Forest model. The performance of the model with collected dataset where poor, however, accuracy was 91% in detecting the anomalies.



Classification Report:

	precision	recall	f1-score	support
0	1.00	0.91	0.95	7258
1	0.00	0.60	0.01	5
accuracy			0.91	7263
macro avg	0.50	0.76	0.48	7263
weighted avg	1.00	0.91	0.95	7263

Figure 8. Confusion Matrix **Figure 9. Classification report**

A total of 7263 samples were analysed here. Here, we have True Positive (TP)=1 which means that only 1 instance in the model predicted correctly as an anomaly or manipulated. True Negative (TN) 6882, meaning that 6882 samples were correctly predicted normal data. False Positive (FP) = 376 [i.e. number of instances which were actually normal, but our model predicted it as anomaly] FN= 4 that is, for 7 cases the model considered normal while these were anomalies. These performance statistics show that this model is less able to detect anomalies of the anomaly class.

6.4 Case Study 4: CNN model with Collected Dataset

The training dataset (manipulated dataset) of recorded EEG signals was used to train the model using CNN algorithm. After that both normal dataset and manipulated dataset were used to test the CNN model. The performance of the model was excellent with 87% of accuracy.

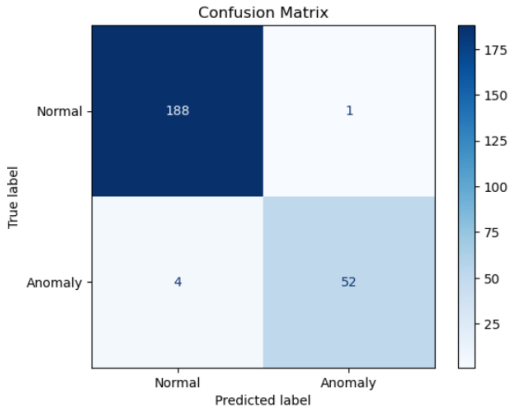


Figure 10. Confusion Matrix

	precision	recall	f1-score	support
Normal	0.98	0.99	0.99	189
Anomaly	0.98	0.93	0.95	56
accuracy			0.98	245
macro avg	0.98	0.96	0.97	245
weighted avg	0.98	0.98	0.98	245

Figure 11. Classification report

There were 189 samples analysed in total here. So, in this model, True Positive (TP) is 52 i.e. there are total 52 instances correctly identified as anomalies or manipulated. TN is 188, This means those are the normal (samples were predicted as normal which was correct) samples. FP is 1 (False Positive) where the model incorrectly predicts an instance in which they were normal as anomalous. FN (False Negative) is 4, which means in other words that there are 4 instances as anomaly, but the model predicts them were normal. The model performance is evident from these statistics as on real time it detects almost 92.85% data manipulation attacks.

6.5 Tensor-Based Data Representation and Encryption

A three-dimensional tensor is created for the recorded EEG dataset. Then the dataset is converted into a 3D array by applying various mathematical calculations such as element-wise addition and contraction. The shape of the converted tensor is shown below.

```
TensorFlow tensor shape: (2, 3, 4)
Element at position [1, 2, 3]: 0.3422674
Modified tensor after addition:
 [[[1.1317538 1.5578326 1.7065123 1.387009 ]
  [1.6917559 1.1909037 1.7110251 1.9765973]
  [1.2348795 1.9593984 1.405099  1.2659248]]

 [[1.3227973 1.4295759 1.9788857 1.6171049]
  [1.3577951 1.3511323 1.6141232 1.0948052]
  [1.2541275 1.8853934 1.2475067 1.3422674]]]
```

This process creates a three-dimensional tensor using TensorFlow, which is a structured way to organize data. Here, the tensor has a shape of (2,3,4). It means that the tensor consists of 2 slices, each containing 3 rows and 4 columns. This representation allows efficient computation and manipulation especially for machine learning model. Additionally,

AES (Advanced Encryption Standard) is used for the encryption with Cipher Block Chaining Mode. To assess the effectiveness of the tensor-based encryption, three types of ciphertext

attacks were simulated using Jupyter Notebook: known-ciphertext attack, ciphertext-only attack, and chosen-plaintext attack. Two of the three attacks were failed and could not acquire the encryption key. However, the chosen-plaintext attack was able to acquire the plaintext length.

7 Discussion

This study involved a comprehensive analysis of the performance of Isolation Forest and Convolutional Neural Network (CNN) algorithms as well as the Tensor-Based Data Representation with AES encryption. Both Machine Learning and Deep Learning algorithms had higher performance metrices and the CNN model is the best among them. With the CNN model, there were total of 528 samples tested with two datasets, among them, 154 samples were in anomaly class. Among them 150 of the anomalies were detected as anomalies and achieved 97.4025% detection rate, which surpasses the detection rate mention in the paper (Mufti, et al., 2021). Integrating the CNN model algorithm with Tensor-Based encryption can fortify the system against noise-based data manipulation attacks. However, there can be false positives in the proposed model due various reasons such as the noise added to the signals can be very small and Real EEG data can contain artifacts and noise from various sources like muscle movements, eye blinks, etc. These noises can make it harder to distinguish between normal and manipulated data

The tensor-based data representation is highly effective in securing data from external access. The tensor decomposition process itself can be used as a layer of encryption. So, the EEG signals remain protected even if the compressed tensor data is encrypted. Before approaching tensor data, the attacker may have to break AES encryption, which is even harder to perform. The CNN model can detect and alarm professional even if an attacker gained access to the EEG signal. Almost all types of noise-based attacks can be detected and alerted based on the proposed solution. Which means that the multiple layers of security frameworks can provide better protection from various attacks compared to previous papers discussed above. However, there are some disadvantages that may affect implementing or calculating tensor dimensions. Tensors can consume a significant amount of memory for large datasets or higher dimensional tensors.

8 Conclusion and Future Directions

This study focuses on detecting noise-based data manipulation attacks on EEG transmission in a BCI environment with machine learning and deep learning algorithms and tensor-based data representation. Various features were selected using manual and automated feature engineering from recorded and collected datasets. Major features were selected using PCA. This approach could enhance the ability of the model to work more effectively by providing key features that would assist the model to make accurate predictions. The proposed model is trained and tested with manipulated datasets. Among the two algorithms namely, Isolation Forest and Convolutional Neural Network algorithms, the CNN model found to be more effective in detecting anomalies from EEG signals. CNN showed 97.4025% accuracy in detecting

manipulated signals. The model contains some false positives and false negatives however, the false negative is very low as negligible. The tensor-based data representation and encryption makes the EEG data transmission more secure by changing the shape of data into different 3D arrays. This makes it harder for an attacker to gain access and decrypt the data.

The future the proposed model could focus on integrate Tensor-Based Data Representation with other data modalities such as Multimodal Data Fusion by combining EEG data with other physiological signals (e.g., ECG, EOG) to create comprehensive model that enhance detection capabilities. Implementing the tensor methods to other domains such as image or video data, to draw parallels and improve the efficiency of EEG analysis. Implementing deep tensor neural networks that can capture complex patterns in higher dimensional data while keeping the benefits of tensor data representations. Additionally, exploring broader range of noise-based attacks other than data manipulation could be carryout by various machine learning and deep learning techniques. Finally, assessing long-term effectiveness of the proposed detection and mitigation strategies against evolving noise-based attacks could be important to conduct further research due to the future scope of BCI technology.

9 References

Ajrawi, S., Rao, R., & Sarkar, M. (2021, 01 01). Cybersecurity in Brain-Computer Interfaces: RFID-based design-theoretical framework. *Informatics in Medicine Unlocked*. doi:10.1016/j.imu.2020.100489

Ashik Mostafa Alvi, Siuly Siuly, & Wang, H. (2021). Developing a Deep Learning Based Approach for Anomalies Detection from EEG Data. *Web Information Systems Engineering – WISE 2021. WISE 2021. Lecture Notes in Computer Science, 13080*, 591-602. doi:10.1007/978-3-030-90888-1_45

Belkacem, A. (2020, 10 01). Cybersecurity Framework for P300-based Brain Computer Interface. *IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 1-6. doi:10.1109/SMC42975.2020.9283100

Bernal, S., Martínez, G., Taynnan, M., Balasubramaniam, S., Celdrán, A., Martínez Pérez, G., & Barros, M. (2020). Security in Brain-Computer Interfaces: State-Of-The-Art, Opportunities, and Future Challenges. doi:10.1145/3427376

Bonaci, T., Herron, J., Matlack , C., & Chizeck, H. (2014). Securing the exocortex: A twenty-first century cybernetics challenge. *2014 IEEE Conference on Norbert Wiener in the 21st Century (21CW)*, 1-8. doi:doi: 10.1109/NORBERT.2014.6893912

Borkotoky, C., Galgate, S., & Nimbekar, S. (2008). Human computer interaction: harnessing P300 potential brain waves for authentication of individuals. *1st Bangalore Annual Compute Conference (COMPUTE '08)*, 1-4. doi:https://doi.org/10.1145/1341771.1341797

De Venuto, D., Annese, V., & Mezzina, G. (2018). Real-time P300-based BCI in mechatronic control by using a multi-dimensional approach. *IET Software, 12*(5), 418-424. doi:10.1049/iet-sen.2017.0340

Enrique Tomás, M., Mario, Q., Sergio, L., Alberto, H., & Gregorio, M. (2021). Noise-based cyberattacks generating fake P300 waves in brain–computer interfaces. *Cluster Computing, 25*. doi:10.1007/s10586-021-03326-z

Escolano, C., Antelis, J., & Minguez, J. (2012, 06). A Telepresence Mobile Robot Controlled With a Noninvasive Brain–Computer Interface. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 42*(3), 793-804. doi:10.1109/tsmcb.2011.2177968

Gui, Q., Yang, W., Jin, Z., Ruiz-Blondet, M., & Laszlo, S. (2016). A residual feature-based replay attack detection approach for brainprint biometric systems. *IEEE International Workshop on Information Forensics and Security (WIFS)*, 1-6. doi:10.1109/WIFS.2016.7823907

Iatropoulos, A., Moysis, L., Giakoumis, A., Volos, C., Ouannas , & Goudos, S. (2021). Medical Data Encryption based on a Modified Sinusoidal 1D Chaotic Map and Its Microcontroller Implementation. *10th International Conference on Modern Circuits and Systems Technologies (MOCAST)*, 1-4. doi:10.1109/MOCAST52088.2021.9493422

Khaled Salhi, Alimi, A., Moncef, M., & Philippe Gorce. (2015, 12 1). Improved secure navigation of wheelchairs using multi-robot system and cloud computing technologies. *2015 11th International Conference on Information Assurance and Security (IAS)*, 50-54. doi:10.1109/ISIAS.2015.7492744

Maiseli, B., Abdalla, A., Massawe, L., Mbise, M., Mkocha, K., Nassor, N., . . . Kimambo, S. (2023). Brain–computer interface: trend, challenges, and threats. *Brain Informatics, 10*(1). doi:10.1186/s40708-023-00199-3

Mauricio, C., Fernando Gomez Cruz, & Sebastian, J. (2020, 09 30). Software architecture for the application of facial recognition techniques through IoT devices. 1-5. doi:10.1109/coniiti51147.2020.9240416

Mezzina, G., Annese, V., & De Venuto, D. (2021). A Cybersecure P300-Based Brain-to-Computer Interface against Noise-Based and Fake P300 Cyberattacks. *Sensors, 21*(24). doi:10.3390/s21248280

NIKOLAS. (2021). *Kaggle*. Retrieved from https://www.kaggle.com/datasets/samnikolas/eeg-dataset/data

Pugh, J., Pycroft, L., Sandberg, A., Aziz, T., & Savulescu, J. (2018, 07 30). Brainjacking in deep brain stimulation and autonomy. *Ethics and Information Technology, 20*(3), 219-232. doi:10.1007/s10676-018-9466-4

Pujari, S. (2024, 3 30). Light weight neural network for ECG and EEG anomaly detection in IOT edge sensors. *World Journal of Advanced Engineering Technology and Sciences, 11*(2), 269-280. doi:10.30574/wjaets.2024.11.2.0111

Rahman, M., Bardhan, S., Neupane, A., Papalexakis, E., & Song, C. (2019). Learning Tensor-Based Representations from Brain-Computer Interface Data for Cybersecurity. *Machine Learning and Knowledge Discovery in Databases, 11053*. doi:https://doi.org/10.1007/978-3-030-10997-4_24

Rathi, N., Singla, R., & Tiwari, S. (2020, 10 1). Authentication framework for security application developed using a pictorial P300 speller. *Brain-Computer Interfaces, 7*(3-4), 70-89. doi:10.1080/2326263x.2020.1860520

Sasko, A., Hillsgrove, T., Gagneja, K., & Katugampola, U. (n.d.). System Usage Profiling Metrics for Notifications on Abnormal User Behavior. *Future Network Systems and Security. FNSS 2019. Communications in Computer and Information Science, 1113*. doi:https://doi.org/10.1007/978-3-030-34353-8_11

Sharaban Tahura, S. M. Hasnat Samiul, Mufti, M., & Kaiser, M. (2021). Anomaly Detection in Electroencephalography Signal Using Deep Learning Model. *International Conference on Trends in Computational and Cognitive Engineering. Advances in Intelligent Systems and Computing, 1309*, 205-217. doi:10.1007/978-981-33-4673-4_18

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I., Chen, S., Liu, D., & Li, J. (2020, 05 15). Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cybersecurity. *Energies, 13*(10), 2509. doi:10.3390/en13102509

Shih, J., Krusienski, D., & Wolpaw, J. (2012, 03). Brain-Computer Interfaces in Medicine. *Mayo Clinic Proceedings, 87*(3), 268-279. doi:10.1016/j.mayocp.2011.12.008

Takabi, H., Bhalotiya , A., & Alohaly, M. (2016). Brain Computer Interface (BCI) Applications: Privacy Threats and Countermeasures. *IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*, 102-111. doi:10.1109/CIC.2016.026

Wolpaw, J., Birbaumer, N., McFarland, D., Pfurtscheller, G., & Vaughan, T. (2002, 6). Brain–computer interfaces for communication and control. *Clinical Neurophysiology, 113*(6), 767-791. doi:10.1016/s1388-2457(02)00057-3

Zhang, Q., Guo, B., Kong, W., Xi, X., Zhou, Y., & Gao, F. (2021). Tensor-based dynamic brain functional network for motor imagery classification. *Biomedical Signal Processing and Control, 69*. doi:10.1016/j.bspc.2021.102940

Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016, 09). A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *104*(09), 1727-1765. doi:10.1109/jproc.2016.2558521