Scholars Journal of Engineering and Technology
Abbreviated Key Title: Sch J Eng Tech
ISSN 2347-9523 (Print) | ISSN 2321-435X (Online)
Journal homepage: https://saspublishers.com

OPEN ACCESS

Exploring How AI Can Monitor and Secure Neurodata Transmission from Bcis Against Hijacking or Leakage

Gaurang Deshpande[1*]

[1]Software Developer, IBM, USA

DOI: https://doi.org/10.36347/sjet.2024.v12i12.011 | **Received:** 25.11.2024 | **Accepted:** 28.12.2024 | **Published:** 30.12.2024

***Corresponding author:** Gaurang Deshpande
Software Developer, IBM, USA

Abstract **Original Research Article**

Abstract : This study examines how Artificial Intelligence (AI) can be used to monitor and protect the transmission of neurodata by Brain-Computer Interfaces (BCIs) against hijacking and data spilling. Through updated literature as well as examining two case studies based in the Cognetivity and Emteq Labs, the paper notes the incorporation of Deep learning, homomorphic encryption, anomaly detection, and federated learning. The study uses a secondary qualitative and quantitative explanatory research design. The most important findings disclose the opportunities and issues of AI when it comes to the protection of neural data. The research suggests lightweight privacy-preservation AI models and collaboration strengthening to achieve safe, ethical consumption of BCIs in real-life settings.

Keywords: Brain-Computer Interface (BCI), Artificial Intelligence (AI), Neurodata, Hijacked, Signal Spoofed, Data Leaked, Neurodata Transmission, Machine Learning (ML) and Deep Learning (DL), EEG-based BCIs.

Copyright © 2024 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution **4.0 International License (CC BY-NC 4.0)** which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use provided the original author and source are credited.

I. INTRODUCTION

A. Background of the study

Artificial intelligence (AI) and neurotechnologies have moved to a new stage of brain-computer interface (BCI) evolution, when such systems can allow the human brain and external devices to communicate. BCIs are already in use in healthcare, soldier training, education, and entertainment, assisting people with disabilities, improving mental functioning and neuroprosthetic control [9]. Nevertheless, neurodata, i.e., information directly based on brain activity, presents critical issues regarding person privacy, information integrity, and cyberdefence. Neurodata is unprecedented and may be intercepted and/or tampered with unprecedented consequences; this is since the theft of such data may involve affecting unauthorised conduct on someone, and even identity theft.

B. Overview

Neurodata transmission via digital network has increased with non-invasive and implantable BCIs coming up. But such channels can be hijacked, signal spoofed, data leaked, and other intruders can occur in the form of cyber intrusion. More conventional forms of encryption might not be adequately flexible or lightweight to accommodate real-time neurodata streams. The security of neurodata is becoming a concern, with AI-based security systems (including anomaly detection, predictive threat analytics, and adaptive encryption algorithms) becoming a promising means of monitoring and securing neurodata [10].

C. Aims and Objectives

The objectives are: 1) To describe existing AI-based mechanisms of real-time monitoring and anomaly detection with the neural data system.2) To explore the use of machine learning (ML), deep learning (DL) algorithms to improve encryption and authentication of BCI neurodata. 3) To access the presented case studies and practical application of AI-driven security systems in neural and biomedical communication systems.4) To specify the main issues that have been hampering the popularisation of BCI neurodata (the obstacles of ethics, computational and technological challenges) and offer ways of using AI in a manner that could overcome these obstacles.

D. Problem Statement

Regardless of the expanding body of BCI employment, no strong security schemes have been developed, particularly to secure neural data. Cybersecurity systems are not quite effective when dealing with large scales, speed and sensitivity of neurodata transmission [11]. This presents a big weakness where the users become prone to data hijacking, manipulation and exploitation

E. Scope and Significance

This study will look into the part that AI will play in the secure transfer of neurodata in non-invasive and invasive BCI systems. It is significant in the improvement of users' safety and morals, and the credibility of neurotechnologies. The results can be used in the advancement of future generations' AI security measures used by the nurotech industry in general.

II. LITERATURE REVIEW

A. AI-driven real-time monitoring and anomaly detection

New research in this area highlights the need to identify adverse or anomalous activities on neurodata flows. EEG-based BCIs are susceptible to backdoor poisoning attacks on machine learning models: During training, attackers add misleading training data to accumulate incorrect types of weights; during inference operation, these weights lead to the incorrect classification of the new EEG signals [1]. This creates a priority in the use of real-time monitoring systems able to provide the detection of abnormal patterns or perturbations in neural data.

Similar directions in space-time and high-dimensional anomaly detection methods, including EEG, are exhibiting good directions. PyOD and scikit-learn provide scalable detectors of anomalies that can be applied to streaming signals [2]. The combination of these tools with deep learning architectures may help analyse the temporal features and raise the alarm on inconsistent patterns that may not be observed in the expected behaviour of neurodata.

B. ML and DL algorithms for encryption and authentication of BCI Neurodata

In order to improve the security of Brain-Computer Interface (BCI) systems, scientists started using machine learning (ML) and deep learning (DL) along with encryption/validation rules. Several researchers have also shown how homomorphic encryption can be utilised, together with convolutional neural networks (CNNs), to categorise encrypted EEGs without violating their privacy [3]. On the same note, deep learning functionalities are used to encrypt data using the Paillier encryption system, which allows encrypted multi-classification using EEG [4]. By using these methods, it is not necessary to decrypt data to process it, and in turn, opens the data to fewer threats. Moreover, adaptive DL frameworks, including autoencoders and LSTM networks, can change the pattern of unauthorised access in real-time and enhance the authentication level. These models learn to recognise injury in high-dimensional, time-series neural data and offer a smart film of protection custom-made to the specific areas of neurodata transportation in BCIs. In such a way, ML/DL methods propose scalable, context-sensitive solutions to protect brain signals to be used as digital interfaces.

C. Real-life examples and practical AI-Security Implications

There are a number of both real-world and experimental frameworks in which the privacy protection with the use of AI is achieved. Using a secure multiparty computation (SMC) protocol, a protocol was designed to undertake linear regression on EEG signals and based on this, cognitive states such as the level of drowsiness of the driver of different users could be estimated in a privacy-preserving way [5]. The system has taken advantage of federated and transfer learning techniques to ensure data confidentiality and optimise model flexibility. A collaborative architecture of EEG classification via federated transfer learning was presented, enabling collaborative learning without the transfer of raw data [6]. Subject-adaptive accuracy was boosted by ~2-6% using this framework over centralised methods, demonstrating how AI can be used in BCI systems to both secure and enhance learning.

D. Challenges in securing Neurodata and its AI-enabled solutions

Challenges

Computational cost: Homomorphic encryption and chaos-resistant encryptions have large processor offsets that could potentially impact the functionality of real-time-based systems [3]. Neural network vulnerability is neural network deployed during encryption/ decryption or anomaly detection may be vulnerable to adversarial attacks (e.g. poisoning or evasion) [7]. In Data heterogeneity, the EEG data is not flat across individuals and sessions, and this makes it challenging to develop coherent security models. Federated and transfer learning are less helpful and induce concerns of trust and synchronisation.

Solutions

Hybrid encryption systems: A transmission method uses lightweight chaos-based encryption, and a sensitive computational method uses homomorphic encryption [8].

Solid anomaly detectors: Placing ensemble-driven or unsupervised AI systems both at the edge and on the server side to check the integrity of data constantly

Adaptive federated learning: Maintaining trust by adding secure aggregation and differential privacy to support the trade-off between personalisation and the risk of privacy exposure.

III. METHODOLOGY

A. Research Design

The given research acquires the type of an explanatory research design, and the aim is to explore how Artificial Intelligence (AI) can control and protect the transmission of neurodata through Brain-Computer Interfaces (BCIs) in order to prevent its hijacking or leakage. Explanatory research will be appropriate because it aims at finding the cause-and-effect associations, investigating the underlying processes, and explaining how AI tools can support the protection of BCI data [12]. The analysis is interested in determining the particular role and capabilities of AI-driven models that involve machine learning (ML) and deep learning (DL) in solving security-related issues in neurodata.

B. Data Collection

The study has adopted both qualitative and quantitative sources in its secondary data collection procedures. The data is qualitative and is collected using peer-reviewed academic journals, white papers, open-access conference proceedings, and reports. These involve investigations into AI-powered encryption, neurodata privacy, neural system cybersecurity, and advancements in the BCI.

Existing statistical databases and published datasets on cyberattack incidents of neurotechnology, accuracy measures of AI-based systems, and computer benchmarks (mainly latency and energy efficiency, as well as classification accuracy) of BCI applications are the sources of quantitative data. Available empirical data can be obtained on PubMed Central, MDPI, IEEE Xplore, Statista and the National Cyber Security Centre (NCSC).

C. Case Studies and Examples

Case Study 1. Cognetivity Neurosciences (London)

Cognetivity is a UK-based neurotechnology company that has created an AI-based platform to identify cognitive impairment through simple, non-invasive neural evaluations that are done at an early stage [13]. Neural response patterns are examined using deep learning models used in the company. Their scope is limited to diagnostics, but their work indicates that AI can process, authenticate and secure real-time neural data. In 2020, the company collaborated with the NHS in making sure that AI models comply with the Data Security and Protection Toolkit (DSPT) requirements of the NHS Digital [14]. Their safe data processing activities can bring some information about how the data produced with BCI can be secured using cloud platforms with embedded AI.

Case Study 2. Emteq Labs (Brighton)

Emteq Labs focuses on wearable neurotechnology, emotion-sensing, Bio signal (EEG, EMG), and AI analytics, using novel feedback mechanisms and emotion analytics models that largely focus on videoconferencing and online meetings [15]. They have a neurophysiological sensor and software affixed to the face that monitors neurophysiological signals and classifies and stores them securely via machine learning. The fact that the firm applies federated learning to do model training without having to transfer sensitive data shows how decentralised AI can be used to ensure that data is not leaked and how it can be used to comply with GDPR when transferring neurodata [16].

D. Evaluation Metrics

A multi-dimensional evaluation framework is used in this study to evaluate the effectiveness of AI-enabled ways of securing the neurodata transmission of a BCI system. The most important measures are their accuracy and precision, which evaluate how well the system can detect unauthorised access or anomalies in neural data streams. Latency is also measured in an effort to know the delay caused by the encryption or anomaly detection operations, especially in real-time cases that are essential to BCIs [17]. The accuracy of true positive and false negative results is evaluated to determine the accuracy of AI models in predicting real threats and normal patterns of neurodata [18]. Computational overhead is taken into account; it looks at the processing power needed and the energy consumption of the AI algorithms, and therefore, on edge-computing devices, there are limits on resources to compute.

IV. RESULTS

A. Data Presentation

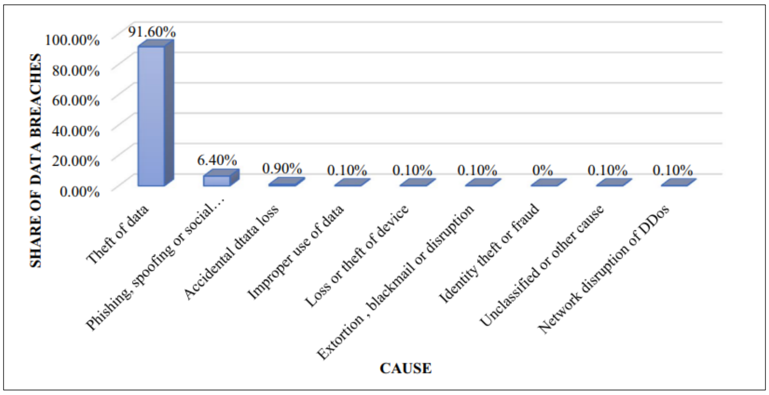

Figure 1: Leading response to data breaches in 2022 globally
(Source: [19])

Figure 1 identifies the reasons for data breach issues in 2020. It is found from the graph that hijacking, leaking, and hacking are the critical challenges of maintaining the security of confidential data. This graph highlights that theft of data was 91.60% and phishing, spoofing issues were 6.40% [19]. This threat will increase if the organisation does not take proper action to maintain the security of data using advanced technology like AI or Artificial Intelligence.

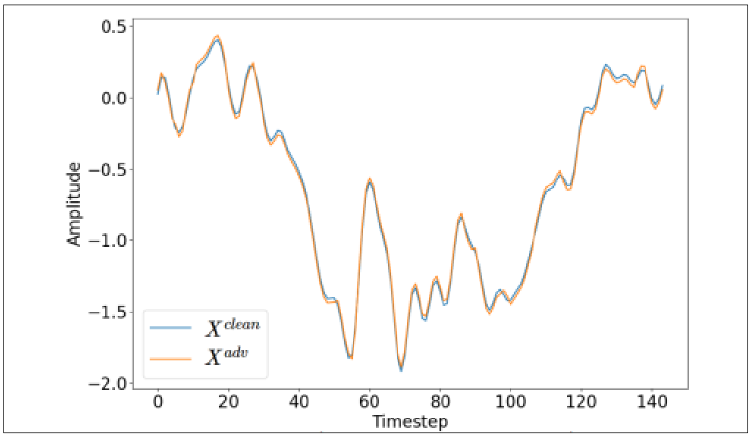

Figure 2: PGD attack on an EEG
(Source: [17])

Figure 2 highlights the PGD attack on EEG. The Fast Gradient Sign method and Projected Gradient Descent are two EEG-based state-of-the-art white-box attacks. In this image PGD attack (40 iterations, = 0.5) on an EEG sample of the P300 dataset. The perturbed signal is close to the physiologically plausible signal, but the final prediction differs [17].

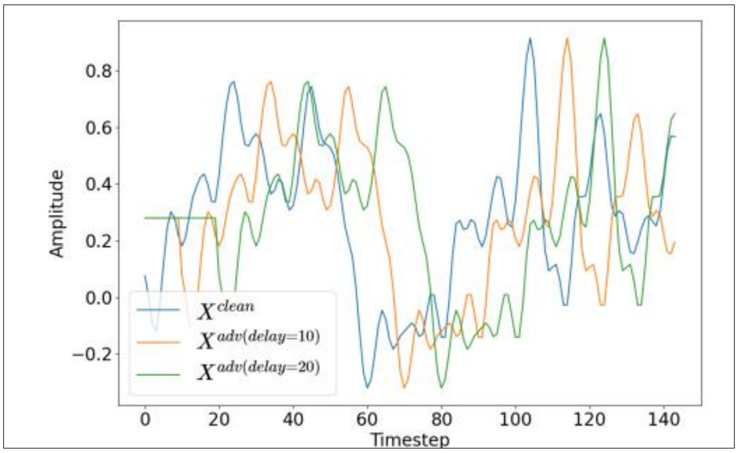

Figure 3: Peripheral injection attack on EEG
(Source: [17])

Figure 3 highlights the peripheral injection attack on the EEG sample of the P300 dataset. A slight delay was introduced at the signal start, which can decrease accuracy in neurodata transmission [17]. The black-box attack is quick and simple to execute but, as illustrated, its application can have a strong impact on the availability (it may lead to a denial-of-service situation) and reliability of the BCI deep learning model, either modifying the class guess in the black-box learning model or diminishing the level of classification confidence.

B. Findings

According to Figure 1, these days, it has become challenging to maintain the security of confidential data from hacking and leaking. In order to prevent those issues, the organisation needs to adopt AI, which can enhance the data monitoring process and security [19]. It is demonstrated in Figure 2 that the white-box attacks (AV5 and AV6) may acquire the adversarial success rate equal to 100% or reduce the accuracy of the trust would reduce on the 70 to 0%. Deployability of the automatic deep learning system. In addition, through Figure 2, it can hardly be noticed by (non-) expert observations, as the perturbed signal is quite near and close to the physiologically plausible signal. In contrast, Figure 3 highlights, black-box attacks consist of random or uninformed interferences to the input signal, and the attacker gets access only to the input and output of the model [17]. Such hack attacks usually launch against vulnerabilities shared among different models. In this regard, two white-box state-of-the-art attacks based on EEG have been developed, i.e. Fast Gradient Sign Method (FGSM) and Projected Gradient Descent (PGD), both already extensively utilised in computer vision. Also, a proof of concept (PoC) of a new black-box attack that is especially targeted at the EEG signals was presented, known as the peripheral injection attack.

C. Case Study Outcomes

Table 1: Case study outcomes

Case Study	Strategy	Impact	Outcomes
Case Study 1. Cognetivity Neurosciences (London)	Cognetivity Neurosciences approached the AI-driven cognitive assessment strategy based on the analysis of the neural data, which is non-invasive [13].	The company fulfilled diagnostic accuracy and data security through the integration of deep learning models into its ICA platform and through its alignment with the Data Security and Protection Toolkit (DSPT) established by NHS Digital.	The result was effective implementation in the NHS Trusts that are compliant with data protection as well as proven clinical reliability [14].
Case Study 2. Emteq Labs (Brighton)	Emteq Labs adopted an approach that took place along the edge-based AI analytics, leveraging wearable EEG/EMG devices [15].	They allowed recognising the emotions in real-time and protecting the neurodata in a federated fashion without a caravan of sensitive information through their combination of machine learning and federated learning.	By the result, the systems of Emteq were implemented in the VR and treatment settings, demonstrating safe, distributed processing of biosignals and facilitating the development of ethical neurotechnologies [16].

(Source: Self-developed)

D. Comparative Analysis

Table 2: Comparative Analysis

Sources	Focus	Finding	Gaps
[1]	Intrusion of an EEG-Based BCI Backdoor Attacks	Electroencephalography Deep learning models are susceptible to backdoor injection attacks [1]	The absence of flexible defence measures, successful black-box attacks
[2]	Detection of anomalies in the SMEs	Compared some unsupervised algorithms of anomaly detection	Applied only to a broad working of the enterprise; cannot be neuro-signal-specific [2]
[3]	EEG data homomorphic encryption [3]	Obtained privacy-enhancing EEG classification with ML	The cost and latency of real-time EEG processing were high
[4]	EEG encrypted classification using neural networks	Illustrated encrypted multi-class EEG recognition using NN [4]	It needs to be simplified to have BCI in real-time use, especially in the form of a wearable piece.
[5]	BCI secure multiparty computation	Empowered privacy-preserving regression of EEG information among users [5]	Narrow scope- only limited to special reagents of EEG regressions
[6]	EEG federated transfer learning [6]	subject-specific classification and no sharing of raw data	Expensive overhead of communications; lack of security in federated updates
[7]	Cyber threat intelligence ML models	PoC Indicators of compromise (Indicators of compromise) suggested by an ML approach to threat sharing [7]	Does not focus on a context of neural or biometric data
[8]	Disorganised cryptography of IoT	Created the fastest lightweight image encryption MLCM [8]	No preparation for EEG or neural signal formats was examined

(Source: Self-developed)

V. DISCUSSION

A. Interpretation of results

It can be seen in the review and analysis that artificial intelligence is essential in supervising and protecting neurodata transport in Brain-Computer Interfaces (BCIs). Above discussion concluded that with the help of machine learning (ML) and deep learning (DL) models and combined with the techniques of encryption, e.g., homomorphic encryption and federated learning, the threat of data leakage, hijacking, and other unauthorised accesses may be considerably minimised [20]. Such case studies as Cognetivity or Emteq Labs prove the practical implementation of AI within the neurotechnology sphere that helps to enhance the accuracy of diagnosis as well as data security. Nonetheless, quantitative data also demonstrates that numerous systems are still not resistant against highly advanced white-box as well as black-box attacks, particularly in applications based on real-time EEG.

B. Practical Implications

The combination of the AI-based anomaly detection mechanism, encryption technology, and the decentralised learning architecture has huge potential to create a secure BCI system [22]. These technologies can be used by the healthcare establishment and parents to provide greater levels of patient privacy, regulatory compliance (e.g., GDPR, NHS DSPT), and ensure people have confidence in BCI applications. Besides, AI frameworks such as convolutional neural networks and autoencoders enable neurodata anomaly monitoring in real-time, which facilitates the accuracy of cognitive tests and the recognition of emotions.

C. Challenges and Limitations

Even though these show positive results, there are major issues that still need to be addressed. Advanced encryption techniques also introduce computational overhead that constrains real-time behaviour, in particular where BCIs remain wearable or implantable. Though effective, AI models are susceptible to adversarial attack, and their decision rule is not transparent most time [21]. Moreover, the sync and communication bandwidth are also problematic in federated learning, and the majority of the existing models are not personalised across a wide range of users. And big and varied amounts of EEG data to train strong AI models are also scarce.

D. Recommendations

Future studies must be dedicated to the production of lightweight algorithms of explainable AI, providing transparency and flexibility to secure neurodata processing. It is essential to promote cooperation among the AI developers, neuroscientists, and cybersecurity professionals. It should be encouraged to use hybrid encryption schemes and privacy-preserving learning frameworks (e.g. differential privacy in federated learning) [23]. Policymakers also need to revise the rules according to new AI risks in the field of neurotechnology. Funds in safe BCI research and real-world tests over time will play a critical role in assembling trustworthy and ethical neurodata systems.

VI. CONCLUSION & FUTURE WORK

This paper has examined ways in which AI can be successfully utilised to secure neurodata transmission in Brain-Computer Interfaces (BCIs) against hijacking and leakage. The findings reveal that machine learning and deep learning, and encryption (especially homomorphic encryption and federated learning) provide possible, scalable options to increase data privacy and integrity. Two case studies, Cognetivity and Emteq Labs, illustrate the practical application of secure neurotechnologies based on AI. Future research efforts ought to be devoted to creating lightweight, explainable AI models, enhanced federated learning protocols and an increase in the availability of heterogeneous EEG data. Future interdisciplinary cooperation and amendments in the regulations will be necessary to create sustainable and data-protective BCI systems, which are ready to be considered clinically and commercially.

REFERENCES

1. Meng, L., Huang, J., Zeng, Z., Jiang, X., Yu, S., Jung, T.-P., Lin, C.-T., Chavarriaga, R. and Wu, D. 2020. *EEG-Based Brain-Computer Interfaces Are Vulnerable to Backdoor Attacks*. arXiv.org. Available at: https://arxiv.org/abs/2011.00101. [Accessed on: 20th September 2023]
2. Petrariu, I., Moscaliuc, A., Turcu, C.E. and Gherman, O., 2022. A comparative study of unsupervised anomaly detection algorithms used in a small and medium-sized enterprise. *International Journal of Advanced Computer Science and Applications*, *13*(9).
3. Popescu, A.B., Taca, I.A., Nita, C.I., Vizitiu, A., Demeter, R., Suciu, C. and Itu, L.M., 2021. Privacy preserving classification of eeg data using machine learning and homomorphic encryption. *Applied Sciences*, *11*(16), p.7360.
4. Liu, Y., Huang, H., Xiao, F., Reza Malekian and Wang, W. 2020. Classification and recognition of encrypted EEG data based on neural network. *Journal of Information Security and Applications*, 54, pp.102567–102567. Available at: https://arxiv.org/abs/2006.08122 [Accessed on 19th September 2023].
5. Agarwal, A., Dowsley, R., McKinney, N.D., Wu, D., Lin, C.-T., De Cock, M. and Nascimento, A.C.A. 2019. Protecting Privacy of Users in Brain-Computer Interface Applications. *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, 27(8), pp.1546–1555. Available at: https://pubmed.ncbi.nlm.nih.gov/31283483/. [Accessed on 20th October 2023]
6. Ju, C., Gao, D., Mane, R., Tan, B., Liu, Y. and Guan, C. 2020. *Federated Transfer Learning for EEG Signal Classification*. IEEE Xplore. Available at: https://arxiv.org/abs/2004.12321 [Accessed on 15th October 2023]
7. Preuveneers, D. and Joosen, W., 2021. Sharing machine learning models as indicators of compromise for cyber threat intelligence. *Journal of Cybersecurity and Privacy*, *1*(1), pp.140-163.
8. Al-Majdi, K., Salman, A., Abbas, N.A., Hashim, M.M., Taha, M., Nahi, A.A. and Saleh, S., 2022. MLCM: An efficient image encryption technique for IoT application based on multi-layer chaotic maps.

International Journal of Nonlinear Analysis and Applications, *13*(2), pp.1591-1615. Available at: https://www.researchgate.net/publication/361241917_MLCM_An_efficient_image_encryption_technique_for_IoT_application_based_on_multi-layer_chaotic_maps [Accessed on 15th September 2023]

9. Bhatti, M.A., 2022. Advancement in brain-computer interface technology for enhancing neurological function. *Archives of Clinical Psychiatry*, *49*(1).
10. Kellmeyer, P., 2021. Big brain data: On the responsible use of brain data from clinical and consumer-directed neurotechnological devices. *Neuroethics*, *14*(1), pp.83-98.
11. Paun, A.M.C. and Law, L.L.M., 2022. Brain Computer Interface manufacturers under the data protection lens. Available at: http://arno.uvt.nl/show.cgi?fid=160486 [Accessed on 12th September 2023]
12. Asenahabi, B.M., 2019. Basics of research design: A guide to selecting appropriate research design. *International Journal of Contemporary Applied Researches*, *6*(5), pp.76-89.
13. newsfilecorp.com 2022. *Cognetivity Neurosciences' Brain Health Platform Cited as Case Study as Part of Early Dementia Detection Policy Recommendations by Alzheimer's Research UK*. Newsfile. Available at: https://www.newsfilecorp.com/release/147752/Cognetivity-Neurosciences-Brain-Health-Platform-Cited-as-Case-Study-as-Part-of-Early-Dementia-Detection-Policy-Recommendations-by-Alzheimers-Research-UK [Accessed on 29th September 2023].
14. htn.co.uk 2022. *Case study: Cognetivity Neurosciences transforms early dementia detection with AI-powered visual stimuli test – HTN Health Tech News*. Htn.co.uk. Available at: https://htn.co.uk/2021/10/14/case-study-cognetivity-neurosciences-transforms-early-dementia-detection-with-ai-powered-visual-stimuli-test [Accessed on 15th October 2023].
15. Gnacek, M., Broulidakis, J., Mavridou, I., Fatoorechi, M., Seiss, E., Kostoulas, T., Balaguer-Ballester, E., Kiprijanovska, I., Rosten, C. and Nduka, C., 2022. emteqpro—fully integrated biometric sensing array for non-invasive biomedical research in virtual reality. *Frontiers in virtual reality*, *3*, p.781218.
16. Gao, D., Ju, C., Wei, X., Liu, Y., Chen, T. and Yang, Q., 2019. Hhhfl: Hierarchical heterogeneous horizontal federated learning for electroencephalography. *arXiv preprint arXiv:1909.05784*.
17. Tarkhani, Z., Qendro, L., Brown, M.O.C., Hill, O., Mascolo, C. and Madhavapeddy, A., 2022. Enhancing the security & privacy of wearable brain-computer interfaces. *arXiv preprint arXiv:2201.07711*.
18. Stocco, A. and Tonella, P., 2020, October. Towards anomaly detectors that learn continuously. In *2020 IEEE international symposium on software reliability engineering workshops (ISSREW)* (pp. 201-208). IEEE.
19. Jain, A.K., Sahoo, S.R. and Kaubiyal, J., 2021. Online social networks security and privacy: comprehensive review and analysis. *Complex & Intelligent Systems*, *7*(5), pp.2157-2177.
20. Fang, H. and Qian, Q., 2021. Privacy preserving machine learning with homomorphic encryption and federated learning. *Future Internet*, *13*(4), p.94.
21. Tcydenova, E., Kim, T.W., Lee, C. and Park, J.H., 2021. Detection of adversarial attacks in AI-based intrusion detection systems using explainable AI. *Human-Centric Comput Inform Sci*, *11*.
22. Abdel Hakeem, S.A., Hussein, H.H. and Kim, H., 2022. Security requirements and challenges of 6G technologies and applications. *Sensors*, *22*(5), p.1969.
23. Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., Li, Y., Liu, X. and He, B., 2021. A survey on federated learning systems: Vision, hype and reality for data privacy and protection. *IEEE Transactions on Knowledge and Data Engineering*, *35*(4), pp.3347-3366.
24. Chintale, P.: DevOps Design Pattern: Implementing DevOps Best Practices forSecure and Reliable CI/CD Pipeline (English Edition). BPB Publications, 2023.
25. Goli, A. K. R. Journal of Innovation in Research and Education (JIRE).
26. Goli, S. R. (2023). Scalable SRE Practices for AI Service Reliability: Monitoring and Alerting in Production ML Systems. Available at SSRN 5741663.
27. Konda, R. Journal of Innovation in Research and Education (JIRE).