Position: On potential malware & new attack vectors for Internet-of-Brains (IoB)

1st Tuomo Lahtinen
Binare Oy, University of Jyväskylä
Jyväskylä, Finland
tuomo.lahtinen@binare.io, tutalaht@jyu.fi

2nd Andrei Costin
University of Jyväskylä
Jyväskylä, Finland
ancostin@jyu.fi

3rd Guillermo Suarez-Tangil
IMDEA Networks Institute
Madrid, Spain
guillermo.suarez-tangil@imdea.org

2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) | 979-8-3503-6729-4/24/$31.00 ©2024 IEEE | DOI: 10.1109/EUROSPW61312.2024.00066

***Abstract*—The Internet of Brains (IoB) is a relatively recent and still emerging computing paradigm connecting different Brain-Computer Interface (BCI) devices to networks, smartphones, cloud, software, and machine-learning models. IoB and BCI usage is expected to grow increasingly thanks to R&D, marketing, and commodification efforts by companies such as Neuralink (with their invasive BCI) and Meta (with their non-invasive BCI coupled to VR/XR).**

This paper presents a position view on existing traditional attack vectors but also introduces and discusses several new attack vectors targeting IoB that could be abused by malware and ransomware actors in the near future. This work aims to initiate and facilitate discussions within the researchers' and practitioners' communities to study such emerging threats as early as possible, considering that IoB and BCI connect critical elements such as the users' brains to possibly hostile environment(s) such as computer networks and the Internet.

***Index Terms*—brain-computer interface, internet of brains, cybersecurity, malware, attack vectors, cyber-physical systems, CPS**

1. Introduction

The Brain-Computer Interface (BCI) research has existed for over 50 years since its establishment in the early 1970s. Once confined to research labs in its early days, BCI technology has rapidly expanded into medicine, industry, and recently into entertainment and eXtended Reality (XR). Between 2009 and 2019, non-medical and medical domains increased the number of publications for EEG devices [1]. The research and development of BCI systems remain strong as Big Tech sees neurotechnology as its next AI frontier [2], especially as these devices become increasingly mature, networked, and feature-rich. Any form of connected BCI(s) system is generally referenced as Internet-of-Brains (IoB) – a term coined in 2008 [3] and subsequently expanded by [4, 5]. Currently, some devices use BCIs to control IoT devices, e.g., Brain-to-Thing Communication (BTC) [6], and these are also part of the expanding IoB landscape.

BCI has been inorganically evolving despite being long established, and the foundational cybersecurity principles have to be sufficiently studied. Prior work has discussed general potential threats in the field of BCI [7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18].

IoB oversees various connected components, including sensor-equipped headsets for brain data recording, gateway devices, data aggregator nodes, analyzer software, and cloud storage and analytics. With the potential offered by the interaction between these popular components, BCI technology is gaining traction. However, BCI's rise exposes critical gaps in IoB security. The current landscape, akin to what Costin et al. identified with IoT [19], risks leaving IoB vulnerable to exploitation. However, identifying these risks poses staggering challenges, greater than in existing technologies [20], due to the heterogeneity and incipient stage of this ecosystem.

These challenges create a landscape ripe for new attack vectors (AV), potentially leaving our BCIs and the entire IoB vulnerable to malware attacks – indeed, it is extremely hard to even imagine having to deal with a "Mirai-style attack for IoB".

Taking these challenges aside, malware targeting less emerging technologies continues to see rampant proliferation [20, 21]. For example, five hundred sixty thousand (560,000) new pieces of malware are detected daily and added into over 1 billion malware's pool [21]. The vast landscape of existing malware, coupled with the evolving capabilities of the industry behind it, makes IoB a prime target for future attacks.

This research emphasizes the importance of practical experimentation with BCI technology to identify new threats. It is suggested that comprehensive penetration testing of BCIs should be conducted, including neural attacks such as brain data decoding and manipulation and stimulation alterations that could affect patient well-being. This approach is because many theoretical discussions of BCI cybersecurity lack empirical validation, highlighting the need for practical testing to support theoretical assumptions. This study reveals existing vulnerabilities and security issues in BCI systems. It also includes theoretical demonstrations to showcase new attack methods that exploit these vulnerabilities and cause software crashes by carefully-controlled brain activity or manipulation of brain data.

The brain is likely to be a person's most valuable and highly protected asset, both from the perspective of password stealers and ransomware attackers. Malware may be used to launch an attack against IoB and BCIs, which could have complex and far-reaching consequences. Therefore, it is important to thoroughly investigate all potential avenues of attack and exploitation to understand better and mitigate this potential threat.

DOI 10.1109/EuroSPW61312.2024.00066

2. Existing attack vectors applied to IoB and BCI

There are 20 known types of risks for BCIs [18], with the top most concerning being 1) personal autonomy, 2) legal considerations, and 3) privacy and security. Security and privacy risks in BCIs include threats of data leakage, malicious hacking of wireless devices, and physical and psychological harm. Fitting terms for this risk theme are 'brain malware' [7], 'brain-hacking' [8], and 'brainjacking' [9]. This section undertakes a literature review to elucidate the threats concerning IoT and IoB within the realms of BT, WiFi, and third-party dependencies. Subsequently, we introduce novel attack vectors tailored specifically for the IoB paradigm.

Assessing the security controls employed by BCI manufacturers is currently challenging. At a minimum, these companies must comply with the laws of the country in which they operate. Additionally, they may utilize standards and recommendations as a reference point. For instance, the FDA (U.S. Food and Drug Administration) has published guides and regulations for medical devices [22], and Yuan et al. [23] have introduced standards for medical devices, including UL 2900 (cybersecurity) and TIR57 (risk management). These are merely actions to improve BCI security and privacy. A potential issue may arise in the future when BCI devices, such as gaming devices, are not subject to FDA approval but have the same capabilities as medical devices.

2.1. Bluetooth and Bluetooth Low Energy

Bluetooth (BT) is the most widely used protocol for short-range wireless connections. This is also true for BCIs as many consumer BCI devices use BT [14, 24] and there are also invasive devices such as Neuralink [25] and Synchron [26] using it. BT and Bluetooth Low Energy (BLE) are not fully safe protocols as both have vulnerabilities [27]. In particular, between 2020 and 2023, 15 vulnerabilities have been discovered, of which six were rated as 'High' severity (including BLE) [28]. These vulnerabilities can be exploited for sniffing attacks, which can expose sensitive information.

Antonioli et al. [29, 30] conducted valuable research on Bluetooth security, presenting the Key Negotiation Of Bluetooth (KNOB) attack (e.g., CVE-2022-25836 and CVE-2022-25837). KNOB [29] attacks allow the threat actors to reduce the entropy of the encryption key. Extending KNOB, BLUFFS [30] BLUFFS attacks break the secrecy of Bluetooth even in the future when reusing keys [30].

FlipperZero [31], a convenient hacking device, can be used for Bluetooth spamming, which involves sending pairing requests repeatedly until the receiver device crashes due to the flood of device pop-ups [32]. This easy attack does not compromise data but enables denial-of-service (DoS). In addition, BlueBorne [33] is an attack vector that could compromise many major Bluetooth-enabled devices and chipsets. It is considered a severe threat as it can penetrate non-Internet connected networks, i.e., air-gapped networks. This attack vector can be used for various malicious purposes, such as network sniffing, data theft, ransomware, and creating botnets.

It is crucial to gain a deeper understanding of Bluetooth-related attacks and infection vectors, and especially of Bluetooth-related setups and communications for IoB because BCIs use both BT and BLE protocols for controlling the devices and transferring the data between wearable sensors (e.g., headbands, headcaps), and gateway and data aggregation devices.

2.2. WiFi

WiFi, the most widely used standard for wireless local area networks (WLANs), is also used in many IoT devices, including BCIs. However, outdated encryption protocols such as WEP (Wired Equivalent Privacy) and WPA2 (WiFi Protected Access) are vulnerable to attacks, making them insecure [34]. We next present an overview of the most prominent attacks relevant to BCI.

Out-of-network attacks can be used to fingerprint IoT devices on the WiFi network by remotely identifying and gaining information about packets. With this knowledge, it is possible to determine the device type and status using ML models. This easy attack is difficult to detect, and the attack time is relatively low (30s was optimal in this research). Furthermore, it may be possible to perform more complex attacks with this information [35].

Ramezanpour et al. [36] conducted a comprehensive privacy and security survey on 5G/6G and WiFi 6. With a rogue access point (AP) attack (evil twin), the target is tricked into selecting the rogue AP over a legitimate one. The attack can lead, for example, to data theft or DoS. Another type of attack is the so-called DoSL attack [36] or battery drain attack [13], where the attacker drains the battery of the device by bombarding it with authentication requests until the battery runs out. In particular, small implanted BCI devices are vulnerable to battery drain attacks. If a BCI device runs out of battery, there is no way to record brain data, control smart devices with the BCI, or treat the user.

2.3. Tools and supply chain

The tool here refers to a tool, library, or software used to communicate with the BCI. Tools can be either open-source or closed-source, and both have strengths and weaknesses. Schryen et al. [37] compared vulnerabilities found in open and closed-source software, and whether the vulnerability was patched or not. Even if an open-source tool has no vulnerabilities, it could serve as a tool for attackers to decrypt live or captured brain data. For example, tools that can handle and decrypt brain data are 'CyKit' for Emotiv devices [38], 'muse-LSL' for Muse devices [39], and 'Arduino Brain Library' for Neurosky devices (requires hardware hacking) [40]. These tools could be used by the attacker to gain easy access to raw or processed brainwave data, thus raising privacy-related concerns.

Moreover, open-source and third-party software supplies introduce their own set of cybersecurity threats and risks that must be carefully considered, especially in the IoB and BCI fields that currently receive less cybersecurity scrutiny as other fields such as ML (e.g., Tensorflow [41, 42]). For example, open-source repositories can be intentionally plagued with malicious code or backdoor functionality [43]. Gershon [44] discovered

a simple rename to be useful against Github repositories which enabled supply chain attacks. Another possible risk is that the attacker creates an open-source repository that includes malicious code as a pre-installation [43]. On the one hand, Bonaci et al. [7] introduces a technique whereby an attacker exploits a legitimate algorithm, where an attacker exploits a legitimate BCI system decoding algorithm for malicious purposes.

Closed-source tools are considered to work on the black-box principle, where the functionality is hidden and it is very difficult for the user to know what the closed-source tool does. Closed-source tools do not have problems with abuse, but third-party tools may be poorly designed or deliberately malicious. This puts the user at risk. Wang et al. [45] identified 433 Java projects that utilized a buggy library version. A total of 55% of the projects were utilizing the library version to a greater extent than 10 versions from the most recent release. The willingness to maintain the versions in an up-to-date state is dependent on the ability to integrate the new version into the project. On occasion, new versions lack certain features that were present in previous versions, or the new version may require substantial alterations to the code base.

In some cases, BCI application developers may be forced to use third-party tools (closed-source) when there is no other choice. It is still the developers' responsibility to ensure that the third-party tool is secure enough to be used. Tarkhani et al. [14] introduced LibArgus, which can be used to improve the tool's security or monitor third-party tools' data flows. This process facilitates identifying anomalous events, such as data transfer to unknown sources.

2.4. APIs by BCI vendors

BCI vendors provide APIs to control and manage the BCI devices and IoB cloud systems they provide. However, this also opens up the possibility of creating malicious applications or websites that can misuse vulnerable or misconfigured APIs to access brain data without the user's or treatment facility's consent [14].

For example, malicious web pages could be crafted and used to retrieve sensitive demographic and medical condition data [10]. In one example, the data was sent to a machine learning-based detection engine while the BCI users were using the target page. The author's model [10] identified the user's age group and alcohol use disorder with 94% and 96% precision, respectively. Studying this type of attack in-depth is challenging because participants must have a pre-existing medical condition, e.g., alcoholism in this case, and this requires both the attackers and the legitimate BCI operators to have robust models to start with. However, few individuals with medical conditions are willing to participate [10]. In another example, Landau et al. [11] reviewed the possibility of legitimately recognizing Alzheimer's disease through an EEG scan and subsequent API queries. Moreover, an attacker could potentially abuse several APIs (e.g., BCI vendor, medical service provider) to extract and compare neural data with the hospital's EEG database to identify an individual.

2.5. Current malware

Depending on the attacker's intent and skill, malware can be viruses, worms, trojans, ransomware, and spyware. Malware could take advantage of open-source vulnerabilities, found in 84% of code bases according to [21].

Malware can be used to gain unauthorized access and execute malicious actions intentionally. Tarkhani et al. [14] conducted a proof of concept attack using commercialized BCI devices from brands such as Muse, NeuroSky, and OpenBCI. They identified more than 300 vulnerabilities across six different attack vectors, some of which were successfully exploited. Meng et al. [46] demonstrated that EEG-based BCI systems are vulnerable to backdoor attacks, where an attacker poisons a small data part of the ML model to create a backdoor. This attack is feasible for individuals who work in data collection, processing, or classifier development. Later, Meng et al. [47] demonstrated a backdoor attack on multiple machine learning models and datasets. Although some examples of the use of malware in BCI systems are shown above, and there are few mentions of malware attacks [11, 13], malware is not widely or explicitly discussed among researchers.

Luckily, malware attacks against BCI, IoB, or the user's brain have not yet been reported. However, we posit there is an increasing risk of IoB malware being developed and used for malicious purposes, such as stealing or manipulating brain or other user data, making BCI devices unresponsive through a DoS attack, affecting user's health or brain sensory perception, or even applying novel attacks and techniques.

3. Novel attack vectors applied to IoB and BCI

In recent decades, research on BCI cybersecurity has focused on discussing privacy and security aspects by adopting existing threat models. However, there is an urgent need to gain a deeper understanding of novel threats, vulnerabilities, exploits, and new malicious avenues that can potentially affect BCIs and IoB. As the BCI devices mature and diversify, the data quality and type improve, making it easier to analyze and (ab)use the data. This data could contain sensitive information, such as credentials and passwords, or detailed identifying information, such as memories, personality, values, and emotions. Therefore, it is important to prevent unauthorized entities from accessing the BCIs [11, 48]. Cybersecurity threats compromise the principles of Confidentiality, Integrity, and Availability (CIA). In this work, we expand the CIA term to Confidentiality, Integrity, Availability, **Safety** (CIAS). Safety represents the integrity of the BCI user's health, specifically their physical and brain condition during or after using BCI devices [16].

Very recently, promising results were achieved in decoding (potentially sensitive) data from the raw brainwave using **non-invasive** technologies, for example, to decode music track [49], language [50], and image reconstruct [51]. Considering the above work on **non-invasive** technologies, it is highly likely that those techniques (and potential attacks) will become even more robust and

stable for **invasive** technologies such as Neuralink [52], Precision Neuroscience [53], and Synchron [54], for which clinical and patient trials have already started.

With this position paper, we aim to introduce and discuss several new attack vectors that we envision for BCIs and IoB scenarios. To our knowledge, these attack vectors have not been proposed nor researched before, even though the attacks described may sound futuristic or infeasible at present.

We characterize these novel attack vectors in Table 1. The complexity, probability, and impact of potential attack vectors were evaluated using existing research and attacks that align with our defined attack vectors, such as [11, 55, 56, 57]. Additionally, our findings of successfully exploited attacks were incorporated into the evaluation process.

Attack vector	Attack characteristics
Brain stimulation device (Fig. 1)	**Complexity:** Medium / Low **Probability:** Very likely **Impacts:** (Physical) Safety of brain/health **Impact probability:** Requires more research
Stored/processed **manipulated** brain data (Fig. 2)	**Complexity:** Very high **Probability:** Very likely **Impacts:** Confidentiality, Integrity
Live **manipulated** brain data BCI device data	**Complexity:** High / Very high **Probability:** Likely **Impacts:** Confidentiality, Integrity, Availability
Live **raw** brainwave data (Fig. 3)	**Complexity:** Extremely high **Probability:** Very unlikely **Impacts:** Confidentiality, Integrity, Availability

TABLE 1. MAIN CHARACTERISTICS OF THE NEW ATTACK VECTORS.

3.1. Brain stimulation devices

The majority of BCIs are "record-only" devices that record brain activity and send the data on. For example, the most commonly used method in BCIs is the EEG, which is used for recording only [58]. A number of methods have been developed which are capable of stimulating the brain. These include transcranial Direct Current Stimulation (tDCS) [59] and Deep Brain Stimulation (DBS) [60], Transcranial Magnetic Stimulation (TMS) [61], Transcranial Electrical Stimulation (tES) [62], Transcranial Focused Ultrasound (tFUS) [63] and neural dust [64], and they can interact at a low level with the brain via contact or contactless stimulation of brain cells or areas.

"Brain or body corruption" is a cyber-physical attack that can cause physical, neurological, or sensory damage or impact to the BCI user (Fig. 1). This attack differs from the standard and existing IT attacks as it can compromise not only the CIA of BCI devices or IoB ecosystem but has the potential to impact the physical integrity of the user, i.e., Safety [13, 16, 65]. One of the biggest concerns in these health-threatening attacks is that causing harm to the user is relatively easy. Pycroft et al. [9] describe this attack as a blind attack, requiring hardly any knowledge about the patient or brain stimulation. At the other end of the complexity spectrum, brain data manipulation requires much more knowledge to implement a successful attack [9, 12].

The attack flow, in a nutshell, is as follows:

1) The attacker **gets control over the BCI device**. This can be achieved via: infection of smartphone/PC controlling the BCI; malicious firmware update to BCI [66]; insecurely-exposed or vulnerable web/control interface of BCI [67].
2) The attacker **changes the BCI's core parameters** for output electric/magnetic values.
3) The BCI operates **output electric/magnetic values dangerous for health**.
4) The brain or health of the user is **directly and immediately** under risk.

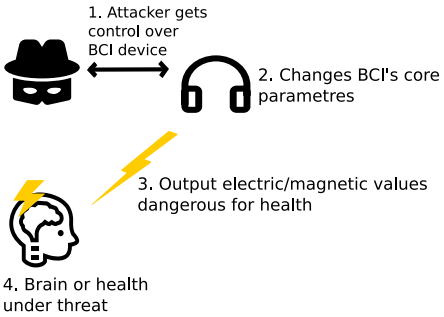

Figure 1. Attack vector: Brain stimulation device.

3.1.1. Implication. This attack vector is the easiest to implement among all the attack vectors presented in this work and has the most severe impact, as it can theoretically cause permanent brain damage to BCI users [8, 16]. The attacker must execute malicious acts that lead to a command-and-control situation where the attacker can control the BCI device (device responsible for data acquisition). A malicious act can trigger the BCI device's unintended functions, such as increasing the current to dangerously high levels. Changing the operating parameters of BCIs beyond safety health limits can cause a variety of side effects [65] – from minimal skin irritation or minor burns to severe and permanent brain damage.

The brain damage could caused by brain-hacking [68], and devices can also cause unintentional harm as suspected by [69]. For example, research by Lopez et al. [17] showed that neuronal flooding and neuronal jamming in cyberattacks can increase the number of spikes of the affected neurons. It is worth noting that devices employing, for example, deep brain stimulation (DBS) and transcranial direct current stimulation (tDCS), are not only used for medical purposes but are also utilized in commercialized products by healthy individuals [8]. This creates more markets for this kind of device and that could attract attackers to choose this attack vector in the future.

3.1.2. Mitigation. One effective method to mitigate BCI vulnerabilities is only to incorporate functions when they are absolutely necessary. For instance, enabling the Internet connection should only be done when it is a mandatory requirement. The Abbott Laboratories' DBS medical device, for instance, has the capability for remote programming, which could potentially open a gateway for attackers. It is somewhat concerning that

the Michael J. Fox Foundation [70] is anticipating an increase in remote control capabilities in the near future. Furthermore, the Food and Drug Administration (FDA) has been more favorable toward conducting BCI trials with animals and humans for a few years [71].

Recently, Lopez et al. [17] researched neural attacks on reconstructed but realistic neuronal topology, specifically on the visual cortex of mice. Their research investigated how attacks such as neuronal flooding or jamming could affect the brain. This still requires more research, on how this kind of attack affects the victim. As ethical issues strongly prevent accurate research in real-life scenarios, reconstructing the brain as accurately as possible could help identify risks [17]. We urge this kind of research to be continued to understand the risks the invasive BCIs are creating. If the BCI users or manufacturers are unaware of the risks, they are most likely less willing to improve the security of the devices.

The implantation of invasive BCI devices carries with it the risk of physical and health complications for the user, as the procedure requires surgery. The first patient participating in the Neuralink trials has now experienced this risk, with some of the electrode threads retracting from the brain tissue just one month after the device was implanted. Neuralink quickly responded to this problem by adjusting data acquisition to be more sensitive [72].

3.2. Manipulated stored brain data

Manipulated stored brain data is an attack vector that affects the correctness of the intermediate/final brain data or the interpretation of the final data and the corresponding diagnosis or conclusion (Table 1 and Fig. 2). In this attack, the attacker manages to alter data in the cloud, storage, or backend part(s) of the BCI ecosystem, and false or manipulated brain data is stored there. An attacker could get access to the cloud, storage, or backend part(s) of the BCI ecosystem using traditional attack vectors such as SQL injections, remote command injections, remote code executions, and related exploitation techniques aiming to affect the Integrity of data or a system. False or manipulated data can lead to wrong diagnoses and potentially to wrong treatment for the patient.

BCI devices and systems have the potential to be used in distributed DoS attacks as part of an IoB botnet, similar to how Command-and-Control (CnC) commands or data are used to create a botnet with IoT devices. BCI devices are typically connected to the internet through a gateway using Bluetooth (§ 2.1) or using a WiFi connection (§ 2.2). It is important to note that if the BCI device has stimulation capabilities and is connected to the internet (e.g. Abbott Laboratories' DBS device [70]), a CnC-based attacker can perform the 'brain corruption' attack almost without any obstruction (§ 3.1).

The attack flow, in a nutshell, is as follows:

1) The attacker **gets unauthorized access** to the server, backend, cloud storage, etc.
2) The attacker **alters stored data**.
3) The clinic accesses recorded brain data to give advice or diagnosis to the patient.
4) Because of the manipulated data, **patient gets wrong or none** health information.

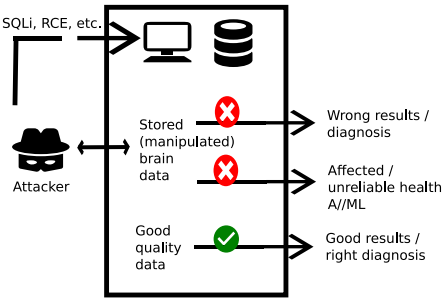

Figure 2. Attack vector: Manipulated stored brain data.

3.2.1. Implication. In this attack vector, possible effects overlap with the "Manipulate live brain data" vector. Despite the existence of overlap in the consequences of the attack vectors, the specific means by which the desired actions are achieved differ. As previously stated, the attacker could exploit conventional attack vectors to gain access to the BCI system and stored data.

The utilization of cloud computing is a prevalent and straightforward approach to data management. Cloud service providers may offer, for instance, Platform as a Service (PaaS) or Software as a Service (SaaS). However, cloud-based services may be susceptible to vulnerabilities, similar to any other system. Alouffi et al. [73] identified data tampering and leakage as the most prevalent security issues. A notable example of data leakage is the AWS S3 backup leakage case, as documented in [74]. In this instance, the data belonging to a company was stored in an individual's S3 bucket, resulting in the compromise of all the information and the possibility of changing existing backup data.

3.2.2. Mitigation. In order to prevent unauthorized access to stored data, it is essential that the BCI system provider ensures the regular updating of all active components, including software, firmware, etc. Furthermore, the implementation of anti-virus and malware detection programs, as well as data traffic management tools, can help to prevent unauthorized access and use of BCIs [16]. Those with access rights should be granted minimal privileges [75]. For instance, the BCI system provider should define access control policies and determine who has access to raw data [48].

Ajrawi et al. [76] proposed an RFID-based (Radio Frequency IDentification) security framework to ensure that only authorized personnel have access to patient data and that data is valid. This proposal would also mitigate the risk of "Manipulating live brain data" in a case where the attacker tries to send malicious artificial data. The BCI system would reject the attacker's exploitation attempt without a valid ID.

3.3. Manipulated live "brain data & BCI device data"

The manipulation of "live brain data" and "device data" from BCI devices are potent attack vectors with very high complexity i.e., the attacker needs to be sure that the system accepts artificial or manipulated brain data [11]. Nevertheless, it is very likely such an attack

would occur in the near future as embedded and IoT devices are known to have weak security [67, 77]. These attacks affect all parts of the CIAS. *Confidentiality* is compromised by unauthorized access to or interception of sensitive brain data, potentially exposing sensitive data to the attacker. *Integrity* of data is compromised as attackers can manipulate live brain data (e.g., cause false diagnoses for the patient [11, 55]), present false results to the BCI user, or give false commands to the controllable device such as drone [55]. *Availability* of critical resources is also at risk, as attackers can disrupt neural communication or impair BCI functionality (e.g., DoS vulnerabilities in the BCI devices or software). To carry out such attacks, attackers may use techniques such as Man-in-the-Middle (MitM) attacks on communication links of BCIs/IoB, gain unauthorized access to BCI devices/systems and control them, or remotely manipulate live brain data (e.g., radio or magnetic interference).

The attack flow, in a nutshell, is as follows:

1) The attacker **takes advantage of weakness inside BCI system** to acquire access into the system.
2) The **attacker manipulates live data (removes, alters, or replaces data)** at data transfer, e.g., after successful MitM.
3) BCI system approves or rejects the manipulated data.
4) If manipulated data is accepted, **the attacker could compromise all parts of CIAS**, depending on the purpose of the attack. The attacker may create a backdoor to steal sensitive data later.

3.3.1. Implication. The successful manipulation of brain data has the potential to result in several adverse outcomes, including the misdiagnosis of patients [11] or the insertion of malicious data into ML model training [46, 47]. This can be achieved similarly to the attack vector described in the section on 'Live raw brainwave data', but in this case, the data is purposely altered to cause problems or desired results at ML model training. Generally, this attack vector affects the quality of the data, thereby compromising all subsequent phases of data acquisition.

Sundararajan [56] reports a successful MitM attack against Emotiv Insight over Bluetooth Low Energy using Adafruit Bluetooth sniffer and Ubertooth One. The attack compromised all parts of CIAS, allowing the attacker to perform unwanted tasks and steal or alter sensitive data for their purposes.

Lopez et al. [17] presented a situation where the attacker analyses stimuli and recreates the desired situation (e.g., causing temporal blindness). This means that the stimulus analysis phase can be counted within the attack vector "BCI device data", while the attacker performing the stimulus recreation would result in "Brain stimulation device" attack vector (§ 3.1). Another possible cause is that malware is used to override the incoming data from the previous phases. This implies integrity or availability problems if the received data is ignored during processing [13].

3.3.2. Mitigation. One of the most important mitigation acts against "Manipulated live brain data & BCI device data" is to validate acquired data before processing it. For data validation, there are some frameworks proposed, such as [76] where the authors proposed an RFID-based data validation. More generically, the best mitigations for this attack involve the use of proven and strong data-integrity and information integrity mechanisms [78, 79].

3.4. Live raw brainwave data

Live raw brainwave data can be used as a raw attack vector, where the attacker sends malicious brainwaves intentionally or unintentionally without needing access to the BCI system (Fig. 3). The reliability and functionality of the BCI system depend heavily on signal acquisition. Interference during this phase can affect results and lead to unwanted functions or incorrect decisions, such as an incorrect disease diagnosis [11], a crash of the controlled device [55] or ML model poisoning for a specific purpose, or accident [46, 47].

The attack flow, in a nutshell, is as follows:

1) The **BCI PC/server software has a vulnerability**, e.g., buffer overflow (unintentional or intentional) or backdoor (intentional).
2) A user (malicious or non-malicious) uses the brain to **find, create, and reproduce a very specific brainwave data flow** towards the BCI software PC/server such that **it triggers the buffer overflow or the backdoor**.
3) The **BCI software vulnerability is exploited** to follow execution paths controlled by the user brain activity.
4) The **user/attacker can perform classical "lateral movement"** from that point onwards.

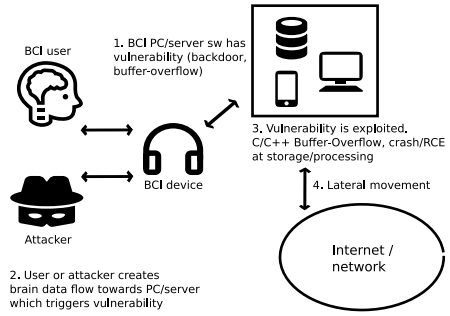

Figure 3. Attack vector: Live raw brainwave data.

3.4.1. Implication. Acquired signals may be influenced by noise caused by facial movements, breathing, or muscle movements, which can impact BCI performance and data quality [1, 24, 80]. Attackers can also create noise, which may result in a DoS, but they may not be able to gain control of the device [11]. It is therefore important to process the data before utilizing it in a BCI system [80]. However, such data (pre-)processing does not fully eliminate the threat of the "live brainwave data" attack vector, as attackers can use prerecorded brainwaves to be injected into data processing flows of IoB using untrustworthy or compromised BCIs.

Landau et al. [11] presented an artificial input attack that weaponizes brainwave-like data to launch a successful attack. Artificial input can be computer-generated or derived from real prerecorded brain data and used for various purposes, including causing a service/system crash or gaining unauthorized access. The latter could involve bypassing the biometric recognition system. For instance,

the hill-climbing attack involves using artificial input until the biometric recognition system grants authorization [81].

As demonstrated by Armengol et al. [55], using such "live brainwave signals" it is possible to crash a drone, force desired characters with a virtual keyboard, or report false meditative states. All three test attacks were successful and were achieved through false brainwaves and remote injection of amplitude-modulated radio-frequency signals to gain control of the BCI device (i.e., the physical layer was remotely hacked). The research in [55] demonstrates the feasibility of using "live brainwave data" as an attack vector (CVE-2023-49914 [82]). Another study [80] investigated the influence of noise-based cyberattacks on the physical layer of BCI systems during the acquisition and processing phases. The purpose was to create fake P300 waves. The attack's impact was higher when the attacker had more knowledge about the BCI system (22% in the acquisition phase with the most knowledge compared to 1% with less knowledge) [80].

Bernal et al. [13] discovered application security problems in BCIs, such as buffer overflow attacks, injection attacks, and misconfiguration. We argue that malicious "live brainwaves" threaten the service's availability during storage and processing. These inputs, if exploited, can trigger outcomes such as C/C++ buffer overflows, leading to program crashes and creating vulnerabilities ripe for exploitation. Furthermore, manipulated brainwaves can extend beyond mere disruption, facilitating CnC situations where the attacker gains leverage over the BCI system.

3.4.2. Mitigation. In order to mitigate the risk associated with this attack vector, it is essential to implement two distinct countermeasures. Firstly, it is crucial to process acquired brain data to identify and neutralize any harmful elements. Secondly, it is imperative to avoid or, if unavoidable, to exercise extreme caution when utilizing insecure programming languages, and to ensure that any such languages are employed under the highest standards of coding practice and automated code analysis.

For the first mitigation, before data processing, it is important to validate data and after validation, data is processed, and desired features are extracted. Brophy et al. [83] presented a state-of-the-art "de-noising" solution with Generative Adversarial Network (GAN). The proposed solution has the potential to enhance the reliability of EEG data, thereby enabling clinicians to remotely and accurately monitor the brain activities of patients.

The second mitigation option concerns using C/C++ and similar languages, which are widely used due to their speed and built-in support for hardware programming. In terms of programming languages, C/C++ has the highest number of vulnerabilities [84]. The top three Common Weakness Enumeration (CWE) categories are buffer errors, input validation, and resource management errors. These vulnerabilities are frequently associated with poor coding practices. Mend.io reports [84] that, despite C being an established language, vulnerabilities spiked in 2017. This indicates that there is still a need for the language and that its use has not been improved.

There are numerous resources available to assist in identifying problematic coding practices with C/C++, including [85] for manual inspection or [86, 87] to do it automatically. Additionally, the White House [88] suggests using memory-safe languages to prevent most memory-based vulnerabilities, avoiding security-prone languages like C/C++.

4. Conclusions

In this paper, we first presented a position view on existing traditional attack vectors. As a key novelty, we introduced and discussed several new attack vectors targeting IoB that could be abused by malware and ransomware actors in the near future. We aim to foster conversations among researchers and practitioners on emerging threats related to IoB (Internet of Brain) and BCI (Brain-Computer Interface). These technologies connect critical elements like users' brains to potentially hostile environments, such as computer networks and the internet. The goal is to identify and address these threats as early as possible to ensure the safety and security of users and their data.

Practical perspectives should be prioritized in BCI and IoB security and privacy research rather than generic ones. While generic research can provide insight into possible threats, it does not assess their feasibility or immediate risks. We point out that 86% of the 58 peer-reviewed articles only discuss attacks and malware, rather than real-world implementation [18]. Highly experimental and practical research could assess the likelihood of malicious BCI actions and their feasibility, facilitating the evaluation of the overall security and privacy of the BCI systems and devices.

Acknowledgment

(Part of this work was) Funded by the European Union (Grant Agreement Nr. 101120962, RESCALE Project). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them. This project was also partially funded by TED2021-132900A-I00 from the Spanish Ministry of Science and Innovation, and Guillermo Suarez-Tangil has been appointed as 2019 Ramon y Cajal fellow (RYC-2020-029401-I) both funded by MCIN/AEI/10.13039/501100011033 — with funds from the EU NextGenerationEU/PRTR and ESF Investing in your future respectively. Also, the authors acknowledge the use of royalty-free icons in Figures 1, 2, and 3 courtesy of https://iconduck.com/.

References

[1] Kaido Värbu, Naveed Muhammad, and Yar Muhammad. Past, present, and future of eeg-based bci applications. *Sensors*, 22(9):3331, 2022.

[2] Madison Mills. Big tech sees neurotechnology as its next ai frontier. https://finance.yahoo.com/news/big-tech-sees-neurotechnology-as-its-next-ai-frontier-100022978.html, 2024. [Accessed 14-05-2024].

[3] Steven B Harris. A million years of evolution. *Year Million*, 2008.

[4] Dehua Ju and Beijun Shen. Internet of knowledge plus knowledge cloud–a future education ecosystem. *Ieri Procedia*, 2012.

[5] Chen Dongwei, Wu Fang, Wang Zhen, Li Haifang, and Chen Junjie. Eeg-based emotion recognition with brain network using independent components analysis and granger causality. In *International Conference on Computer Medical Applications (ICCMA)*. IEEE, 2013.

[6] Ariel Teles, Maurıcio Cagy, Francisco Silva, Markus Endler, Victor Bastos, and Silmar Teixeira. Using brain-computer interface and internet of things to improve healthcare for wheelchair users. In *11th International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM)*, volume 1, pages 92–94, 2017.

[7] Tamara Bonaci, Ryan Calo, and Howard Jay Chizeck. App stores for the brain: Privacy & security in brain-computer interfaces. In *2014 IEEE International Symposium on Ethics in Science, Technology and Engineering*, pages 1–7. IEEE, 2014.

[8] Marcello Ienca and Pim Haselager. Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity. *Ethics and Information Technology*, 18:117–129, 2016.

[9] Laurie Pycroft, Sandra G Boccard, Sarah LF Owen, John F Stein, James J Fitzgerald, Alexander L Green, and Tipu Z Aziz. Brainjacking: implant security issues in invasive neuromodulation. *World neurosurgery*, 2016.

[10] Ajaya Neupane, Kiavash Satvat, Mahshid Hosseini, and Nitesh Saxena. Brain hemorrhage: When brainwaves leak sensitive medical conditions and personal information. In *2019 17th International Conference on Privacy, Security and Trust (PST)*, pages 1–10. IEEE, 2019.

[11] Ofir Landau, Rami Puzis, and Nir Nissim. Mind your mind: Eeg-based brain-computer interfaces and their security in cyber space. *ACM Computing Surveys (CSUR)*, 53(1):1–38, 2020.

[12] Sergio Lopez Bernal, Alberto Huertas Celdran, Lorenzo Fernandez Maimo, Michael Taynnan Barros, Sasitharan Balasubramaniam, and Gregorio Martinez Perez. Cyberattacks on miniature brain implants to disrupt spontaneous neural signaling. *IEEE Access*, 8:152204–152222, 2020.

[13] Sergio López Bernal, Alberto Huertas Celdrán, Gregorio Martínez Pérez, Michael Taynnan Barros, and Sasitharan Balasubramaniam. Security in brain-computer interfaces: state-of-the-art, opportunities, and future challenges. *ACM Computing Surveys (CSUR)*, 54(1):1–35, 2021.

[14] Zahra Tarkhani, Lorena Qendro, Malachy O'Connor Brown, Oscar Hill, Cecilia Mascolo, and Anil Madhavapeddy. Enhancing the security & privacy of wearable brain-computer interfaces. *arXiv preprint arXiv:2201.07711*, 2022.

[15] Francisco Brocal. Brain-computer interfaces in safety and security fields: risks and applications. *Safety science*, 160:106051, 2023.

[16] Tuomo Lahtinen and Andrei Costin. Linking computers to the brain: Overview of cybersecurity threats and possible solutions. In *International Symposium on Business Modeling and Software Design*. Springer, 2023.

[17] Victoria Magdalena López Madejska, Sergio López Bernal, Gregorio Martínez Pérez, and Alberto Huertas Celdrán. Impact of neural cyberattacks on a realistic neuronal topology from the primary visual cortex of mice. *Wireless Networks*, pages 1–15, 2024.

[18] Brandon J King, Gemma JM Read, and Paul M Salmon. The risks associated with the use of brain-computer interfaces: a systematic review. *International Journal of Human–Computer Interaction*, 40(2):131–148, 2024.

[19] Andrei Costin and Jonas Zaddach. Iot malware: Comprehensive survey, analysis framework and case studies. *BlackHat USA*, 1(1):1–9, 2018.

[20] Ömer Aslan Aslan and Refik Samet. A comprehensive review on malware detection approaches. *IEEE access*, 8:6249–6271, 2020.

[21] Nivedita James Palatty. 30+ malware statistics you need to know in 2024. https://www.getastra.com/blog/security-audit/malware-statistics/, 2023. [Accessed 06-02-2024].

[22] U.S. Food and Drug Administration. Medical devices. https://www.fda.gov/medical-devices, 2024. [Accessed 11-05-2024].

[23] Sean Yuan, Anura Fernando, and David C Klonoff. Standards for medical device cybersecurity in 2018, 2018.

[24] Krzysztof Dobosz and Piotr Wittchen. Brain-computer interface for mobile devices. *Journal of Medical Informatics & Technologies*, 24, 2015.

[25] Mike Dano. Connecting humans to computers with 5g? actually it's bluetooth. https://www.lightreading.com/digital-transformation/connecting-humans-to-computers-with-5g-actually-it-s-bluetooth, 2023. [Accessed 09-05-2024].

[26] Simon Spichak. Meet the stentrode: A bluetooth implant to give you mind control over computers. https://www.beingpatient.com/stentrode-synchron-bci/, 2022. [Accessed 09-05-2024].

[27] Shaikh Shahriar Hassan, Soumik Das Bibon, Md Shohrab Hossain, and Mohammed Atiquzzaman. Security threats in bluetooth technology. *Computers & Security*, 74:308–322, 2018.

[28] CVEdetails. Bluetooth : Security vulnerabilities, cves. https://www.cvedetails.com/vulnerability-list/vendor_id-11436/Bluetooth.html, 2024. [Accessed 21-02-2024].

[29] Daniele Antonioli, Nils Ole Tippenhauer, and Kasper B Rasmussen. The {KNOB} is broken: Exploiting low entropy in the encryption key negotiation of bluetooth {BR/EDR}. In *28th USENIX security symposium (USENIX security 19)*, pages 1047–1061, 2019.

[30] Daniele Antonioli. Bluffs: Bluetooth forward and future secrecy attacks and defenses. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, pages 636–650, 2023.

[31] Flipper Devices Inc. Flipper zero — multi-tool device for geeks. https://flipperzero.one/, 2024. [Accessed 13-03-2024].

[32] Sparkleo Technologies. Flipper zero bluetooth attack: Spamming until they crash, 2023. [Accessed 14-03-2024].

[33] Armis Inc. Blueborne vulnerabilities impact amazon echo and google home. https://www.armis.com/research/blueborne/, 2024. [Accessed 13-03-2024].

[34] Vishal Kumkar, Akhil Tiwari, Pawan Tiwari, Ashish Gupta, and Seema Shrawne. Vulnerabilities of wireless security protocols (wep and wpa2). *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 1(2):34–38, 2012.

[35] Mnassar Alyami, Ibrahim Alharbi, Cliff Zou, Yan Solihin, and Karl Ackerman. Wifi-based iot devices profiling attack based on eavesdropping of encrypted wifi traffic. In *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*, pages 385–392. IEEE, 2022.

[36] Keyvan Ramezanpour, Jithin Jagannath, and Anu Jagannath. Security and privacy vulnerabilities of 5g/6g and wifi 6: Survey and research directions from a coexistence perspective. *Computer Networks*, 221:109515, 2023.

[37] Guido Schryen and Rouven Kadura. Open source vs. closed source software: towards measuring security. In *Proceedings of the 2009 ACM symposium on Applied Computing*, pages 2016–2023, 2009.

[38] Github - cymaticorp/cykit: Python 3x server to deliver neural eeg data to browser and generic clients via tcp stream. https://github.com/CymatiCorp/CyKit, 2024. [Accessed 13-03-2024].

[39] Alexandre Barachant, Dano Morrison, Hubert Banville, Jason Kowaleski, Uri Shaked, Sylvain Chevallier, and Juan Jesús Torre Tresols. muse-lsl, May 2019.

[40] Github - kitschpatrol/brain: Arduino library for reading neurosky eeg brainwave data. https://github.com/kitschpatrol/Brain, 2024. [Accessed 13-03-2024].

[41] Build software better, together. https://github.com/tensorflow/tensorflow/security/advisories, 2024. [Accessed 25-03-2024].

[42] Vulnerability roundup 109: tensorflow-2.4.2: 32 advisories [7.8]. https://github.com/NixOS/nixpkgs/issues/150701, 2024. [Accessed 25-03-2024].

[43] Marc Ohm, Henrik Plate, Arnold Sykosch, and Michael Meier. Backstabber's knife collection: A review of open source software supply chain attacks. In *Detection of Intrusions and Malware, and Vulnerability Assessment: 17th International Conference, DIMVA 2020, Lisbon, Portugal, June 24–26, 2020, Proceedings 17*, pages 23–43. Springer, 2020.

[44] Aviad Gershon. Attacking the software supply chain with a simple rename, 2022. [Accessed 26-03-2024].

[45] Ying Wang, Bihuan Chen, Kaifeng Huang, Bowen Shi, Congying Xu, Xin Peng, Yijian Wu, and Yang Liu. An empirical study of usages, updates and risks of third-party libraries in java projects. In *2020 IEEE International Conference on Software Maintenance and Evolution (ICSME)*, pages 35–45. IEEE, 2020.

[46] Lubin Meng, Xue Jiang, Jian Huang, Zhigang Zeng, Shan Yu, Tzyy-Ping Jung, Chin-Teng Lin, Ricardo Chavarriaga, and Dongrui Wu. Eeg-based brain-computer interfaces are vulnerable to backdoor attacks. *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, 2023.

[47] Lubin Meng, Xue Jiang, Xiaoqing Chen, Wenzhong Liu, Hanbin Luo, and Dongrui Wu. Adversarial filtering based evasion and backdoor attacks to eeg-based brain-computer interfaces. *Information Fusion*, page 102316, 2024.

[48] Joseph O'Hagan, Pejman Saeghe, Jan Gugenheimer, Daniel Medeiros, Karola Marky, Mohamed Khamis, and Mark McGill. Privacy-enhancing technology and everyday augmented reality: Understanding bystanders' varying needs for awareness and consent. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2023.

[49] Ludovic Bellier, Anaïs Llorens, Déborah Marciano, Aysegul Gunduz, Gerwin Schalk, Peter Brunner, and Robert T Knight. Music can be reconstructed from human auditory cortex activity using nonlinear decoding models. *PLoS biology*, 21(8):e3002176, 2023.

[50] Jerry Tang, Amanda LeBel, Shailee Jain, and Alexander G Huth. Semantic reconstruction of continuous language from non-invasive brain recordings. *Nature Neuroscience*, 2023.

[51] Yohann Benchetrit, Hubert Banville, and Jean-Rémi King. Brain

decoding: toward real-time reconstruction of visual perception. *arXiv:2310.19812*, 2023.

[52] Reuters. Musk's neuralink to start human trial of brain implant for paralysis patients. https://www.reuters.com/technology/musks-neuralink-start-human-trials-brain-implant-2023-09-19/, 2023. [Accessed 22-01-2024].

[53] Ashley Capoot. Neuralink competitor precision neuroscience conducts its first clinical study to map human brain signals. https://www.cnbc.com/2023/06/23/precision-a-neuralink-competitor-conducts-its-first-clinical-study.html, 2023. [Accessed 22-01-2024].

[54] Susan Kelly. Synchron brain-computer interface implanted in first 6 us patients. https://www.medtechdive.com/news/synchron-brain-computer-interface-implanted-first-patients/692843/, 2023. [Accessed 22-01-2024].

[55] Alexandre Armengol-Urpi, Reid Kovacs, and Sanjay E Sarma. Brain-hack: Remotely injecting false brain-waves with rf to take control of a brain-computer interface. In *Proceedings of the 5th Workshop on CPS&IoT Security and Privacy*, pages 53–66, 2023.

[56] Kaushik Sundararajan. Privacy and security issues in brain computer interface. https://openrepository.aut.ac.nz/server/api/core/bitstreams/f6edfe94-1b2f-4cbc-aeea-49f917709734/content, 2017.

[57] Sergio López Bernal, Alberto Huertas Celdrán, and Gregorio Martínez Pérez. Eight reasons why cybersecurity on novel generations of brain-computer interfaces must be prioritized. *arXiv preprint arXiv:2106.04968*, 2021.

[58] Jayant Arora. Eeg and bcis — how do they work together? https://jayant-arora.medium.com/eeg-and-bcis-how-do-they-work-together-8964998bfd8f, 2021. [Accessed 09-05-2024].

[59] Michael A Nitsche, Leonardo G Cohen, Eric M Wassermann, Alberto Priori, Nicolas Lang, Andrea Antal, Walter Paulus, Friedhelm Hummel, Paulo S Boggio, Felipe Fregni, et al. Transcranial direct current stimulation: state of the art 2008. *Brain stimulation*, 1(3):206–223, 2008.

[60] Joel S Perlmutter and Jonathan W Mink. Deep brain stimulation. *Annu. Rev. Neurosci.*, 29:229–257, 2006.

[61] Masahito Kobayashi and Alvaro Pascual-Leone. Transcranial magnetic stimulation in neurology. *The Lancet Neurology*, 2(3):145–156, 2003.

[62] Anna Fertonani and Carlo Miniussi. Transcranial electrical stimulation: what we know and do not know about mechanisms. *The Neuroscientist*, 23(2):109–123, 2017.

[63] Wynn Legon, Tomokazu F Sato, Alexander Opitz, Jerel Mueller, Aaron Barbour, Amanda Williams, and William J Tyler. Transcranial focused ultrasound modulates the activity of primary somatosensory cortex in humans. *Nature neuroscience*, 17(2):322–329, 2014.

[64] Dongjin Seo, Ryan M Neely, Konlin Shen, Utkarsh Singhal, Elad Alon, Jan M Rabaey, Jose M Carmena, and Michel M Maharbiz. Wireless recording in the peripheral nervous system with ultrasonic neural dust. *Neuron*, 91(3):529–539, 2016.

[65] Warren M Grill. Safety considerations for deep brain stimulation: review and analysis. *Expert review of medical devices*, 2(4):409–420, 2005.

[66] Ang Cui, Michael Costello, and Salvatore Stolfo. When firmware modifications attack: A case study of embedded exploitation. 2013.

[67] Andrei Costin, Jonas Zaddach, Aurélien Francillon, and Davide Balzarotti. A {Large-scale} analysis of the security of embedded firmwares. In *23rd USENIX security symposium*, 2014.

[68] Sandra Boccard-Binet and Arjune Sen. Safety of transcranial direct current stimulation in healthy participants. *Epilepsy & Behavior Reports*, 15, 2021.

[69] Baris Ekici. Transcranial direct current stimulation-induced seizure: analysis of a case. *Clinical EEG and neuroscience*, 46(2):169, 2015.

[70] The Michael J. Fox Foundation. Currently available deep brain stimulation devices. https://www.michaeljfox.org/news/currently-available-deep-brain-stimulation-devices, 2024. [Accessed 11-05-2024].

[71] Eric Smalley. The business of brain-computer interfaces. *Nat. Biotechnol*, 37(9):978, 2019.

[72] Amaris Encinas. Human with neuralink brain chip sees improvement after initial malfunction, company says. https://eu.usatoday.com/story/tech/news/2024/05/11/neuralink-malfunction-resolved-bps-improved/73647719007/, 2024. [Accessed 12-05-2024].

[73] Bader Alouffi, Muhammad Hasnain, Abdullah Alharbi, Wael Alosaimi, Hashem Alyami, and Muhammad Ayaz. A systematic literature review on cloud computing security: threats and mitigation strategies. *IEEE Access*, 9:57792–57807, 2021.

[74] Maciej Pocwierz. How an empty s3 bucket can make your aws bill explode. https://medium.com/@maciej.pocwierz/how-an-empty-s3-bucket-can-make-your-aws-bill-explode 2024. [Accessed 12-05-2024].

[75] Aliya Tabasum, Zeineb Safi, Wadha AlKhater, and Abdullatif Shikfa. Cybersecurity issues in implanted medical devices. In *2018 International Conference on Computer and Applications (ICCA)*, pages 1–9. IEEE, 2018.

[76] Shams Ajrawi, Ramesh Rao, and Mahasweta Sarkar. Cybersecurity in brain-computer interfaces: Rfid-based design-theoretical framework. *Informatics in Medicine Unlocked*, 22:100489, 2021.

[77] Andrei Costin, Apostolis Zarras, and Aurélien Francillon. Automated dynamic firmware analysis at scale: a case study on embedded web interfaces. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, 2016.

[78] Gopalan Sivathanu, Charles P Wright, and Erez Zadok. Ensuring data integrity in storage: Techniques and applications. In *Proceedings of the 2005 ACM workshop on Storage security and survivability*, pages 26–36, 2005.

[79] Kelsey Harley and Rodney Cooper. Information integrity: Are we there yet? *ACM Computing Surveys (CSUR)*, 54(2):1–35, 2021.

[80] Enrique Tomás Martínez Beltrán, Mario Quiles Pérez, Sergio López Bernal, Alberto Huertas Celdrán, and Gregorio Martínez Pérez. Noise-based cyberattacks generating fake p300 waves in brain–computer interfaces. *Cluster Computing*, pages 1–16, 2021.

[81] Emanuele Maiorana, Gabriel Emile Hine, Daria La Rocca, and Patrizio Campisi. On the vulnerability of an eeg-based biometric system to hill-climbing attacks algorithms' comparison and possible countermeasures. In *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, pages 1–6. IEEE, 2013.

[82] National Institute of Standards and Technology. Cve-2023-49914 detail. https://nvd.nist.gov/vuln/detail/CVE-2023-49914, 2023. [Accessed 09-05-2024].

[83] Eoin Brophy, Peter Redmond, Andrew Fleury, Maarten De Vos, Geraldine Boylan, and Tomás Ward. Denoising eeg signals for real-world bci applications using gans. *Frontiers in Neuroergonomics*, 2:805573, 2022.

[84] Mend.io. Most secure programming languages. https://www.mend.io/most-secure-programming-languages/, 2021. [Accessed 12-05-2024].

[85] Yuri Yakimenko. Most frequent memory allocation errors in c/c++ made by developers. https://www.hoist-point.com/most-frequent-memory-errors-in-cpp.htm. [Accessed 12-05-2024].

[86] Xiao Cheng, Haoyu Wang, Jiayi Hua, Guoai Xu, and Yulei Sui. Deepwukong: Statically detecting software vulnerabilities using deep graph neural network. *ACM Transactions on Software Engineering and Methodology (TOSEM)*, 30(3):1–33, 2021.

[87] Nurit Dor, Michael Rodeh, and Mooly Sagiv. Cssv: Towards a realistic tool for statically detecting all buffer overflows in c. In *Proceedings of the ACM SIGPLAN 2003 conference on Programming language design and implementation*, pages 155–167, 2003.

[88] Les Pounder. White house urges developers to avoid c and c++, use 'memory-safe' programming languages, 2024. [Accessed 21-03-2024].