Linking Computers to the Brain: Overview of Cybersecurity Threats and Possible Solutions

Tuomo Lahtinen, Andrei Costin

Faculty of Information Technology, University of Jyväskylä, P.O. Box 35, Jyväskylä, 40014 Finland {tutalaht,ancostin}@jyu.fi https://jyu.fi/it/

Abstract. The brain-computer interface (BCI) is a growing field of technology, and it has become clear that BCI systems' cybersecurity needs amelioration. When BCI devices are developed with wireless connection capabilities, more often than not, this creates more surface area for attackers to concentrate their attacks. The more invasive BCI technology is used, the greater the threat to the users' physical health. In this paper, we summarize and outline the main cybersecurity threats and challenges that BCI systems may face now and in the future. Furthermore, we present avenues for the future BCI systems including cybersecurity solutions and requirements. We emphasize the importance of the health layer to be considered as important as technical layers in BCI systems as people cannot endure life-threatening situations where attackers could cause permanent brain damage to the BCI user.

Keywords: Brain–Computer Interface · Deep Brain Stimulation · Cybersecurity · Vulnerability · Privacy.

1 Introduction

The brain-computer interface (BCI) is a growing field of technology among researchers [29] that can make people's lives easier. Initially, BCIs were mainly made for medical purposes, but in the last ten years research direction has been shifting into non-medical research [42]. BCI applications are influential in the fields of healthcare and well-being, gaming, smart homes and cities, military, and more. BCIs are not a new research topic; BCI research was established in the early '70s at the University of California [43]. In this early BCI research, researchers tried to prove that direct brain-computer communication was plausible through multiple experiments. At first, BCI systems were used only for brain activity recording, but nowadays BCI systems are also capable of stimulating brain activity, which makes BCI systems bidirectional.

Cybersecurity development of the BCI is at the early stages as cybersecurity has not been considered a consequential part of the BCI. The lack of cybersecurity requirements is real in BCI systems [5,11,28]. BCI systems' cybersecurity can be evaluated with security the triangle "CIA," where "C" stands for **confidentiality**, "I" for **integrity** and "A" for **availability**. Bernal et al. [11] added one more "security and safety" component to the CIA triad. The CIAS is a new

approach to security in BCI systems, where "S" stands for **safety**. CIA focuses on the technical side of a BCI system, but safety refers to the user's physical integrity. In other words, is the use of a BCI device safe for the user, and can the device cause harm to the physical integrity of the user?

In this paper, we state some of the challenges that BCI systems may encounter in the future (Section 3). One of the challenges is that attacks and breaches against the medical healthcare industry are rising [31,38,45] and BCIs can be used for medical purposes as well. Sensitive medical data is attracting malicious attackers and could be worth hundreds of dollars on the dark web [38].

In Section 3 we address more specifically the rising technologies such as transcranial direct current stimulation (tDCS) 3.1 and deep brain stimulation (DBS) 3.2. DBS devices nowadays have wireless connection possibilities that are creating a threat to the integrity of the BCI user's health.

Finally, we present possible future layers to secure the BCI system in Section 4. The layer-based cybersecurity model (Figure 1) includes eight layers that all need to be considered when a BCI system is designed and developed.

2 Brain-Computer Interface: Applications

BCI systems have many different use purposes, and there are also multiple technologies that are separated into two categories, which are brain wave acquisition techniques and brain stimulation techniques. The most common techniques in brain wave acquisition are electroencephalography (EEG), electrocorticography (ECoG), functional magnetic resonance imaging (fMRI), and magnetoencephalography (MEG). The most common stimulation techniques are transcranial magnetic stimulation (TMS), transcranial electrical stimulation (tES), transcranial focused ultrasound (tFUS), tDCS and DBS. Neural dust is technology that is used for both purposes [10].

Kapitonova et al. [28] listed a range of domains, from working and employment, productivity, cognitive enhancement, education, art, gaming, entertainment and virtual reality (VR), neuromarketing, smart homes and smart cities, to security and military-related BCI applications. Using BCIs for medical purposes can be seen as a primary purpose. There are two types in the medical domain. BCIs can be used for diagnosing or supportive purposes [29]. Supporting could mean, for example, treating Parkinson's symptoms or controlling a wheelchair, and diagnosing could mean diagnosing Alzheimer's disease. Of course, some BCI use can be partly seen as being for medical purposes if a patient with restriction in moving/lifting/completing normal daily routines gets help by using a BCI, for example, to control smart home devices. Teles et al. [40] used the union of Internet of Things (IoT) and BCI systems to achieve control, which was called the Brain-to-Thing Communication (BTC) system. The Michael J. Fox Foundation [24] listed three different manufacturers that offer DBS-based BCIs that are approved by the U.S Food and Drug Administration (FDA). All three manufacturers' devices are used to treat Parkinson's symptoms. Devasia et al. [20] introduced a BCI system that assisted quadriplegic people (the state of paralysis

where the body is paralyzed from the shoulders down) in performing some of their daily activities by themselves.

Although BCIs have been used mostly for medical purposes in the past, we have seen the direction shift in the last 10 years from medical to non-medical as non-medical domains have more potential users around the world [42]. Usage such as aerial device control has been presented in a few studies. Rosca et al. [36] introduced a quadcopter controlled via a BCI, and Prasath et al. [34] conducted research in a similar field where an unmanned aerial vehicle (UAV) was controlled using a BCI. One of the richest research field using BCIs is smart home control or BTC, as Teles et al. [40] called their solution. Often, integrating BCI and IoT together is driven by the urge to make life more convenient and to help impaired patients. A few different IoT-related studies are those of Saboor et al. [37], where BCI-controlled smart glasses were used to control devices; Chicaiza et al. [16], who used a P300 speller to command IoT devices; and Parui et al. [33], who used Muse headband sensor, which captured EEG signals with an eye blink. In research conducted by Saboor et al. [37], participants controlled a smart home system with an accuracy of over 80%. Elshenaway et al. [23] demonstrated a new method for authenticating IoT devices using EEG signals and hand gestures. The accuracy was 92%, which could be acceptable for using some smart home IoT devices, but what if your door refuses to unlock every tenth time? Moreover, researchers demonstrated that a large population of IoT devices are vulnerable [18,19], which leads to them being prime targets for IoT specific malware attacks [17] further leading to Internet-wide botnets and attacks [6].

Another venue for BCI usage is gaming, but there is a problem with satisfactory user experience. Better user experience often requires more invasive BCI techniques, such as ECoG [11]. Marshall et al. [30] conducted a survey about using BCIs in gaming. Their conclusion was that using BCI technology is limited, and BCIs in gaming can be used for training or testing purposes of BCI technology. Simple games can be developed to use BCIs, such as Tetris [44], or "Neuro Wander" – a game based on the fairy tale Hansel and Gretel [46].

3 Brain-Computer Interface: Challenges

There are privacy concerns about the future of BCIs, and privacy seems to be the most noted challenge in BCI systems. Takabi et al. [39] wondered the question, Is it possible that in the future, we will be able to get more results from the raw brain data analyzed, and can this later reveal critical data? This was noted especially when the brain data is handled publicly because of open research. The critical data is always anonymized in research but is that enough? If data is exposed to a malicious attacker, it could put the user's life at risk [39].

Kapitonova et al. [28] stated that security and privacy should be handled as defaults and part of the design of BCI systems. The problem in this vision of security and privacy as defaults is that it is not clear how that would be achieved in effective practical terms. To mitigate security and privacy problems, we need

Confidentiality	**Integrity**	**Availability**
Noise adding [29] - Goal: Disrupt data sending - Complexity: High	Noise adding [29] - Goal: Disrupt data sending - Complexity: High	Neuronal jamming [8,9] - Goal: Denial of service - Complexity: Low
Stimuli altering [29] - Goal: Misdiagnosis or misuse - Complexity: Medium	Stimuli altering [29] - Goal: Misdiagnosis or misuse - Complexity: Medium	Neuronal flooding [8,9] - Goal: Collapse of network - Complexity: Low
Artificial input [29] - Goal: Misdiagnosis or misuse - Complexity: High	Artificial input [29] - Goal: Misdiagnosis or misuse - Complexity: High	Drain the battery [14,35] - Goal: Denial of service - Complexity: Low
Modified input (MitM) [29] - Goal: Misdiagnosis or misuse - Complexity: High	Modified Input (MitM) [29] - Goal: Misdiagnosis or misuse - Complexity: High	Interfere BCI connections [14] - Goal: Denial of service - Complexity: Low
Data leakage [29,35] - Goal: Misuse of obtained brain data - Complexity: Medium	Data leakage [29,35] - Goal: Misuse of obtained brain data - Complexity: Medium	Switch off IPG [35] - Goal: Denial of service - Complexity: Medium
Neuronal spoofing [9] - Goal: Steel data - Complexity: Very high	Neuronal selective forwarding [9] - Goal: Selectively drop packets - Complexity: High	
Neuronal sybil [9] - Goal: Computer hijack - Complexity: Very high	Neuronal sinkhole [9] - Goal: Manipulate routing - Complexity: High	
Neuronal nonce [9] - Goal: Replay attack - Complexity: Low	Tampering data [14,35] - Goal: Modify data - Complexity: High	
Neuronal scanning [9] - Goal: Identify vulnerable services - Complexity: Medium		

Table 1. Attacks organized under CIA

to address issues by recognizing possible cybersecurity challenges and threats that BCI systems are facing or may face in the future.

Bernal et al. [11] created an informative list of attacks, impacts, and countermeasures for BCI systems. Attacks have various effects in corresponding CIAS (confidentiality, integrity, availability and security) domains. Safety can be considered the most important aspect for the BCI user. If use of the BCI system puts a user's life at risk, it is not worth using the system. Safety can be threatened in two ways: technology- or attack- created threat. Section 3.1 explains more about the threat created by technology in tDCS.

The concern is that causing harm to the BCI user is easier than manipulating data. Bernal et al. [7] and Pycroft et al. [35] stated that if an attacker is only trying to cause harm to the user or patient, the attacker hardly needs any knowledge about brain stimulation or specific information about the patient. This kind of attack can be described as a blind attack [35]. In Table 1, attacks are listed under CIA according to the attack surface. Some attacks affect multiple fields and in that case, the attack is mentioned in more than one or in the most suitable field of the CIA.

3.1 Challenges in tDCS

In recent years transcranial direct current stimulation (tDCS) has gained popularity because of its potential to improve mood and cognitive function [2]. tDSC is a non invasive brain stimulation technique that directs a low electric current to the scalp, but it is not approved by the FDA [4]. tDSC has shown that it can

enhance brain functioning, such as learning, attention, creativity and memory. Although there is still research to do with tDSC, it could be used as an effective tool to boost mental performance and well-being without being invasive [2].

As a BCI technology, tDCS seems quite harmless, as side effects (e.g., minor burns) tend to be rare, with mild or disappearing symptoms after the experiment; still there are some issues with this technology. Moioli et al. [32] envisioned that in the future, there will possibly be a need to consider undesired signals that affect the brain stimulus through wireless networks in BCI systems. BCIs could receive unwanted read and write signals, which could affect human behavior, thus having individual and social influence [32]. Boccard-Bine and Sen [12] suspected that tDCS had caused seizures, and the same suspicion was raised by Ekici [21]. When buying a tDCS device, buyers should always make sure that the device is safe to use. This can be elevated when choosing a known brand [2].

Besides the upper neural change or damage cases, if tDCS devices are connected to the Internet, they are vulnerable to all the most common attacks against networks and devices. Also, data sent, handled, and stored on a network is vulnerable to attacks such as sniffing, MitM, phishing, and DoS.

3.2 Challenges in DBS

DBS is a technique used mainly for health care, for example, treating neurological disorders. In DBS, electrodes are implanted in the deep regions of the brain by stereotactic neurosurgical techniques [26], and DBS can be included in the most invasive BCI technology. According to the Michael J. Fox Foundation [24], there are currently a few different DBS devices approved by the U.S FDA. The devices are from the manufacturers Abbott, Medtronic and Boston Scientific and are designed to help reduce symptoms of Parkinson's disease. Parkinson's disease is a neurodegenerative disorder of aging that is affecting both motor and cognitive function. Parkinson's disease is progressive and cannot be cured, but there are effective medications to treat it, and DBS can also be used for reducing symptoms, especially in medication-resistant cases [25]. These DBS devices are invasive and use directional stimulation where pulses are sent directly to the target areas of the brain.

The Michael J. Fox Foundation [24] stated that Abbott developed the first device offering remote programming, and this capability is likely to become more widely available in the future. This trend is inevitably increasing threats that BCI systems will face as BCIs are becoming remote controllable and more attack surface is exposed [41]. In terms of DBS-based BCIs where the stimulus is invasive and pulses are sent straight to the brain, there is a serious threat against the physical integrity of the patient. In Table 1, there are eight different neural attacks presented that could be used against DBS.

In the research by Bernal et al. [8], it was highlighted that using wireless communications, such as Bluetooth, can expose sensitive knowledge about the instant of attack, the voltage used in a device, or the list of targeted neurons in the BCI. The need for remote control must be well motivated in the sense that remote control should create more value to the user than it creates health-related

threats. For example, CVE-2022-25837 [1] permits an unauthenticated MitM to acquire credentials.

4 Discussion

BCI systems are becoming more advanced, and as they are developed, more threats will emerge. We need a general design guide or framework for BCI systems. Kapitonova et al. [28] presented a good framework for preserving privacy and cybersecurity in BCIs, but this does not cover every aspect of the BCI system (e.g., physical threats caused by the BCI). The world is full of different standards and guides trying to explain, clarify and enhance security in IT systems. For example, OSI 7 created by the International Organization for Standardization (ISO) 1984 is an architecture where seven layers are linked together to transmit data from one layer to another. OSI 7 defines layers and functions at layers in order to secure data transfer between layers [3,13]. There are many other layer-based guides similar to OSI 7 that can be used to evaluate data security. For example, Elijah et al. [22] presented seven cybersecurity layers for Industry 4.0.

	Description	Actions to increase security
HUMAN LAYER	Humans are to key component to create secured systems but also to use them securetly.	Increasing cybersecurity awarness through educations and training.
PERIMETER SECURITY	Physical and digital security techniques are involved here including perimeter security control.	Firewalls, antivirus sw, data encryption, network monitoring, device management etc.
NETWORK SECURITY	Network is connecting BCI system sensors, devices, storages etc. Who has access and how wide access rights are?	Systems need to have access control in order to preserve security. Access should only cover necessary parts of the system.
ENDPOINT SECURITY	Devices at endpoints to send and receive data.	Make sure that data is encrypted on both ends.
APPLICATION SECURITY	Data processing and handling at computer or mobile app in BCI system.	Keep applications and devices updated, and manage access control.
DATA SECURITY	In BCI systems data is brain data and analyses data from brain data processing, and user data.	Data needs to be encrypted always, when processing, transmitting or storing.
CRITICAL ASSETS	Critical information which must safeguard e.g. personal health records.	Risk analysis, creating safe architecture for BCI, addressing all the above levels with sufficient interest.
HEALTH LAYER	Health related issues such as surgery for BCI implant etc. and integrity of the physical health of the user.	Surgery must be conducted by professionals and securing other layers will secure this layer against neural attacks.

Fig. 1. Layers to secure BCI systems.

Normally, IT systems do not cause harm to the users, but there is a growing amount of health care devices that have a risk of malicious attackers cause harm to the user. As mentioned in subsection 3.2, DBS devices pose life-threatening risks, and Jackson et al. [27] explored the Medical Internet of Things (MIoT) and found several mentions of life-threatening risks. The risk comes when the MIoT device is wirelessly connected and there is a possibility to monitor and control the device remotely [27].

To understand BCI system requirements, we provide BCI system layering in Figure 1. These layers can be used to describe the cybersecurity of the BCI system and enhance cybersecurity awareness. The layers follow the seven cybersecurity layers of Elijah et al. [22], but we added an eighth layer, the **Health Layer**, to provide a better understanding about the BCI system as a whole.

In Figure 1, the layers are as follows: 1) Human Layer, 2) Perimeter Security, 3) Network Security, 4) Application Security, 5) Endpoint Security, 6) Data Security, 7) Critical Assets, and 8) Health Layer. Layers from 1 to 7 are related to data inside the BCI system. Layer 8 contains health-related issues, such as the physical integrity of the user and surgery for BCI implants. As the health layer holds the biggest threat against users, it is important to research actions to reduce risks in this layer. For example, Chiaramello et al. [15] studied how DBS could be improved to be less invasive. They discovered that minimal invasiveness and proven biocompatibility, makes magneto-electric nanoparticles (MENP) mediated DBS, representing a big improvement towards less invasive and more secured stimulation of the deep neural tissues. This kind of research is welcome, as less invasive techniques lower not only physical threats caused by surgery but also neural attacks as the invasiveness level decreases.

The second important layer is the Human Layer, as humans make errors. It cannot be precisely stated how many successful data breaches are caused by human error, but it is the most effective layer to make improvements in the cybersecurity field. BCI system users need education and knowledge to avoid misuse of BCI devices or being affected by phishing attacks, malware, viruses, and so on. Education and training are mentioned in many studies to reduce data breaches [10,31,38,45].

Other layers require technical security. For privacy attack prevention, the commonly suggested techniques are access control, efficient encryption, and adding noise into brain data passed back and forth between various hardware and software components of the BCI system. Takabi et al. [39] mentioned that a BCI application should never have access to the raw brain data, as it is more easily accessible by an attacker. All the devices that are part of the BCI system should be protected by keeping them up to date with the latest software/firmware updates and fixes [18]. Firewalls, antivirus, data traffic monitoring should be used if possible to detect malicious data and unauthorized access.

When conducting future and further research among BCI systems, there is a need to carry out hands-on testing to see how secure BCI systems really are. Testing should involve as many layers as possible in the BCI system. Related to the testing, it poses some ethical issues and it is not possible to use human volunteers in research when conducting tests for neural attacks, as this could cause at least a skin burn or at most serious damage to the brain.

5 Conclusion

In the future, the cybersecurity of BCI systems must be followed closely. Non-medical BCIs are gaining more ground by replacing medical BCIs from the lead

research and development post. Medical BCIs focus on small targets of patients, whereas non-medical BCIs target all individuals globally. As we have already discovered from IoT development and marketing, the security aspect of devices has been neglected when devices have been pushed into the market as fast as possible to maximize profit. Regulation, validation or standardization among BCI devices could improve the safety of the devices (e.g., FDA or other authority approval for using devices in medical treatment).

We must be aware that when a BCI system is designed and developed, it is needed to address all the layers from Figure 1 to ensure that the BCI system's security is at an adequate level. A BCI system is as strong as the weakest link in the system, which means the weakest layer defines the rigorousness of BCI systems.

References

1. Cve-2022-25837 detail (2022), https://nvd.nist.gov/vuln/detail/CVE-2022-25837, accessed April 24, 2023
2. Best tdcs devices of 2023 (2023), https://tdcs.com/best-tdcs-devices/, accessed April 18, 2023
3. Layers of osi model (2023), https://www.geeksforgeeks.org/layers-of-osi-model/, accessed April 18, 2023
4. What is transcranial direct current stimulation? (2023), https://neuromodec.org/what-is-transcranial-direct-current-stimulation-tdcs/, accessed April 24, 2023
5. Ajrawi, S., Rao, R., Sarkar, M.: Cybersecurity in brain-computer interfaces: Rfid-based design-theoretical framework. Informatics in Medicine Unlocked **22**, 100489 (2021)
6. Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L., Kallitsis, M., et al.: Understanding the mirai botnet. In: 26th {USENIX} security symposium ({USENIX} Security 17). pp. 1093–1110 (2017)
7. Bernal, S.L., Celdran, A.H., Maimo, L.F., Barros, M.T., Balasubramaniam, S., Perez, G.M.: Cyberattacks on miniature brain implants to disrupt spontaneous neural signaling. IEEE Access **8**, 152204–152222 (2020)
8. Bernal, S.L., Celdrán, A.H., Pérez, G.M.: Neuronal jamming cyberattack over invasive bcis affecting the resolution of tasks requiring visual capabilities. computers & security **112**, 102534 (2022)
9. Bernal, S.L., Celdrán, A.H., Pérez, G.M.: Eight reasons to prioritize brain-computer interface cybersecurity. Communications of the ACM **66**(4), 68–78 (2023)
10. Bernal, S.L., Celdrán, A.H., Pérez, G.M., Barros, M.T., Balasubramaniam, S.: Cybersecurity in brain-computer interfaces: State-of-the-art, opportunities, and future challenges. arXiv preprint arXiv:1908.03536 (2019)
11. Bernal, S.L., Pérez, M.Q., Beltrán, E.T.M., Pérez, G.M., Celdrán, A.H.: When brain-computer interfaces meet the metaverse: Landscape, demonstrator, trends, challenges, and concerns. arXiv preprint arXiv:2212.03169 (2022)
12. Boccard-Binet, S., Sen, A.: Safety of transcranial direct current stimulation in healthy participants. Epilepsy & Behavior Reports **15** (2021)
13. Briscoe, N.: Understanding the osi 7-layer model. PC Network Advisor **120**(2), 13–15 (2000)

14. Camara, C., Peris-Lopez, P., Tapiador, J.E.: Security and privacy issues in implantable medical devices: A comprehensive survey. Journal of biomedical informatics **55**, 272–289 (2015)
15. Chiaramello, E., Fiocchi, S., Bonato, M., Marrella, A., Suarato, G., Parazzini, M., Ravazzani, P.: Magnetoelectric nanoparticles: Evaluating stimulation feasibility of the possible next generation approach for deep brain stimulation. IEEE Access **10**, 124884–124893 (2022)
16. Chicaiza, K.O., Benalcázar, M.E.: A brain-computer interface for controlling iot devices using eeg signals. In: 2021 IEEE Fifth Ecuador Technical Chapters Meeting (ETCM). pp. 1–6. IEEE (2021)
17. Costin, A., Zaddach, J.: Iot malware: Comprehensive survey, analysis framework and case studies
18. Costin, A., Zaddach, J., Francillon, A., Balzarotti, D.: A large-scale analysis of the security of embedded firmwares. In: 23rd {USENIX} Security Symposium ({USENIX} Security 14). pp. 95–110 (2014)
19. Costin, A., Zarras, A., Francillon, A.: Automated dynamic firmware analysis at scale: a case study on embedded web interfaces. In: 11th ACM on Asia Conference on Computer and Communications Security. pp. 437–448 (2016)
20. Devasia, D., Roshini, T., Jacob, N.S., Jose, S.M., Joseph, S.: Assistance for quadriplegic with bci enabled wheelchair and iot. In: 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS). pp. 1220–1226. IEEE (2020)
21. Ekici, B.: Transcranial direct current stimulation-induced seizure: analysis of a case. Clinical EEG and neuroscience **46**(2), 169 (2015)
22. Elijah, O., Ling, P.A., Rahim, S.K.A., Geok, T.K., Arsad, A., Kadir, E.A., Abdurrahman, M., Junin, R., Agi, A., Abdulfatah, M.Y.: A survey on industry 4.0 for the oil and gas industry: Upstream sector. IEEE Access **9**, 144438–144468 (2021)
23. Elshenaway, A.R., Guirguis, S.K.: Adaptive thresholds of eeg brain signals for iot devices authentication. IEEE Access **9**, 100294–100307 (2021)
24. Foundation, M.J.F.: Currently available deep brain stimulation devices, https://www.michaeljfox.org/news/currently-available-deep-brain-stimulation-devices, accessed April 18, 2023
25. Fröhlich, F.: Chapter 23 - parkinson's disease. In: Fröhlich, F. (ed.) Network Neuroscience, pp. 291–296. Academic Press, San Diego (2016)
26. Hemm, S., Wårdell, K.: Stereotactic implantation of deep brain stimulation electrodes: a review of technical systems, methods and emerging tools. Medical & biological engineering & computing **48**, 611–624 (2010)
27. Jackson Jr, G.W., Rahman, S.: Exploring challenges and opportunities in cybersecurity risk and threat communications related to the medical internet of things (miot). arXiv preprint arXiv:1908.00666 (2019)
28. Kapitonova, M., Kellmeyer, P., Vogt, S., Ball, T.: A framework for preserving privacy and cybersecurity in brain-computer interfacing applications. arXiv preprint arXiv:2209.09653 (2022)
29. Landau, O., Puzis, R., Nissim, N.: Mind your mind: Eeg-based brain-computer interfaces and their security in cyber space. ACM Computing Surveys (CSUR) **53**(1), 1–38 (2020)
30. Marshall, D., Coyle, D., Wilson, S., Callaghan, M.: Games, gameplay, and bci: the state of the art. IEEE Transactions on Computational Intelligence and AI in Games **5**(2), 82–99 (2013)
31. McLeod, A., Dolezel, D.: Cyber-analytics: Modeling factors associated with healthcare data breaches. Decision Support Systems **108**, 57–68 (2018)

32. Moioli, R.C., Nardelli, P.H., Barros, M.T., Saad, W., Hekmatmanesh, A., Silva, P.E.G., de Sena, A.S., Dzaferagic, M., Siljak, H., Van Leekwijck, W., et al.: Neurosciences and wireless networks: The potential of brain-type communications and their applications. IEEE Communications Surveys & Tutorials pp. 1599–1621 (2021)
33. Parui, S., Samanta, D., Chakravorty, N.: An advanced healthcare system where internet of things meets brain-computer interface using event-related potential. In: 24th International Conference on Distributed Computing and Networking. pp. 438–443 (2023)
34. Prasath, M., Naveen, R., Sivaraj, G.: Mind-controlled unmanned aerial vehicle (uav) using brain–computer interface (bci). Unmanned Aerial Vehicles for Internet of Things (IoT) Concepts, Techniques, and Applications pp. 231–246 (2021)
35. Pycroft, L., Boccard, S.G., Owen, S.L., Stein, J.F., Fitzgerald, J.J., Green, A.L., Aziz, T.Z.: Brainjacking: implant security issues in invasive neuromodulation. World neurosurgery **92**, 454–462 (2016)
36. Rosca, S., Leba, M., Ionica, A., Gamulescu, O.: Quadcopter control using a bci. In: IOP Conference Series: Materials Science and Engineering. vol. 294, p. 012048. IOP Publishing (2018)
37. Saboor, A., Rezeika, A., Stawicki, P., Gembler, F., Benda, M., Grunenberg, T., Volosyak, I.: Ssvep-based bci in a smart home scenario. In: Advances in Computational Intelligence: 14th International Work-Conference on Artificial Neural Networks, IWANN 2017, Cadiz, Spain, June 14-16, 2017, Proceedings, Part II 14. pp. 474–485. Springer (2017)
38. Seh, A.H., Zarour, M., Alenezi, M., Sarkar, A.K., Agrawal, A., Kumar, R., Ahmad Khan, R.: Healthcare data breaches: insights and implications. In: Healthcare. vol. 8, p. 133. MDPI (2020)
39. Takabi, H., Bhalotiya, A., Alohaly, M.: Brain computer interface (bci) applications: Privacy threats and countermeasures. In: 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC). pp. 102–111. IEEE (2016)
40. Teles, A., Cagy, M., Silva, F., Endler, M., Bastos, V., Teixeira, S.: 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). vol. 1, pp. 92–94 (2017)
41. Uppal, R.: Brain-computer interfaces (bci) are vulnerable to cyber attacks and need security and safety measures (2023), https://idstch.com/cyber/brain-computer-interfaces-bci-vulnerable-cyber-attacks-need-security-safety-measures/, accessed April 24, 2023
42. Värbu, K., Muhammad, N., Muhammad, Y.: Past, present, and future of eeg-based bci applications. Sensors **22**(9), 3331 (2022)
43. Vidal, J.J.: Toward direct brain-computer communication. Annual review of Biophysics and Bioengineering **2**(1), 157–180 (1973)
44. Wang, Z., Yu, Y., Xu, M., Liu, Y., Yin, E., Zhou, Z.: Towards a hybrid bci gaming paradigm based on motor imagery and ssvep. International Journal of Human–Computer Interaction **35**(3), 197–205 (2019)
45. Wikina, S.B.: What caused the breach? an examination of use of information technology and health data breaches. Perspectives in health information management **11**(Fall) (2014)
46. Yoh, M.S., Kwon, J., Kim, S.: Neurowander: a bci game in the form of interactive fairy tale. In: 12th ACM international conference adjunct papers on Ubiquitous computing-Adjunct. pp. 389–390 (2010)