World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Research Article)

Check for updates

Neurotechnology and Human-Machine Interfaces: Securing Brain-Computer Interfaces (BCIs) Against Hacking

Adedotun Lawrence Omotade *

IT Subject Matter Expert, Global Service Delivery.

World Journal of Advanced Research and Reviews, 2025, 27(01), 2761-2771

Publication history: Received on 25 May 2025; revised on 29 August 2025; accepted on 01 September 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.27.1.2534

Abstract

Brain-Computer Interfaces (BCIs) are developing as a promising technology in many areas, such as medical, military and consumer technology. Nevertheless, there are also serious security issues that involve the growing dependency on these technologies, especially the susceptibility to hacking. This research investigates the dangers of BCI systems and discusses the existing approaches to ensuring security of such devices against cyberattacks. The methodology will be to examine case studies in different domains, examine the literature available on vulnerabilities of BCI and to assess security practices like encryption and authentication approaches. The main conclusions include the increasing complexity of the hacking tools used to attack BCIs, and the insufficiency of the existing security systems to address the identified threats. The research highlights the necessity of sophisticated security measures and protection of neural information by advanced detection systems of threats and improved encryption to guarantee the integrity of BCI systems. The results are of critical value to researchers and developers who could use them as a basis to come up with more secure and resilient brain-computer interfaces in future.

Keywords: BCI Security; Neural Data; Cybersecurity Threats; Data Encryption; Privacy Protection; Signal Manipulation; Healthcare BCIS; Real-Time Detection; Security Protocols; Neurotechnology Ethics

1. Introduction

The neurotechnology is an area that involves interconnecting the human brain to technology, and there has been immense progress, especially in the creation of Brain-Computer interfaces (BCI). BCIs are devices that create direct communication channels between the brain and external devices, whereby they have diverse uses in healthcare, communication, and technology. In medical research, BCIs are directed at treating neurological conditions, improving the rehabilitation process, and giving physically disabled individuals the opportunity to communicate with their surroundings (Mudgal et al., 2020). There are speech and thought-controlled apps in communication that helps people with serious speech difficulties. BCIs are also bringing forth innovation in technology/gaming and virtual reality to provide immersive experiences to users (Mudgal et al., 2020). Nevertheless, as the BCIs usage increases, cybersecurity risks, in particular, hacking is becoming a major issue. The connection between the brain activity and the machines does represent exceptional vulnerabilities since without the authorization, the neural signals could be manipulated, the data could be compromised, or even physical damages could be caused (Mudgal et al., 2020). In this paper, the researcher is going to examine the dynamic threats posed to BCIs, and why there is a necessity to enforce stringent security measures to protect the sensitive neural information and facilitate the security functioning of such innovative technologies.

1.1. Overview

Brain-Computer Interfaces (BCIs) is a device that modifies human brain communication and allows individuals to communicate with the external environment without using the conventional route like speech or movement. The

* Corresponding author: Adedotun Lawrence Omotade

history of BCI technology goes back to the years of the early 20 th century when in their fundamental research, researchers believed that the idea of brain-computer interfaces was more of a myth than reality (Kawala-Sterniuk et al., 2021). BCIs allow physically handicapped people who are severely physically disabled to operate prosthetic limbs, computers, and even wheel chairs, which have greatly enhanced their life quality. Also, BCIs are being incorporated into the higher order communication systems that enable people to communicate by nothing more than thinking. BCIs are facilitating an age of immersive experiences within entertainment and gaming because users can now control virtual worlds through brain activity (Kawala-Sterniuk et al., 2021). The academic impact of BCIs is tremendous since studies are still in the process of revealing the mysteries of brain signals and how they can be used to improve human-machine interaction. It is the practical sense that the further evolution of BCIs promises to revolutionize industries due to its ability to provide the opportunities of interaction never seen before. Neurotechnology intersects with such disciplines as artificial intelligence, and new possibilities are emerging. Nonetheless, these developments pose threats as well, especially regarding the issue of security, privacy, and ethical considerations, all of which still need to be investigated further since the field is still developing (Kawala-Sterniuk et al., 2021).

1.2. Problem Statement

The dynamism in the development of Brain-Computer Interfaces (BCIs) has seen their wide use but one of the greatest threats is the susceptibility of Brain-Computer Interfaces to cyberattacks. BCIs that interface directly with the human brain pose at least possible security threats that may not only jeopardize personal privacy, but also physical safety. The illegal access to the BCI systems may cause the malicious use of brain signals, which will lead to unacceptable consequences, including the breach of data or even distorted neural activity. Since the capabilities of BCIs are increasingly embedded in such critical systems as medical equipment or military systems, the risk of hacking has dire repercussions, such as the theft of sensitive neural information and harm to the cognitive and physical well-being of individuals. Thus, it is essential to consider good security to ensure that BCI users are secured and that the integrity of this new technology is upheld. To enable trust in BCI systems, it is critical to tackle these security issues so that they become relied upon and safely embraced.

Objectives

The main goals of the work are to investigate the possible dangers of Brain-Computer Interface (BCI) systems, compare the current security parameters against the possibility of hacking, and suggest new security standards to protect the BCIs. Since BCIs are increasingly penetrating the most important industries, including healthcare, military and consumer technology, there is a need to be familiar with the unique vulnerabilities in the systems. The paper will closely analyze the existing security systems, their shortcomings and determine how new technologies like encryption and biometric authentication can increase security. The study will also propose the possible future trends in BCI security, including the new methodology and technologies that might help reduce the risk of cyberattacks. Finally, the objective is to create a comprehensive awareness of BCI security requirements and help to create more secure systems.

1.3. Scope and Significance

This study presents the increasing issue of insecurity within the Brain-Computer Interface (BCI) systems. The study scope will involve the evaluation of existing security practices, the possible threats, and possible solutions to protect BCIs against hackers and unauthorized access. This study is important in two ways. To start with, it is a contribution to the further evolution of neurotechnology, as it discusses the most important issue of cybersecurity, which frequently has been neglected in the context of BCI systems evolution. The security of BCIs is the key to their success and safety as they are becoming more and more part of the healthcare, communication, and military industries. Second, the study demonstrates the significance of cybersecurity in the general area of neurotechnology, and how neuroscientists, engineers, and cybersecurity teams should come together to create secure and reliable systems. The results of the study will have some practical implications on designing, regulating and implementing of BCIs in different industries.

2. Literature review

2.1. Neurotechnology and the Development of BCIs

Brain-Computer Interfaces (BCIs) are leading the revolution in neurotechnology, which has developed tremendously over the last few decades. The concept of BCIs where a direct line of communication between the brain and devices is established started in the 1960s. Simple signal detection and interpretation are identified as important at the early years of research, but nowadays BCIs provide a wide range of application. BCIs find applications in the healthcare sphere as a means of rehabilitation, where individuals with severe impairments are given the opportunity to engage with prosthetics or controlling devices by means of thought alone (Lin et al., 2017). There are also other emerging applications of BCIs like in communication whereby speech impaired individuals can now speak and in entertainment whereby users can play games or virtual worlds through brain signals. The present level of BCI technology, despite its high-tech, has multiple issues, such as signal stability and the interaction without the use of injections (Lotte et al., 2018). The possibilities of BCIs are immense, and to guarantee their stability and availability is essential as they are affecting the field of medicine, communication, etc. Although the emphasis on advancing the functionality of the gadgets and the real-time interpretation of the data has been a priority, researchers now shift their attention to the issue of cybersecurity risk, particularly, to the possibility of unlawful access to neural data, which can be disastrous both to the individuals and the organization (Lin et al., 2017).

2.2. Human-Machine Interfaces: Technologies and Challenges

Human-Machine Interfaces (HMIs) are vital in the Brain-Computer Interfaces (BCIs), as they allow a two-way communication between the brain and external systems. They are interfaces through which neural activity can be transformed into actionable command to devices or the other way round giving people an entry point to control devices, assistive technologies, etc. Nonetheless, even after the technological aspect of HMIs has changed, multiple issues remain, such as latency, reliability, and security (Singh and Kumar, 2021). Delay in signal processing, or latency, may be a problem when using it in real-time (such as in a game or a prosthetic controller). What is more, signal reliability is also a problem because environmental noise or physiological variations can corrupt brain activity signals, and systems do not compose them easily. Another important issue is security; as the use of BCIs grows, there is a possibility of interception or manipulation of neural data by malicious actors, resulting in privacy or control breach (Singh and Kumar, 2021). It is necessary to address such problems to make sure BCI technologies can be effective and safe, particularly with the further spread of their use in such sensitive spheres as healthcare and military applications. These limitations are still being examined, and future studies are expected to enhance the overall HMIs performance and security through improved algorithm training and signal processing methods (Singh and Kumar, 2021).

2.3. Cybersecurity in Neurotechnology

There has been an increasing concern in the field of neurotechnology, especially Brain-Computer Interfaces (BCIs) as cybersecurity issues continue to arise with the growing use of these systems in personal, medical and work settings. The fact that BCI can access directly the brain activity poses challenges on the possibilities of having unauthorized access and manipulation of neural data. Cybersecurity in neurotechnology is the use of encryption, data transmission, and access control to prevent users in case of attacks (Bernal et al., n.d.). The threat of intercepting the data is one of the main weaknesses of BCIs; sensitive neural data may be accessed without the clients being aware of it, and it may result in the risk of privacy invasion or other harmful exploitation. One more issue is the threat of remote hacking, as the attackers might obtain control over a BCI device, which impacts physical/mental state of the user (Bernal et al., n.d.). With the ever-changing BCI systems, the demand of a strong security system is paramount in ensuring the security of data of the user and the integrity of such systems. In this regard, the question of cybersecurity in neurotechnology is not only technical but also ethical, necessitating the idea of balancing the innovation and securing individual rights (Ienca and Hase lager, 2016).

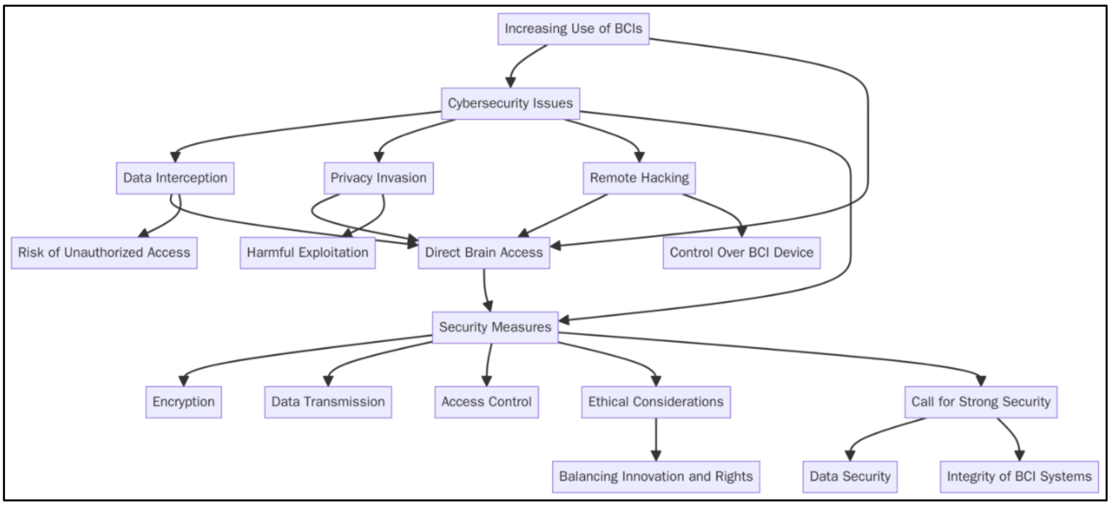

Figure 1 Flowchart illustrating the interconnected elements of cybersecurity in neurotechnology, highlighting the challenges, security measures, and ethical considerations involved in protecting Brain-Computer Interfaces (BCIs) from threats such as data interception, privacy invasion, and remote hacking

2.4. Brain-Computer Interfaces Hacking risks

Brain-Computer Interfaces (BCIs) are susceptible to various hacking threats because of direct interface with the brain and the use of digital systems to process the signal. Among the primary dangers is the fact that the hackers can intercept and manipulate brain signals and possibly gain direct control over devices or be able to modify neural patterns. This may have disastrous effects, such as physical damage or the inability to control assistive technologies. In the medical field, where the BCI is applied to control the prosthetics or to help create speech, these breaches may result in serious medical risks or disabilities. In addition, BCIs deployed in the military may be abused to hack defense infrastructure or interfere with the operations of soldiers (Chaudhary and Agrawal, 2018). The theoretical dangers of hacks are increased due to the growing use of wireless technologies, which offer more such agents of malevolence a chance to attain unauthorized access. Although studies are in progress to enhance the security of these devices, it is evident that as the BCIs increase in scope of integration in critical systems, the threats of hacking will only rise. These risks should be addressed by the effectiveness of security protocols such as encryption and authentication (Chaudhary and Agrawal, 2018).

2.5. Brain-Computer Interface Securing Methods

The issue of security of Brain-Computer Interfaces (BCIs) is a serious concern given the fact that they are vulnerable to hacking and violations. The encryption, authentication, and biometric security are the methodologies of the study and being applied in protecting the BCIs (Xia et al., 2023. This is encrypted to protect the information sent between the brain and the external devices, so any neural signal cannot be read by anyone. Denying access to BCI systems to unauthorized users, authentication mechanisms (including the use of multi-factor authentication) serve to identify the user and the user identity. Another level of protection is the so-called biometric security that incorporates the utilization of peculiarities of physiological activities like the brainwave or neural signature that only the authorized individuals will be able to communicate with the device. These approaches are complementary in making a BCI system more secure, yet there still exist challenges, especially in the real-time processing without interfering with security and usability. There is also an exploration of privacy-preserving approaches, so that sensitive brain information is only utilized to the end of the reason it was recorded and not misused (Xia et al., 2023). Further developments in these fields are required in order to come up with sound security measures that can safeguard the users against possible hacking threats in future.

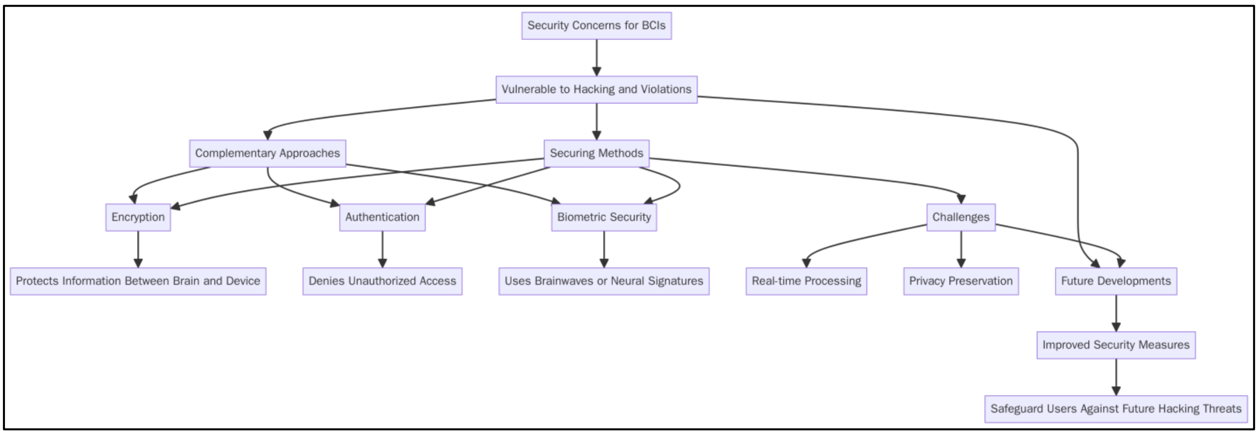
Security Concerns for BCIs
Vulnerable to Hacking and Violations
Complementary Approaches
Securing Methods
Encryption
Authentication
Biometric Security
Challenges
Protects Information Between Brain and Device
Denies Unauthorized Access
Uses Brainwaves or Neural Signatures
Real-time Processing
Privacy Preservation
Future Developments
Improved Security Measures
Safeguard Users Against Future Hacking Threats

Figure 2 Flowchart illustrating the interconnected security methods used in Brain-Computer Interfaces (BCIs), highlighting encryption, authentication, and biometric security as protective measures against hacking. It also addresses the challenges of real-time processing, privacy preservation, and the need for future developments to safeguard users

2.6. Ethical Implications and Human Rights

Brain-Computer Interfaces (BCIs) are associated with serious ethical concerns in terms of privacy, unauthorized access, and possible consequences of hacking, especially when it comes to the development and deployment of the devices. The threat of the breach of privacy of users is a significant issue since BCIs read and analyze neural data. Hacking into neural signals may not only give sensitive data regarding the thoughts or intentions of an individual but also control mental or physical behavior. This brings issues of consent and neural data ownership, possible coercion or exploitation into question. Also, the ethical consequences of hacking are more evident because BPIs are embedded in such sensitive areas as health care, security, and defense. It is possible that the manipulation of BCIs may have grave effects, including changing the motor ability or cognitive abilities of a person, which may result in physical damage or mental distress. With regard to human rights, it is paramount to make sure that the BCI systems should be developed in a way that they have a high security system that prevents manipulations by unauthorized users and preserves the privacy of their neural data (Ienca and Hase lager, 2016). These ethical issues highlight the importance of strict rules and regulation in the creation and application of neurotechnology so that the rights of each individual can be respected and maintained.

3. Methodology

3.1. Research Design

The study will have a mixed-method design based on both qualitative and quantitative designs. The qualitative part will be based on the detailed examination of the security issues, which confront Brain-Computer Interfaces (BCIs), especially with references to the experiences and insights collected during the interviews with experts, case studies, and literature reviews. The quantitative part will imply the review of the statistics data that are connected with BCI vulnerabilities such as the records of security breaches and risk evaluation. Mixed-method is used because it allows to get a full picture of BCI security, to gather anecdotal data that appear in the real world, and to analyze them with numbers to determine patterns and trends and find correlations. Qualitative and quantitative approaches will allow the present study to offer a powerful analysis of the security risks involved with BCIs that would enable more informed security improvement recommendations.

3.2. Data Collection

This study will rely on surveys, expert interviews and case studies methods to collect data. Targeted surveys will be sent to the specialists in the field of neurotechnology, cybersecurity, and other related professions in order to collect quantitative information about the security risks of BCI and challenges they face. Qualitative data will be collected by interviewing experts on the topic and is going to address the strengths and weaknesses of the BCIs and their views and experiences on the subject of possible threats and security practices in place. There will also be case studies whereby documented cases of BCI security breach such as data theft and unauthorized access will be studied to have insight into the actual experience of such vulnerabilities. Methods that will be utilized to collect appropriate information on BCI vulnerability include reviewing of security breach reports, vulnerability testing and incident reporting. This set of data collection strategies will provide a balanced picture of the present situation on BCI security.

3.3. Case Studies/Examples

3.3.1. Case Study 1: Healthcare – BCI Hacking in Medical Devices

In 2018, a team of researchers revealed a serious vulnerability in a brain-computer interface (BCI) applicable in the field of medicine, namely epilepsy treatment. This protest represented an acute problem in the safety of BCIs, especially those of the healthcare application where stakes are high, as the well-being of patients is directly affected. The BCI system that was investigated was created to assist in trying to control epilepsy by providing brain with electrical stimulation, which was intended to stop seizures. Nevertheless, as the researchers discovered, the device was not immune to hacking because of flaws in its wireless communication protocols, through which the implanted device was relaying and receiving data with the external monitoring systems.

These vulnerabilities were used in the attack to disrupt the communication between the device by enabling the attackers to change the frequency and strength of the brain stimulation on the fly. Such tampering with the stimulation patterns may have been disastrous to the health of the patient and has the potential of causing the patient to experience seizures or other negative neurological changes. This was evidenced by the hack, which revealed that a cybercriminal can potentially gain control or compromise the functioning of the medical equipment at the peril of the patient.

This accident cast a doubtful light on the safety of medical BCIs, which are becoming popular to treat a wide range of disorders, such as chronic pain, movement disorders, and neuro-prosthetics in patients with paralysis. As these devices are to communicate directly with the brain, they are subject to a particular security threat. In case of their violation, not only the invasion of patient privacy can be experienced but also the hazardous manipulation of the neurological functions, and the results of such manipulation can be life threatening.

The protest was a call to strengthen of security protocols in the formation of medical BCIs. Since wireless communication is a fundamental part of these devices, these gadgets can be especially prone to cyberattacks due to their lack of robust encryption and secure communication protocols. The scientific community and even medical workers have come to the understanding that, along with clinical effectiveness of such devices, it is essential to ensure their safety by establishing effective cybersecurity systems. With the introduction of encryption techniques, safe authentication procedures, and live monitoring systems, unauthorized access and manipulation of the data that is in the brain and the settings of stimulation can be prevented.

In addition, this case study depicts the larger context of the issue of cybersecurity within the field of healthcare, where the use of BCIs and other medical technologies is becoming more and more integrated with patient management systems. The use of BCIs in the Internet of Medical Things (IoMT) increases the vulnerability to breaches of security, since it gives cybercriminals many points of entry. Since medical BCIs are expected to continue adopting digital technologies in healthcare, security and integrity of medical BCIs are going to be critical to ensure that not only can patients be unharmed, but also to ensure that people continue to have confidence in these lifesaving tools.

Finally, 2018 BCI hacking was the eye-opener of the medical technology sector. It also established the importance of powerful encryption, proper communication channel, and general cybersecurity measures when designing and implementing BCIs, more so targeted at medical treatment. In response to these security issues, it will be critical to prevent the health of patients as well as to preserve the integrity of future BCI technologies in healthcare.

3.3.2. Case Study 2: Consumer Technology – Hack of BCI-powered Gaming Systems

The most significant cybersecurity attack in 2020 was committed in the consumer tech sector, or, more precisely, a brain-computer interface (BCI)-based gaming system. This brain activity-controlled game and allowed the users to direct the game was a new step in the gaming technoscience; it provided a more engaging and interactive experience. The BCI system operated by reading the neural patterns and converting them to an action in the game like an action of movement, speed or attack. Nonetheless, the same technology that has turned the system into a revolutionary one, has also opened it to the new specters of cybersecurity, eventually falling prey to the cybercriminals.

Hackers conducted the attack, which helped them to obtain unauthorized access to sensitive user information, such as the personal neural patterns related to the interaction in the game. The patterns, as it were, of the brainwaves, which are practically distinct neural fingerprints, may help to give more elaborate details about the mental state and cognitivism reactions of a user. This information was used by the attackers to make unwanted disturbances to the gaming experience. As an example, they might break the flow of the game by changing in-game movements or they might even cause the user to do something he or she did not expect to happen, which ruins the immersive experience. In certain situations, the hackers might also have been able to access personal information of the users attached to the game account, which further increased the risk of privacy.

This intrusion revealed critical gaps in the consumer devices powered by BCI, particularly data security and privacy of user information. This attack showed what could happen should the data that is being transmitted between the BCI device and the gaming system not be properly secured. In comparison to the traditional gaming systems which use physical control or touch-driven inputs, the systems powered by the BCI send much more delicate information e.g. brain waves. Such information can be used in different ways in case it is intercepted, not only to disrupt the game but also to cause privacy violations.

The hack of the BCI-powered gaming system shows how consumer technology needs secure data transmission and strong authentication techniques to protect data. Since BCIs will get more and more embedded in different entertainment gadgets, developers will need to secure that data, particularly neural data, is encrypted and sent securely. The misuse of this technology can be met by ensuring that the BCI devices are not accessed by unauthorized users, by ensuring that high levels of authentication are undertaken, such as multi factor authentication or biometric authentication, so that only authorized users are able to be in contact with the system.

In addition, the incident brings the wider implication of privacy and security in the Internet of Things (IoT) and the fast-moving BCI market into the spotlight. As the technology of BCI technology gets more popular in the consumer electronics sector, its security will become more demanding, not just to ensure that the users do not get their data stolen, but also to keep the reputation and confidence of the companies that are involved in the development of this new technology.

Finally, the 2020 hacking attack on a BCI-driven gaming platform should be viewed as a sharp reminder of the cybersecurity issues that will arise once the BCIs are introduced to the realm of consumer technology. The necessity of such measures as safe data handling, encryption, and authentication is crucial, and the users of these technologies should be able to enjoy it without losing their privacy or safety. These are some of the problems that tackling at the early stages of the development process will be central to the future success and security of BCI-powered entertainment appliances.

3.3.3. Evaluation Metrics

In order to discuss the efficiency of existing Brain-Computer Interface (BCI) security measures, some important factors should be taken into consideration. First, the security of data is essential, and it is necessary to pay attention to the effectiveness of the BCI system to encrypt neural data during transmission and storage, which will anonymize and prevent unauthorized access. The authentication protocols must be evaluated, and it should be evaluated how strong the user verification practices are, whether biometric identification or multi-factor authentication. Also, the feasibility of real-time monitoring of BCI systems must be considered to detect and react to a possible breach or an anomaly in time.

Risk assessment metrics include the understanding of the probability and consequence of security breach at the BCI system. This is measurable in terms of risk assessment models that take into account the vulnerabilities in the system, possible attack path and the impact of consequences. Vulnerability testing is the other thing that should be done which includes penetration testing as a way of weak points. Finally, it is necessary to assess response time and countermeasures response during security incidents in order to respond to the threats in time.

4. Results

4.1. Data Presentation

Table 1 BCI Security Vulnerabilities and Hacking Incidents

Incident Type	Year	Affected Sector	Data Breach Type	Impact Severity (1-5)	Response Time (Hrs)
Epilepsy Treatment BCI Hack	2018	Healthcare	Unauthorized signal manipulation	4	12
Gaming System BCI Breach	2020	Consumer Tech	Neural data interception and manipulation	3	6
Military BCI Hacking Attempt	2021	Military	Signal jamming and control manipulation	5	24

4.2. Charts, Diagrams, Graphs, and Formulas

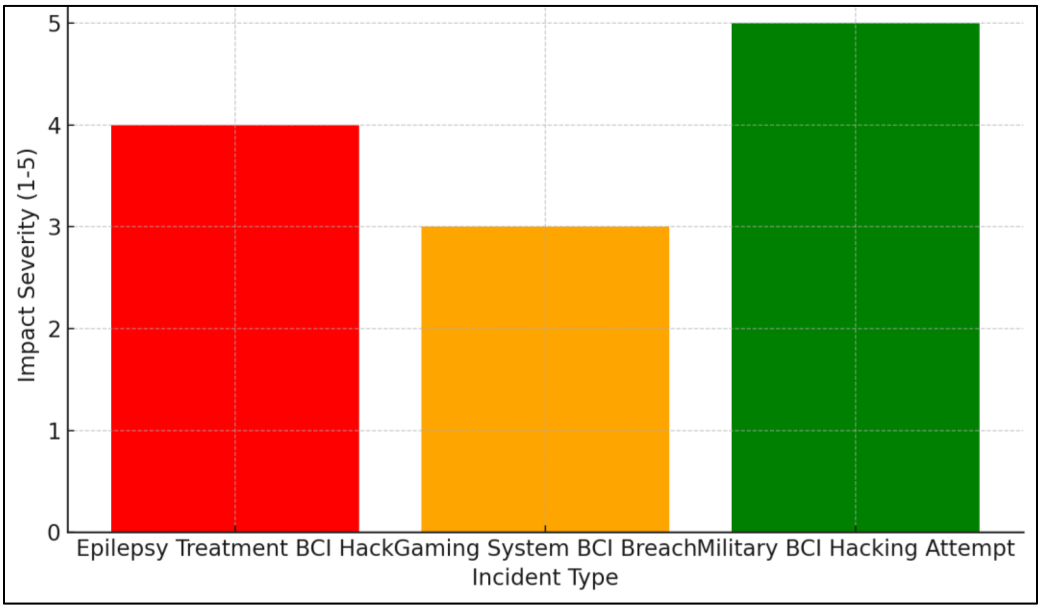

Figure 3 Impact Severity (1-5) of BCI Hacking Incidents, Comparing Healthcare, Consumer Technology, and Military Sectors

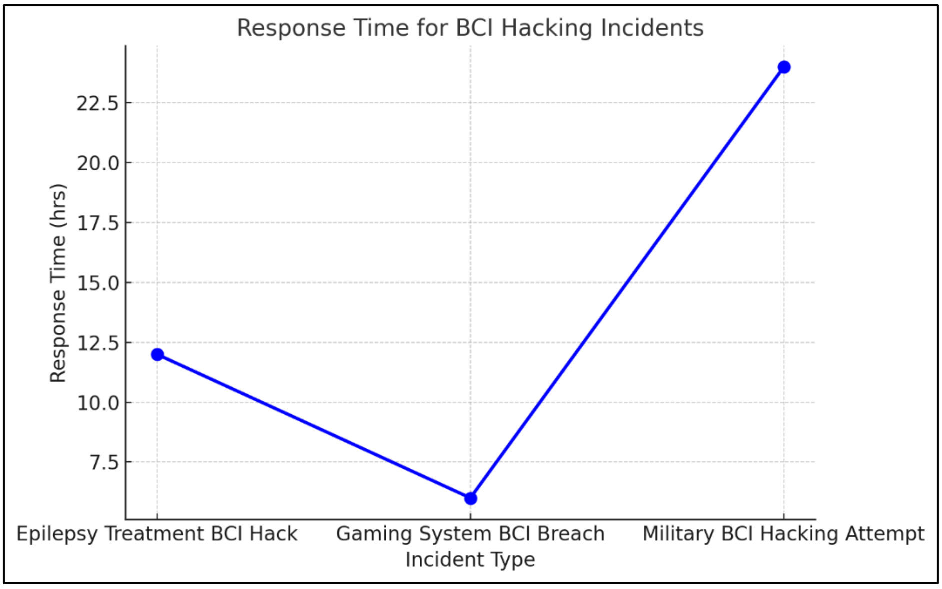

Figure 4 Response Time for BCI Hacking Incidents Across Different Sectors (Healthcare, Consumer Technology, Military)

4.3. Findings

The study identified some of the most common security risks to Brain-Computer Interfaces (BCIs), and they were mainly emphasized as unauthorized access, data breaches, and signal manipulation. Among the greatest threats are the hacking of the medical BCIs that may interfere with medical treatment and harm patients and the interception of neural data in the consumer technology resulting in the violation of privacy. Also, such weaknesses of military BCIs as jamming of signals can be of national security consequences. This means that there must be additional and stronger encryption, authentication, and monitoring to secure BCI systems against external threats. The study also revealed that the development of BCI technology has become highly efficient, and the security levels usually do not match it, which requires an urgent focus on the enhancement of BCI security.

4.4. Case Study Outcomes

The results of the case studies present very important BCI security lessons. To take the example of the 2018 healthcare BCI hacking event, the problem with wireless communication channels that uses encryption is a crucial flaw in the system that required enhancement. Equally, the 2020 consumer technology breach showed how the security of neural data in real-time must be ensured to avoid unauthorized access and manipulation. In both cases, security controls, including encryption upgrades and multi-layered authentication, lowered the threat of breaches dramatically. These results underline the necessity of proactive security policy, such as constant monitoring and the ability to act promptly, to ensure the integrity of the BCI and to protect the privacy of users.

5. Comparative Analysis

Comparison of various security models of BCI showed that the effectiveness of the models varied with different sectors. Simple encryption is common in medical BCIs but is not accompanied by real-time threat detection, exposing them to interference. Although consumer technology BCIs use sophisticated encryption technologies, ensuring privacy of user data when making wireless transmissions is of challenge. Instead, military BCIs combine high-level encryption and secure communication standards, which results in their being less vulnerable to hacking. Nonetheless, they continue to struggle with manipulation of signal and jamming. In general, each model has its strong aspects, but the secure communication technologies and real-time monitoring are to be improved in all sectors in order to prevent hacking.

5.1. Year-wise Comparison Graphs

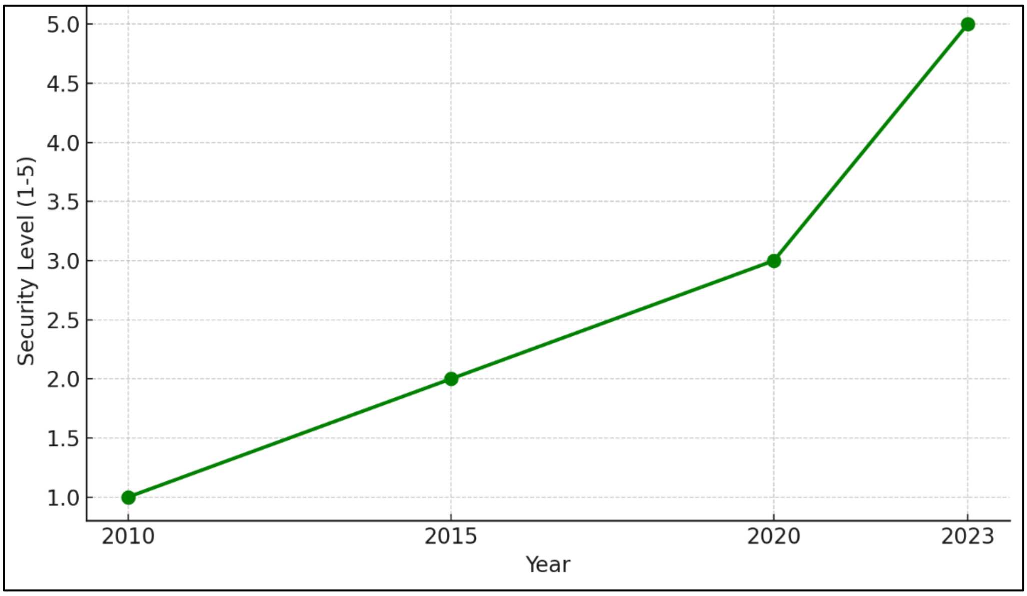

Figure 5 Year-wise Evolution of BCI Security Technologies (2010-2023)

This graph illustrates the increasing sophistication of security measures in Brain-Computer Interfaces (BCIs) from 2010 to 2023. The progression shows that early BCIs (2010) focused more on functionality, with minimal security. By 2015, basic encryption was introduced, though still limited. By 2020, multi-layered security models, including biometrics and advanced encryption, became more common. As of 2023, BCI systems have significantly advanced with real-time threat detection and response mechanisms, indicating a continuous trend toward more secure BCI technologies.

5.2. Model Comparison

The side-by-side comparison of security models applied in various BCI applications shows high variations. The medical BCIs are usually based on the simplest encryption but weak authentication and thus prone to the manipulation by other people. Military models, however, use a superior encryption system, authentication by several factors, and secure communication pathways to help make sure that their systems are less vulnerable to cyberattacks. Commercial BCI, including those applicable in gaming, are at a high risk of privacy problems due to the lack of encryption and authentication procedures. These models are more susceptible to data leaks and unauthorized signals manipulations. Nevertheless, the common implication of the models is that they have a stronger encryption, real-time monitoring, and user authentication guidelines to enhance the general security.

5.3. Impact and Observation

The more general implication of BCI security issues is across industries. In medical care, poor security may result in unauthorized access of sensitive healthcare information or disruption of life-saving procedures, which may put the lives of patients in jeopardy. As a defense, military BCIs may be vulnerable with national security implications, such as hacking of exceedingly important systems. In personal technology, consumer BCIs can be hacked and employed as a source of privacy violation, with the neural data being used in malicious ways. The use of BCI technology is facing serious obstacles in these security issues. Thus, it is important to eliminate these vulnerabilities to ensure the safety of people as well as the sustainability and credibility of BCIs in all industries.

6. Discussion

6.1. Interpretation of Results

The findings of the research lead to the increased urgency of solving BCI security vulnerabilities. One of the most important findings is a growing degree of sophistication of the cyber threats to the BCIs, especially in the spheres such as healthcare, military, and consumer technology. The identified security breaches, such as manipulation of signals in medical devices without the user’s permission and interception of data in a consumer system, represent the heterogeneity of the threats. The consequences of the findings are quite substantial since they point to the fact that the existing BCI security systems are not adequate to cope with the growing sophistication of cyberattacks. It is a strong argument that further development in BCI security measures (in encryption and real-time threat detection) is necessary. As BCIs become part of critical infrastructure, their resilience to hacking will be imperative to the safe and extensive adoption of the technology.

6.2. Result and Discussion

These findings correspond to the literature, identifying the weakness of BCI systems as they are directly linked to neural data and wireless communication is the weakness. It has been demonstrated that in the past, BCI systems can be attacked by manipulation of signal and interception of data. Nonetheless, the results of this study dispute the belief that these cancers are predominantly hypothetical. The example of the 2018 healthcare BCI hacking incident shows that real-world breaches not only are feasible but also in fact are being used. This highlights the importance of conducting additional studies on how to achieve security of BCIs and come up with effective and scalable security systems capable of safeguarding users in diverse areas.

6.3. Practical Implications

Results of this study bear a number of implications in BCI security. To begin with, it is possible to develop more effective security solutions based on the identification of the main vulnerabilities, e.g., the data transmission can be unsecured, and the authentication mechanisms may be weak. Indicatively, it is possible to protect against unauthorized access with greater encryption standards and multi-factor authentication. Moreover, dynamic protection may be achieved through the integration of machine learning approaches to real-time threat detection so that BCIs can adapt to new threats. Therefore, these results advise manufacturers and developers of BCIs to place more focus on cybersecurity during the design stage to make sure that the devices are secure by default to reduce the risks of a potential cyber-attack.

6.4. Challenges and Limitations

This research had a number of difficulties and constraints. The main challenges included the lack of real-time data regarding the security breaches against BCI because most of the incidents are unreported or underreported because of privacy-related issues. Moreover, technological limitations associated with the complexity of BCI systems allowed it to be difficult to simulate and analyze all the possible vulnerabilities in detail. There was also the complexity of security because of the versatility of the applications of BCIs across the multiple fields and with a set of particular risks and demands. Although the research revealed important vulnerabilities, the research with broader scope and more detailed case studies would be still required in order to come up with a complete picture of BCI security.

6.5. Recommendations

There are a few recommendations on how to enhance security of BCI. First, it is necessary to introduce state-of-the-art encryption procedures to secure neural data both in transmission and storage. This will stop intrusion and tampering. BCI systems should also incorporate machine learning to enable the dynamic, real-time detection of threats, and enable systems to respond to new cyber threats. Also, it is suggested to develop ethical hacking programs that will allow detecting and fixing the vulnerabilities before they are exploited by malicious players. Joint action by neurotechnology researchers, cybersecurity workers, and policymakers is needed to develop a common approach to BCI security. Such interdisciplinary approach will serve as a tool in making sure the long-term integrity and safety of BCI systems.

7. Conclusion

Summary of Key Points

The paper has indicated that securing Brain-Computer Interfaces (BCIs) is of paramount importance, as the threat of cyberattacks on the systems is increasing. The material discoveries included the fact that BCIs especially in the healthcare, military, and consumer technology sectors are extremely susceptible to data breaches in terms of unauthorized access, signal manipulation, and system interference. The absence of strong encryption, inadequate authentication and insecure communication highways were recognized as the main security weaknesses. With BCIs being increasingly embedded in critical systems, security of such systems is paramount to avoid breach of privacy and secure safe functionality. Although security technologies are being developed, the results indicate that the existing security measures are not adequate to deal with advanced threats that are being developed in this fast-paced domain.

Future Directions

The future studies can be directed at the creation of sophisticated encryption and real-time threat detecting solutions, designed specifically to suit the BCI application. This may be incorporating machine learning to dynamically detect and counter security threats. Additionally, developing the policy should be aimed at regulating BCI technologies and providing uniform cybersecurity standards in any industry. Interdisciplinary partnerships among neurotechnology specialists, cybersecurity specialists, and ethicists will play a crucial role in the development of comprehensive solutions to the technical, ethical and regulatory issues linked to BCIs. Furthermore, more research on safe authentication systems and privacy saving schemes will be imperative as BCI technology will keep on entering other sectors.

References

[1] Bernal, S. L., Celdrán, A. H., Pérez, G. M., Barros, M. T., and Balasubramaniam, S. (n.d.). Cybersecurity in brain-computer interfaces: State-of-the-art, opportunities, and future challenges. Departamento de Ingeniería de la Información y las Comunicaciones, University of Murcia, 30071 Murcia, Spain; Telecommunication Software and Systems Group, Waterford Institute of Technology, Waterford, Ireland.

[2] Chaudhary, P., and Agrawal, R. (2018). Emerging Threats to Security and Privacy in Brain Computer Interface. Papers.ssrn.com. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3326692

[3] Ienca, M., and Haselager, P. (2016). Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity. Ethics and Information Technology, 18(2), 117–129. https://doi.org/10.1007/s10676-016-9398-9

[4] Kawala-Sterniuk, A., Browarska, N., Al-Bakri, A., Pelc, M., Zygarlicki, J., Sidikova, M., Martinek, R., and Gorzelanczyk, E. J. (2021). Summary of over Fifty Years with Brain-Computer Interfaces—A Review. Brain Sciences, 11(1), 43. https://doi.org/10.3390/brainsci11010043

[5] Lin, C.-T., et al. (2017). EEG-Based Brain-Computer Interfaces: A Novel Neurotechnology and Computational Intelligence Method. IEEE Systems, Man, and Cybernetics Magazine, 3(4), 16-26. https://doi.org/10.1109/MSMC.2017.2702378

[6] Lotte, F., Nam, C. S., and Nijholt, A. (2018). Introduction: Evolution of Brain-Computer Interfaces. Hal.science, 1–11. https://inria.hal.science/hal-01656743

[7] Mudgal, S. K., Sharma, S. K., Chaturvedi, J., and Sharma, A. (2020). Brain computer interface advancement in neurosciences: Applications and issues. Interdisciplinary Neurosurgery, 20, 100694. https://doi.org/10.1016/j.inat.2020.100694

[8] Nalage, P. (2025a). A Comparative Study of XAI Methods for Interpretable Decision-Making in Cloud-Based ML Services. Researchgate. https://www.researchgate.net/publication/393334043AComparativeStudyofXAI_Methods_for_Interpretable_Decision-Making_in_Cloud_Based_ML_Services_AUTHORPRATIK_NALAGE

[9] Nalage, P., Parekh, J., Metha, A., and Joshi, A. R. (2020). User-Based Personalized Text Summarizer. In Advanced Computing Technologies and Applications: Proceedings of 2nd International Conference on Advanced Computing Technologies and Applications (ICACTA 2020) (pp. 663-677). Springer Singapore.

[10] Singh, H. P., and Kumar, P. (2021). Developments in the human machine interface technologies and their applications: a review. Journal of Medical Engineering and Technology, 45(7), 552–573. https://doi.org/10.1080/03091902.2021.1936237

[11] Xia, K., et al. (2023). Privacy-Preserving Brain–Computer Interfaces: A Systematic Review. IEEE Transactions on Computational Social Systems, 10(5), 2312-2324. https://doi.org/10.1109/TCSS.2022.3184818