SCIENTIFIC Publishing Limited

Digital Technologies Research and Applications
http://ojs.ukscip.com/index.php/dtra

Review

Cybersecurity Issues in Brain-Computer Interfaces: Analysis of Existing Bluetooth Vulnerabilities

Dimitris Angelakis [*]**, Errikos Ventouras, Spyros Kostopoulos and Pantelis Asvestas**

Department of Biomedical Engineering, University of West Attica, Athens 12243, Greece
[*] Correspondence: dangelakis@uniwa.gr

Received: 31 May 2024; **Revised:** 28 June 2024; **Accepted**: 9 July 2024; **Published**: 10 July 2024

Abstract: Brain-computer interfaces (BCIs) hold immense promise for human benefits, enabling communication between the brain and computer-controlled devices. Despite their potential, BCIs face significant cybersecurity risks, particularly from Bluetooth vulnerabilities. This study investigates Bluetooth vulnerabilities in BCIs, analysing potential risks and proposing mitigation measures. Various Bluetooth attacks such as Bluebugging, Bluejacking, Bluesnarfing, BlueBorne, Location Tracking, Man-in-the-Middle Attack, KNOB, BLESA and Reflection Attack are explored, along with their potential consequences on commercial BCI systems. Each attack is examined in terms of its modus operandi and effective mitigation strategies.

Keywords: Brain-Computer Interfaces; Cybersecurity; Bluetooth

1. Introduction

A Brain-Computer Interface (BCI) is a system designed to measure and transform the activity of the central nervous system (CNS) into artificial output. This technology plays a pivotal role in replacing, restoring, supplementing, or enhancing natural CNS output. It fundamentally alters ongoing CNS interactions with both external and internal environments [1]. BCIs have had a significant impact on the medical field, providing revolutionary solutions for patients with neurological disorders or serious physical disabilities. BCIs have the potential to enable paralyzed patients to operate robotic prosthetics, as well as to aid communication in locked-in syndrome situations, thus restoring independence and enhancing the quality of life for a broad spectrum of patients. The integration of medical science and technological innovation in BCIs creates unprecedented opportunities for therapeutic interventions and neurological rehabilitation. In addition to medical applications, BCIs are crucial in the field of neuroprosthetics. By directly connecting the brain with external devices, people with amputations or paralysis are empowered to regain motor control. This enables them to manipulate prosthetic limbs and interact with the environment. The fusion of neurological science and engineering acumen not only improves physical capabilities but also alters social attitudes towards ability and disability. Additionally, BCIs hold great promise for the richly immersive experiences that come with augmented and virtual reality technologies. Because BCIs tap neural signals directly, they can create intuitive interactions within virtual environments without interruption. This combination of neurotechnology and AR/VR widens the scope of entertainment, education and simulation, providing users with experiences that challenge the boundaries between the physical and the virtual [2,3]. Despite the benefits of BCIs, the technology was not widely adopted in healthcare when it was initially introduced. One of the primary restrictions of BCIs was that the signals received by the brain were susceptible to interference. In addition, legal and ethical issues such as the risk of infection or damage caused when a patient's intent to control an external device fails, and the safeguarding and confidentiality of patient data were some of the challenges BCI encountered in healthcare[4]. However, the

https://doi.org/10.54963/dtra.v3i2.286

challenges impeding the integration of BCIs in healthcare have received limited attention thus far. This lack of focus can be attributed to several factors, including advancements in assessing the requirements of individuals with disabilities, the accessibility of robust computer tools capable of translating BCI research findings into practical applications, and the development of more effective techniques for collecting and interpreting brain signal data. Furthermore, a deeper understanding of how BCI research could positively impact the broader population has contributed to the minimal exploration of these challenges [4].

The use of the BCI communication link benefits from the technology in many ways, which include the working capacity of human peripheral nervous system through substitution or strengthening, which in turn provide some degree of freedom. Neuromedical benefits such as neuronal rehabilitation, improving user authentication, promoting affective computing, revolutionizing gaming and entertainment, robotics, smartphone -based applications, artificial intelligence and much more [5]. The widespread use of BCIs has garnered immense interest among researchers. This popularity stems from the potential to enhance our understanding of how these interfaces can improve interactions between users and various systems. Researchers are particularly focused on expanding BCIs' applications to facilitate a deeper connection between humans and technology.

Despite many promises of BCI research, there are also risks associated with its use. The developing industry primarily focuses on the benefits and multiple applications of BCI, while largely ignoring the cybersecurity issues related to BCI algorithms and devices. As numerous security breaches have occurred in the past, cybersecurity professionals have begun to address the issues pertaining to BCI security. These attacks or breaches can take many forms, with user brain patterns serving as a prime target for adversaries and threat actors. In terms of security, BCIs are still in an early and immature stage. Only recently, the literature has emphasized the significance of security as an essential aspect of BCI, resulting in the emergence of new fields such as neuro-security (which refers to the protection of the security and integrity of neural data, brain signals, and devices that interact with the brain), neuro-privacy (which involves safeguarding the privacy of an individual's neural information, thoughts, and cognitive processes from unauthorized access or misuse.), neuro-confidentiality (which is related to keeping neural information confidential, ensuring that sensitive brain data is not disclosed or accessed without proper authorization), brain hacking (which involves exploiting vulnerabilities in neurotechnological devices or systems to gain unauthorized access to neural data, control devices, or manipulate cognitive functions), and neuro-ethics (which involves the ethical considerations and principles related to neuroscience, neurotechnology, and the use of BCIs) [6].

The primary objectives of this paper are threefold: first, to conduct a systematic and extensive analysis of existing literature, providing a comprehensive overview of the current state of cybersecurity in BCIs; second, to elucidate the prospects for fortifying the security of BCIs, exploring cutting-edge technologies and strategies; and third, to scrutinize the vulnerabilities introduced by the integration of Bluetooth technology, offering insights and recommendations for mitigating associated risks.

The landscape of Brain-Computer Interfaces (BCIs) has witnessed a transformative evolution, marked notably by the surging prevalence of Bluetooth integration. The integration of Bluetooth technology into BCIs holds pivotal implications for the seamless communication between the user's brain and external devices or systems. This integration facilitates enhanced user experience, real-time data transmission, and expanded functionalities.

In recent years, the proliferation of Bluetooth-enabled BCIs has become increasingly pronounced, reflecting a paradigm shift in the field. The inherent advantages of Bluetooth, such as wireless connectivity, low energy consumption, and broad device compatibility, have driven its adoption as a preferred communication protocol in BCI systems. This shift is pivotal in enabling diverse applications, ranging from medical interventions to assistive technologies and entertainment.

While the advantages of Bluetooth integration are evident, it is imperative to acknowledge the vulnerabilities associated with this technology within the context of BCIs. These vulnerabilities pose potential threats to the confidentiality, integrity, and availability of neural data, necessitating a comprehensive exploration of security challenges and potential mitigations.

The integration of Bluetooth technology into BCIs stands as a defining feature of contemporary neurotechnology. Acknowledging its prevalence sets the stage for a nuanced exploration of security concerns, thereby enriching the discourse on safeguarding the integrity and privacy of neural data in Bluetooth-enabled BCIs.

By weaving together findings from the literature review, technological prospects, and Bluetooth vulnerabilities, the paper aspires to offer readers a cohesive narrative that facilitates a nuanced comprehension of the challenges and opportunities in this rapidly evolving field.

Bluetooth integration is increasingly prevalent in BCI systems, and scrutinizing its specific vulnerabilities provides practical insights that are crucial for developers, researchers, and policymakers. This research adopts a multifaceted approach, incorporating an introduction that establishes the ubiquity of Bluetooth technology and the concurrent rise in security risks, particularly in workplace environments. The subsequent sections delve into the specifics of Bluetooth security threats, encompassing various wireless and networking attacks. Then transitions to a discussion on Bluetooth attacks, providing detailed insights into Bluebugging, Bluejacking, Bluesnarfing, BlueBorne, location tracking, Man-in-the-Middle Attack, KNOB, BLESA and Reflection Attack . Each attack is elucidated with a description, its impact on Brain-Computer Interface systems, and mitigation strategies.

1.1. The History of Bluetooth Integration in Brain-Computer Interfaces

Historically, the development of Brain-Computer Interfaces (BCIs) to utilize Bluetooth technology is a relatively recent advancement. BCIs have been under development since the mid-20th century[7], initially focusing on wired connections for data transmission due to technological limitations. However, the integration of Bluetooth into BCIs began to gain traction in the early 21st century, driven by advancements in wireless communication and the miniaturization of electronic components .Here's a brief historical overview.

Early Development (20th Century): The concept of BCIs dates to the 1970s, with early research focusing on invasive techniques such as implantable electrodes to record brain activity. These early BCIs relied on wired connections to transmit neural signals between the brain and external devices for control or feedback purposes.

Advancements in Wireless Technology (Late 20th Century): Throughout the late 20th century, there were significant advancements in wireless communication technology, paving the way for the development of wireless BCIs. However, Bluetooth technology had not yet been widely adopted for consumer electronics or medical devices during this period.

Introduction of Bluetooth (Early 21st Century): Bluetooth technology was officially introduced in the mid-1990s, initially aimed at simplifying data exchange between mobile devices and peripherals. As Bluetooth technology became more prevalent and standardized, researchers began exploring its potential applications in BCIs for wireless data transmission [8].

Integration of Bluetooth into BCIs (Mid-2000s): By the mid-2000s, researchers started integrating Bluetooth modules into BCI prototypes, enabling wireless communication between the BCI device and external systems or devices. This integration offered benefits such as enhanced mobility, flexibility, and user comfort.

Commercialization and Adoption (Late 2000s to Present): As Bluetooth-enabled BCIs demonstrated feasibility and utility in research settings, efforts were made to commercialize and refine these devices for broader applications. Today, Bluetooth-enabled BCIs are available commercially and used in various fields, including healthcare, assistive technology, gaming, and neurofeedback.

Overall, the historical development of BCIs to use Bluetooth technology reflects the evolution of both neurotechnology and wireless communication. The integration of Bluetooth has played a significant role in advancing BCIs, making them more accessible, user-friendly, and versatile for a wide range of applications.

1.2. Bluetooth Architecture in Brain-Computer Interfaces

The integration of Bluetooth technology into BCI devices facilitates wireless communication between the BCI device and external devices, such as computers, smartphones, or tablets. This integration enables real-time or near real-time data transmission and control without the constraints of wired connections, thereby providing greater mobility, flexibility, and user comfort.

At the core of the Bluetooth architecture in a BCI device is the Bluetooth module. This module is responsible for establishing, maintaining, and terminating the wireless communication link between the BCI device and the master device, which is typically a computer, smartphone, or tablet. The BCI device is configured as a slave device, while the master device assumes the role of the controlling entity in the Bluetooth communication link. The master device initiates the Bluetooth connection with the BCI device, controls the data transmission process, and manages the overall communication protocol.

The data transmission in a Bluetooth-enabled BCI device involves several stages. First, the BCI device collects and processes brain signals, such as Electroencephalogram (EEG) or Electromyogram (EMG) signals, from the user. The processed data is then formatted and encapsulated for transmission. Bluetooth profiles, such as the Serial Port Profile (SPP) or the Bluetooth Low Energy (BLE) Generic Attribute Profile (GATT), are utilized to establish and manage the Bluetooth connection and data transmission between the BCI device and the master device. These profiles define the communication protocols, data formats, and transmission rates, ensuring efficient and reliable data transfer.

Security is a critical aspect of the Bluetooth architecture in BCI devices. To ensure secure and private communication between the BCI device and the master device, Bluetooth security features are implemented. The pairing process is used to establish a trusted relationship between the devices, and encryption and authentication mechanisms are employed to protect the transmitted data from eavesdropping and tampering.

A user-friendly interface is provided on the master device, such as a computer application or mobile app, to allow the user to interact with the BCI device, control its settings, and visualize the brain signals in real-time. This interface facilitates the monitoring of the user's brain activity, adjustment of the BCI device's parameters, and interpretation of the received data.

Bluetooth-enabled BCI devices are utilized in various applications, including neurofeedback training, assistive technology for people with disabilities, research, and brain-computer interface gaming. The wireless connectivity offered by Bluetooth technology enhances the flexibility, mobility, and user experience of the BCI device, making it more accessible and user-friendly.

The Bluetooth architecture in BCI devices involves the integration of a Bluetooth module into the BCI device to enable wireless communication with external devices, such as computers or smartphones. This wireless connectivity facilitates real-time or near real-time data transmission, control, and user interaction, enhancing the flexibility, mobility, and user experience of the BCI device. The implementation of Bluetooth profiles, security features, and a user-friendly interface ensures efficient, secure, and user-friendly operation of the Bluetooth-enabled BCI device [9,10].

1.3. Bluetooth Protocol Stack

Bluetooth Protocol Stack is a hierarchical structure composed of various protocols and profiles that define the functionalities and capabilities of Bluetooth communication. It is divided into three main layers: the Controller/Physical Layer, Link Layer, and Protocol Stack. The Controller/Physical Layer is responsible for the physical transmission and reception of Bluetooth signals. This layer includes the Bluetooth Radio, which handles the modulation and demodulation of the radio signals, and the Baseband, which manages the physical link establishment, data packet formation, and error control. The Link Layer provides the core Bluetooth functionalities and includes the Logical Link Control and Adaptation Protocol (L2CAP), Radio Frequency Communication (RFCOMM), and Generic Attribute Profile (GATT). L2CAP provides multiplexing of data between different higher-layer protocols and features segmentation and reassembly, Quality of Service (QoS) management, and support for multicast and broadcast data transmission. RFCOMM emulates serial port communication over Bluetooth and features data framing, flow control to manage data flow and prevent buffer overflow and port emulation to allow legacy serial port applications to communicate over Bluetooth. GATT defines the structure and functionality of the data exchanged between Bluetooth devices and features attribute-based data access, a client-server architecture for data exchange between devices, and profile configuration for customization and configuration of Bluetooth profiles for specific applications.

The Protocol Stack layer encompasses the higher-layer protocols responsible for the communication and interaction between Bluetooth devices. It includes the Service Discovery Protocol (SDP) for allowing Bluetooth devices to discover and advertise available services, Telephony Control Protocol (TCS) for facilitating telephony-related control functions in Bluetooth devices, Object Exchange (OBEX) for supporting the exchange of objects such as files and contacts between Bluetooth devices, Audio/Video Control Transport Protocol (AVCTP) for managing the control functions for audio and video streaming over Bluetooth, and Audio/Video Distribution Transport Protocol (AVDTP) for handling the transmission and reception of audio and video data over Bluetooth.

The Bluetooth Protocol Stack is a comprehensive architecture that encompasses the Controller/Physical Layer, Link Layer, and Protocol Stack to facilitate efficient and reliable communication between Bluetooth devices. The Logical Link Control and Adaptation Protocol (L2CAP), Radio Frequency Communication (RFCOMM), and Generic Attribute Profile (GATT) are essential components of the Link Layer, providing multiplexing, data framing, and attribute-based data access functionalities, respectively, to ensure seamless data transmission and interaction between Bluetooth devices [11].

Figure 1 diagram depicts the various components involved in the Bluetooth communication link. The Master Device, which can be a computer, smartphone, or tablet, serves as the controlling entity in this communication setup. The Bluetooth Application is the software application on the master device responsible for interfacing with the user and controlling the BCI device. The Bluetooth Stack encompasses the Bluetooth protocol stack, which includes profiles such as Logical Link Control and Adaptation Protocol (L2CAP), Radio Frequency Communication (RFCOMM), or Generic Attribute Profile (GATT). The HCI and LMP (Host Control Interface and Link Manager Protocol) serves as the interface between the Bluetooth stack and the Bluetooth radio and baseband. The Bluetooth Radio & Baseband is the component responsible for the actual wireless communication. The BCI Device refers to the Brain-Computer Interface device, and the Bluetooth Module (Slave) is the integrated Bluetooth module in the BCI device facilitating wireless communication with the master device. Lastly, the BCI Processing Unit processes the brain signals collected by the EEG signal sensors, which are the sensors that collect brain signals from the user.

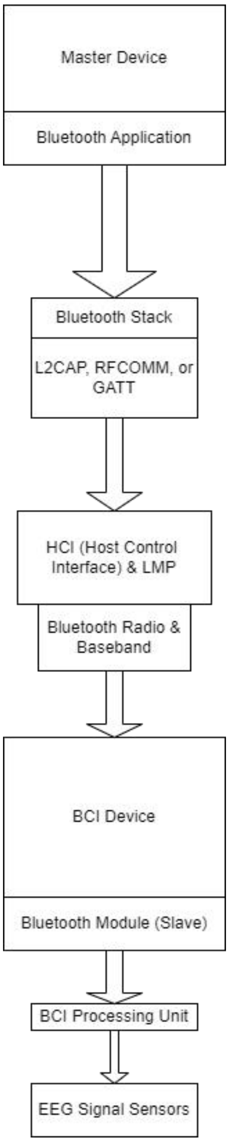

Figure 1. Bluetooth architecture in BCI devices diagram.

1.4. Understanding Brain-Computer Interfaces from a Cybersecurity Perspective

BCI is a technique designed to convert users' brain signals into control signals or commands. An important aspect of BCI research is the mutual adjustment of brain-BCI system interaction to find appropriate signal processing and conversion algorithms. These algorithms transform electrical neural signals into control or operational signals that computers can detect quickly and accurately in real-time.

Interfaces between the brain and computer were developed in the 1970s to investigate and process brain activity, and to convert brain processes for machinery and devices. After decades of research, BCI research has made it possible to record and stimulate brain activity. This implies that BCI research covers two main areas: recording neural activity and stimulating it [12]. Neural activity is acquired and recorded through the communication of neurons with one another. The neurons generate signals which are recorded by the BCI and converted into digital data. The BCI then analyses the data to direct the intended action of the machine connected to it.

To stimulate brain activity, the BCI functions in such a way that, when the intended action is determined by the data coming from the neural activity, it generates a more intense pattern of neural activity, which is ultimately transferred to the brain to trigger neurons [12]. This means that the BCI operates either unidirectionally, from the brain to external devices, or bidirectionally between them (Figure 2).

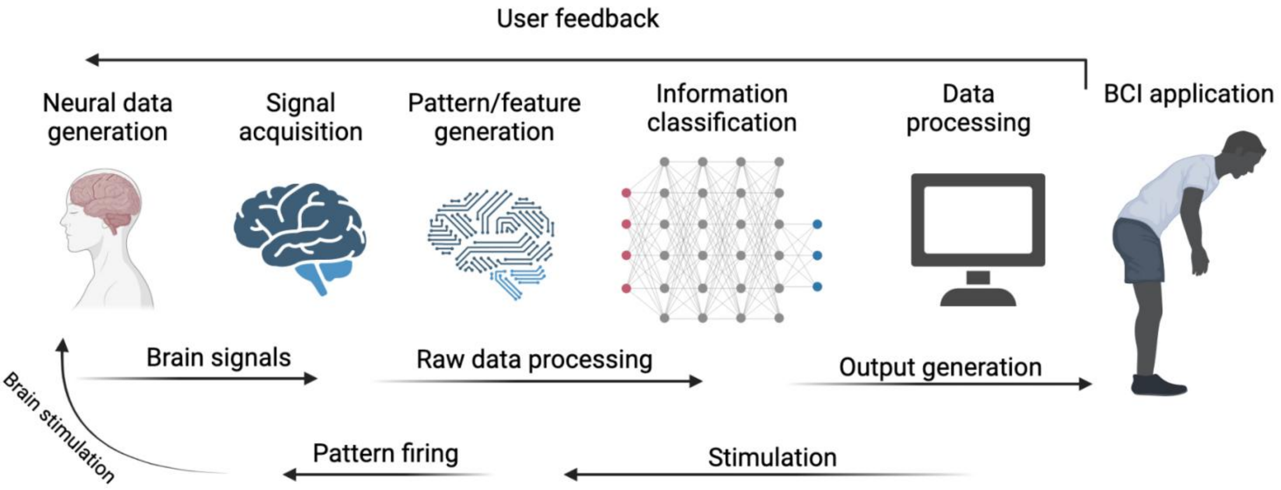

Figure 2. The unidirectionality and bidirectionality of brain-computer interfaces.

By inspecting Figure 2 and considering the above discussion, it is possible to identify points where the implementation of security measures is crucial to address potential system vulnerabilities. Data breaches may occur at various stages, including data generation, processing, and interference at the application system level, which can compromise the devices' security.

1.5. Challenges Faced at the Forefront of BCI Research

Significant research has been conducted on BCIs over the last few years, leading to novel assistive technologies with potential applications. At its current state of development, BCI technology might produce a large-scale market breakthrough in the near future. However, some key challenges exist in each component of the BCI scheme that should be addressed to make further progress in this field. These challenges can be broadly classified into two categories: psychophysiological/neurological challenges and technological challenges [13]. Both categories encompass challenges and issues with the modalities and headsets used in BCI applications such as electroencephalogram (EEG) modalities. Challenges include a lack of ideal data analysis methods, difficulties in performance evaluation and comparison metrics, the low information transfer rate of BCI systems, and discrepancies between in vitro and in vivo modelling of BCI, amongst others [14]. However, these issues can be addressed, and ongoing efforts are made to reduce the gaps brought about by these challenges. Additionally, another crucial challenge faced by BCI is cybersecurity breaches. Network security is a vital determinant of the effectiveness of BCI applications [15]. Research indicates that information can be captured, read, and manipulated using readily available essential hardware tools. Moreover, different attacks can occur in BCI's vulnerable modules, disrupting BCI's intended purpose and corrupting it.

1.6. List of the Current Consumer Market BCI Devices

Consumer-level wireless BCI systems are available from various commercial companies, including Emotiv, Neurosky, MyndPlay, PLX Devices, and OpenBCI Technologies. These companies offer their own wireless BCI devices as well as various gaming, utility, and mental state monitoring applications. Wireless BCI devices for consumers will be examined in this section.

Presented below is a list of the most frequently utilized BCI systems designed for consumer use:

(a) EPOC headset by Emotiv [16];

(b) MindSet by NeuroSky [17];

(c) MyndBand headset by MyndPlay [18];

(d) Xwave headset by PLX devices [19];

(e) Ultracortex Mark IV OpenBci [20].

Emotiv markets the EPOC headset, a wireless BCI system with multiple. The headgear has 14 saline-based, wet-contact resistance electrodes to monitor the EEG, the electrooculogram (EOG), and the face electromyogram (EMG). Moreover, the EPOC headset has a two-axis gyroscope for the purpose of sensing head rotation. This technology utilizes 2.4 GHz wireless networking and is compatible with PCs, laptops, and smartphones. The EPOC headset software suite includes built-in signal processing algorithms for processing EEG data. The built-in algorithms determine the user's conscious goals, emotional states, and facial expressions using EEG, EMG, and EOG data. The device is suitable for brain state monitoring, game control, and virtual reality.

Neurosky's MindSet is a device for collecting EEG signals. It contains earbuds, a microphone, and a single electrode for monitoring EEG on the user's head. Additionally, the device features a unique technology called eSense, which enables EEG recording. The algorithm employed assesses the mental states of the user, such as concentration and meditation, by measuring the power level of the EEG signals in specified frequency bands, including theta rhythms. Brain state monitoring is utilized to generate control directives.

The MyndBand, developed by MyndPlay, and the XWave, developed by XWave Devices, comprise a BCI system integrated into their headsets. Specifically, the XWave headset features the ThinkGear ASIC module, a system-on-a-chip integrated circuit designed by Neurosky, which includes sensors for signal collection [21]. These devices come in two varieties: a headset and a harness. Numerous PC and mobile applications, including media players, cognitive state visualizations, and arcade games, can be controlled through these devices.

OpenBCI develops open-source tools for biosensing and neuroscience. The Galea hardware and software platform incorporates EEG, EMG, electrodermal activity (EDA), photoplethysmography (PPG), and eye-tracking, all in one headset. The Ultracortex, an open-source, 3D-printable headset, is designed to function with the OpenBCI system, recording research-grade EEG data. The Ultracortex is available in either an 8 or 16-channel configuration, depending on which Arduino-compatible neural interface is used. Typically, utilizing more electrodes will distribute the pressure on the scalp downwards, resulting in greater user comfort [22].

2. Search Strategy

The search strategy aimed to systematically identify relevant literature concerning cybersecurity challenges related to Bluetooth vulnerabilities and BCIs. The objective was to comprehensively review existing research, identifying gaps and synthesizing knowledge on the intersection of cybersecurity and neurotechnology. The studies included specifically addressed cybersecurity issues related to BCIs. Both medical and non-medical applications of BCIs were examined.

The search terms were carefully selected to cover key concepts related to cybersecurity, BCIs, and potential vulnerabilities associated with BCIs. The terms included variations and synonyms to capture a broad range of relevant literature. Example terms include:

- "cybersecurity" OR "information security " OR "computer security" OR "cyber threats";
- "Brain-computer interface" OR "BCI" OR "neurotechnology" OR "neural interface";
- "Bluetooth security" OR "Bluetooth vulnerabilities" OR "Bluetooth attacks" OR "Bluetooth risks".

The search strategy combined the identified terms using Boolean operators (AND, OR) to ensure a comprehensive and focused approach to identifying relevant literature. An example search string is as follows: ("cybersecurity" OR "information security" OR "computer security" OR "cyber threats") AND ("brain-computer interface" OR "BCI" OR "neurotechnology" OR "neural interface") AND ("Bluetooth security" OR "Bluetooth vulnerabilities" OR "Bluetooth attacks" OR "Bluetooth risks").

The search was conducted in key databases, including PubMed, IEEE Xplore, Scopus, and others, to ensure coverage across various disciplines and publication sources. Publications after 2010 were considered, allowing for the inclusion of studies to capture the evolution of cybersecurity challenges in BCIs. The search was conducted in English, but efforts were made to consider relevant studies in other languages if translation resources were available. Grey literature, such as conference proceedings, theses, and reports, was considered to capture additional insights beyond peer-reviewed journals. Unpublished studies were included if relevant and accessible. The search was executed in 2024, and additional manual searches of reference lists from key articles were performed to identify potentially missed relevant studies.

Table 1 presents the criteria for inclusion or exclusion of articles in the present review study.

Figure 3 presents the block diagram of the review approach.

Table 1. Inclusion and exclusion criteria of bibliography.

Criterion	Inclusion	Exclusion
Publication type	Peer-reviewed articles published in academic journals.	Non-peer-reviewed articles, conference abstracts, editorials, letters, and opinion pieces.
Topic	Studies focused on cybersecurity issues specifically related to brain-computer interfaces and Bluetooth vulnerabilities.	Studies not directly addressing cybersecurity issues in brain-computer interfaces.
Publication time frame	Studies published after 2010.	Studies published before 2010.
Study design	Any type of study design, including experimental studies, case studies, reviews, and surveys, as long as they provide relevant insights into cybersecurity concerns in BCIs and Bluetooth vulnerabilities.	Studies lacking clear methodological rigor or relevance to cybersecurity concerns in BCIs.
Cybersecurity aspects	Studies addressing various aspects of cybersecurity, such as data privacy, authentication, encryption, secure communication protocols, and protection against malicious attacks in the context of BCIs and Bluetooth vulnerabilities.	Studies not providing substantial information on cybersecurity concerns or solutions in the context of BCIs.
Language	Articles published in English.	Articles not published in English.
	Studies included: 42.	Studies excluded: 47.

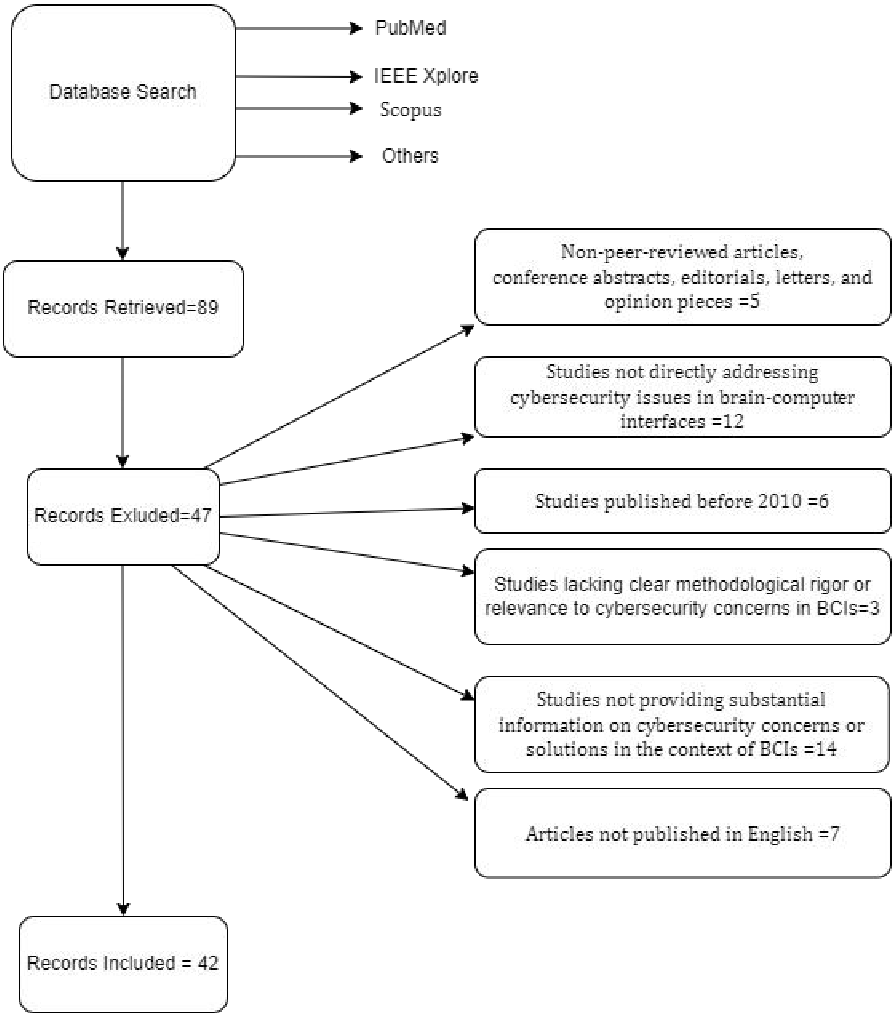
Database Search
PubMed
IEEE Xplore
Scopus
Others
Records Retrieved=89
Records Exluded=47
Non-peer-reviewed articles, conference abstracts, editorials, letters, and opinion pieces =5
Studies not directly addressing cybersecurity issues in brain-computer interfaces =12
Studies published before 2010 =6
Studies lacking clear methodological rigor or relevance to cybersecurity concerns in BCIs=3
Studies not providing substantial information on cybersecurity concerns or solutions in the context of BCIs =14
Articles not published in English =7
Records Included = 42

Figure 3. Review approach block diagram.

2.1. Previous Work

The research on BCI security and privacy has progressed significantly over the years. Table 2 presents a chronological summary of key studies on BCI privacy and security, highlighting the evolution of research in this field. Takabi et al. (2016) explored privacy threats in BCI applications, highlighting concerns such as unauthorized access to sensitive brain data. They proposed various countermeasures, including anonymization techniques, robust access control mechanisms, and encryption to safeguard the data [23]. Wahlstrom et al. (2016) focused on privacy disruptions across different BCI systems, identifying key issues like confidentiality attacks where sensitive information could be leaked, and data availability challenges that might hinder the reliable functioning of BCIs [24]. In the same year, Takabi (2016) proposed a firewall specifically designed for BCIs to create a privacy-preserving ecosystem, emphasizing the importance of secure multiparty computation and encryption to protect users' brain data [25]. Pycroft et al. (2016) introduced the concept of brainjacking, which addresses the security vulnerabilities in BCI implants. They discussed how these implants could be hacked to manipulate neurological functions, posing significant risks to users' mental and physical health [26]. Ienca et al. (2018) analyzed privacy issues related to consumer neurotechnology, examining the impact of GDPR on neurodata protection. They offered policy recommendations to enhance user privacy and ensure that consumer neurotechnology adheres to stringent data protection regulations [27].

Landau et al. (2020) investigated security issues specific to EEG-based BCIs, focusing on risks like EEG signal manipulation and the security of brain signal acquisition and stimulation processes. Their study highlighted the potential for malicious entities to interfere with EEG signals, which could lead to serious security breaches [28]. Belkacem (2020) presented a cybersecurity framework for P300-based BCIs, concentrating on securing P300 Evoked Potentials. They conducted various attack simulations and proposed countermeasures to enhance the security of these systems against potential cyber threats [29]. Bernal et al. (2021) provided a comprehensive review of the state-of-the-art in BCI security. They addressed key security concerns such as confidentiality, integrity, and availability, and discussed challenges and opportunities for improving BCI lifecycle security [30]. In 2022, Bernal et al. examined the impact of neuronal jamming cyberattacks on invasive BCIs, focusing on how such attacks could affect the spike rate and the performance of tasks requiring visual capabilities in both artificial and biological environments [31]. Lahtinen and Costin (2023) provided an overview of cybersecurity threats in BCIs, exploring potential solutions to mitigate these threats. They discussed various technical and procedural strategies to enhance the security of BCI systems [32]. Jiang et al. (2023) surveyed existing cybersecurity risks in neural interfaces, discussing issues across central and peripheral nervous systems, different neural modalities, and data permission and model levels. They identified future trends and research directions in neural interface cybersecurity [33]. Thomopoulos et al. (2024) conducted a systematic review of phishing cyberattacks using EEG and eye-tracking methods. They highlighted experimental research on phishing and outlined the challenges in protecting against such attacks using these novel methods [34].

Table 2. Summary of key studies on BCI privacy and security.

Study	Year	Title	Focus	Key Point
Takabi et al.	2016	Brain Computer Interface (BCI) Applications: Privacy Threats and Countermeasures	Privacy threats and countermeasures in BCI applications	Discusses privacy threats in BCI applications, such as unauthorized access to brain data. Explores anonymization, access control, encryption, and BCI app stores.
Wahlstrom et al.	2016	Privacy and Brain-Computer Interfaces: Identifying Potential Privacy Disruptions	Privacy disruptions in BCI systems	Identifies privacy issues across different BCI types, confidentiality attacks, and data availability concerns.
Takabi	2016	Firewall for Brain: Towards a Privacy Preserving Ecosystem for BCI Applications	Privacy preserving ecosystem for BCI applications	Proposes a firewall for BCI privacy, emphasizing secure multiparty computation and encryption.
Pycroft et al.	2016	Brainjacking: Implant Security Issues in Invasive Neuromodulation	Implant security issues in neuromodulation	Explores brainjacking, security vulnerabilities in BCI implants, and hacking communication protocols.
Ienca et al.	2018	Brain Leaks and Consumer Neurotechnology	Neurotechnology privacy, GDPR impact, policy recommendations	Analyzes privacy issues in consumer neurotechnology, GDPR's impact, and policy recommendations for enhanced privacy and security.
Landau et al.	2020	Mind Your Mind: EEG-Based Brain-Computer Interfaces and Their Security in Cyber Space	EEG-based BCI security	Investigates EEG-based BCI security issues, including EEG signal manipulation and brain signal acquisition and stimulation security.
Belkacem	2020	Cybersecurity Framework for P300-Based Brain Computer Interface	Development of a cybersecurity framework for P300-based BCI	Presents a cybersecurity framework for P300-based BCIs, focusing on P300 evoked potential security, attack simulations, and countermeasures.
Bernal et al.	2021	Security in Brain-Computer Interfaces: State-of-the-Art, Opportunities, and Future Challenges	Comprehensive review of Security in BCIs	Reviews BCI security, addressing confidentiality, integrity, availability, and lifecycle security challenges and opportunities.

Table 2. *Cont.*

Study	Year	Title	Focus	Key Point
Bernal et al.	2022	Neuronal Jamming Cyberattack over Invasive BCI Affecting the Resolution of Tasks Requiring Visual Capabilities	Neuronal jamming cyberattack over invasive BCI	Examines the impact of neuronal jamming cyberattacks on invasive BCIs, focusing on spike rate and performance in visual tasks.
Lahtinen & Costin	2023	Linking Computers to the Brain: Overview of Cybersecurity Threats and Possible Solutions	Overview of cybersecurity threats and solutions in BCIs	Provides an overview of cybersecurity threats in BCIs and explores potential solutions, including technical and procedural strategies.
Jiang et al.	2023	Cybersecurity in Neural Interfaces: Survey and Future Trends	Survey and future trends in neural interface cybersecurity	Surveys cybersecurity risks in neural interfaces, discussing central and peripheral nervous systems, neural modalities, and future trends.
Thomopoulos et al.	2024	A Systematic Review and Research Challenges on Phishing Cyberattacks from an Electroencephalography and Gaze-Based Perspective	Phishing cyberattacks, EEG and gaze-based perspective	Conducts a systematic review of phishing cyberattacks using EEG and eye-tracking methods, highlighting experimental research and challenges.

2.2. Cyber Exploits by Non-State and State Actors

Potential vulnerabilities in BCIs and neurotechnologies, including Bluetooth, are significant and multifaceted when considering the activities of both non-state and state actors.

Direct Cyber Attacks: BCIs and Bluetooth-enabled neurotechnologies are susceptible to direct cyber attacks, such as malware and ransomware. The WannaCry ransomware attack, which caused widespread disruption globally, exemplifies how malware can cripple critical systems [35,36]. If BCIs or Bluetooth devices are compromised, attackers could manipulate neural signals or intercept data transmissions, potentially leading to altered cognitive functions or unauthorized access to sensitive information, posing severe ethical and security risks.

Data Theft and Espionage: Advanced Persistent Threats (APTs) engage in long-term cyber espionage to gather sensitive information, and similarly, BCIs could be exploited to extract neural data. State actors may use this capability for intelligence purposes, accessing private thoughts or classified information processed by these technologies [37,38]. The interception of Bluetooth signals poses additional risks for unauthorized data collection and surveillance.

Manipulation and Sabotage: Non-state actors, including terrorists and organized crime groups, could exploit BCIs to manipulate individuals or sabotage operations. Hacktivists might target these technologies to disrupt services or further political agendas, similar to their broader activities in cyberspace [36,38]. The potential for direct neural manipulation via compromised BCIs opens new avenues for cyber terrorism, transforming the human brain into a target for malicious activities.

Privacy and Ethical Concerns: The integration of BCIs and Bluetooth-enabled neurotechnologies raises significant privacy issues. Unauthorized access to neural data or Bluetooth communications could lead to invasive surveillance and a loss of autonomy, paralleling concerns over traditional cyber surveillance but at a much more intimate level, affecting individuals' thoughts and behaviors [39].

The broader context of cyber exploits by non-state actors, such as organized criminal gangs, hacktivist groups, and terrorists, demonstrates their significant impact in cyberspace. These groups exploit the anonymity and reach of the internet to conduct activities ranging from financial crimes to cyberterrorism. Organized crime groups, for instance, engage in ransomware attacks and “Dark Net” markets, causing considerable economic damage and operational disruptions [35,36].

State actors frequently use non-state entities as proxies to achieve strategic goals while maintaining plausible deniability. This tactic is evident in state-sponsored APT operations, involving sophisticated, long-term cyber espionage and sabotage efforts targeting other nations [37,38].

Significant cyber incidents like WannaCry and NotPetya underscore the destructive potential of state-sponsored cyber exploits. The WannaCry ransomware, attributed to North Korean actors, and the NotPetya malware, linked to Russian actors, caused extensive global damage, highlighting the complexities of attributing cyberattacks and emphasizing the geopolitical dimensions of cyber warfare [35,36].

Furthermore, non-state actors such as terrorists use cyberspace for propaganda, recruitment, and coordination of attacks, broadening the scope of cyber threats. The strategic use of cyber tools by non-state actors illustrates the evolving nature of cyber warfare and underscores the need for robust cybersecurity measures to mitigate these threats [37,39]. The intricate interplay between state and non-state actors in cyberspace reflects the multifaceted nature of contemporary cyber threats, necessitating a comprehensive understanding to develop effective strategies for mitigating these risks [38,39].

While existing studies provide valuable insights into privacy and security issues in BCIs, they do not specifically address Bluetooth vulnerabilities. This research fills this critical gap by focusing on Bluetooth-specific risks, which are increasingly relevant due to the reliance on Bluetooth for wireless communication in BCIs. This focus is essential for developing a comprehensive security framework that can effectively safeguard BCI systems against the unique threats posed by Bluetooth-based attacks. By addressing these previously underexplored vulnerabilities, the research advances BCI cybersecurity, ensuring safer and more reliable use of this transformative technology.

3. Bluetooth Vulnerabilities

In today's world, Bluetooth technology is a necessity. The widespread availability of tablets, smartphones, personal computers, and game controllers has established Bluetooth as a popular short-range wireless communication technology. However, Bluetooth security flaws are becoming more common as the technology sees broader utilization, posing a threat to user privacy. Bluetooth security is crucial, as devices are susceptible to various wireless and networking attacks including denial of service attacks, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation. Bluetooth security must also address specific attacks related to Bluetooth, targeting known vulnerabilities in Bluetooth implementations and specifications, and potentially providing attackers with unauthorized access.

Businesses encounter security risks due to the increasing usage of Bluetooth devices in the workplace. Several hazards are associated with Bluetooth technology and linked devices, such as message manipulation, denial of service attacks, espionage, “man in the middle” attacks, and resource theft [40]. Preventing unwanted users from communicating via the pairing method is challenging. When people hear the phrase "hacking", they often think of computer systems and laptops. However, until a few years ago, the focus was primarily on computers and laptops. Only a very small number of individuals are aware that various Bluetooth attacks can be used to hack phones, as smartphones have also been targeted in recent years. Due to their similarity to pocket computers and their ability to perform many of the same functions, smartphones have become popular targets for hackers.

As technology advances, hackers will gain an even greater edge. The following is a condensed list of Bluetooth-related attacks that can be applied to any system using these technologies, including commercial BCI systems.

3.1. Bluebugging

It's a type of Bluetooth attack that allows hackers to gain access to the device and eavesdrop on conversations, send and receive messages and emails, and connect to the Internet and phone calls—all while the owner remains unaware. Most of the time, this hacking can be executed on outdated phones. If the phone is on a GSM network, it is also possible to hear the conversations of other nearby phones. This attack can be completed in less than two seconds if it goes off without a hitch. An attacker may then use additional devices to intercept incoming calls. Hackers have shifted their attention to mobile phone hacking as the number of smartphones on the market has increased [41]. Attacks like this one are generally confined by the 10-meter range of Bluetooth connections. Some assailants utilize gain antennas to enhance the range of their attacks. Like bugging a traditional phone line, it can be done without having direct access to the equipment.

3.1.1. Bluebugging's Impact on BCI

Bluebugging can grant unauthorized access to the BCI. If successful, this intrusion could allow eavesdropping on neural signal transmissions or manipulation of the BCI's functions. This interference could lead to the misinterpretation of neural data or unauthorized control over the BCI.

3.1.2. Mitigation Strategies

Mitigating Bluebugging's potential impact on BCIs requires a multi-layered approach that combines technical fortification, user vigilance, and regular security updates to ensure the integrity and security of the neural interface system. The following is a comprehensive list of mitigation actions:

- Enhanced Authentication Protocols: Implementing stringent authentication methods for pairing devices can mitigate the risk of unauthorized access. Utilizing encrypted and secure pairing mechanisms can prevent unauthorized connections.
- Frequent Security Audits and Updates: Regular security audits and timely software updates for the BCI's firmware and software are crucial. These updates should address known Bluetooth vulnerabilities, reducing the risk of successful Bluebugging attacks.
- Limiting Bluetooth Connectivity: Disabling Bluetooth when not in use or employing settings that allow the BCI to connect only with authorized and trusted devices can limit the attack surface.
- User Education: Educating BCI users about the risks of Bluebugging and best practices for securing Bluetooth connections is essential. Users should be vigilant and cautious about pairing with unknown or untrusted devices.

3.2. Bluejacking

“Bluejacking” refers to the practice of transmitting unsolicited messages over Bluetooth to devices equipped with Bluetooth capabilities, such as mobile phones, tablets, or laptops. This practice exploits the Bluetooth communication protocol to disseminate messages that are generally benign in nature and may comprise texts, images, or audio clips. The methodology of bluejacking encompasses several steps:

- Activation of Bluetooth: The initiator enables the Bluetooth function on their device and commences a search for proximate Bluetooth-enabled devices.
- Device Discovery: The initiator's device enumerates all Bluetooth devices within the immediate area that are configured to be discoverable.
- Message Composition: The initiator formulates a message, which might be a textual message, an image, or an audio snippet.
- Transmission of the Message: The composed message is dispatched to the selected receiving device. Upon reception, the recipient is notified of an incoming message or file.
- Response of the Recipient: The recipient possesses the discretion to either accept or decline the message. If accepted, the message is exhibited or the file is stored on the recipient’s device.

It is pertinent to acknowledge that bluejacking is predominantly undertaken for entertainment purposes and is not intrinsically harmful. Nevertheless, it may be perceived as intrusive or bothersome, particularly when the messages are uninvited or deemed inappropriate. Furthermore, while bluejacking in itself is not malevolent, it serves as a reminder of the security risks associated with maintaining an open and discoverable Bluetooth setting on devices, thereby potentially making them susceptible to more maleficent activities such as "Bluesnarfing." This latter term describes a scenario wherein an attacker illicitly acquires access to information on a device [42].

3.2.1. Impact on BCI by Bluejacking

Bluejacking, while not directly compromising data or control over the BCI, can still disrupt its function by bombarding it with unsolicited messages. This could cause distractions or interruptions during critical neural signal transmissions, potentially affecting the user's interaction with the BCI.

3.2.2. Mitigation Strategies

Combining these strategies presented below can minimize the disruptive impact of Bluejacking on the BCI, ensuring a more reliable and uninterrupted interaction between the user and the neural interface system:Filtering and Blocking Mechanisms: Implementing filters or blocking options on the BCI to prevent the reception of unsolicited messages can reduce the impact of Bluejacking. These filters could discard messages from unknown or unauthorized sources.

- Awareness and User Settings: Educating users on how to manage Bluetooth settings on the BCI can empower them to switch to non-discoverable modes or configure settings to only receive messages from trusted sources.
- Regular Monitoring and Auditing: Continuous monitoring of incoming messages and auditing the Bluetooth connections of the BCI can help detect and prevent Bluejacking attempts.
- Device Isolation: Using the BCI in environments where Bluetooth interference is minimized can reduce the likelihood of Bluejacking. Additionally, keeping the BCI in a controlled environment can limit exposure to such attacks.

3.3. Bluesnarfing

"Bluesnarfing" is a term used to describe the act of gathering data from unencrypted wireless networks. Bluesnarfing attacks may be launched by hackers within 75 to 90 m (approximately 250–300 ft). This is one of the most threatening Bluetooth attacks since hackers may access all of an individual's personal information, even if the device is in non-discoverable mode. Everything on the device is at their disposal, such as images, movies, and contact information, including phone numbers, email addresses, and passwords. Using the device in invisible mode, however, makes it more difficult for hackers to figure out the model and name of the device. A Bluesnarfing attack may occur if someone uses Bluetooth in public and the phone is regularly in discoverable mode [43].

It's remarkable how much the attacker can perpetrate or accomplish without detection. Any emails, contact lists, phone numbers, passwords, and photos could all be stolen from the phone or device. An outrageous phone bill is incurred when a Bluesnarfing attacker uses the victim's phone to make long-distance calls. Because the victim is unaware of what is happening, assaults can last for a long period.

3.3.1. Impact on BCI by Bluesnarfing

Bluesnarfing presents a severe threat to the privacy and security of BCIs. Successful Bluesnarfing attacks can lead to the extraction of sensitive neural signal data, compromising the confidentiality of the user's cognitive activities and potentially exposing personal information transmitted through the BCI.

3.3.2. Mitigation Strategies

Protecting BCIs from Bluesnarfing necessitates a combination of technical fortification, user awareness, and stringent security measures to safeguard the privacy and integrity of the neural data exchanged through the interface as shown here:Encryption and Data Protection: Implement strong encryption protocols for all data transmitted through the BCI. This includes neural signal data and any personal information, preventing unauthorized access in the event of a Bluesnarfing attempt.

- Regular Security Updates: Keep the BCI's firmware and software updated to patch known Bluetooth vulnerabilities, reducing the likelihood of successful Bluesnarfing attacks.
- Limiting Discoverable Mode: Set the BCI to non-discoverable mode when not actively pairing with authorized devices. This reduces exposure to potential Bluesnarfing attempts.
- User Training and Vigilance: Educate users on the risks of Bluesnarfing and the importance of securing their BCI's Bluetooth connections. Encourage them to only pair with trusted devices and to be cautious in public settings.

3.4. BlueBorne

BlueBorne is an attack vector, specifically a virus, that enables hackers to gain access to and control Bluetooth-enabled devices, including desktop computers, smartphones, and Internet of Things (IoT) devices. The attacker's smartphone does not need to be paired or set discoverable mode to initiate the assault on the targeted device. Armis Labs has discovered eight zero-day vulnerabilities, demonstrating the significant potential for this attack. According to Armis, many vulnerabilities in Bluetooth-enabled systems may still be uncovered [44]. These flaws are fully operational and can be quickly exploited, as demonstrated by this research. Techniques such as remote code execution and Man-in-the-Middle attacks are among those that the BlueBorne can employ. To initiate a BlueBorne attack, the hacker first infects the device with software, which allows them to take control. The virus can also spread to other connected devices through the initially infected device. Devices are vulnerable to BlueBorne attacks, even more so if a virtual private network (VPN) is not in use [45].

Viruses like BlueBorne can gain full control of the infected device. For this method to be effective, the target device does not need to be connected to the attacker's device or in a discoverable state. The virus will be transmitted to the device if its Bluetooth is activated and it is near another already infected device. Consequently, neither human interaction nor an internet connection is required.

Almost all devices can communicate over short distances using Bluetooth, the most widely used short-range communication protocol. BlueBorne opens the door to cyber espionage, data theft, and ransomware assaults. Beyond endangering industrial systems, government institutions, and critical infrastructure with cyberattacks, it might also enable hackers to penetrate “air-gapped” internal networks that are isolated from the internet for security reasons. With the expansion of the Internet of Things and smart home technologies, severe security breaches may occur due to the responsibilities assigned to these devices and the sensitive information they handle.

The attacker starts by scanning the area for any active Bluetooth connections and can identify devices even if "discoverable" mode is disabled. The attacker obtains the device’s unique “MAC address” to identify it, studies the operating system, and creates an exploit to leverage that knowledge [42]. Finally, the hacker exploits a vulnerability in the Bluetooth protocol to gain control of the device through a Man-in-the-Middle attack or by gaining total device control.

Although most manufacturers and operating system developers have provided security upgrades, data management, endpoint protection, network security solutions and firewalls often do not detect IP-based attacks. Consequently, new methods of defending against airborne attacks like BlueBorne are needed [45].

3.4.1. Impact on BCI by BlueBorne

BlueBorne, a complex attack vector, poses a severe threat to BCIs by exploiting various vulnerabilities. If successful, it can completely compromise the BCI's control and functionality, resulting in unauthorized access to neural data, signal manipulation, or even total control of the BCI by malicious entities.

3.4.2. Mitigation Strategies

Mitigating the potential impact of BlueBorne on BCIs requires a proactive and multi-layered approach, combining immediate action against known vulnerabilities, stringent security measures, and continuous monitoring to ensure the integrity and security of the neural interface system. These actions include:Immediate Patching and Updates: Apply immediate security patches and updates to the BCI's software and firmware to address known vulnerabilities exploited by BlueBorne, thereby reducing the risk of successful intrusion.

- Enhanced Encryption and Security Measures: Implement robust encryption methods and stringent security protocols to fortify the BCI's communication channels, preventing unauthorized access or control.
- Strict Access Controls: Limit the attack surface for potential BlueBorne intrusions by restricting access to the BCI, allowing it to pair only with authorized and trusted devices.
- Continuous Monitoring and Response: Employ real-time monitoring to detect any unusual activities or attempts at unauthorized access, and swiftly respond to potential threats to mitigate the impact of a BlueBorne attack.

3.5. Location Tracking

Location tracking involves using Bluetooth to track and find other devices. Fitness enthusiasts are especially at risk since their Bluetooth-enabled fitness devices are always in use [44].

3.5.1. Impact of Location Tracking on BCI

Location tracking through Bluetooth poses a risk to the privacy and security of BCI users. It could inadvertently disclose the user’s physical whereabouts, potentially compromising their anonymity and safety, especially in sensitive environments such as medical or research settings.

3.5.2. Mitigation Strategies

Protecting BCI users from the risks associated with Bluetooth-based location tracking involves a combination of user education, privacy guidelines, and environmental controls to mitigate potential exposure to privacy breaches, as presented below:

- Bluetooth Usage Awareness: Educate BCI users about the potential risks of Bluetooth-based location tracking and advise them to minimize the use of Bluetooth in sensitive or public environments.
- Geolocation Controls: Implement controls on the BCI to limit or disable geolocation data transmitted through Bluetooth, preventing unintentional disclosure of the user's whereabouts.
- Physical Environment Measures: Use the BCI in controlled environments where the risk of unauthorized location tracking is minimized, thus reducing potential exposure to these privacy risks.
- User Privacy Guidelines: Provide users with guidelines on managing their BCI's settings to avoid sharing location information via Bluetooth. Encourage them to exercise caution in public spaces.

3.6. Man-in-the-Middle Attack

A Man-in-the-Middle (MitM) or impersonation attack involves the modification of data between devices communicating in a Bluetooth Piconet [46]. A Bluetooth piconet is a network of Bluetooth-enabled devices connected in an ad-hoc manner. In a piconet, one device acts as the master, and up to seven other devices act as slavesThe master device initiates the connection by sending out synchronization packets. Slaves that are in range and want to join the piconet respond to the master's synchronization packets and synchronize their clocks to the master's clock. Bluetooth uses frequency hopping spread spectrum (FHSS) to avoid interference and provide secure communication. The master and slaves in a piconet hop between 79 different frequencies in the 2.4 GHz ISM band. Multiple piconets can coexist and communicate with each other in what is called a scatternet. In a scatternet, a device can be a master in one piconet and a slave in another, allowing for more complex and flexible network configurations. Bluetooth piconets are commonly used in various applications, including wireless headphones, hands-free car kits, wireless mice and keyboards, and many other consumer electronics devices. The effective range of a Bluetooth piconet is typically up to 10 m (about 33 ft), although this can vary depending on the Bluetooth class and environmental factors. Bluetooth piconets support encryption and authentication to ensure secure communication between devices. In summary, a Bluetooth piconet is a short-range wireless network formed by a master device and up to seven slave devices communicating via Bluetooth technology [47].

In a MitM attack, the attacker relays authentication messages between two devices in order to authenticate without knowing the shared secret keys. By forwarding the messages of two devices trying to pair, an attacker can trick the devices into believing they are paired with each other when, in fact, they have paired with the attacker.

3.6.1. Impact on BCI by MitM Attack

Attackers can exploit the MitM or impersonation attack to impersonate the BCI device and establish a connection with the external device without the need for authentication. This can lead to unauthorized access to the BCI device and the sensitive data it transmits. Once the attacker has established a connection with the external device, they can intercept and manipulate the data being transmitted between the BCI device and the external device, potentially leading to incorrect readings or commands being sent to the BCI device. Exploiting the MitM or impersonation attack can compromise the user's privacy by allowing attackers to access and potentially misuse their personal and sensitive information. Disrupting the authentication process can cause the connection between the BCI device and the external device to become unstable or unresponsive, leading to device malfunction.

3.6.2. Mitigation Strategies

Mitigating the impact of MitM and impersonation attacks on BCIs necessitates a comprehensive strategy involving advanced authentication protocols, robust encryption methods, heightened user awareness, and strategic network segmentation. This holistic approach ensures the safeguarding of data and reinforces the security of the interface system. The strategy includes:

- Incorporate Piconet-Specific Information: Integrate detailed Piconet information, such as timestamps and nested mutual authentication, into the pairing process to validate the authenticity of device challenges before responding.
- Strengthen Authentication Mechanisms: Employ robust authentication techniques, such as Secure Simple Pairing (SSP) [48] or Out-of-Band (OOB) [49] authentication, to verify device identities and thwart MitM or impersonation attempts.
- Apply Strong Encryption: Implement advanced encryption algorithms with substantial key lengths to ensure secure data transmissions between the BCI and external devices.
- Ensure Secure Key Management: Adopt rigorous key management protocols to securely generate, store, and exchange encryption keys between the BCI and external devices.
- Increase User Awareness: Educate users about MitM and impersonation threats and provide guidelines for the secure use of Bluetooth-enabled BCIs, including recognizing and reporting suspicious activities.
- Implement Network Segmentation: Separate the BCI device from other networked devices to reduce the impact of a successful MitM or impersonation attack.

3.7. KNOB Attack

The KNOB (Key Negotiation Of Bluetooth) attack is a significant vulnerability that affects the Bluetooth BR/EDR (Basic Rate/Enhanced Data Rate) specification. This vulnerability, discovered in 2019, allows attackers to intercept and manipulate the encryption key negotiation process between two Bluetooth devices. By exploiting this vulnerability, attackers can conduct MitM attacks and decrypt the data being transmitted between the devices [50].

3.7.1. Impact on BCI by KNOB

Attackers can exploit the KNOB vulnerability to intercept and decrypt the data being transmitted between the BCI device and the external device it is connected to. This can lead to unauthorized access to sensitive user data, including brainwave patterns and personal information. In addition to intercepting data, attackers can also manipulate the data being transmitted between the BCI device and the external device. This could result in incorrect readings or commands being sent to the BCI device, potentially leading to incorrect interpretations of the user's brain activity. Exploiting the KNOB vulnerability can compromise the user's privacy by allowing attackers to access and potentially misuse their personal and sensitive information.

Manipulating the encryption key negotiation process can disrupt the connection between the BCI device and the external device, causing the BCI device to malfunction or become unresponsive.

3.7.2. Mitigation Strategies

Addressing the KNOB attack's potential effects on BCIs calls for a proactive strategy encompassing timely firmware updates, strong encryption practices, and extensive user education. These actions collectively strengthen the security framework of BCIs, protecting them from this particular vulnerability:

- Frequent Firmware Updates: Consistently update the BCI device firmware to address the KNOB vulnerability and enhance security.
- Adopt Strong Authentication: Implement robust authentication mechanisms, such as Secure Connections or OOB authentication, to verify device identities and prevent KNOB attacks.

- Utilize Strong Encryption: Apply strong encryption algorithms with significant key lengths to protect data transmissions between the BCI and external devices.
- Secure Key Management: Ensure encryption keys are securely generated, stored, and exchanged using stringent key management practices.
- Enhance User Education: Educate users about the KNOB vulnerability and provide guidelines for the secure use of BLE-enabled BCIs, including identifying and reporting suspicious activities.
- Implement Network Segmentation: Isolate the BCI device from other networked devices to minimize the impact of a successful KNOB attack.

3.8. BLESA

BLESA (Bluetooth Low Energy Spoofing Attack) is a vulnerability that affects the Bluetooth Low Energy (BLE) protocol [51]. Discovered in 2020, BLESA allows attackers to impersonate a legitimate BLE device and establish a connection with a targeted device without the need for pairing or authentication. This vulnerability can be exploited to intercept sensitive data or execute malicious activities on the targeted device.

3.8.1. Impact on BCI by BLESA

Attackers can exploit the BLESA vulnerability to impersonate the BCI device and establish a connection with the external device without the need for authentication. This can lead to unauthorized access to the BCI device and the sensitive data it transmits. Once the attacker has established a connection with the external device, they can intercept and manipulate the data being transmitted between the BCI device and the external device, potentially leading to incorrect readings or commands being sent to the BCI device.

Exploiting the BLESA vulnerability can compromise the user's privacy by allowing attackers to access and potentially misuse their personal and sensitive information.

Disrupting the connection between the BCI device and the external device can cause the BCI device to malfunction or become unresponsive.

3.8.2. Mitigation Strategies

Countering the risks associated with BLESA requires a blend of technical enhancements and user education. Ensuring regular updates to security protocols and educating users about emerging threats help maintain the integrity and security of BLE-enabled BCIs. Below is an analytical approach, providing a detailed list of mitigation actions:

- Firmware Updates: Regularly update the firmware of the BCI device to patch the BLESA vulnerability and improve its overall security posture.
- Authentication Mechanisms: Implement strong authentication mechanisms, such as Secure Connections or OOB authentication, to verify the identity of the devices participating in the BLE connection and prevent BLESA attacks.
- Encryption: Use strong encryption algorithms and key lengths to protect the data transmitted between the BCI device and the external device.
- Key Management: Implement secure key management practices to ensure that encryption keys are securely generated, stored, and exchanged between the BCI device and the external device.
- User Awareness: Educate users about the BLESA vulnerability and provide guidance on how to use BLE-enabled BCIs securely, including how to recognize and report any suspicious activity or behavior.
- Network Segmentation: Isolate the BCI device from other networked devices to minimize the potential impact of a successful BLESA attack.

3.9. Reflection Attack

A reflection attack, also known as a relay attack, exploits the authentication process between two Bluetooth devices by impersonating one of the devices. In a reflection attack, the attacker relays (reflects) the received information from one target device to another during the authentication process [52]. Unlike traditional MitM attacks, reflection attacks do not target encryption but focus on bypassing authentication.

3.9.1. Impact on BCI by Reflection Attack

Attackers can exploit the reflection attack to impersonate the BCI device and establish a connection with the external device without the need for authentication. This can lead to unauthorized access to the BCI device and the sensitive data it transmits.

Once the attacker has established a connection with the external device, they can intercept and manipulate the data being transmitted between the BCI device and the external device, potentially leading to incorrect readings or commands being sent to the BCI device. Exploiting the reflection attack can compromise the user's privacy by allowing attackers to access and potentially misuse their personal and sensitive information.

Disrupting the authentication process can cause the connection between the BCI device and the external device to become unstable or unresponsive, leading to device malfunction.

3.9.2. Mitigation Strategies

Mitigating reflection attacks on BCIs demands a multi-faceted security approach, incorporating robust authentication mechanisms, strong encryption practices, effective key management, and thorough user education. These combined efforts significantly bolster the security and reliability of Bluetooth-enabled BCIs:

- Robust Authentication Mechanisms: Implement strong authentication mechanisms, such as Secure SSP or OOB authentication, to verify device identities and prevent reflection attacks.
- Apply Strong Encryption: Although reflection attacks do not target encryption, using strong encryption algorithms and key lengths can add an extra layer of security for data transmissions.
- Adopt Secure Key Management: Ensure encryption keys are securely generated, stored, and exchanged using rigorous key management protocols.
- User Education: Inform users about the risks of reflection attacks and provide guidelines for the secure use of Bluetooth-enabled BCIs, including recognizing and reporting suspicious activities.
- Network Segmentation: Separate the BCI device from other networked devices to reduce the impact of a successful reflection attack.

3.10. Comparative Analysis

It is crucial to understand the varying degrees of risk posed by different types of attacks. While some vulnerabilities present significant threats with potentially severe consequences, others are less harmful and more manageable as Table 3 presents.

Table 3. Comparative analysis of the Bluetooth attacks.

Study	Attack Type	Impact on BCIs	Key Mitigation Strategies
Qian et al. (2022)	Bluebugging	Unauthorized access	Enhanced authentication protocols
Wei (2020)	Bluejacking	Minor disruption	Filtering mechanisms
Shrestha et al. (2021)	Bluesnarfing	Data theft	Strong encryption and regular updates
Lonzetta et al. (2018)	BlueBorne	Complete control and data compromise	Immediate patching, enhanced encryption
Yun et al. (2020)	Location tracking	Privacy risk	Geolocation controls
Haataja and Toivanen (2010)	Man-in-the-Middle	Intercepted and altered data	Secure pairing protocols
Antonioli et al. (2019)	KNOB	Decrypted data and potential command manipulation	Advanced key management
Wu et al. (2020)	BLESA	Unauthorized device impersonation and data manipulation	Secure key management, strong encryption
Panse and Panse (2013)	Reflection attack	Unauthorized access and data interception	Robust authentication, network segmentation

BlueBorne is a major risk due to its comprehensive attack vector, which can exploit multiple vulnerabilities, allowing for diverse attack types, including remote code execution and Man-in-the-Middle (MitM) attacks. It can give attackers full control over the BCI, allowing them to manipulate its functions, intercept neural signals, and access all transmitted data. The attack does not require the device to be in discoverable mode, significantly increasing the risk of an undetected attack. Additionally, BlueBorne can spread from one infected device to others, creating a chain of compromised systems and amplifying the attack's scope. Given the sensitive nature of data handled by BCIs, including neural signals, BlueBorne poses a particularly dangerous threat for espionage and data theft.

Man-in-the-Middle attacks are another significant risk due to their ability to intercept and alter data transmitted between the BCI and external devices, leading to incorrect readings or commands, which can severely impact the user's interaction with the BCI. These attacks can trick devices into authenticating with the attacker instead of the intended device, bypassing security protocols and gaining unauthorized access. By intercepting communications, attackers can access sensitive neural data and personal information, compromising the user's privacy. Additionally, disrupting the authentication process can cause instability in the connection between the BCI and external devices, leading to device malfunction.

Bluejacking is a minor risk because it is generally used for sending unsolicited messages and is typically not intended to harm the device or steal data. While it can disrupt the BCI's function by bombarding it with messages, it does not grant the attacker control over the device or access to its data. The impact of Bluejacking can be effectively mitigated by implementing filters or blocking options and educating users on managing Bluetooth settings.

Location tracking also is a minor risk because it poses a privacy risk rather than a direct threat to the control or function of the BCI. The severity of location tracking depends on the context and environment in which the BCI is used. In non-sensitive settings, the impact may be minimal. This risk can be reduced through user education about the potential risks and providing guidelines for minimizing Bluetooth usage in sensitive environments. Implementing geolocation controls and using BCIs in controlled environments can further mitigate this risk.

4. Discussion

The cybersecurity landscape for Brain-Computer Interfaces (BCIs) is evolving rapidly due to emerging trends and advanced technologies aimed at mitigating Bluetooth vulnerabilities. Addressing these risks requires a comprehensive strategy that integrates advanced encryption, robust authentication mechanisms, regular system updates, and thorough user education. These measures are essential for safeguarding the integrity and privacy of neural data exchanged through BCIs.

Ethical and legal integrity in BCI cybersecurity is fundamental for maintaining user trust and complying with regulatory standards. Ethical considerations involve protecting user privacy, ensuring data integrity, and obtaining informed consent for data collection and processing. Given the sensitive nature of neural data, stringent measures are necessary to prevent unauthorized access and misuse. Compliance with frameworks such as the General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the United States is crucial. These regulations mandate strict data protection practices and grant users rights over their data, including access, correction, and deletion, thereby shielding developers and companies from legal liabilities.

To protect BCIs against Bluetooth vulnerabilities, robust encryption protocols, strong authentication mechanisms, and secure communication practices are essential. Using Advanced Encryption Standard (AES) with 256-bit keys ensures comprehensive protection for data transmitted between BCI devices and external devices. Multi-Factor Authentication (MFA), requiring multiple forms of verification, adds an extra layer of security. Biometric verification, such as fingerprint, facial recognition, or neural pattern recognition, provides a high level of security due to the uniqueness of biometric data.

Regular firmware updates and security patches are critical for addressing newly discovered vulnerabilities. Automated update mechanisms can maintain security without requiring user intervention. Secure pairing and communication protocols, such as SSP and OOB authentication, enhance the Bluetooth pairing process. Ensuring data integrity and authenticity through digital signatures and cryptographic hash functions further secures transmitted data. Security considerations should be incorporated at every stage of the BCI development process, including threat modeling and security assessments. Applying the principle of least privilege ensures minimal access necessary for users and processes, reducing potential security risks.

User education is crucial for maintaining the security of Bluetooth-enabled BCIs. Training users to recognize suspicious activities and providing clear mechanisms for reporting security incidents are vital. Users should learn to configure their devices securely, including setting Bluetooth to non-discoverable mode when not in use and enabling secure pairing options. Regular maintenance, such as checking for and installing firmware updates and security patches, should be encouraged. Guidelines for safe Bluetooth usage, such as avoiding pairing devices in public places and using strong passwords, are essential. Educating users on the importance of protecting personal and neural data, emphasizing strong passwords and careful sharing of sensitive information, is also crucial.

Future research in BCI cybersecurity should focus on developing lightweight encryption techniques suitable for resource-constrained hardware, ensuring efficiency and effectiveness for devices with limited processing power and battery life. Investigating secure communication protocols resilient to various wireless attack vectors, such as jamming, eavesdropping, and interference, is also critical. Emerging technologies like quantum-resistant encryption offer potential solutions to future-proof BCI security against advanced threats. Biometric authentication based on neural patterns provides a secure means of verifying user identity. Leveraging machine learning and artificial intelligence (AI) for real-time threat detection and anomaly analysis can significantly enhance proactive defense mechanisms. AI-powered predictive models can identify and mitigate Bluetooth security breaches, enhancing overall resilience. Future research should also explore secure data storage mechanisms to protect sensitive neural data from unauthorized access or tampering and develop adaptive security measures that evolve with emerging threats.

The future of Bluetooth security in BCIs holds significant promise, with research opportunities focusing on specialized security measures tailored to Bluetooth vulnerabilities. Advanced encryption techniques, novel authentication methods, and the integration of machine learning and AI for proactive threat detection can significantly strengthen the security and ethical foundations of Bluetooth-enabled BCIs. Upholding ethical principles and legal standards is essential for ensuring the responsible development and deployment of these technologies, thus advancing the field while safeguarding user privacy and security.

A comprehensive review of current research on BCI cybersecurity emphasizes the urgent need to address Bluetooth vulnerabilities in these critical information systems. The literature highlights the inherent vulnerabilities in BCIs, particularly concerning Bluetooth attacks, data privacy, and unauthorized access. Existing solutions often lack specificity and innovation, revealing a significant gap in tailored security solutions for BCIs. The absence of novel and adaptive security measures poses a considerable challenge in mitigating the evolving threats targeting BCIs.

Balancing security and usability is crucial in BCI technology. Stringent security measures are necessary to protect sensitive neural data and ensure user privacy without compromising usability and seamless operation. The future of BCI cybersecurity hinges on advancements that integrate tailored security solutions, particularly in addressing Bluetooth vulnerabilities. Innovations in authentication methods, encryption techniques, and behavioral analysis hold significant potential for enhancing the security posture of BCIs. Additionally, a paradigm shift in device development is required, prioritizing security features alongside functionality to ensure robust and user-friendly security measures.

Table 4 presents the cause and effect analysis of mitigation parameters.

Table 4. Cause and effect analysis.

Parameter	Cause	Effect
Advanced Encryption	Implementation of robust encryption protocols such as Advanced Encryption Standard (AES) with 256-bit keys.	Ensures comprehensive protection for data transmitted between BCI devices and external devices, making it difficult for unauthorized parties to intercept and decipher the data.
Robust Authentication Mechanisms	Utilization of Multi-Factor Authentication (MFA) and biometric verification (e.g., fingerprint, facial recognition, neural pattern recognition).	Adds multiple layers of security, significantly reducing the likelihood of unauthorized access to BCI systems.

Table 4. *Cont.*

Parameter	Cause	Effect
Regular Firmware Updates and Security Patches	Implementation of automated update mechanisms for regular firmware updates and security patches.	Addresses newly discovered vulnerabilities promptly, reducing the risk of security breaches due to outdated software.
Secure Pairing and Communication Protocols	Adoption of Secure Simple Pairing (SSP) and Out-of-Band (OOB) authentication protocols.	Enhances the security of the Bluetooth pairing process, minimizing the risk of unauthorized device connections.
User Education	Comprehensive training programs for users to recognize suspicious activities and configure devices securely.	Empowers users to take proactive measures in securing their BCIs, reducing the likelihood of successful phishing and other social engineering attacks.
Lightweight Encryption Techniques	Research into lightweight encryption suitable for resource-constrained BCI hardware.	Ensures efficient and effective encryption for devices with limited processing power and battery life, maintaining security without compromising performance.
Quantum-Resistant Encryption	Development and implementation of encryption methods resistant to quantum computing threats.	Future-proofs BCI security against potential advances in quantum computing, ensuring long-term data protection.
Machine Learning and AI for Threat Detection	Leveraging machine learning and AI for real-time threat detection and anomaly analysis.	Enhances proactive defense mechanisms, enabling early identification and mitigation of security breaches.

This analysis demonstrates the critical need for specialized security solutions tailored to the unique requirements of BCI technology. Bridging the gap between research insights and practical implementation demands an interdisciplinary approach, integrating human factors into the development and deployment of security solutions. By addressing practical challenges and aligning research findings with user-centric solutions, BCIs can be fortified against Bluetooth attacks while ensuring user acceptance and usability.

5. Conclusions

This research highlights the paramount importance of cybersecurity in Brain-Computer Interfaces (BCIs), given the sensitive nature of neural data and the expanding use of BCIs in medical, assistive, and recreational domains. Ensuring the security of BCIs is essential for enhancing user trust and promoting the broader adoption of these transformative technologies, particularly for individuals with disabilities.

The originality of this study lies in its focus on the relatively unexplored area of Bluetooth vulnerabilities within BCIs. By thoroughly analysing various Bluetooth attacks and their specific impacts on BCIs, this research addresses a critical gap in the literature. The novel intersection of Bluetooth technology and BCIs underscores the urgency and relevance of addressing these vulnerabilities, considering the widespread adoption of Bluetooth-enabled devices.

This study maintains methodological rigor through a systematic review process involving detailed search strategies, database selections, and strict inclusion/exclusion criteria. This comprehensive literature review provides a reliable foundation for the findings. Furthermore, the structured framework used to analyse Bluetooth attacks, including their mechanisms, impacts on BCIs, and mitigation strategies, adds clarity and depth to the research.

While the study offers significant insights, it also acknowledges potential limitations. The primary focus is Bluetooth, although other wireless protocols used in BCIs may also require investigation. Advanced encryption and authentication methods, warrant further exploration to enhance BCI security. Integrating machine learning and AI for anomaly detection and proactive defence mechanisms can significantly strengthen security. Ethical and legal considerations remain crucial, ensuring user privacy and compliance with regulatory standards.

A major concern for commercial BCI devices is the safety and privacy of data transmission. Despite the necessity for robust security and privacy in headsets and gadgets, these issues are often not prioritized. This review examines various ways in which BCI devices can be compromised, analysing the effectiveness of Bluetooth attacks and vulnerability detection. The threats posed by Bluetooth attacks emphasize the need for improved BCI security designs and greater attention to privacy in headset manufacturing. A thorough investigation of security and privacy issues is essential before deploying BCI devices.

Manufacturers of hardware and software should focus not only on device durability and mobility but also on addressing threats such as hostile entry and service outages. This review indicates that Bluetooth transmissions can be read and manipulated using basic hardware equipment. Various Bluetooth attacks might exploit newly discovered flaws, compromising the intended function of the technology and causing disruption, modification, or corruption. Reducing Bluetooth attacks on BCI devices may be achievable if manufacturers adopt the BLE 4.2 security standard instead of the cheaper and more common BLE 4.0 standard. Effective risk management and user protection can be achieved if developers adhere to this framework.

In conclusion, this review underscores the ongoing need to address the cybersecurity aspects of BCI devices, which handle highly sensitive user data. By emphasizing the importance of cybersecurity in BCIs, demonstrating originality and innovation, ensuring methodological rigor, addressing potential weaknesses, and proposing future research directions, this study lays a robust foundation for advancing BCI security. Implementing these findings and recommendations can help ensure that BCIs are secure, reliable, and trusted by users, paving the way for their broader and more impactful application.

Author Contributions

Conceptualization, D.A.; methodology and validation, D.A., P.A., S.K. and E.V.; formal analysis, D.A.; investigation, D.A.; resources,. D.A.; writing—original draft preparation, D.A.; writing—review and editing, D.A.; visualization, P.A.; supervision, D.A.; project administration, D.A. All authors have read and agreed to the published version of the manuscript.

Funding

This research received no external funding.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

Not applicable.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Hill, N.J.; Wolpaw, J.R. Brain–Computer Interface. In *Reference Module in Biomedical Sciences*, 1st ed.; Larry R. Squire, Floyd E. Bloom, Nicholas C. Spitzer, Fred Gage, Tom Albright; Elsevier: Netherlands, 2016, pp 429–437. [CrossRef]
2. Shih, J.J.; Krusienski, D.J.; Wolpaw, J.R. Brain-Computer Interfaces in Medicine. *Mayo Clin. Proc.* **2012**, *87*, 268–279. [CrossRef]
3. Kübler, A. The History of BCI: From a Vision for the Future to Real Support for Personhood in People with Locked-in Syndrome. *Neuroethics* **2020**, *13,* 163–180. [CrossRef]
4. Iroju, O.; Ikono, R.; Ishaya, G.; Ojerinde, O.A.; Olaleke, J. Prospects and Problems of Brain Computer Interface in Healthcare. *Curr. J. Appl. Sci. Technol.* **2018**, *29*, 1–17. [CrossRef]
5. Umair, A.; Ashfaq, U.; Khan, M.G. Recent Trends, Applications, and Challenges of Brain-Computer Interfacing (BCI). *Int. J. Intell. Syst. Appl.* **2017**, *9*, 58. [CrossRef]

6. Pycroft, L.; Aziz, T.Z. Security of implantable Medical Devices with Wireless Connections: The dangers of Cyber-Attacks. *Expert Rev. Med. Devices* **2018**, *15*, 403–406. [CrossRef]
7. Leuthardt, E.C.; Schalk, G.; Roland, J.; Rouse, A.; Moran, D.W. Evolution of Brain-Computer Interfaces: Going Beyond Classic Motor Physiology. *Neurosurg. Focus* **2009**, *27*, E4. [CrossRef]
8. Zeadally, S.; Siddiqui, F.; Baig, Z. 25 Years of Bluetooth Technology. *Future Internet* **2019**, *11*, 194. [CrossRef]
9. Berezhnoy, D.; Bergaliyev, T.; Sakhno, S. Application of the Bluetooth Protocol for Data Transfer from Computer to the Brain in Active BCI-Interfaces and Development of the Small Bluetooth Neural Stimulation Device. In Proceedings of the 2020 International Conference Engineering and Telecommunication, Dolgoprudny, Russia, 25–26 November 2020. [CrossRef]
10. Bruno, R.; Conti, M.; Gregori, E. Bluetooth: Architecture, Protocols and Scheduling Algorithms. *Cluster Comput.* **2002**, *5*, 117–131. [CrossRef]
11. Bluetooth Protocol Stack—MATLAB Simulink. Available online: https://www.mathworks.com/help/bluetooth/ug/bluetooth-protocol-stack.html (accessed on 1 April 2024).
12. Ajrawi, S.; Rao, R.; Sarkar, M. Cybersecurity in Brain-Computer Interfaces: RFID-Based Design-Theoretical Framework. *Inf. Med. Unlocked* **2021**, *22*, 100489. [CrossRef]
13. Saha, S.; Mamun, K.A.; Ahmed, K.; Mostafa, R.; Naik, G.R.; Darvishi, S.; Khandoker, A.H.; Baumert, M. Progress in Brain Computer Interface: Challenges and Opportunities. *Front. Systems Neurosci.* **2021**, *15*, 578875. [CrossRef]
14. Rashid, M.; Sulaiman, N.; PP Abdul Majeed, A.; Musa, R.M.; Ab. Nasir, A.F.; Bari, B.S.; Khatun, S. Current Status, Challenges, and Possible Solutions of EEG-Based Brain-Computer Interface: A Comprehensive Review. *Front. Neurorobot.* **2020**, *14*, 25. [CrossRef]
15. Wu, D.; Xu, J.; Fang, W.; Zhang, Y.; Yang, L.; Xu, X.; Luo, H.; Yu, X. Adversarial Attacks and Defenses in Physiological Computing: A Systematic Review. *Natl. Sci. Open* **2023**, *2*, 20220023. [CrossRef]
16. EMOTIV. Available online: https://www.emotiv.com/epoc/ (accessed on 17 December 2023).
17. EEG & ECG Biosensor. Available online: https://neurosky.com/ (accessed on 17 December 2023).
18. MYNDPLA. Available online: https://myndplay.com/ (accessed on 17 December 2023).
19. XWave. Available online: https://www.eyecomtec.com/3405-XWave,%22 (accessed on 17 December 2023).
20. ULTRACORTEX "MARK IV" EEG HEADSET. Available online: https://shop.openbci.com/products/ultracortex-mark-iv (accessed on 17 December 2023). (accessed on 17 December 2023).
21. TajDini, M.; Sokolov, V.; Kuzminykh, I.; Shiaeles, S.; Ghita, B. Wireless Sensors for Brain Activity—A Survey. *Electronics* **2020**, *9*, 2092. [CrossRef]
22. OpenBCI. Available online: https://openbci.com/ (accessed on 17 December 2023).
23. Takabi, H.; Bhalotiya, A.; Alohaly, M. Brain Computer Interface (BCI) Applications: Privacy Threats and Countermeasures. In Proceedings of the 2016 IEEE 2nd International Conference on Collaboration and Internet Computing, Pittsburgh, PA, USA, 1–3 November 2016. [CrossRef]
24. Wahlstrom, K.; Fairweather, N.B.; Ashman, H. Privacy and Brain-Computer Interfaces: Identifying Potential Privacy Disruptions. *Acm Sigcas Comput. Soc.* **2016**, *46*, 41–53. [CrossRef]
25. Takabi, H. Firewall for Brain: Towards a Privacy Preserving Ecosystem for BCI Applications. In Proceedings of the 2016 IEEE Conference on Communications and Network Security, Philadelphia, PA, USA, 17–19 October 2016. [CrossRef]
26. 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 Neurosurg.* **2016**, *92*, 454–462. [CrossRef]
27. Ienca, M.; Haselager, P.; Emanuel, E.J. Brain Leaks and Consumer Neurotechnology. *Nat. Biotechnol.* **2018**, 36, 805–810. [CrossRef]
28. Landau, O.; Puzis, R.; Nissim, N. Mind Your Mind: EEG-Based Brain-Computer Interfaces and Their Security in Cyber Space. *ACM Comput. Surv.* **2020**, *53*, 1–38. [CrossRef]
29. Belkacem, A.N. Cybersecurity Framework for P300-based Brain Computer Interface. In Proceedings of the 2020 IEEE International Conference on Systems, Man, and Cybernetics, Toronto, ON, Canada, 11–14 October 2020. [CrossRef]
30. Bernal, S.L.; Celdrán, A.H.; Pérez, G.M.; Barros, M.T.; Balasubramaniam, S. Security in Brain-Computer Interfaces: State-of -the-Art, Opportunities, and Future Challenges. *ACM Comput. Surv.* **2021**, *54*, 1–35. [CrossRef]
31. Bernal, S.L.; Celdrán, A.H.; Pérez, G.M. Neuronal Jamming Cyberattack over Invasive BCIs Affecting the Resolution of Tasks Requiring Visual Capabilities. *Comput. Secur.* **2022**, *112*, 102534. [CrossRef]
32. Lahtinen, T.; Costin, A. Linking Computers to the Brain: Overview of Cybersecurity Threats and Possible Solutions. In Proceedings of the International Symposium on Business Modeling and Software Design, Utrecht, Netherlands, 3–5 July 2023. [CrossRef]
33. Jiang, X.; Fan, J.; Zhu, Z.; Wang, Z.; Guo, Y.; Liu, X.; Jia, F.; Dai, C. Cybersecurity in Neural Interfaces: Survey and Future Trends. *Comput. Biol. Med.* **2023**, *167*, 107604. [CrossRef]

34. Thomopoulos, G.A.; Lyras, D.P.; Fidas, C.A. A Systematic Review and Research Challenges on Phishing Cyberattacks from an Electroencephalography and Gaze-Based Perspective. *Pers. Ubiquitous Comput.* **2024**, 1–22. [CrossRef]
35. Rid, T. Cyber war will not take place. *J. Strateg. Stud.*, **2012**, *35*, 5–32. [CrossRef]
36. Strategic Cyber Security. Available online: https://ccdcoe.org/uploads/2018/10/2011_Proceedings_0-1.pdf (accessed on 26 June 2024).
37. Sigholm, J. Non-State Actors in Cyberspace Operations. *J. Mil. Stud.* **2013**, *4*, 1–37. [CrossRef]
38. Stoddart, K. Non and Sub-State Actors: Cybercrime, Terrorism, and Hackers. In *Cyberwarfare: Threats to Critical Infrastructure*, 1st ed.; Stoddart, K., Ed.; Palgrave Macmillan: Cham, Switzerland, 2022; pp. 351–399. [CrossRef]
39. Stoddart, K. Hacking the Human. In *Cyberwarfare. Palgrave Studies in Cybercrime and Cybersecurity*, 1st ed.; Stoddart, K., Ed.; Palgrave Macmillan: Cham, Switzerland, 2022; pp. 281–349. [CrossRef]
40. Acharige, K.M.; Albuquerque, O.; Fantinato, M.; Peres, S.M.; Hung, P.C. A Security Study of Bluetooth-Powered Robot Toy. *J. Surveill., Secur. Saf.* **2021**, *2*, 26–41. [CrossRef]
41. Qian, Y.; Ye, F.; Chen, H.H. Bluetooth Security. In *Security in Wireless Communication Networks*, 1st ed.; Qian, Y., Ye, F., Chen, H.H., Eds.; John Wiley & Sons: Hoboken, NJ, USA, 2022; pp. 153–175. [CrossRef]
42. Wei, F. Detecting Bluetooth Attacks Against Smartphones by Device Status Recognition. In Proceedings of the Artificial Intelligence and Security: 6th International Conference, Hohhot, China, 17–20 July 2020. [CrossRef]
43. Shrestha, S.; Irby, E.; Thapa, R.; Das, S. SoK: A Systematic Literature Review of Bluetooth Security Threats and Mitigation Measures. In Proceedings of the International Symposium on Emerging Information Security and Applications, Copenhagen, Denmark, 12–13 November 2021. [CrossRef]
44. Lonzetta, A.M.; Cope, P.; Campbell, J.; Mohd, B.J.; Hayajneh, T. Security Vulnerabilities in Bluetooth Technology as Used in IoT. *J. Sens. Actuator Networks* **2018**, *7*, 28. [CrossRef]
45. Yun, Y.H.; Kim, D.W.; Choi, J.A.; Kang, S.H. An Intelligent Bluetooth Intrusion Detection System for the Real Time Detection in Electric Vehicle Charging System. *Convergence Secur. J.* **2020**, *20*, 11–17. [CrossRef]
46. Haataja, K.; Toivanen, P. Two Practical Man-in-the-Middle Attacks on Bluetooth Secure Simple Pairing and Countermeasures. *IEEE Trans. Wireless Commun.* **2010**, *9*, 384–392. [CrossRef]
47. Johansson, P.; Kazantzidis, M.; Kapoor, R.; Gerla, M. Bluetooth: An Enabler for Personal Area Networking. *IEEE Network* **2001**, *15*, 28–37. [CrossRef]
48. Phan, R.C.W.; Mingard, P. Analyzing the Secure Simple Pairing in Bluetooth v4.0. *Wireless Pers. Commun.* **2012**, *64*, 719–737. [CrossRef]
49. Mirzadeh, S.; Cruickshank, H.; Tafazolli, R. Secure Device Pairing: A Survey. *IEEE Commun. Surv. Tutorials* **2013**, *16*, 17–40. [CrossRef]
50. Antonioli, D.; Tippenhauer, N.O.; Rasmussen, K. Low Entropy Key Negotiation Attacks on Bluetooth and Bluetooth Low Energy. *Cryptol. ePr. Arch.* **2019**.
51. Wu, J.; Nan, Y.; Kumar, V.; Tian, D.J.; Bianchi, A.; Payer, M.; Xu, D. BLESA: Spoofing Attacks against Reconnections in Bluetooth Low Energy. In Proceedings of the 14th USENIX Workshop on Offensive Technologies, Online, 11 August 2020.
52. Panse, T.; Panse, P. A Survey on Security Threats and Vulnerability attacks on Bluetooth Communication. *Int. J. Comput. Sci. Inf. Technol.* **2013**, *4*, 741–746.

Publisher's Note: The views, opinions, and information presented in all publications are the sole responsibility of the respective authors and contributors, and do not necessarily reflect the views of UK Scientific Publishing Limited and/or its editors. UK Scientific Publishing Limited and/or its editors hereby disclaim any liability for any harm or damage to individuals or property arising from the implementation of ideas, methods, instructions, or products mentioned in the content.