

A Comparative Study of Data Privacy Measures in Invasive vs. Non-Invasive Brain-Computer Interfaces

Satish Kumar Verma¹, Diwakar Kumar², Nitish Kumar,³ Himanshu Kumar⁴, Pintu Kumar Mehta⁵,
Binita Roshima Hinz^{1*}

¹²³⁴⁵Student, Department of CSE, RTC Institute of Technology, Ranchi

¹Asst. Professor, Department of CSE(CS), RTC Institute of Technology, Ranchi

Email- satishkumar620609@gmail.com¹, binita_hinz@rtcit.ac.in^{1*}

Abstract

Brain-Computer Interfaces (BCIs) represent one of the most transformative technological advancements of the 21st century, enabling direct communication between the human brain and external devices. These systems are broadly categorized into invasive BCIs, which involve surgical implantation of electrodes into the brain, and non-invasive BCIs, which utilize external sensors such as EEG headsets. While BCIs offer revolutionary applications in healthcare, gaming, education, defense, and assistive technologies, they also generate highly sensitive neural data that raises serious privacy concerns. This paper presents a comparative study of data privacy measures in invasive and non-invasive BCIs. It examines data collection methods, security vulnerabilities, regulatory challenges, ethical concerns, and technical safeguards. The study finds that invasive BCIs require stronger privacy protection due to deeper neural access and continuous monitoring, whereas non-invasive BCIs face broader consumer-data risks because of easier adoption and cloud-based ecosystems. Brain data is the most intimate form of data; however, security protocols often lag behind hardware innovation. Recommendations are proposed for encryption, consent management, anonymization, zero-trust architectures, and international policy frameworks.

Keywords: Brain-Computer Interface, Data Privacy, Invasive BCI, Non-Invasive BCI, Neural Data Security, Cyber Ethics

1. Introduction

Brain-Computer Interfaces (BCIs) are systems that establish a direct communication pathway between the human brain and computers. BCIs interpret neural signals and translate them into commands that can control devices such as prosthetics, wheelchairs, computers, and smart systems.

BCIs are divided into two major categories:

Invasive BCIs – Implanted directly into the brain tissue through surgery.

Non-Invasive BCIs – Use external sensors placed on the scalp to capture brain activity.

As BCI technology advances, concerns regarding data privacy, ownership, surveillance, identity exposure, and cybersecurity are increasing. Neural data can reveal thoughts, emotions, health status, intentions, and behavioral patterns. Therefore, protecting such data is essential.

This paper compares privacy measures used in invasive and non-invasive BCIs and identifies best practices for secure deployment.

1.2 Types of Brain-Computer Interfaces

1.2.1. Invasive BCI

Invasive BCIs involve implantation of microelectrodes into the cortex.

Examples:

- Neural implants for paralysis treatment
- Deep brain stimulation interfaces
- Robotic arm control systems

Advantages:

- High signal quality
- Precise neural recording
- Fast response time

Privacy Risks:

- Continuous neural monitoring
- Health data leakage
- Remote hacking of implants
- Permanent identity-linked data storage

1.2.2 Non-Invasive BCI

Non-invasive BCIs use wearable sensors like EEG, MEG, or fNIRS.

Examples:

- EEG headsets for gaming
- Attention monitoring systems
- Mental wellness devices

Advantages:

- Low cost
- No surgery required
- Easy adoption

Privacy Risks:

- Cloud-based data collection
- Consumer profiling
- Third-party app misuse
- Weak device authentication

2. Literature Review

Recent studies have highlighted that neural data should be considered among the most sensitive categories of personal data.

- Invasive BCIs offer high signal precision but collect richer and continuous brain activity data.
- Non-invasive BCIs are commercially widespread and integrated with mobile/cloud platforms, increasing risks of unauthorized sharing.
- Researchers propose neuro-rights, including mental privacy, cognitive liberty, and identity protection.

The trajectory of Brain-Computer Interface (BCI) technology has undergone a seismic shift, evolving from specialized laboratory experiments designed for

clinical rehabilitation into a burgeoning sector of consumer electronics. Originally conceived as a "lifeline" for individuals with severe motor impairments or neurodegenerative diseases, BCIs are now being redefined as dynamic systems capable of augmenting human information-processing and everyday digital interaction [1]. The Clinical Foundation: Restoring Independence. For decades, BCI research was synonymous with medical intervention. These systems focused primarily on neurorehabilitation, helping patients regain lost functions such as communication and motor control after strokes or spinal cord injuries [1]. The clinical sector remains a dominant force, driven by the fact that over 3 billion people globally were affected by neurological conditions as of 2025 (Persistence Market Research, 2026). In this context, BCIs serve as critical assistive tools, with recent breakthroughs demonstrating that long-term functional electrical stimulation can significantly enhance neuroplasticity and functional recovery in elderly stroke patients [1]. The Commercial Leap: From Patient to Consumer By 2026, the BCI landscape has expanded beyond the hospital. The global BCI market is projected to reach \$2.0 billion in 2026, with a significant portion of this growth attributed to non-invasive technologies (Persistence Market Research, 2026). This shift is characterized by several key factors: Safety and Accessibility: Non-invasive BCIs, particularly those utilizing Electroencephalography (EEG), are expected to account for 58% of the market revenue in 2026 due to their portability and cost-effectiveness (Persistence Market Research, 2026). Beyond Restoration to Augmentation: Technology is moving toward "passive BCIs" that monitor user psychological states for applications in entertainment, gaming, and even intelligent lighting systems that adjust based on emotional data (Wang et al., 2026; Sciaraffa et al., n.d.). The AI Catalyst: The integration of deep learning and real-time signal decoding has been "the key that unlocks it all," allowing consumer devices to filter out electrical "noise" and accurately translate brain activity into digital commands (Panda International, 2025). The Emerging Challenge: Neuro-Privacy As BCIs transition into the hands of the general public, the nature of the data being collected has created a new frontier of risk. Unlike traditional biometric data, neural signals capture real-time cognitive and affective responses, potentially allowing for the interpretation of thoughts before they are even consciously expressed (New America, 2026). This shift from "research-grade" to "consumer-grade" technology necessitates a rigorous comparison of data

privacy measures, as the unrestricted access to brain signals in commercial applications presents a unique vulnerability to digital hackers (Wang et al., 2026; PMC, 2023).

3. Table-1: Comparative Analysis of Privacy Measures

Parameter	Invasive BCI	Non-Invasive BCI
Data Sensitivity	Very High	High
Signal Accuracy	High	Medium
Device Access	Restricted Medical Use	Consumer Accessible
Privacy Risk Level	Critical	High
Cybersecurity Need	Very Strong	Strong
Consent Complexity	High	Medium
Data Ownership Issues	Severe	Moderate
Real-Time Monitoring Risk	High	Medium

4. Major Data Privacy Threats

4.1 Unauthorized Access-Hackers or unauthorized users may gain access to confidential data through weak passwords, poor authentication, or system vulnerabilities.

4.2 Behavioral Profiling-Brain data may reveal preferences, stress levels, attention span, or emotions.

4.3 Medical Data Exposure-Invasive BCIs may expose neurological disorders, treatment records, or disability conditions.

4.4 Surveillance Risks-Employers, governments, or advertisers may misuse BCI data for monitoring users.

4.5 Consent Misuse-Users may not fully understand what data is collected or how long it is stored.

5. Privacy Protection Measures

5.1 End-to-End Encryption -All neural data should be encrypted during collection, transmission, and storage.

5.2 Differential Privacy-Adding statistical noise can protect identity while allowing research analysis.

5.3 Role-Based Access Control-Only authorized doctors, researchers, or users should access neural data.

5.4 Federated Learning-AI models can train locally without transferring raw brain data to cloud servers.

5.5 Consent Dashboards-Users should control permissions, revoke access, and monitor data usage.

5.6 Zero-Trust Security Architecture-Every access request must be continuously verified.

6. Ethical Considerations

- Mental autonomy must be preserved.
- Individuals should own their neural data.
- No manipulation of decisions using BCI analytics.
- Transparent AI algorithms should be used.
- Equal privacy rights for disabled users.

7. Regulatory Frameworks

Existing laws like GDPR, HIPAA, and data protection acts partly cover BCI data but are insufficient.

Needed Policies:

- Classification of neural data as sensitive biometric data
- Mandatory security certification for BCI devices
- Right to delete neural history
- Explicit informed consent standards
- Cross-border neural data restrictions

8. Proposed Comparative Privacy Model

Multi-Layer Security Framework

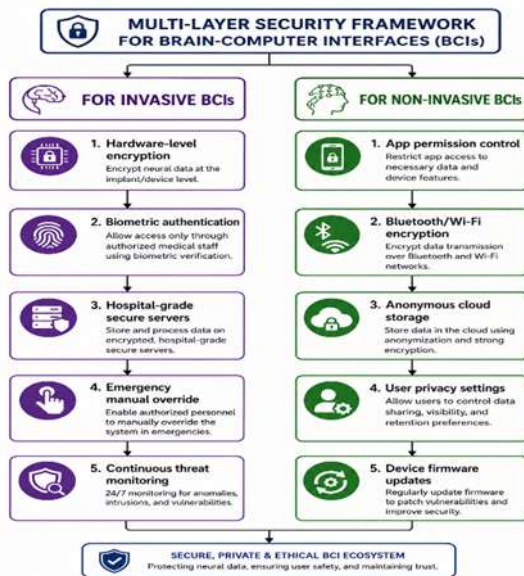


Figure-1: Multi-Layer Security Framework

9. Findings

Invasive BCIs demand stronger protection because they capture deeper and medically sensitive neural signals. Non-invasive BCIs face higher mass-market risks due to rapid commercialization. Current privacy laws are not fully prepared for neuro data governance. Technical solutions must be integrated with ethical and legal frameworks.

10. Conclusion

Brain-Computer Interfaces are reshaping human-machine interaction, but they also introduce unprecedented privacy challenges. Invasive BCIs present critical risks due to direct brain access and continuous monitoring, while non-invasive BCIs create scalable privacy threats through wearable ecosystems and consumer platforms. A comparative approach shows that privacy strategies must differ based on device invasiveness, signal depth, and deployment context. Strong encryption, transparent consent, user ownership of neural data, and dedicated neuro-rights legislation are essential for responsible BCI adoption. Future research should focus on privacy-preserving AI models and international standards for neural data governance.

11. References

- [1] Wang, Y., Ge, M., & Xu, S. (2026). Advances in brain-computer interfaces (BCI): Challenges and opportunities. *Biomimetics*, 11(2), 157. <https://doi.org/10.3390/biomimetics11020157>.
- [2] New America. (2026). *Brain-computer interfaces: Fundamentals and applications in commercial and medical contexts*. <https://www.newamerica.org/insights/the-rise-of-neurotech-and-the-risks-for-our-brain-data/>
- [3] Panda International. (2025). *BCI breakthroughs: Connecting brains and technology*. <https://www.panda-int.com/insights/inside-the-bci-race-how-a-global-push-to-bridge-minds-and-machines-is-taking-shape/>
- [4] Persistence Market Research. (2026). *Brain computer interface market size, share, and growth forecast, 2026 – 2033*. <https://www.persistencemarketresearch.com/market-research/brain-computer-interface-market.asp>
- [5] PMC. (2023). Brain-computer interface: trend, challenges, and threats. *PMC*, 10403483. <https://pmc.ncbi.nlm.nih.gov/articles/PMC10403483/>



Satish Kumar Verma is Final Year student, B. Tech in Computer Science and Engineering. The areas of interest include Artificial Intelligence, Brain-Computer Interfaces, Data Privacy, and Cybersecurity. They are actively involved in research and academic projects related to emerging technologies.



Diwakar Kumar Final Year student, B. Tech in Computer Science and Engineering. Their areas of interest include Artificial Intelligence, Brain-Computer Interfaces, Data Privacy, and Cybersecurity. They are actively involved in research and academic projects related to emerging technologies.



Nitish Kumar Final Year student, B. Tech in Computer Science and Engineering. Their areas of interest include Artificial Intelligence, Brain-Computer Interfaces, Data Privacy, and Cybersecurity. They are actively involved in research and academic projects related to emerging technologies.



Himanshu Kumar Final Year student, B. Tech in Computer Science and Engineering. Their areas of interest include Artificial Intelligence, Brain-Computer Interfaces, Data Privacy, and Cybersecurity. They are actively involved in research and academic projects related to emerging technologies.



Pintu Kumar Mehta Final Year student, B. Tech in Computer Science and Engineering. Their areas of interest include Artificial Intelligence, Brain-Computer Interfaces, Data Privacy, and Cybersecurity. They are actively involved in research and academic projects related to emerging technologies.