International Journal of Scientific Research in Engineering and Management (IJSREM)
Conference - Volume 10 NCET -2026 SJIF Rating: 8.659 ISSN: 2582-3930

SecureMind: A Multi-Layer Cybersecurity Framework for Future Brain–Computer Interfaces

A.N. Maryam[1]

[1] B.Sc. Information Technology and Cybersecurity
Department of Computer Science
Thassim Beevi Abdul Kader College for Women
maryamnikmath@gmail.com

J.A. Riswana Barvin[2]
[2] Co-Author

Abstract

Brain–Computer Interfaces (BCIs) are emerging technologies that enable direct communication between the human brain and digital systems. Future BCI applications may support immersive virtual environments for education, healthcare, communication, entertainment, and smart industries. At the same time, these systems may face cybersecurity threats, including unauthorized access, interception of brain signals, identity theft, malware, and privacy leakage. This paper proposes SecureMind, a conceptual multi-layer cybersecurity framework for protecting future BCI systems. The framework integrates Multi-Factor Authentication (MFA), secure communication, Artificial Intelligence (AI)-based threat detection, privacy protection, and emergency isolation. The proposed architecture is intended to provide coordinated protection across authentication, communication, monitoring, privacy, and incident-response stages. Because SecureMind is conceptual, its effectiveness remains to be validated through simulation and practical experiments using BCI devices.

Keywords: Brain–Computer Interface (BCI), Cybersecurity, Artificial Intelligence, Authentication, Privacy Protection, Secure Communication, Virtual Environment.

1. Introduction

Brain–Computer Interface (BCI) technology enables direct communication between the human brain and computers without relying exclusively on conventional input devices such as keyboards or controllers. Future developments in BCI technology may allow users to interact with immersive virtual environments through brain-derived signals. Such capabilities could support applications in healthcare, education, communication, remote work, entertainment, and other digital services.

The security requirements of these systems are particularly important because BCI communication may involve sensitive brain-related information and interactions with digital environments. A compromised BCI could expose information, permit unauthorized access, interfere with transmitted signals, or disrupt communication between the user and a virtual environment. Consequently, security should be considered as an integrated part of the BCI architecture rather than as a separate component.

To address this requirement, this paper introduces SecureMind, a conceptual multi-layer cybersecurity framework for future BCI environments. The framework combines user authentication, secure communication, AI-based threat detection, privacy protection, and emergency isolation within a unified architecture.

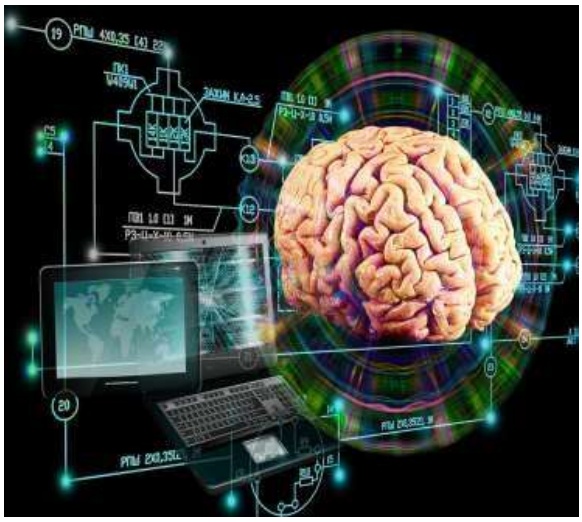


Figure 1. Conceptual architecture of a secure Brain–Computer Interface system connecting the human brain to immersive virtual environments.

2. Literature Survey

The source literature considered in this work indicates that BCI technology has been investigated for applications such as prosthetic control, assistance for people with neurological disorders, and human–computer interaction. These developments demonstrate the potential of BCI technology to support healthcare, communication, and immersive digital environments [1,4,5].

Alongside functional development, the security and privacy of brain-related information require careful consideration. The material reviewed for this conceptual framework identifies risks associated with unauthorized access, interception, manipulation of information, and privacy exposure. Cybersecurity guidance such as the NIST Cybersecurity Framework provides a general basis for organizing security activities, but the present work focuses specifically on a BCI-oriented multi-layer architecture [3].

Based on the reviewed material, existing approaches do not, within the scope of this paper, provide the complete combination of authentication, encrypted communication, AI-based threat detection, privacy protection, and emergency isolation proposed by SecureMind. The proposed framework therefore combines these security functions into one conceptual architecture. A detailed experimental comparison with individual security mechanisms is left for future work.

3. Problem Statement

Future BCI systems may become targets for cyberattacks because they process brain-related signals and may provide access to sensitive digital services. If an attacker compromises a BCI system, possible consequences include unauthorized access, manipulation of transmitted information, exposure of private data, and disruption of communication between the user and the virtual environment.

A further challenge is the absence, within the scope of this conceptual study, of a single security architecture that coordinates authentication, communication security, continuous threat monitoring, privacy protection, and emergency response. A multi-layer framework is therefore proposed to organize these functions into a coordinated security workflow.

4. Research Objectives

The main objectives of the proposed research are:

- To examine cybersecurity threats relevant to future Brain–Computer Interface systems.
- To design a multi-layer cybersecurity framework for BCI communication and digital interaction.
- To protect user privacy and the confidentiality of brain-signal communication.
- To incorporate Artificial Intelligence for continuous threat monitoring and cyberattack detection.
- To provide an emergency isolation mechanism for responding to detected security threats.
- To establish a conceptual foundation for future implementation and experimental evaluation of secure BCI systems.

5. Proposed SecureMind Framework

SecureMind consists of five coordinated security layers. Each layer addresses a different stage of the BCI security process, while the complete framework provides end-to-end conceptual protection.

Layer	Security Function	Purpose
Layer 1	Multi-Factor Authentication	Verifies authorized users before a BCI connection is established.
Layer 2	Secure Communication	Protects transmitted brain-signal data against interception or unauthorized modification.
Layer 3	AI-Based Threat Detection	Monitors communication activity and identifies suspicious or abnormal behaviour.
Layer 4	Privacy Protection	Protects sensitive brain-related information through encryption and controlled access.
Layer 5	Emergency Isolation	Disconnects the affected BCI connection when a cyberattack is detected and supports recovery procedures.

The five layers are intended to operate as a coordinated security chain. Authentication establishes user access control; secure communication protects data in transit; AI-based monitoring provides continuous threat observation; privacy protection controls sensitive information; and emergency isolation provides a response mechanism when a threat is detected.



Figure 2. Proposed SecureMind multi-layer cybersecurity architecture for protecting future Brain–Computer Interface communication.

6. Methodology

The proposed SecureMind framework follows a conceptual methodology for protecting future BCI systems. The workflow begins with brain-signal acquisition and proceeds through authentication, secure transmission, AI-based threat detection, privacy protection, and emergency response.

Step 1: Brain-Signal Acquisition

The user wears a BCI device that captures brain signals and converts them into digital data for subsequent processing and communication.

Step 2: User Authentication

Before a connection is established, the user is verified through Multi-Factor Authentication (MFA). This step is intended to restrict access to authorized users.

Step 3: Secure Data Transmission

The collected brain-signal data is protected using encryption and transmitted through a secure communication channel to reduce the risk of interception or unauthorized modification.

Step 4: AI-Based Threat Detection

An AI-based monitoring component continuously examines communication activity. Suspicious or abnormal behaviour is treated as an indication of a potential cyberattack requiring further response.

Step 5: Privacy Protection

Sensitive brain-related information is stored and accessed using encryption and access-control mechanisms intended to preserve confidentiality and privacy.

Step 6: Emergency Isolation

When a cyberattack is confirmed, the BCI connection to the virtual environment is disconnected and recovery procedures are activated to limit further impact.

7. System Workflow

SecureMind operates as a continuous security workflow in which authentication, protected communication, threat monitoring, privacy controls, and emergency response are coordinated. If the AI-based monitoring stage does not identify an attack, the communication proceeds toward the virtual environment. If a threat is detected and confirmed, the emergency-isolation mechanism interrupts the connection and initiates the response process.



Figure 3. SecureMind system workflow showing secure communication, AI-based threat monitoring, and emergency response.

8. Advantages of the Proposed Framework

Within the conceptual scope of this work, the SecureMind framework provides the following intended advantages:

- Provides multiple coordinated layers of cybersecurity rather than relying on a single security mechanism.
- Protects sensitive brain-signal and related information through secure communication, encryption, and access control.
- Restricts unauthorized access through Multi-Factor Authentication.
- Provides continuous AI-based monitoring for suspicious or abnormal communication activity.
- Includes an emergency-isolation mechanism to limit the impact of a confirmed cyberattack.
- Supports privacy-aware interaction with future virtual environments.
- Provides a structured foundation for future implementation and experimental evaluation of secure BCI systems.

9. Future Scope

The proposed SecureMind framework provides a conceptual foundation for cybersecurity in future BCI systems. Future work can extend the framework by integrating advanced Artificial Intelligence algorithms, blockchain-based identity management, quantum-resistant encryption, and real-time intrusion detection mechanisms.

The framework should also be evaluated using simulation environments and practical BCI devices. Such evaluation can examine security effectiveness, detection performance, communication overhead, response time, privacy protection, and system reliability. The framework may subsequently be studied in application contexts such as healthcare, education, defence, and smart-city environments, subject to appropriate technical and ethical requirements.

10. Conclusion

Brain–Computer Interface technology has the potential to transform human–computer interaction by enabling direct communication between the human brain and digital systems. However, the protection of brain-related information and secure communication is an important challenge for future BCI environments.

This paper presented SecureMind, a conceptual multi-layer cybersecurity framework designed to organize protection mechanisms for future BCI systems. The framework integrates Multi-Factor Authentication, Secure Communication, AI-Based Threat Detection, Privacy Protection, and Emergency Isolation within a unified architecture. The proposed workflow coordinates these layers from user authentication through secure communication and monitoring to emergency response.

SecureMind is currently conceptual and does not claim experimentally demonstrated performance. Its main contribution at this stage is the integration of the identified security functions into a single BCI-oriented architecture. Future simulation and practical experimentation are required to quantify its effectiveness, overhead, and suitability for real BCI applications.

References

1. Wolpaw, J. R., & Wolpaw, E. W. Brain–Computer Interfaces: Principles and Practice. Oxford University Press.
2. IEEE Brain Initiative. Brain–Computer Interface Research.
3. National Institute of Standards and Technology (NIST). Cybersecurity Framework (CSF) 2.0.
4. Journal of Neural Engineering. Research articles on Brain–Computer Interfaces.
5. IEEE Xplore Digital Library. Publications on Artificial Intelligence, Cybersecurity, and Brain–Computer Interfaces.