International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Security for Brain-Computer User Interface Requirements: A Review on Machine Learning-Driven Security Frameworks

Palak Singh
M.Tech (Computer Science & Engineering)
Amity University Uttar Pradesh, Lucknow, India

Abstract - Brain–Computer Interfaces (BCIs) enable direct communication between the human brain and external devices by converting neural signals into actionable commands. With rapid adoption in healthcare, assistive technologies, gaming, and defense, BCIs introduce critical security and privacy challenges. EEG-based systems process highly sensitive neural data, exposing users to risks such as identity leakage, behavioral inference, and unauthorized access. This paper presents a comprehensive review of security requirements in BCI systems, including confidentiality, integrity, authentication, availability, and privacy preservation.

The study further explores machine learning-driven security frameworks for detecting anomalies and adversarial behavior in neural signals. Various attack vectors such as spoofing, replay attacks, wireless interception, denial-of-service, and adversarial machine learning are analyzed. Performance metrics including accuracy, detection rate, and false alarm rate are discussed for evaluating system robustness. Finally, future research directions such as federated learning, differential privacy, and lightweight encryption for wearable BCIs are presented.

Keywords - Brain–Computer Interface, EEG, Machine Learning, Security, Privacy, Authentication, Anomaly Detection

I. INTRODUCTION

Brain–Computer Interface (BCI) technology establishes a direct communication pathway between human brain signals and external computing devices. These systems are widely used in assistive technologies, enabling individuals with disabilities to interact with machines using neural intent. However, the integration of machine learning and wireless communication introduces serious cybersecurity risks.

EEG signals contain highly sensitive personal information including emotional states, cognitive patterns, and neurological conditions. Unlike passwords, neural data cannot be easily changed if compromised. Additionally, adversarial machine learning attacks can manipulate model predictions, leading to unsafe system behavior. Therefore, ensuring secure and reliable BCI systems is a critical research challenge.

II. AIM AND OBJECTIVES

The aim of this paper is to analyze and evaluate security requirements in BCI systems and propose machine learning-driven solutions.

Objectives:
1. Identify security requirements in BCI systems
2. Analyze vulnerabilities in EEG-based architectures
3. Review ML-based anomaly detection techniques
4. Evaluate performance metrics
5. Suggest future research directions

III. REVIEW OF LITERATURE

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Recent studies highlight the emergence of neurosecurity as a critical domain. Researchers have demonstrated that EEG signals can leak sensitive user information. Machine learning models used in BCIs are vulnerable to adversarial attacks, data poisoning, and model extraction.

Authentication using EEG biometrics has shown promising results but suffers from variability issues. Encryption techniques provide communication security but fail to address ML-based attacks. Recent approaches include anomaly detection using autoencoders and LSTM networks, as well as federated learning for privacy preservation.

IV. METHODOLOGY

This study follows a structured approach analyzing the BCI pipeline including signal acquisition, preprocessing, feature extraction, classification, and transmission. Threat models such as spoofing, replay attacks, and adversarial ML are examined.

Machine learning techniques such as supervised classification, unsupervised anomaly detection, and deep learning models are analyzed. Performance evaluation is conducted using accuracy, detection rate, and false alarm rate.

V. RESULTS AND DISCUSSION

The analysis indicates that BCI security requires a multi-layered approach integrating encryption, authentication, and anomaly detection. Deep learning models provide high detection accuracy but require significant computational resources. Lightweight models are suitable for wearable devices but may compromise detection performance.

A balance between security and usability is essential. False alarms must be minimized while maintaining high detection rates. Hybrid frameworks combining ML and cryptographic techniques provide the most effective solution.

VI. FUTURE WORK

Future research should focus on developing robust adversarial defenses, lightweight ML models for edge devices, continuous authentication systems, and privacy-preserving learning techniques such as federated learning and differential privacy.

VII. CONCLUSION

BCI systems present unique security challenges due to the sensitivity of neural data and dependence on machine learning. This paper highlights the importance of integrating multi-layer security frameworks to ensure safe and reliable BCI deployment.

REFERENCES

[1] T. Bonaci et al., Cyber Security Threats in BCIs, 2014.
[2] S. Stober et al., EEG-based learning, 2016.
[3] M. Ienca et al., Neurosecurity ethics, 2016.
[4] A. Nguyen et al., Adversarial ML, 2015.