УДК 004.057.4
Titova A.M. student of group 125-22-2
(Dnipro University of technology, Dnipro, Ukraine)

SECURITY AND DATA PROTECTION IN BRAIN COMPUTER INTERFACE SYSTEMS

In recent years, there has been rapid development of Brain-Computer Interface (BCI) technologies that allow humans to interact with computers using brain signals. BCI creates new opportunities for people with physical disabilities in the fields of medicine, play, learning and communication. A Brain-Computer Interface (BCI) allows people to interact with computers directly using brain signals. Using sensors implanted in the brain or in the head, BCI reads the electrical activity of the brain and converts these signals into commands that can control external devices such as computers, prostheses or robotic systems [1-2].

Sensors that directly measure the electrical activity of the brain are the first component, non-invasive sensors that are attached to the scalp or invasive sensors that are implanted directly into the brain. Electroencephalography (EEG) electrodes, noninvasive sensors, measure electrical potentials generated by neural activity in the cerebral cortex through the scalp. However, invasive sensors such as microelectrode arrays or electrocorticographic (ECoG) electrodes directly measure electrical activity on the surface of the brain or in specific brain regions. Modern BCI signal amplifiers are extremely sensitive and have low intrinsic noise. They can also amplify brain signals thousands of times while preserving their basic functions. The third element is the signal processor, which can be a computer or other computing device that filters and analyzes the amplified brain signals to detect certain patterns of activity, a process known as feature extraction and uses various digital signal processing techniques and machine learning to identify unique characteristics signals that meet specific goals or user instructions.

Together, these four parts—sensors, signal amplifiers, a signal processor, and an output device—form a complete BCI system that enables direct communication between the brain and the world around it. BCI developers continue to improve these parts through cutting-edge research in engineering, neuroscience, and machine learning. They aim to create more powerful, reliable, and easy-to-understand brain-computer interfaces that could transform many aspects of human activity. BCI can record brain signals using various methods, such as electroencephalography (EEG), electrocorticography (ECoG), magnetoencephalography (MEG), and functional magnetic resonance imaging (fMRI). EEG, which measures electrical activity on the surface of the head using electrodes attached to the skin, is the most common method.

Secure data storage and management practices are also required to protect collected BCI data from unauthorized access or manipulation. For storing sensitive BCI data, it is best to use modern encryption algorithms such as AES or RSA. Role-based or permission-based access delimitation mechanisms must strictly control access to this data to allow only authorized individuals to view or modify the information. In addition, anonymization and data restriction techniques may be used to protect the privacy of BCI users. Anonymization means removing any personally identifiable information from a data set.

Establishing a strong ethical and regulatory framework to guide the development and use of these technologies is another important element of BCI security and privacy. As BCIs become increasingly sophisticated, clear standards and guidelines need to be established to ensure that they are used responsibly and ethically. Institutional ethics committees, government standards for monitoring research and BCI use, and professional codes of conduct can be established for this purpose [3-4].

Measures to ensure the security and privacy of BCI are already being implemented internationally. For example, the IEEE P2731 standard was developed by the Institute of Electrical and Electronics Engineers (IEEE) to ensure the secure and confidential collection, transmission, storage, and use of neurotechnology data. The goal of this standard is to create

uniform rules for BCI manufacturers, researchers, and healthcare professionals to protect user data and adhere to ethical principles.

The development of universal standards that can effectively address all security and privacy concerns is complicated by the rapid development of technology and the variety of potential applications of BCI. In addition, achieving international consensus on the effective management of BCI can be difficult as a result of differences in cultural values, ethical norms and legal systems of different countries [1,5-6].

Although Brain-Computer Interface (BCI) technology has many opportunities to improve people's lives and poses many risks and safety concerns, it also needs to be carefully studied. A BCI uses sophisticated software to process and interpret brain signals, so any flaws or errors in it can be used by hackers to gain unauthorized access, manipulate data, or seize control of the system. For example, attackers can install hidden backdoors or "parasites" of the BCI software so that they can secretly control the BCI system.

Physical attacks and tampering can also affect BCI hardware parts such as processors, signal amplifiers, and sensors. Adversaries may attempt to compromise or physically interfere with the BCI hardware to steal sensitive data or alter system functionality. For example, commercially available BCI devices may be vulnerable to third-party attacks that use electromagnetic leakage or power consumption to collect personal user data.

CONCLUSION

Development of more advanced methods of encoding and obfuscating BCI data to protect user privacy is another promising area of research. Although traditional encryption methods such as AES or RSA are extremely secure in transit and storage, they can also be vulnerable to attack if there is sufficient computing power or access to encryption keys. Processing and analysis of BCI data is possible using more advanced cryptographic techniques, such as homomorphic encryption or secure multiparty computation, storing it in encrypted form, reducing the risk of compromising privacy.

REFERENCE

1. Abiri R, Borhani S, Sellers EW, Jiang Y, Zhao X. A comprehensive review of eeg-based brain-computer interface paradigms. J Neural Eng. 2019;16:011001. doi: 10.1088/1741-2552/aaf12e.

2. Mudgal SK, Sharma SK, Chaturvedi J, Sharma A. Brain computer interface advancement in neurosciences: applications and issues. Interdiscip Neurosurg. 2020;20:100694. doi: 10.1016/j.inat.2020.100694.

3. OLISHEVSKYI I.H. Substantiation of energy efficiency of automated heating technology at HPS / OLISHEVSKYI I.H., // Електротехніка та електроенергетика. / Запорізький нац. ун-т «Запорізька політехніка». – Запоріжжя, 2024. – № 2. – С. 36-43 https://doi.org/10.15588/1607-6761-2024-2-4

4. OLISHEVSKYI I.H. (2024). DATAWARE AND SOFTWARE OF THE AUTOMATED TECHNOLOGY FOR COMPUTER-INTEGRATED CONTROL OF HEAT PUMP SYSTEMS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (2), 205–212. https://doi.org/10.31891/2219-9365-2024-78-23

5. OLISHEVSKYI I.H. (2024). RESULTS OF DEVELOPMENT AND RESEARCH OF THE TECHNOLOGY FOR AUTOMATED ENERGY-EFFICIENT CONTROL OF HEAT PUMP SYSTEMS BY MEANS OF COMPUTER EXPERIMENT. Herald of Khmelnytskyi National University. Technical Sciences, 335(3(1), 419-428. https://doi.org/10.31891/2307-5732-2024-335-3-58

6. Peksa J, Mamchur D. State-of-the-Art on Brain-Computer Interface Technology. *Sensors*. 2023; 23(13):6001. https://doi.org/10.3390/s23136001