Neurochain: A Blockchain-Secured Framework for BCI-Based Smart Home Automation

Avram Brînduşa
Faculty of Engineering in Foreign Languages
University of Politehnica of Bucharest
Bucharest
trufan_brindusa@yahoo.com

Raluca Purcaruș
Faculty of Engineering in Foreign Languages
University Politehnica of Bucharest
Bucharest
raluca.purcarus@sts.net

Bianca Ebrasu
Faculty of Engineering in Foreign Languages
University Politehnica of Bucharest
Bucharest
bianca.ebrasu@gmail.com

Abstract— Brain-Computer Interfaces (BCIs) enable direct communication between the brain and external devices, unlocking new interaction paradigms. This paper proposes an integrated system that combines BCIs, smart home automation, and blockchain technology. The system provides secure, decentralized, and biometric-based control of home environments using cognitive commands. We outline the system architecture, explore challenges in signal processing, and examine how blockchain ensures data integrity, access control, and event traceability. Our proposed model enables secure, accessible, and privacy-preserving smart home solutions for users, including those with limited mobility.

Keywords— Brain-Computer Interface (BCI), Smart Home, Blockchain, Cognitive Control, Secure Automation

I. INTRODUCTION

The convergence of neurotechnology, Internet of Things (IoT), and distributed systems is enabling innovative human-computer interactions. BCIs offer a non-muscular communication pathway, while smart home environments aim to improve comfort, efficiency, and accessibility. However, the adoption of these systems introduces new concerns regarding privacy, trust, and control. Blockchain provides a tamper-proof ledger and decentralized access management. This paper explores a novel integration: using BCI for smart home control, with blockchain ensuring secure authentication and traceable execution [1], [2].

II. THEORETICAL FOUNDATIONS AND RELATED WORK

A. Brain-Computer Interfaces: Trends and Innovations

Recent advances in neural decoding have made BCIs more accessible, robust, and adaptable to real-world applications. Studies have shown successful use of EEG-based systems in detecting motor imagery, visual stimuli, and emotional states [1], [3]. The intersection of BCI with AI has enhanced signal classification through deep learning models such as convolutional neural networks (CNNs) and long short-term memory (LSTM) networks.

B. Cognitive IoT in Smart Environments

The concept of Cognitive IoT (CIoT) integrates AI-driven decision-making with connected devices, creating responsive and context-aware smart homes. CIoT aims to reduce user interaction complexity by inferring intentions through implicit inputs like brain signals or biosignals.

C. Decentralization and Trust in Home Automation

Traditional smart home systems rely heavily on centralized platforms, posing risks of data breaches and unauthorized access. Blockchain's decentralized nature addresses these limitations by offering immutable records and transparent access control. Smart contracts further enable autonomous and conditional execution of commands [2], [5].

III. PROPOSED RESEARCH FRAMEWORK

This paper introduces a conceptual framework where BCI input serves as a secure, cognitive-based control mechanism within a smart home system reinforced by blockchain. The novelty lies in merging:

- **Biometric-based authentication via EEG signatures** [4], which ensures that only authorized users—recognized by their unique brainwave patterns—can initiate control commands within the environment.
- **Decentralized access control and command logging using blockchain** [5], which eliminates single points of failure and provides a tamper-proof, chronological record of all user interactions.
- **Neural-driven interaction with connected home devices**, enabling hands-free, context-aware control over lighting, temperature, entertainment, and security systems.

The research investigates how BCI signal confidence, command accuracy, and user identity can be embedded into blockchain transactions to create a secure, verifiable command structure. In this model, each BCI-derived action is hashed and stored as a smart contract execution or a signed transaction on the blockchain ledger, linking intent, execution, and user authentication into a unified audit trail.

We further explore how blockchain can act as a mediator between privacy constraints and command traceability. For example, sensitive EEG data are never stored directly on-chain; instead, the blockchain references hashed summaries or encrypted data pointers stored off-chain (e.g., in IPFS).

This ensures that users maintain full privacy while still enabling forensic auditing of command history. Additionally, permissioned blockchain architectures (e.g., Hyperledger Fabric) are evaluated for their ability to offer fine-grained access control and scalability within smart home networks.
This hybrid BCI–blockchain system not only enhances security through multi-factor cognitive authentication but also establishes an immutable trust layer for all neural interface commands. As cognitive computing continues to advance, such architectures may pave the way for fully autonomous, human-centered smart environments.

IV. Experimental Design and Evaluation Criteria

To validate the proposed framework, future work will focus on a series of experimental objectives. First, signal processing evaluation will be conducted by benchmarking classification accuracy across multiple user sessions and assessing the system's robustness against noise and external interference. Second, blockchain performance metrics will be analyzed by measuring the latency of smart contract executions initiated by BCI commands and evaluating the system's scalability in multi-user scenarios with concurrent requests. Third, user experience and accessibility will be examined through usability testing with individuals who have limited mobility, as well as by assessing cognitive workload using tools such as NASA-TLX or EEG-based workload indicators. Insights from these evaluations will guide the development of a prototype platform for further testing and refinement.

V. Conclusion

This paper presents a secure, decentralized system integrating BCI, smart home, and blockchain technologies. By harnessing neural input and distributed authentication, we envision future smart environments that are accessible, private, and resilient. The proposed architecture serves as a blueprint for cognitive-based automation in next-generation IoT ecosystems.

References

[1] L. F. Nicolas-Alonso and J. Gomez-Gil, "Brain computer interfaces, a review," *Sensors*, vol. 12, no. 2, pp. 1211–1279, 2012.

[2] The Linux Foundation, "Hyperledger Architecture White Paper," 2021.

[3] A. Bashashati et al., "A survey of signal processing algorithms in brain-computer interfaces based on electrical brain signals," *Journal of Neural Engineering*, vol. 4, no. 2, pp. R32–R57, 2007.

[4] OpenBCI, "OpenBCI Documentation," [Online]. Available: https://docs.openbci.com/

[5] W. Lin et al., "Blockchain-based authentication and authorization for smart homes," *IEEE Access*, vol. 8, pp. 11794–11801, 2020.