biomimetics

Article

BCI Cybersecurity for Neurohaptics Telekinesis Avatars

Adriano Cavalcanti [1,2,*], Yash J. Patel [1,2], John Knudson [1,2], and Wei-Ying Hsaio [3]

[1] Brain-Computer Interface Laboratory, Department of Computing, Informatics and Data Science, St. Cloud State University, St. Cloud 56301, USA;
[2] Cloud Computing Club, St. Cloud State University, St. Cloud 56301, USA;
[3] School of Education, University of Alaska-Anchorage; Anchorage AK 99508, USA
* Correspondence: adriano.cavalcanti@stcloudstate.edu

Abstract

The convergence of Brain-Computer Interfaces (BCI) and neurohaptics represents a transformative frontier in biomimetics, where the central objective is to replicate the seamless integration of biological control and sensory feedback. This research draws direct inspiration from the brain's intrinsic architecture to address point towards the future for brain detanglement and neural restoration. By applying biomimetic principles to brain hardware restoration and nanotechnology neural repair, this paper proposes a framework that transcends simple interfacing; it provides the pathway to restore and emulate the brain's natural functional geometry. Such a bio-inspired approach ensures that the digital-to-biological transition is grounded in the trifecta perfect geometry of the nervous system's endogenous electrical foundations. Ultimately, the BCI EEG system relies on these fundamental biological principles to decode the complex, living symphony of human neural activity. At the forefront of human-computer interaction, Brain-Computer Interface (BCI) technology is redefining system integration, enabling a future where the Internet of Things (IoT) and robotic systems are seamlessly controlled by neural intent. As BCI-integrated systems shape the future internet, real-time distributed solutions will increasingly rely on AI and machine learning (ML), orchestrated through users' thoughts. This article presents an open-source automation platform designed for BCI systems, developed in compliance with data privacy regulations. By streamlining documentation and protecting neural data through RSA-based encryption and automated file management, the platform enhances security and accountability while ensuring participant confidentiality.A comprehensive case study demonstrates the platform's capabilities through an "Avatar" system that integrates Unmanned Aerial Vehicles (UAVs) and humanoid robotics using a dataset of over 4,000 EEG readings. The framework utilizes a dual-stream video architecture to facilitate immersive telepresence, bridging the gap between remote aerial sensing and localized human presence. This implementation is driven by the fundamental belief that human thoughts, when mapped through BCI-driven kinematics, possess the physical power to move and interact with the world. The open-source software solution—supporting PyTorch, TensorFlow, and JAX—is available on GitHub, providing a scalable foundation for brain-cloud connectivity and neuroscientific innovation.

Academic Editor: Firstname Lastname

Received: 19 December 2025
Revised: date
Accepted: date
Published: date

Citation: To be added by editorial staff during production.

Keywords: integrative medicine, robotics, nanotechnology, artificial intelligence, biomedical computing, big data analytics, biomimetics, brain-computer interfaces, cloud computing, clinical trial, ethics and regulatory frameworks, augmented humans, new integrative science, biohybrid systems, immersive reality, avatar, quantum computing, quantum blockchain.

1. Introduction

Distributed AI is crucial for BCI avatars as it enables real-time processing, analysis, and interpretation of brain signals, allowing for seamless interaction between the user's brain and the avatar. This is made possible by the fast processing of brain signals, decoding of complex patterns and intentions, and adaptability to individual users' brain activity patterns. To support this, cloud computing plays a vital role in implementing BCI avatar solutions, providing scalable infrastructure to handle large amounts of brain signal data, high-performance computing capabilities for complex AI model training and deployment, and vast data storage for analysis and model training. Additionally, cloud-based platforms facilitate seamless collaboration among researchers, developers, and users. By leveraging cloud computing, BCI avatar solutions can process large datasets, train complex models for brain signal analysis, and provide real-time feedback to users, ultimately enhancing the overall experience. In essence, the combination of Distributed AI and cloud computing enables effective implementation and deployment of BCI avatar solutions.

*1.1. **Motivation and Outlook***

Human-Computer Interaction (HCI) is a rapidly evolving field that focuses on designing intuitive and user-friendly interfaces to make technology more accessible and enjoyable for everyone. With the increasing integration of technology in our lives, HCI is experiencing significant growth, and its market is projected to reach $1,663.88 billion by 2030, growing at a Compound Annual Growth Rate (CAGR) of 15.4%. HCI encompasses various aspects, including user experience (UX) design, interface prototyping, data analysis, and accessibility, making it a multidisciplinary field that combines principles from computer science, design, psychology, and engineering. Professionals with expertise in HCI are in high demand across industries like technology, healthcare, finance, manufacturing, retail, and education, with median salaries ranging from $110,000 to over $200,000 per year, depending on specialization and location. Emerging trends in HCI include natural language processing, voice assistants, gesture-based interfaces, virtual reality (VR), and augmented reality (AR), which are transforming the way we interact with technology. Moreover, the trajectory of Human-Computer Interaction (HCI) is being fundamentally reshaped by cutting-edge advancements in Brain-Computer Interfaces (BCIs) [1]. These systems leverage advances in EEG brain mapping (Figure 1-1) to enable direct neural control of external devices, thereby revolutionizing traditional interaction paradigms. HCI applications currently span a broad spectrum, ranging from ubiquitous consumer electronics to complex industrial systems, encompassing user interface (UI) design, data visualization, control mechanisms, alarm management, and remote access. The significance of HCI resides in its capacity to optimize user experience, bolster

Figure 1. Differential Cortical Activation Demonstrating Task-Dependent Changes in Brain Activity.

productivity, and enhance accessibility—factors essential to contemporary technological development. By prioritizing HCI, organizations can engineer more intuitive and effective products, fostering customer loyalty and securing a competitive market advantage [2]. Furthermore, BCIs are poised to facilitate breakthroughs for individuals with disabilities, augment human cognition, and redefine the boundaries between biological and digital systems. As miniaturized devices and emerging technologies continue to evolve [3], brain-computer interfaces represent the next frontier, harnessing neural potential to transform the human-technology relationship while unlocking substantial commercial opportunities [4].

The concept of Brain Computer Interfaces (BCIs) has undergone significant transformations since its beginnings in the 1960s and 1970s. Early systems used implantable electrodes to read neural signals, mainly for medical research and helping paralyzed patients control devices [5],[6],[7]. However, the risks associated with these invasive methods, such as infection and stability issues, led to a shift towards non-invasive alternatives [8]. EEG-based BCIs, which use electroencephalography to detect brain activity, have become increasingly popular due to their safety, affordability, and ease of use. While they may not be as precise as invasive methods, advancements in AI and signal processing have greatly improved their functionality. Today, EEG-based BCIs are being applied in various fields, including healthcare, gaming, and marketing, revolutionizing the way we interact with technology.

Human-Computer Interaction (HCI) is a rapidly evolving field that focuses on designing intuitive and user-friendly interfaces to make technology more accessible and enjoyable for everyone. With the increasing integration of technology into our daily lives, HCI is experiencing significant growth, and its market is projected to reach US$6 billion by 2030, growing at a Compound Annual Growth Rate (CAGR) of 17.2% [4]. HCI encompasses various aspects, including user experience (UX) design, interface prototyping, data analysis, and accessibility, making it a truly multidisciplinary field that combines principles from computer science, design, and psychology. As technology continues to advance, the principles and innovations of HCI will be critical in ensuring that the digital world remains human-centric, effective, and inclusive (Figure 2).

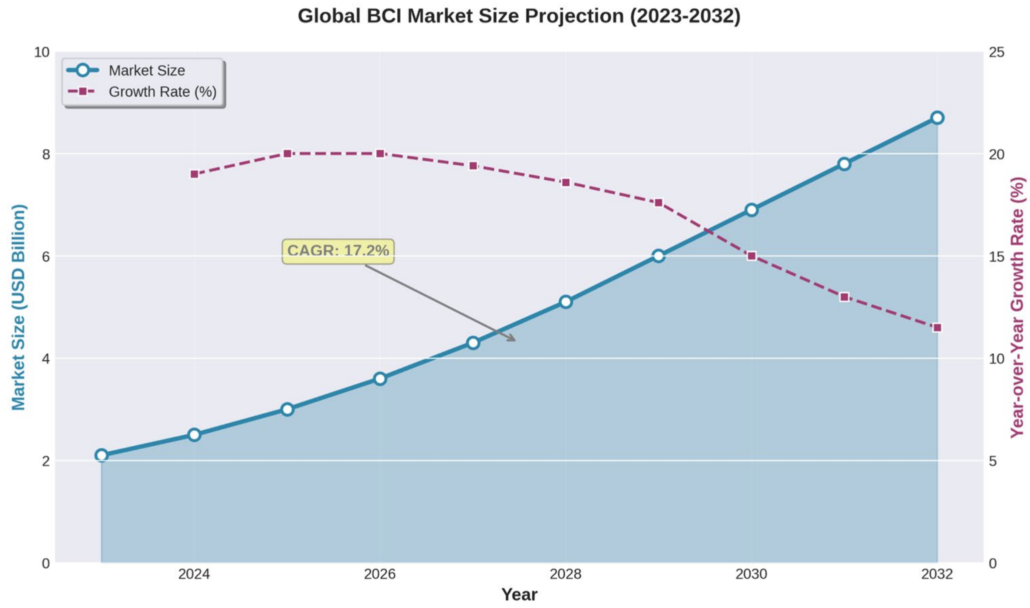

Figure 2. Detailed Forecast of Annual Market Size Growth from 2024 to 2032.

1.2 Current Development

The EEG market is poised for explosive growth, with a projected annual surge of 7.8% through 2030 [4],[9]. This boom is driven by breakthroughs in brain-computer interfaces, electrode tech, and non-invasive solutions. At the forefront of this revolution are companies like Neuralink, Meta, Emotiv, and NeuroSky, which are harnessing the power of brain signals to transform industries like healthcare, gaming, and augmented reality. Google is also exploring brain-computer interfaces, having announced a groundbreaking non-invasive technology that uses electroencephalography (EEG) and near-infrared spectroscopy (NIRS) to measure neural activity. This technology allows users to control devices with their thoughts, potentially revolutionizing human-computer interaction.

The US military is also getting in on the action, with DARPA researching brain-controlled drones and other cutting-edge applications [10]. By decoding brain activity, BCIs are shattering traditional boundaries between humans and machines. For people with disabilities, this technology is a lifeline, offering unprecedented control over prosthetics, communication devices, and more. As BCIs continue to evolve, they're unlocking new possibilities for both everyday life and medical breakthroughs [6].

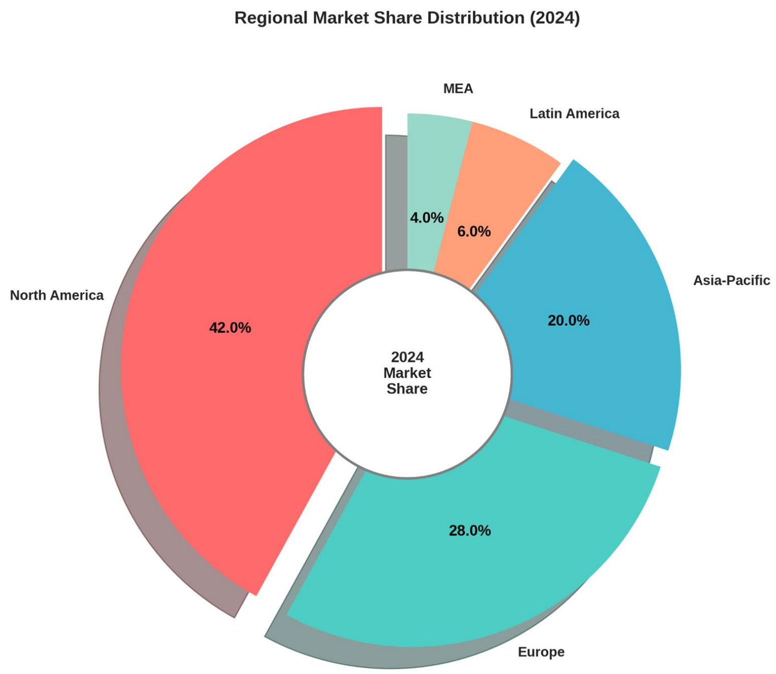

Figure 3. Present Market Share Segmentation Across BCI Application Categories.

Recent developments in the field include [11],[12],[13]:

- **Key Players:**
  Neuralink: Developing implantable brain-machine interfaces to treat medical conditions, with a job opening for a machine learning engineer.
  Synchron: Backed by Jeff Bezos and Bill Gates, this Australian startup is accelerating BCI development.
  Meta: Showcasing new neural interface tech and building brain-computer interfaces for typing and skin-hearing.
  Google: Exploring non-invasive BCIs that use EEG and NIRS to measure neural activity.
- **Market Projections:**
  The Brain Computer Interface Market is expected to reach $7,419.0 million by 2033.
  Another projection suggests the market will be worth $12.40 billion by 2034.
- **Applications:**
  Key sectors will benefit directly from BCI, including but not limited to
  Healthcare: BCIs are being explored for treating medical conditions and assisting individuals with disabilities.
  Gaming: Neurotechnology is enhancing gaming experiences.
  Military: DARPA is researching brain-controlled drones and other applications [1] [2].

The rapid expansion of the Brain-Computer Interface (BCI) market is catalyzed by significant advancements in neurotechnology, substantial capital investment from major technology corporations, and a diversifying range of applications across global regions (Figure 3) and industrial sectors (Figure 4). As these technologies mature, further innovations are anticipated to fundamentally redefine the paradigms of human-computer interaction [14],[15].

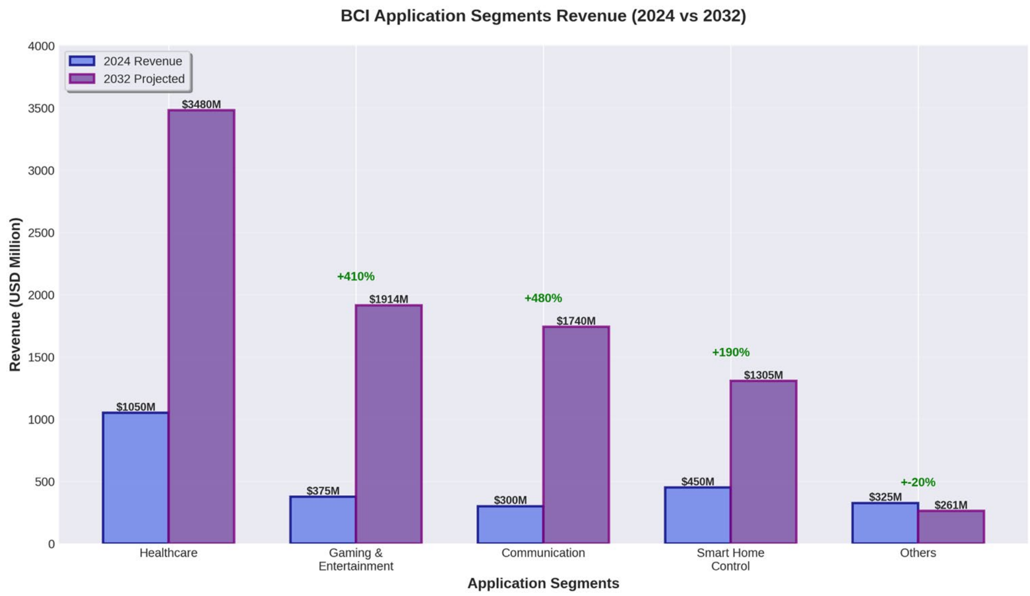

Figure 4. Projected BCI Market Growth Across Specific Social and Economic Sectors.

1.3 Brain Detanglement

Neuro-homeostasis is a multidimensional, synergistic process essential to neural recovery, categorized into **Hardware Restoration** (biochemical integrity) and **Software Entrainment** (brain tuning, memory defragmentation, mind compiling and debugging) [16]. This framework posits that cognitive clarity is a function of maintaining organic structures while simultaneously harmonizing their electromagnetic signatures with universal mathematical constants.

1.3.1 Brain Hardware Restoration

At the physiological level, restoration focuses on the **pineal gland**, the brain's primary neuroendocrine transducer. Residing outside the blood-brain barrier, the pineal gland is uniquely susceptible to pathological calcification—often via mineral accumulation and fluoride—which creates dielectric interference in hormonal signaling [17]. To mitigate this, we propose a "Detox Stack" centered on molecular sequestration and enzymatic dissolution:

- **Molecular Sieves:** Utilizing Zeolite and Activated Charcoal to sequester heavy metals [18].
- **Proteolytic Dissolution:** Application of Nattokinase and Bromelain to address the fibrin-calcium matrix [19].
- Gut-Brain Modulation: Supplementation with *L. reuteri* to optimize the biosynthetic supply of serotonin and GABA, the precursors for melatonin-driven systemic repair [20].

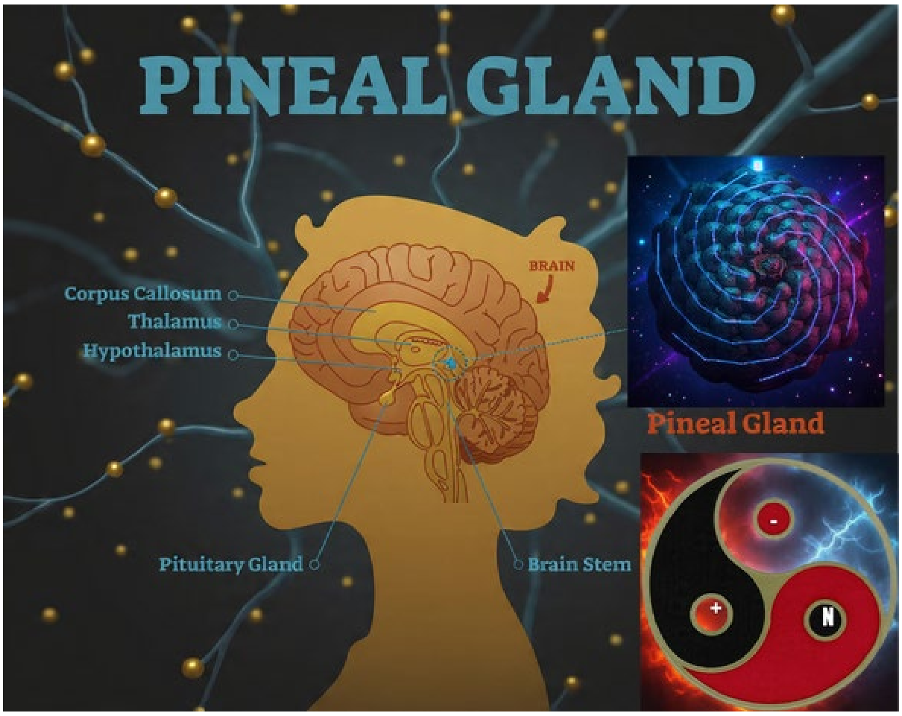

Figure 5. Brain integrative tuning through hardware restoration and software entrainment.

1.3.2 Mind Software Entrainment

Parallel to biochemical maintenance is the synchronization of neural oscillations. This framework utilizes the **Fibonacci sequence** and **3-6-9 numerical theory** to establish a resonant baseline for neuro-optimization [21]. By initiating Fibonacci-based protocols at a base frequency of 3, the model aligns with Solfeggio scale roots (e.g., 528 Hz and 963 Hz).

These mathematical ratios mirror the fractal architecture of the human cochlea and the pineal gland, facilitating acoustic propagation with minimal impedance [22]. Utilizing **Hemispheric Synchronization (Hemi-Sync)**, the brain can be guided into **Theta (4–8 Hz)** states. This allows for "conscious wakefulness," emulating the entropy-reducing benefits of slow-wave sleep (SWS) while maintaining functional alertness [23].

1.3.3 Nanotechnology Neural Repair

Biomimetic integration further explores engineered gold nanoparticles (AuNPs) as catalysts for energy restoration. Unlike commercial "ORMUS" or monoatomic gold, precisely engineered AuNPs (e.g., CNM-Au8) offer targeted therapeutic effects:

- **Metabolic Enhancement:** Reversing deficits in ATP production to improve nerve function [24].
- **Neurogenesis:** Electromagnetized AuNPs promote the creation of new neurons in aged substrates [25].
- **Synaptic Synchronization:** Nanostructured gold electrodes enhance neural network formation and signal coherence in BCI interfaces [26].

1.3.4 Trifecta Perfect Geometry

The concept of a "trifecta" (Positive, Negative, Neutral) finds its technical equivalent in BCI signal acquisition (Figure 5). This relationship is often represented by the **Gankyil (Triple Yin-Yang)**, symbolizing the interdependence of energy in motion.

1.3.4.1 BCI Electrical Foundation

In BCI systems, the "trifecta" is essential for isolating neural intent from environmental noise [27]:

1. **Active (Signal):** Captures the fluctuating ionic potential of firing neurons.
2. **Reference (Differential):** Provides a baseline to calculate the difference and isolate brain activity.
3. **Ground (Neutral):** Ensures system stability and prevents electrical interference.

1.3.4.2 Geometric Signal Processing

While the Fibonacci sequence is not the "cause" of electricity, it appears in the study of ladder networks where total equivalent resistance converges toward the **Golden Ratio [28]**. In BCIs, "Geometric Machine Learning" uses these recursive structures to map high-dimensional brainwave data into low-dimensional manifolds, effectively "detangling" the signal from entropy [29].

1.3.5 Signal Entropy Mitigation

Systemic resilience requires the active avoidance of "Signal Disruptors" that increase cognitive load:

- **Acoustic Entropy:** Dissonant ratios (e.g., the Tritone, 2:1) that induce neural dissonance and metabolic exhaustion.
- **Electromagnetic Entropy:** RF/EMF interference that decouples the brain from the **Schumann Resonance (7.83 Hz)** [30]

1.3.6 Killing Burnout

The integrated approach through the Tesla Model of Resilience shifts the paradigm of neural recovery from passive rest to active, frequency-based restoration. By combining pineal decalcification (Hardware) with Fibonacci-based entrainment (Software), this simplistic approach provides a blueprint for non-invasive neuro-rehabilitative technologies. Future applications in BCI may utilize targeted transcranial stimulation to replicate these constants, offering a scalable method for mitigating burnout and enhancing cognitive endurance.

1.4 BCI Quantum Computing

The intersection of neurotechnology and quantum informatics represents a transformative frontier. **Integrating Brain-Computer Interfaces (BCI) with Quantum Computing is the realization of "Quantum Neuro-Informatics"—a framework where the non-linear, stochastic nature of neural firing is mapped directly onto quantum states.** While still in early developmental stages as of late 2025, this synergy focuses on using quantum algorithms to enhance the speed and accuracy of neural signal decoding.

1.4.1 Core Research Areas

- **Quantum Machine Learning (QML) for Biosignals**: Researchers are developing hybrid quantum-classical neural networks, such as **quEEGNet**, to process electroencephalogram (EEG) data [31]. These models leverage quantum variational principles to classify brain states more efficiently than traditional classical methods.

- **Cognitive Analysis**: Quantum neural networks (QNNs) are being explored to understand brain functions and diagnose neurological disorders by categorizing brain signals into distinct frequency bands with higher precision.
- **Neuro-Prosthetics & Stimulation**: Quantum AI is envisioned for high-speed control of neuro-prosthetics, where real-time processing of neural intent is critical for natural movement.

1.4.2 Key Benefits

- **Complex Pattern Recognition**: Quantum computers use **superposition** and **entanglement** to evaluate vast combinations of neural firing patterns simultaneously, which may eventually solve the "noise" problem in BCI data that currently limits reliability [32].
- **Dimensionality Reduction**: The brain's high-dimensional data is a natural fit for quantum systems, which can map complex relationships in a Hilbert space more effectively than classical processors.

1.5 Qubits for BCI

Traditional Brain-Computer Interfaces (BCIs) face a fundamental scaling bottleneck: the classical decoding of high-dimensional, stochastic neural signals in real-time. In 2025, quantum computing, underpinned by the **qubit**, has emerged as a transformative cornerstone for BCIs by providing a computational framework that inherently mirrors the complex, non-linear dynamics of biological neural networks.

1.5.1. Quantum-Enhanced Signal Decoding and Parallelism

Biological neural processes are characterized by massively parallel, probabilistic interactions [33].

- **Superposition and State-Space Representation:** Utilizing qubits allows for the representation of exponential state-spaces, enabling BCI systems to model complex neural feedback loops that are computationally intractable for classical architectures.
- **Parallel Processing:** The inherent parallelism of quantum gates allows for the simultaneous analysis of multi-channel neural data, significantly reducing latency—a critical requirement for the seamless control of high-degree-of-freedom neuroprosthetics.

1.5.2 Quantum Computing

The integration of **Quantum Neural Networks (QNNs)** represents a biomimetic evolution of artificial intelligence.

- **Pattern Recognition:** Recent 2025 breakthroughs, such as **QEEGNet**, demonstrate that hybrid quantum-classical models can extract subtle features from "noisy" electroencephalogram (EEG) signals with significantly higher precision than traditional deep learning [31].
- **Noise Modeling:** Quantum noise may more faithfully mirror the inherent randomness of ion channel activity, allowing for more robust neural "emulation" rather than mere simulation.

1.5.3. Quantum Tunneling Sensors

A primary barrier in BCI research is the "skull barrier," which attenuates high-frequency neural signals.

- **Signal Detection:** Research in 2025 indicates that **quantum tunneling**—the passage of particles through potential barriers—can be leveraged to detect weak, deep-brain electromagnetic fields without invasive surgical implantation [34].
- **Subcortical Access:** This mechanism potentially enables high-resolution acquisition from subcortical regions, expanding the therapeutic scope of non-invasive BCIs to include complex neurodegenerative and psychiatric conditions.

1.5.4 Quantum Deployment

- **Nascent Industry**: While theoretical frameworks exist, widespread practical demonstration of QML-assisted BCI systems is still limited.
- **Hardware Constraints**: Current quantum processors (typically 100–1,000 qubits) face high error rates and decoherence, making it difficult to run the long-duration algorithms required for continuous BCI monitoring.
- **Post-Quantum Readiness**: Financial institutions and cybersecurity firms are concurrently focused on "post-quantum readiness" to protect sensitive data from future quantum-enabled decryption attacks.

1.6 Quantum Blockchain

The integration of quantum blockchain into BCI architectures represents a critical shift from reactive encryption to **proactive physical defense**. By transcending the mathematical vulnerabilities of the silicon era, we ensure that the transition to "brain-to-brain" synchronization is grounded in a framework of **Information-Theoretic Security**. In classical blockchain architectures, the integrity of neural records is maintained by "majority rules" consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS). This reliance creates a vulnerability to **51% attacks**, where an adversary gaining control of the majority of network resources could retroactively rewrite neural transaction histories or manipulate the "neural digital twin."

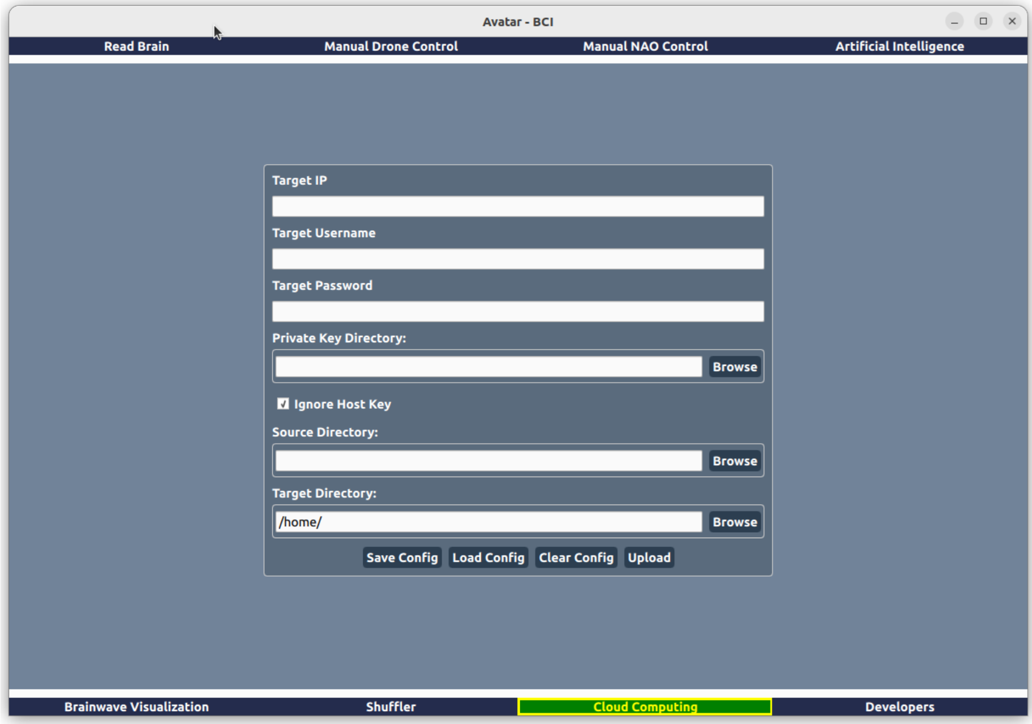

Figure 6. Cloud Connectivity Interface Facilitating the Transmission of Brainwave Data to the S3 Data Bucket.

1.6.1 Quantum-Linkage 357

A "True Quantum Blockchain" replaces classical cryptographic hashing with **Temporal Quantum Entanglement [35]**. In this paradigm, blocks are not merely digitally signed; they are physically linked through a history of entangled photons. 358

- **Entangled Chronology:** Utilizing **entanglement swapping**, a current block can be entangled with a preceding block that has already been measured or "consumed." This creates a chronological record where the present state of the BCI ledger is fundamentally dependent on its antecedent quantum states. 361
- **Physical Immutability:** To alter a record of brain-to-brain communication, an attacker would need to manipulate a quantum state that no longer exists in its original form. Under the **No-Cloning Theorem**, it is physically impossible to perfectly replicate or retroactively forge these quantum states [36]. 365

1.6.2 Resilience to Consensus Attacks 369

Within a BCI network secured by temporal entanglement, security is governed by physical laws rather than computational difficulty: 370

Figure 7. Transmission of Brainwave Data to Cloud Storage with Secure Encryption for Thought Streaming and Privacy Protection.

1. **Tamper Evidence:** Any attempt to retroactively modify neural data necessitates an alteration of the entangled history. Such an intervention violates **Bell's Inequalities**, triggering immediate physical decoherence that is detectable by all nodes across the network.
2. **Decentralized Verification:** Rather than solving resource-intensive mathematical puzzles, nodes verify the "quantum signature" of the entanglement. This verification is nearly instantaneous, providing the high-speed throughput essential for real-time neural synchronization while eliminating the massive energy overhead associated with classical consensus.

1.6.3 Quantum Defense Layer

By transitioning to a quantum-entangled ledger, the BCI ecosystem moves from **probabilistic security**—the probabilistic reinforcement that an attacker lacks the requisite computational power hack a BCI Quantum Blockchain. This provides the physical certainty that a breach is impossible without violating the fundamental laws of physics. This framework ensures that "Shared Cognition" remains a closed, secure loop, safeguarding cognitive liberty against even the most sophisticated quantum-enabled adversaries.

2. Cloud Privacy

The increasing use of brain-computer interfaces (BCIs) has sparked intense debate about the protection of human privacy, particularly in the context of collecting, analyzing, and storing brainwave data in cloud computing environments (Figure 6). As researchers and developers harness the power of electroencephalographic (EEG) signals to decode neural activity, concerns about informed consent, data anonymization, and potential misuse have come to the forefront.

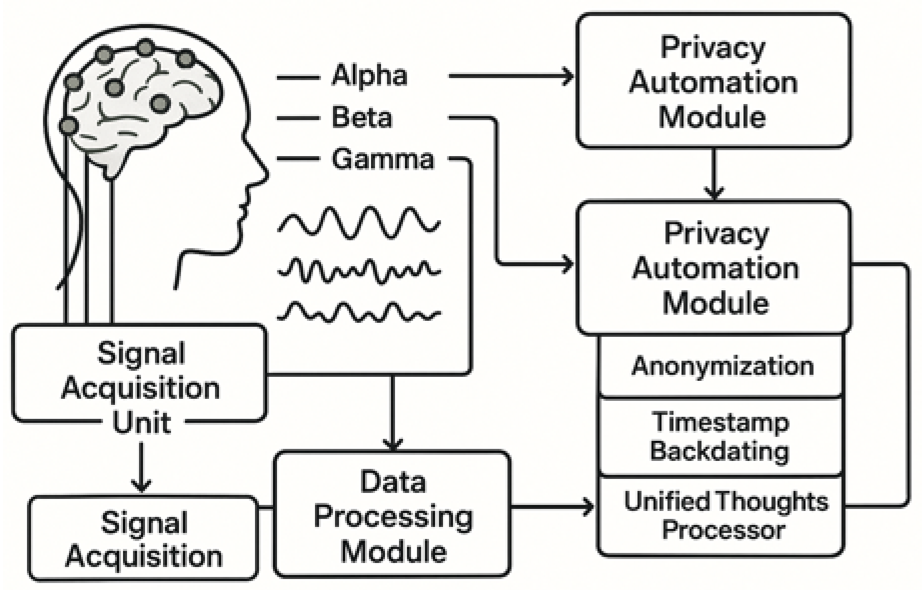

Figure 8. Data anonymization assurance flow.

The integration of cloud computing and big data storage has enabled the scalable and efficient processing of vast amounts of brainwave data. This is particularly crucial for practical AI applications in BCI, as cloud computing provides the necessary infrastructure for handling large-scale data processing, storage, and analysis. Cloud-based solutions allow for on-demand scalability, enabling BCI systems to adapt to varying workloads and user demands.

In real-world enterprise user applications, cloud computing is essential for BCI systems to handle the complexity and volume of brainwave data generated by multiple users. Cloud-based AI processing enables the deployment of sophisticated machine learning models that can learn from large datasets, improve over time, and provide accurate and personalized feedback to users. Moreover, cloud computing facilitates the integration of BCI systems with other enterprise applications, such as healthcare, education, and gaming, enabling seamless interactions and unlocking new use cases.

However, the reliance on cloud computing for BCI also raises significant concerns about data security, confidentiality, and ownership. When brainwave data is stored in cloud-based repositories, it becomes vulnerable to unauthorized access, data breaches, and potential exploitation by malicious actors (Figure 7). Furthermore, the application of artificial intelligence (AI) and distributed processing techniques to brainwave data analysis introduces additional risks and challenges.

From an Institutional Review Board (IRB) perspective, ensuring the anonymity and confidentiality of brainwave data is paramount. Researchers must implement robust de-identification methods, such as data masking, encryption, and secure storage protocols, to safeguard participants' sensitive information. This requires careful consideration of data handling practices, storage, and sharing protocols to prevent unauthorized access or re-identification.

To mitigate these risks, researchers and developers can adopt best practices for secure cloud-based data storage and AI-powered analysis, such as:

- Implementing end-to-end encryption for data transmission and storage
- Using secure authentication and access controls to limit data access
- Developing and adhering to strict data sharing and collaboration policies
- Ensuring transparency and accountability in AI-driven data analysis and decision-making

Moreover, IRBs and regulatory bodies must establish clear guidelines for the collection, analysis, and sharing of brainwave data in cloud computing environments. This includes ensuring that informed consent procedures are robust and transparent, and that participants are aware of potential risks and benefits associated with BCI research.

Ultimately, the responsible development and use of BCI technology require a nuanced understanding of human privacy, cloud computing security, and AI ethics. By prioritizing anonymization, confidentiality, and transparency, researchers can build trust with participants and stakeholders, while advancing our understanding of the human brain and its intricate functions.

2.1. Data Anonymization

The protection of sensitive neural data necessitates a privacy architecture that transcends simple heuristics to provide formal, quantifiable guarantees. This section critically examines proposed ad-hoc anonymization techniques and introduces a hierarchy of rigorous mathematical models for privacy (Figure 8), culminating in the gold standard of differential privacy.

2.1.1. Ad-Hoc Anonymization

The proposed architecture includes methods such as file shuffling [37], random renaming, and altering file creation timestamps to anonymize neural data. While these procedures may obscure direct identifiers in a file system, they do not provide formal privacy guarantees. Such techniques fall into the category of data obscurity and are vulnerable to linkage attacks. For instance, if the content of EEG data itself contains unique patterns attributable to an individual, shuffling files does not prevent an adversary from re-identifying the data source by analyzing signal characteristics. Altering file metadata is a form of data tampering that fails to protect against content-based analysis. These limitations necessitate adoption of formal privacy models that provide provable guarantees against re-identification and attribute disclosure.

2.1.2. The k-Anonymity Statistical Control

A first step towards formal privacy is statistical disclosure control [38], which aims to make individuals in a dataset indistinguishable.

- k-Anonymity: A dataset satisfies k-anonymity if for every record, there are at least k−1 other records that are identical with respect to a set of identifying attributes known as quasi-identifiers (QIs) (e.g., age, gender, zip code). This ensures that any individual cannot be uniquely identified within a group of at least k.
- l-Diversity: This model addresses a key weakness of k-anonymity known as the homogeneity attack, where all individuals in a k-anonymous group share the same sensitive attribute value. A dataset has l-diversity if every equivalence class (a group of records with identical QIs) has at least l "well-represented" values for the sensitive attribute.
- t-Closeness: This model is a further refinement that mitigates attribute disclosure attacks based on the overall distribution of sensitive values. An equivalence class satisfies t-closeness if the distance between the distribution of a sensitive attribute

within that class and its distribution in the entire dataset is no more than a threshold t. The Earth Mover's Distance (EMD) is often used to measure this distance between the cumulative distribution functions P and Q of the attribute in the equivalence class and the full dataset, respectively.

A) Provable Differential Privacy

The most robust and widely accepted formal privacy framework is differential privacy. This framework represents a paradigm shift from attempting to anonymize the data itself to providing a provable guarantee on the output of any computation performed on the data. The raw data may remain identifiable to a trusted data curator, but any information released—be it a statistical query or a trained machine learning model guarantees privacy-preserving.

- **Formal Definition:** A randomized algorithm M satisfies (ϵ,δ)-differential privacy if, for any two adjacent datasets D1 and D2 that differ in the data of a single individual, and for any set of possible outputs S, the following inequality holds:

$$\Pr[M(D1) \in S] \leq e\epsilon \cdot \Pr[M(D2) \in S] + \delta$$

The parameters define the strength of the privacy guarantee:

- ϵ (epsilon), the privacy budget, is a small positive real number. A smaller ϵ means the outputs of the algorithm on the two adjacent datasets are more indistinguishable, implying stronger privacy.
- δ (delta) represents the probability that the pure ϵ-privacy guarantee is broken. It should be a cryptographically small value, typically less than the inverse of the dataset size.

This definition ensures that an adversary, upon observing the output of M, cannot confidently infer whether any single individual's data was included in the input dataset, thus protecting individual privacy.

- **The Laplace Mechanism:** A common method for achieving ϵ-differential privacy for functions that return a numeric value (e.g., a statistical mean, or a model parameter) is the Laplace mechanism. It involves adding carefully calibrated noise to the true output of the function. The amount of noise is scaled according to the function's L1-sensitivity, Δf, which is the maximum possible change in the function's output when one individual's data is removed or changed.

$$\Delta f = \max\_\{D1,D2\} \ \| f(D1) - f(D2) \|_1 \tag{1}$$

The differentially private mechanism M(D) then returns:

$$M(D) = f(D) + \mathrm{Lap}(\Delta f/\epsilon) \tag{2}$$

where Lap(b) denotes a random variable drawn from the Laplace distribution with scale b, which has the probability density function:

$$p(x|b) = (1/2b)e\hat{}\{-|x|/b\} \tag{3}$$

For neural interface systems, this mechanism could be applied in several ways [39], such as adding noise to the aggregated features used for model training or, more powerfully, integrating noise into the training process itself (e.g., Differentially Private Stochastic Gradient Descent) to produce a privacy-preserving machine learning model for deployment in the cloud. This approach provides a mathematically rigorous and defensible privacy architecture far superior to ad-hoc data manipulation.

3. BCI Avatar Systems

BCI technology enables direct communication between the brain and external devices, offering groundbreaking opportunities for neuroscientific research [5], medical interventions, and assistive technologies. However, the ethical implications of working with human subjects in BCI studies necessitate stringent oversight and adherence to Human Privacy Act.

The Institutional Review Board (IRB), a fundamental pillar of ethical research, ensures the safeguarding of human participants by rigorously evaluating the risks and benefits of proposed studies. Adherence to IRB regulations is essential to guarantee the ethical treatment of research subjects and the validity of study outcomes. Research involving human subjects is a crucial driver of scientific and medical progress, providing invaluable insights across various disciplines. However, to ensure the ethical and responsible conduct of such studies, obtaining proper authorization from human subjects is imperative. This authorization not only protects the well-being and rights of individual participants but also upholds the integrity of the research process. The primary rationale for seeking human subject authorization is to safeguard the rights and well-being of individuals participating in research studies. Human subjects have the inherent right to be treated with respect, dignity, and fairness throughout the research process.

Resilience to Attacks	Type of Protection	Privacy Guarantee	Approach Definition	Privacy Technique
Medium; vulnerable to homogeneity and background knowledge attacks	Data Anonymization	Protection against identity disclosure via record linkage	Every record is indistinguishable from at least k−1 others on quasi-identifiers	**k-Anonymity**
Medium; vulnerable to skewness and semantic proximity attacks	Data Anonymization	Protection against homogeneity attacks	Each equivalence class has at least distinct sensitive attribute values	**l-Diversity**
High; robust guarantee that is resilient to post-processing and composition of queries	Privacy-Preserving Computation	Provable, quantifiable protection against membership inference and attribute disclosure	Probabilistic indistinguishability of algorithm outputs on adjacent datasets	**(ϵ,δ)-Differential Privacy**
High; robust guarantee that is resilient to post-processing and composition of queries or auditing	Automated Data Anonymization	No record linkage: increase protection against identity disclosure	A practical, heuristic, and randomized procedure, implemented with Linux system tools	**Shuffler: Timestamp Alteration + Disabled log**

Informed consent is typically obtained through a detailed and transparent process. It involves providing participants with comprehensive information about the study, allowing them to make informed decisions regarding their involvement. Informed consent ensures that individuals understand the nature of the research, the potential risks and benefits, the voluntary nature of their participation, and the measures in place to protect their confidentiality. Human subject authorization is closely tied to ethical considerations in research. Researchers must adhere to ethical guidelines to maintain the trust of participants and the broader community. Obtaining proper authorization helps researchers navigate potential ethical dilemmas, such as ensuring the confidentility of participant information, minimizing harm, and promoting fairness in participant selection. Ethical research practices contribute to the credibility and reliability of research outcomes.

Many countries and institutions have specific regulations and laws governing research involving human subjects. Obtaining proper authorization ensures compliance with these legal requirements, protecting both researchers and participants. Failure to adhere to these regulations can lead to serious consequences, including legal action, reputational damage, and potential suspension of research activities. Researchers must establish clear protocols for data collection, storage, and dissemination to protect sensitive information. Obtaining proper authorization allows participants to understand how their data will be handled and ensures that researchers adhere to stringent privacy measures.

Building and maintaining trust between researchers and human subjects are essential for the success of any research endeavor. Proper authorization processes contribute to transparent communication, fostering trust and collaboration. When participants are confident that their rights are respected and their well-being is a top priority, they are more likely to engage in research activities, leading to more robust and reliable results.

In recent years, advancements in Brain-Computer Interface (BCI) technology have paved the way for innovative applications in healthcare, research, and beyond. As researchers delve into the possibilities of BCI, ethical considerations and compliance with Institutional Review Board (IRB) regulations become paramount. To address these concerns, the development of open-source automation software for BCI and other Human Subject applications not only fosters collaboration but also ensures adherence to ethical standards. Ongoing technological breakthroughs have significantly expanded the frontiers of human-machine interaction, paving the way for revolutionary applications across diverse industries. A notable example of this progress is the pioneering integration of Brain-Computer Interface (BCI) technology with Humanoid Robots and Unmanned Aerial Vehicles (UAVs). By the use of cameras, sensors, and augmented reality, implementation of Avatars became feasible. This synergy of neuroscience with hardware and software technologies unlocks vast potential, offering unprecedented control and capabilities for Avatar operations. Furthermore, the BCI platform enables the exploration of novel haptic interfaces, heralding a new era in Human-Computer Interaction and user interface design.

Brainwave Machine Learning enables mind-controlled drones and robots, turning thoughts into action. With Brain-Computer Interface (BCI) technology, users can command digital or robotic avatars with their brain signals, opening up new possibilities for remote interaction and control. These avatars, whether virtual or physical, can execute a range of tasks and respond to their environment based on the user's thoughts and brain activity.

4. BCI Best Practices

Implementing machine learning in Brain-Computer Interfaces (BCIs) is a complex task that requires careful consideration of several factors to ensure accurate, reliable, and user-friendly performance. BCIs are systems that enable people to control devices or communicate with others using only their brain signals. Machine learning algorithms can be used to decode brain signals and translate them into meaningful commands or actions. However, the development of effective BCIs requires a deep understanding of both machine learning and brain signal processing.

4.1. Data Collection and Calibration

High-quality brain signal data is the foundation of effective Brain-Computer Interfaces (BCIs). To develop BCIs that can accurately decode brain signals and translate them into meaningful commands or actions, researchers and developers must prioritize data quality. This involves:

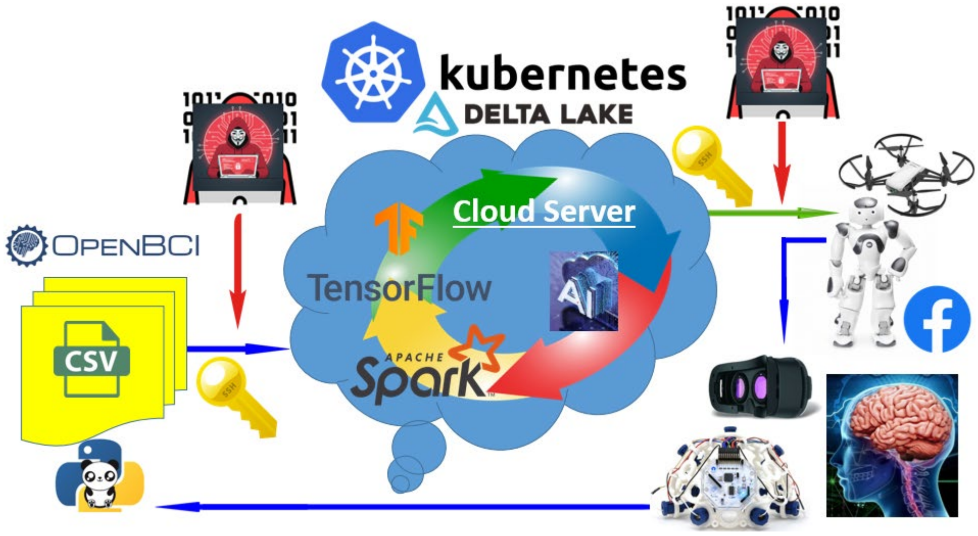

Figure 9. Scalable Cloud Kubernetes Architecture for Spark and AI/Machine Learning Applied to Neurohaptics Integration.

- **Utilizing specialized equipment:** Employ equipment specifically designed for brain signal acquisition, such as electroencephalography (EEG) or functional near-infrared spectroscopy (fNIRS), to capture high-quality data.
- **Minimizing noise and artifacts:** Implement techniques like filtering, amplification, and shielding to reduce noise and artifacts in the data, ensuring that the signals are clear and reliable.
- **Annotating data with precision:** Label the data with relevant targets or annotations to enable supervised learning, allowing the machine-learning model to learn from the data and make accurate predictions.
- **Collecting diverse data:** Gather data from a diverse range of subjects and conditions to improve the generalizability of the model, enabling it to perform well in various contexts.

Minimizing calibration time and improving user experience is very important. User calibration is a critical step in developing effective BCIs. Researchers and developers should minimize calibration time and improve user experience by:

- **Using adaptive calibration techniques:** Use adaptive calibration techniques to adjust the model to the user's changing needs and preferences.

- **Providing user feedback:** Provide user feedback to help the user understand the system's performance and limitations.
- **Minimizing user burden:** Minimize user burden by reducing the amount of data required for calibration.

To foster a foundation of trust with volunteers, it is essential to prioritize transparency in the collection and use of brain signal data. By being open and clear about the data collection process, researchers and developers can ensure that volunteers feel informed and confident in their participation. This transparency not only promotes trust but also lays the groundwork for the development of effective Brain-Computer Interfaces (BCIs) that are grounded in high-quality data (Figure 9).

4.2. Analysis, Modeling and Classification

Proper analysis for feature engineering is a critical step in developing effective BCIs. Relevant features can be extracted from brain signal data using various techniques, such as:

- Time-domain features: Extract features from the time domain, such as amplitude, latency, and duration.
- Frequency-domain features: Extract features from the frequency domain, such as power spectral density and coherence.
- Time-frequency features: Extract features from the time-frequency domain, such as wavelet coefficients and Hilbert-Huang transform.
- Feature selection: Select the most relevant features that contribute to the model's performance.

The choice of machine learning model depends on the specific BCI application. Researchers and developers should consider the following factors when selecting a model:

- Problem type: Choose a model that is suitable for the specific problem type, such as classification, regression, or clustering.
- Model complexity: Balance model complexity with interpretability and computational resources.
- Hyperparameter tuning: Tune the hyperparameters of the model to optimize its performance.
- Model evaluation: Evaluate the model's performance using metrics such as accuracy, precision, and recall.

Model evaluation is a critical step in developing effective BCIs. Researchers and developers should use various metrics to evaluate the model's performance, such as:

- Accuracy: Evaluate the model's accuracy in decoding brain signals and translating them into meaningful commands or actions.
- Precision: Evaluate the model's precision in detecting specific patterns or features in brain signal data.
- Recall: Evaluate the model's recall in detecting specific patterns or features in brain signal data.
- Confusion matrix: Use a confusion matrix to visualize the model's performance and identify areas for improvement.

4.3. Real-Time Processing

Real-time processing is essential for BCIs that require immediate feedback or control. In real-time BCIs, brain signals are acquired, processed, and translated into commands or actions with minimal delay, allowing users to receive immediate feedback and control the system. This requires advanced signal processing techniques, machine learning algorithms, and optimization methods to ensure accurate and reliable performance. Developers should optimize the model for real-time performance by:

Figure 10. Automated Developer Ranking Solution Based on Approved and Merged Code Review Pull Requests.

- Using efficient algorithms: Use efficient algorithms and data structures to reduce computational complexity.
- Parallel processing: Use parallel processing techniques to take advantage of multi-core processors.
- Optimizing memory usage: Optimize memory usage to reduce latency and improve performance.
- Low Latency: Real-time BCIs require low latency to ensure that the system responds quickly to user input. High latency can lead to frustration and decreased user performance.
- High Accuracy: Real-time BCIs require high accuracy to ensure that the system correctly interprets user intent. Inaccurate classification or detection can lead to errors and decreased user trust.
- Signal Variability: Brain signals can vary significantly between users and even within the same user over time. Real-time BCIs must be able to adapt to these changes to maintain accurate performance.
- Noise and Artifacts: Real-time BCIs must be able to handle noise and artifacts in the brain signal data, such as those caused by muscle activity, eye movements, or electrical interference.

5. Materials and Methods

Our Avatar project is an open-source BCI automation software that provides transparency in the development and implementation of experimental protocols. Researchers and developers can collaborate to refine the software, enhancing its functionality and addressing any ethical concerns that may arise during the development process. IRB compliance often requires customization of experimental protocols to meet the specific needs of diverse research studies. Open-source BCI automation software

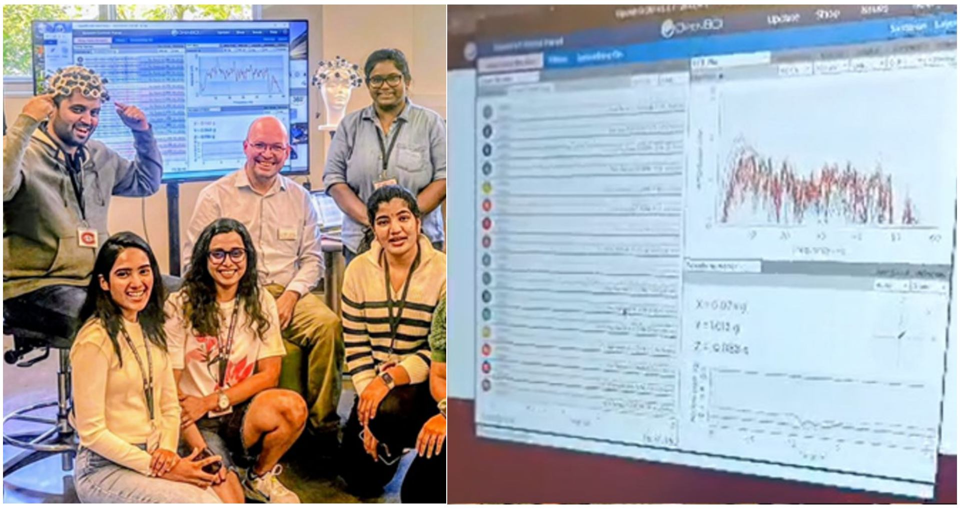

Figure 11. Calibration and Adjustment of the EEG Headset for Live Brainwave Acquisition and Upload to the Cloud Computing Club Avatar Server.

allows researchers to tailor protocols according to their study objectives while ensuring adherence to ethical guidelines.

Open-source development has become increasingly popular for promoting collaboration, transparency, and innovation across various fields [40]. In BCI research, open-source automation software is instrumental in ensuring compliance with IRB regulations. By leveraging community input and collective expertise, this software fosters a collaborative approach to ethical oversight. Through peer review and shared knowledge, researchers can identify and address potential ethical challenges, ultimately strengthening research practices and upholding the highest ethical standards.

Open-source software is freely accessible, making it a cost-effective solution for researchers with limited resources. This accessibility promotes inclusivity in BCI research, allowing a broader range of researchers to engage in ethical and compliant studies. Our open-source development approach allows the system implementation to move safe, allow transparency and collaboration (Figure 11).

Automation software can include features for real-time monitoring of BCI experiments, ensuring that researchers can promptly respond to any unforeseen ethical issues. Additionally, robust data security measures can be implemented to safeguard sensitive information, addressing another critical aspect of IRB compliance.

5.1. Open-Source Compliance Framework

The efficacy of open-source projects, including the Avatar initiative, rests upon a foundation of sustained, trustworthy community contributions. To safeguard this environment, the Avatar project has established a rigorous framework of governance and enforcement protocols that address both social conduct and technical integrity. This model permits Maintainers to institute disciplinary actions, ranging from preliminary private warnings to permanent contributor exclusion, reserved for instances of persistent, egregious, or malicious behavior.

The Avatar project categorizes breaches that necessitate contributor exclusion into three distinct domains: Socio-Ethical Conduct, Technical and Policy Non-Compliance, and Development Process Adherence.

5.1.1. Socio-Ethical Conduct and the Code of Conduct

Strict adherence to the project's Code of Conduct (CoC) is mandatory, as breaches directly undermine community well-being. Prohibited behaviors include: Harassment and Aggression (personal attacks, derogatory commentary); misuse involving Inappropriate Content; Unauthorized Disclosure of Private Information (Doxing); and sustained Disruptive Behavior (trolling or creating irrelevant, resource-draining issues).

5.1.2. Digital Authorship Misrepresentation

The Avatar project deems accurate intellectual attribution non-negotiable. Digital Authorship Misrepresentation is an acute ethical violation spanning multiple forms:

Description and Impact	**Form of Misrepresentation**
Unauthorized utilization and presentation of external code or ideas without proper citation.	**Plagiarism**
Exclusion of a substantive contributor from project credit listings.	**Undisclosed Authorship**
Inclusion of non-contributing individuals to confer undue prestige or authority.	**Fictitious Authorship**
The critical issue arising from non-functional changes that corrupt the evidential history of contribution.	**Technical Attribution Obfuscation**

The most significant technical threat is Technical Attribution Obfuscation (Version Control Misrepresentation). This occurs when automated, non-substantive changes, such as mass reformatting, alter nearly all lines of code. This action directly compromises the utility of version control tools like `git blame`, which subsequently register the reformatting commit author as the last person to touch the lines. This technical artifact generates a false attribution of effort, severely eroding the documentation of the original code authors.

5.1.3. **Operational Compliance and Integrity Standards**

To maintain the security and operational health of the repository, the Avatar project enforces strict technical compliance:

- **Abusive Automation:** Includes undisclosed bot activity or Spamming (high volume, low-value commits) flagged by platform mechanisms.
- **Security Violations:** Encompasses Malicious Activity (hosting malware, unauthorized security breaches) that poses systemic risk.
- **Resource Misuse:** Excessive Resource Consumption via actions workflows that compromise shared project infrastructure.
- **Regulatory Triggers:** Actions that violate platform policies or jurisdictional laws (e.g., sanctioned access, intellectual property breaches), often resulting in platform-level exclusion.

5.1.4. Preserving History Mandate

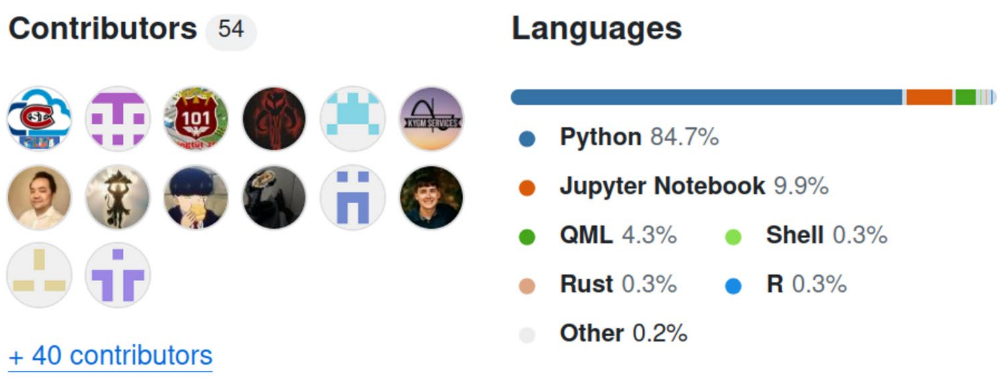

Figure 12. The Avatar Community, coordinated by the Cloud Computing Club, currently comprises 54 contributors, with system integration primarily conducted in Python.

The Avatar Project has codified a Mandatory Mitigation Protocol to safeguard Git history integrity against technical obfuscation, viewing compliance as non-negotiable for project participation:

1. **Mandatory Consensus:** Prior to initiating any large-scale, non-functional code alteration, explicit agreement from Project Maintainers must be secured via a formal proposal.
2. **Commit Isolation:** The reformatting changes must be strictly isolated in commits and Pull Requests, separating them entirely from functional code changes or bug fixes.
3. **SHA-1 Exclusion Protocol:** Upon merging, the resultant commit SHA-1 hash must be registered within the project's dedicated .git-blame-ignore-revs file. This institutionalized measure forces all Git tooling to skip the non-substantive changes, thereby sustaining the attribution to the original code authors.

The Avatar project concludes that while technical reformatting does not equate to legal infringement, the act of compromising evidential authorship undermines the transparency and respect foundational to the open-source ethos, justifying strict disciplinary action. Integrity and attribution are core values for the Avatar project, particularly regarding contribution history and author recognition.

5.2. Cybersecurity

To fortify the cybersecurity and anti-hacking defenses of Brain-Computer Interface (BCI) systems, the implementation of RSA public-private key infrastructure serves as a highly effective mitigation strategy. Adopting a comprehensive RSA-based authentication protocol significantly reduces the risk of unauthorized access and data exfiltration. In our framework, we supplement these cryptographic defenses with periodic penetration testing, simulating targeted cyberattacks against the Avatar server—specifically the S3 data storage buckets—to assess the system's security posture and identify exploitable vulnerabilities. Unlike standard vulnerability scanning, this penetration testing protocol actively exploits system weaknesses to model malicious activities and quantify potential risks to the integrity, confidentiality, and availability of application services. This assessment is conducted using industry-standard tools such as Metasploit for exploit

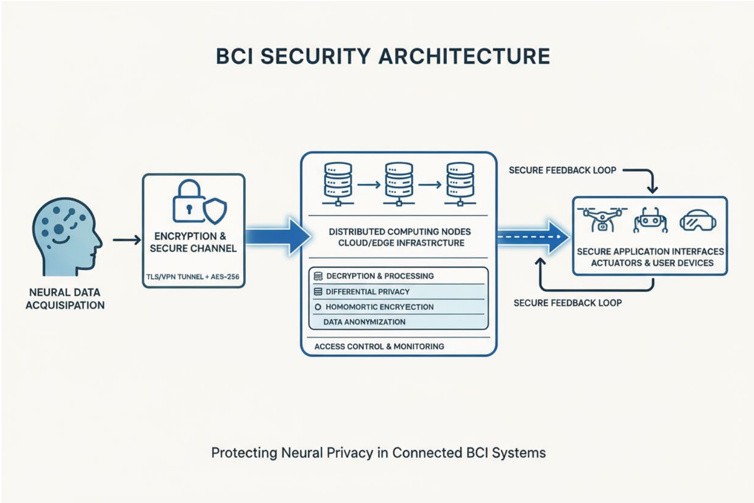

Figure 13. BCI System Architecture Featuring Brainwave Privacy Protection.

verification, Nmap for network discovery and security auditing, and Burp Suite for analyzing web-based vulnerabilities. The resulting protocol represents a robust defense mechanism designed to prevent server takeover attempts while ensuring that individual information remains anonymous and untraceable through a methodical, automated file management system [41].

5.2.1. *Mitigating Brute-Force Attacks*

The persistence of brute-force attacks poses a fundamental threat to the availability and integrity of Internet-facing services. These attacks, which rely on the automated, iterative submission of credentials until a successful combination is discovered, consume excessive server resources and ultimately compromise system security.

To counteract this persistent threat, security architectures frequently employ adaptive intrusion prevention systems such as Fail2Ban. This framework distinguishes itself by implementing a dynamic defense mechanism rooted in real-time log file analysis. The system operates by continuously parsing application log streams to identify patterns indicative of malicious activity, specifically repeated authentication failures originating from a single source IP address within a defined time window.

Upon confirmation of attack criteria, Fail2Ban executes immediate remediation by programmatically modifying the host machine's firewall rules (e.g., utilizing `iptables`). This action serves to temporarily drop all subsequent network traffic from the offending IP address, thereby instantaneously neutralizing the attack vector and protecting the service layer from further resource exhaustion or successful compromise. This capability to dynamically adapt security policy based on observation represents a critical layer of defense against automated login assaults.

5.2.2. *Implementing RSA Key-Based Authentication*

A crucial step in securing BCI systems is to transition from traditional password-based authentication to RSA key-based authentication. This method utilizes a pair of cryptographic keys: a public key and a private key. The public key is stored on the server,

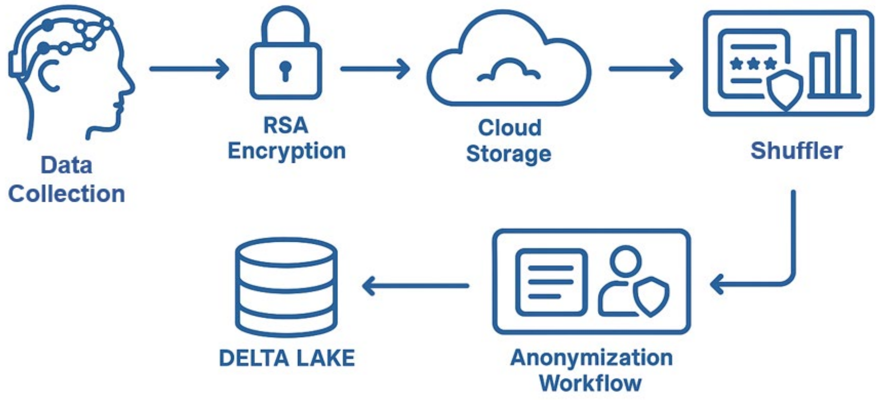

Figure 14. Privacy Architecture Utilizing RSA Encryption for Protecting S3 Delta Lake Data Transmission.

while the private key is kept secure by the user. When a user attempts to access the server, the RSA key pair is used to authenticate the user, ensuring that only authorized individuals with the corresponding private key can gain access. This approach provides a significantly higher level of security compared to password-based authentication, as it is much more difficult for attackers to compromise or guess the private key.

5.2.3. Generating and Managing Key Pairs

To ensure the security and integrity of the RSA key-based authentication system, it is essential to generate and manage key pairs properly. This involves:

- **Secure Key Generation:** Generate RSA key pairs using a secure method, such as a trusted random number generator, to prevent predictability and ensure the keys are cryptographically secure.
- **Private Key Storage:** Store private keys securely, using measures such as encryption, access controls, and secure storage devices, to prevent unauthorized access.
- **Key Rotation:** Rotate keys periodically to limit the potential damage in case a private key is compromised.
- **Access Revocation:** Revoke access to the server when a user's private key is compromised or when an employee leaves the organization.

5.2.4. Configuring SSH for Key-Based Authentication

To utilize RSA key pairs for authentication, configure Secure Shell (SSH) to use key-based authentication. This involves:

- **Public Key Deployment:** Copy the public key to the server and store it in a secure location.
- **SSH Client Configuration:** Configure the SSH client to use the private key for authentication, ensuring that the client can establish a secure connection with the server.
- **Server Configuration:** Configure the server to accept RSA key pairs for authentication, disabling password-based authentication once the key-based system is in place.

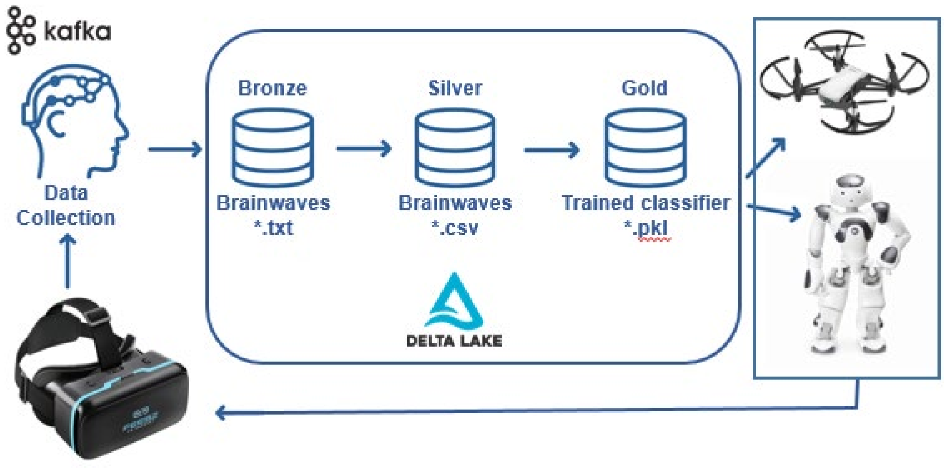

Figure 15. The Delta Lake-Enabled Data Flow Diagram for BCI Avatar Systems.

5.2.5. Disabling Password-Based Authentication

Once the RSA key-based authentication system is set up and tested, disable password-based authentication to prevent unauthorized access. This ensures that even if passwords are compromised, attackers cannot access the server without the corresponding private key.

5.2.6. Cloud Data Reliability and Recovery

In addition to robust security measures, ensuring the reliability and recoverability of cloud computing servers and data is crucial. Delta Lake and bucket data storage can significantly improve the reliability and data recovery capabilities of cloud-based BCI systems.

- **Delta Lake:** Delta Lake is an open-source storage layer that provides ACID transactions, scalable metadata handling, and unifies batch and streaming data processing. By using Delta Lake, organizations can ensure data consistency, reliability, and performance, even in the face of failures or concurrent modifications.
- **Bucket Data Storage:** Bucket data storage, such as Amazon S3 or Google Cloud Storage, provides a scalable and durable remote file system for storing and retrieving data. By storing data in buckets, organizations can ensure data is highly available, durable, and protected against data loss.

The combination of Delta Lake and bucket data storage provides several benefits, including:

- **Improved Data Reliability:** Delta Lake ensures data consistency and reliability, while bucket data storage provides durable and highly available storage.
- **Enhanced Data Recovery:** With Delta Lake's versioning and bucket data storage's data durability, organizations can recover data in case of failures or data corruption.

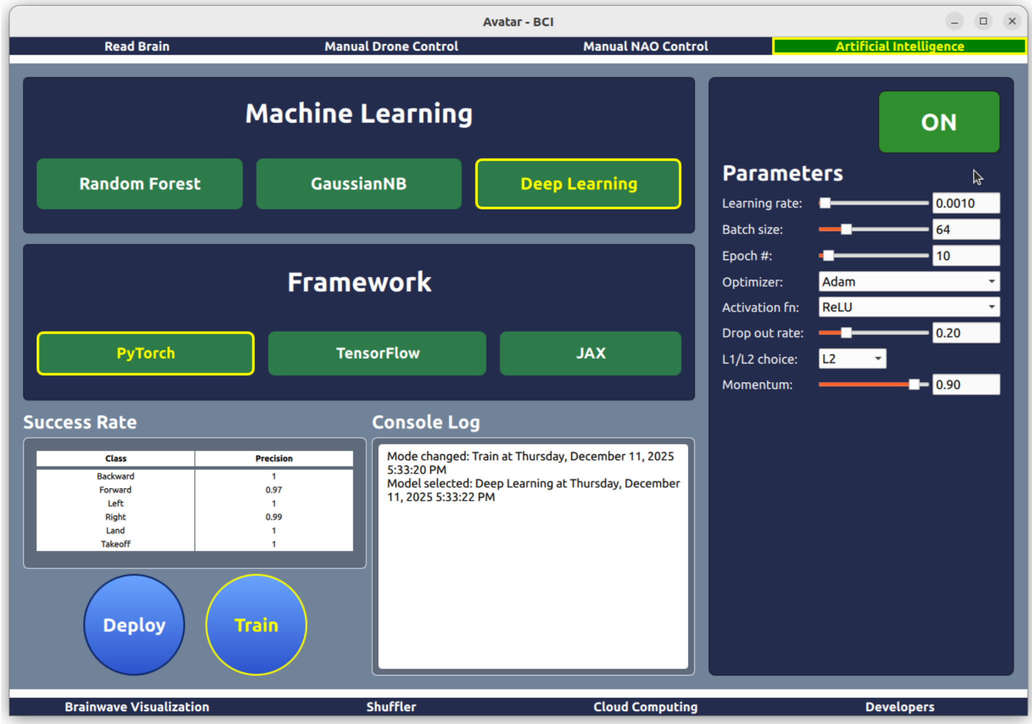

Figure 16. Architecture for Brainwave Pattern Identification, featuring three AI frameworks and two supporting machine learning models.

- **Scalability and Performance:** Delta Lake and bucket data storage can handle large amounts of data and scale to meet the needs of growing BCI systems.

5.2.7. Improved Security

To further enhance the security of BCI systems, consider implementing additional measures, such as:

- **Two-Factor Authentication (2FA):** Require users to provide a second form of verification, such as a biometric scan or a one-time password, in addition to the RSA key pair.
- **Access Controls:** Implement strict access controls to limit user privileges and ensure that users can only access necessary resources.
- **Regular Security Audits:** Perform regular security audits to identify and address potential vulnerabilities, ensuring the security and integrity of the system.

By implementing RSA public-private key pairs, disabling password-based authentication, and leveraging Delta Lake and bucket data storage, organizations can significantly enhance the security, reliability, and recoverability of their BCI systems, protecting against unauthorized access and data breaches.

5.3. Machine Learning

A.I. machine learning provides the key elements to allow the implementation of applicable Brain-Computer Interfaces (BCIs). BCIs are systems that enable people to control devices or communicate with others using only their brain signals. Machine learning enables BCIs by providing a way to analyze and interpret brain signals. By training machine learning models on brain signal data, researchers can develop systems that can recognize patterns in brain activity and translate them into specific commands or actions. This can be used to control devices, such as prosthetic limbs or computers, or to communicate with others.

Supervised machine learning is a fundamental approach in the field of artificial intelligence, where a model is trained on labeled data to make accurate predictions on new, unseen data. This paradigm has been widely adopted in various applications, including image classification, natural language processing, and predictive analytics. Two popular approaches for supervised learning are Random Forest Classifier and Deep Learning, each with its strengths and weaknesses.

5.3.1. Random Forest Classifier Approach

Random Forest is an ensemble learning method that combines the predictions of multiple decision trees to improve the accuracy and robustness of predictions. This approach works by training multiple decision trees on random subsets of the data and features, and then combining their predictions through a voting mechanism. Each decision tree in the ensemble is trained on a bootstrap sample of the data, which helps to reduce overfitting and improve the overall performance of the model.

The Random Forest Classifier is particularly well-suited for classification problems, where the goal is to predict a categorical label or class membership. This approach has several advantages, including:

- **Handling high-dimensional data:** Random Forest can handle datasets with many features, making it an ideal choice for applications where the number of features is large.
- **Handling missing values:** Random Forest can handle missing values in the data, which is common in many real-world applications.
- **Robustness to outliers:** Random Forest is robust to outliers and noisy data, which can improve the overall performance of the model.
- **Interpretability:** Random Forest provides feature importance scores, which can be used to understand the relationships between the features and the target variable.
- **Random Forest Classifier:** it is an ensemble learning method that operates by constructing a multitude of decision trees at training time and outputting the class that is the mode of the classes of individual trees [42].
- **Decision Tree and Gini Impurity:** The fundamental building block of a Random Forest is the decision tree. Each node in the tree splits data based on a feature value. The quality of a split is measured by its ability to reduce impurity. The Gini impurity is a common metric used for this purpose. For a given set of samples S at a node, where pk is the fraction of samples belonging to class k out of K total classes, the Gini impurity is defined as:

$$G(S) = 1 - \Sigma\ (k=1 \text{ to } K)\ pk^2 \quad (4)$$

- A Gini impurity of 0 represents a pure node (all samples belong to one class), while a value of 0.5 (for a two-class problem) indicates maximum impurity. The decision tree algorithm selects the feature and threshold that results in greatest reduction in Gini impurity.
- **Ensemble Prediction:** A Random Forest model consists of an ensemble of B decorrelated decision trees, Tb}b=1B. Each tree is trained on a bootstrap sample (a random sample with replacement) of training data. For a new input vector x, the final prediction, ŷ, is determined by a majority vote among all trees in the forest:

$$\hat{y} = \text{argmax}(ck \in Y)\ \Sigma\ (b=1 \text{ to } B)\ I(Tb(x) = ck) \quad (5)$$

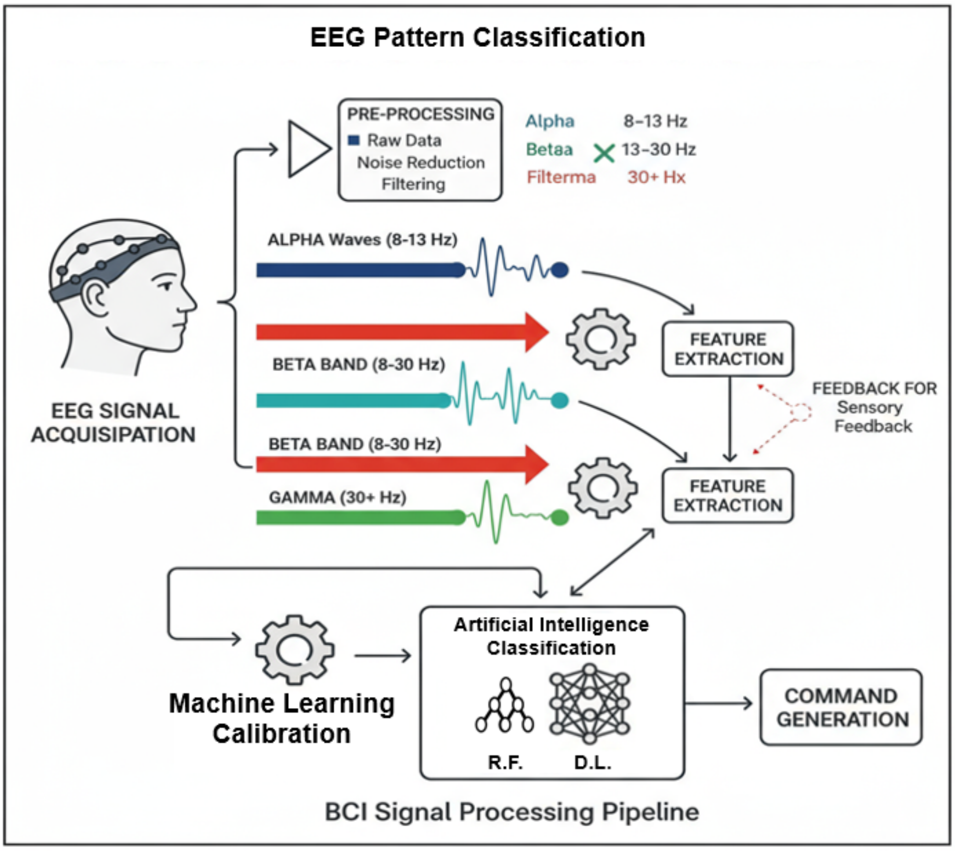

Figure 17. Implementation of Deep Learning and Random Forest Techniques for Enhanced BCI Classification.

- where I(·) is the indicator function. This ensemble approach reduces overfitting and improves the model's robustness compared to a single decision tree.
-

5.3.2. Deep Learning Approach

Deep Learning is a subset of machine learning that involves the use of neural networks with multiple layers. These models are capable of learning complex patterns in data by stacking multiple layers, each of which extracts relevant features from the input data. Deep learning models can automatically extract features from the data, eliminating the need for manual feature engineering.

Deep Learning is particularly well-suited for complex classification problems, such as image and speech recognition, where the data is high-dimensional and complex. This approach has several advantages, including:

- **Learning complex patterns:** Deep neural networks can learn complex patterns in data, making them ideal for applications where the relationships between the features and the target variable are non-linear.
- **Automatic feature extraction:** Deep learning models can automatically extract relevant features from the data, eliminating the need for manual feature engineering.

- **Handling large datasets:** Deep learning models can handle large datasets and learn from them, making them ideal for applications where the amount of data is vast.
- **Sequence data:** Deep learning models can handle sequence data, such as text and time series data, making them ideal for applications where the data is sequential in nature.
- **Convolutional Layer (Conv1D):** This layer applies to a set of learnable filters (or kernels) across input signals [43]. For a 1D input signal X and a kernel K, the discrete convolution operation produces an output feature map S where each element S(i) is computed as:

$$S(i) = (X * K)(i) = \sum_m X(m)K(i - m) \tag{6}$$

- **Batch Normalization:** Applied after convolutional layers, this technique normalizes activations of the previous layer for each mini batch. This stabilizes and accelerates the training process. An input x is transformed as follows:

$$\hat{x} = \frac{x - \mu}{\sqrt{\sigma^2 + \epsilon}}, y = \gamma\hat{x} + \beta \tag{7}$$

- where μ and σ^2 are the mean and variance of the mini-batch, and γ and β are learnable scaling and shifting parameters.
- **Max Pooling:** This is a down-sampling operation that reduces spatial dimensions of the feature map, providing a degree of translational invariance and reducing computational complexity. For a given region of size p and stride s, it outputs the maximum value:

$$y_i = max(x_{i \cdot s}, x_{i \cdot s+1}, \dots, x_{i \cdot s+p-1}) \tag{8}$$

- **Dense Layer and SoftMax Activation:** After several convolution and pooling layers, flattened feature maps are passed through one or more fully connected (dense) layers. A dense layer performs a linear transformation Wx+b. The final dense layer outputs a vector of logits, which are then converted into a probability distribution over the K classes using the SoftMax activation function [43]. For the i-th logit zi, the SoftMax probability is:

$$Softmax(z_i) = \frac{e^{z_i}}{\sum_{j=1}^{K} e^{z_j}} \tag{9}$$

- For readers interested in seeing how these mathematical operations translate into code, our open-source code repository on GitHub provides a simplified Python pipeline that demonstrates Butterworth filtering, data reshaping, and training a 1D-CNN classifier on EEG signals [44].

5.3.3. Comparison between Random Forest Classifier and Deep Learning

When comparing Random Forest Classifier and Deep Learning, several factors come into play. Some of the key differences between the two approaches include:

- **Interpretability:** Random Forest Classifier is more interpretable than Deep Learning models, providing feature importance scores that can be used to understand the relationships between the features and the target variable.
- **Complexity:** Deep Learning models can handle more complex problems than Random Forest Classifier, making them ideal for applications where the relationships between the features and the target variable are non-linear.

- **Data requirements:** Deep Learning models require larger datasets than Random Forest Classifier, making them ideal for applications where the amount of data is vast.
- **Computational resources:** Deep Learning models require more computational resources than Random Forest Classifier, making them more challenging to train and deploy.

5.3.4. Choosing between Random Forest Classifier and Deep Learning

The choice between Random Forest Classifier and Deep Learning depends on the specific problem and dataset. Consider the following factors:

- Problem complexity: If the problem is complex, Deep Learning might be a better choice, as it can handle non-linear relationships between the features and the target variable.
- Data size: If the dataset is large, Deep Learning might be a better choice, as it can handle large datasets and learn from them.
- Interpretability: If interpretability is important, Random Forest Classifier might be a better choice, as it provides feature importance scores that can be used to understand the relationships between the features and the target variable.

6. Privacy Automation

Bash programming, also known as Bash scripting, is the process of writing scripts in the Bash shell programming language. Bash, which stands for "Bourne-Again SHell," is a Unix shell and command-line interpreter written by Brian Fox for the GNU Project. Bash programming involves writing scripts that use Bash commands, syntax, and features to automate tasks, manipulate data, and interact with the operating system. Bash scripts typically have a .sh extension and are executed by the Bash shell.

Bash programming is commonly used for:

- System administration: Automating system tasks, backups, and maintenance.
- Data processing: Manipulating text files, data analysis, and reporting.
- Software development: Building tools, automating builds, and testing.
- System integration: Integrating different systems, services, and applications.

Bash programming features include: Variables; Conditionals (if/then/else); Loops (for/while/do); Functions; Arrays; File operations (read/write/copy); Command substitution; Regular expressions. Bash scripts can be used for simple tasks, like automating backups, or complex tasks, like building software packages. Bash programming is a powerful tool for automating tasks and simplifying system administration.

Bash can invoke a diverse range of programs, which are part of a comprehensive toolset designed to automate tasks [45]. These tools are typically developed using programming languages such as C, Bash, Rust, or Assembly, and are integrated into the system to provide efficient automation capabilities.

6.1. Hijacking Syslog for Anonymity

To successfully satisfy the rigorous ethical covenants and judicial mandates—especially when dealing with privileged biometrics like brainwave captures—investigators are obligated to deploy every available mechanism to render the origin untraceable. A crucial, often unacknowledged, bulwark in this defense strategy is the preemptive programmatic governance of the Linux System Log, or Syslog.

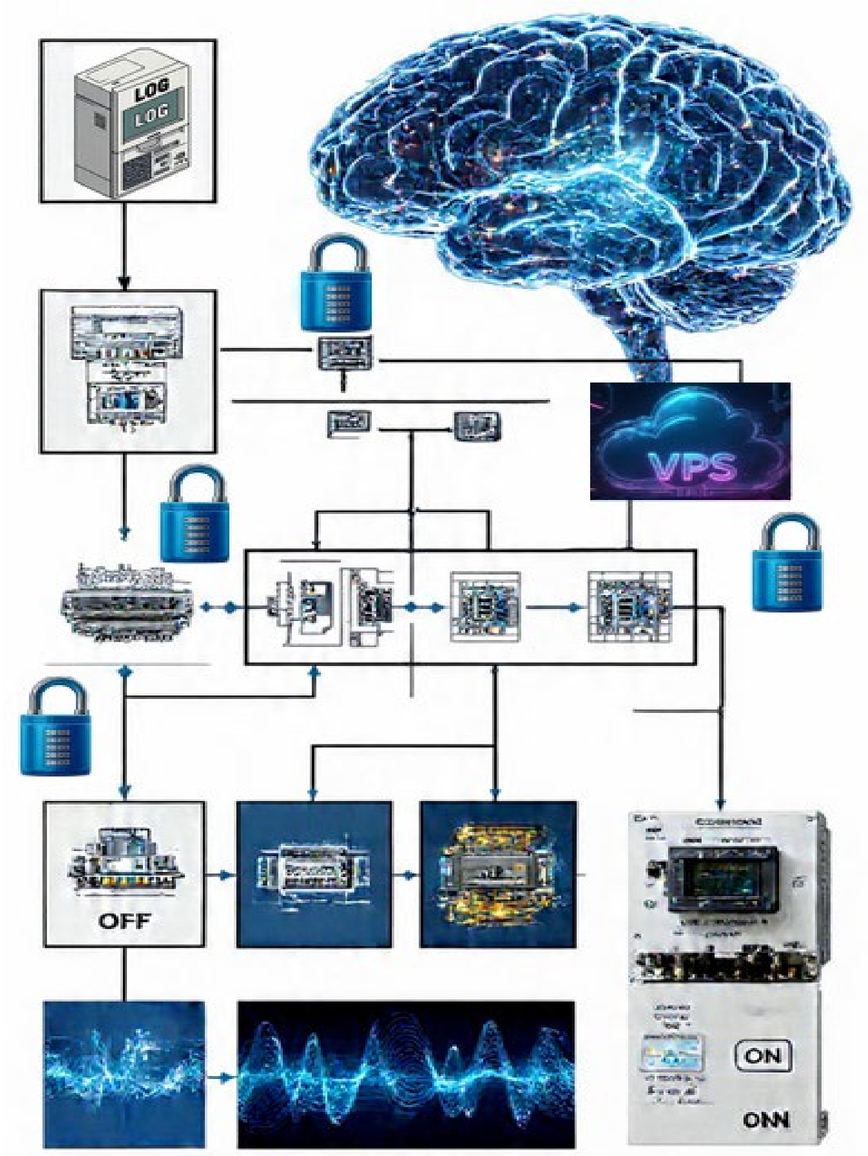

Figure 18. Deactivation of the Avatar Linux SysLog to Ensure Data Anonymity and Regulatory Compliance with the Privacy Act.

In scenarios where file-level data anonymization is executed via automated server workflows, actively managing Syslog becomes an assurance mechanism (Figure 18). It acts to prevent the capture of any underlying system metadata that could serve as an inadvertent tether, connecting the sanitized digital assets back to their originating machine or human source.

Ordinarily, the active Linux Syslog process (such as rsyslog or syslog-ng) functions as a tireless scribe, diligently documenting precise file system interactions initiated by processes or users. While this vigilant record-keeping is vital for operational vigilance, it simultaneously creates a hazardous metadata aperture that compromises anonymization integrity:

Implication for Identity Exposure	System Artifacts Cataloged
Pinpoints the specific digital persona or application engine responsible for asset manipulation, creation, or transfer.	**Originator Identifier / Executing Process Tag**
Records the file's designation prior to its masking or shuffling sequence.	**Pre-Sanitization Label**
Captures the exact moment the masking routine was executed or the sensitive file was initially manifested.	**Chronological Markers (Temporal Footprint)**

6.2. Crontab and Cron

Crontab, the cron daemon, was not implemented using Bash programming [25-46]. The original cron daemon was written in C programming language. Crontab, the cron daemon and the cron table, was created by Brian Kernighan in 1975, while he was working at Bell Labs. At the time, Kernighan was part of a team developing the Unix operating system. The concept of cron was inspired by the clockwork mechanisms of the ancient Greeks, which used gears and levers to automate tasks. The name "cron" comes from the Greek word "chronos," meaning time.

Kernighan's implementation of cron was designed to automate system maintenance tasks, such as backups and disk cleanups, by scheduling them to run at specific times or intervals. The crontab format, with its five fields (minute, hour, day, month, and day of the week), was also introduced by Kernighan. Since then, cron has become a standard tool in Unix-like operating systems, including Linux and macOS, and is widely used for automating tasks and workflows.

- Crontab Configuration: A user creates a crontab file using the crontab -e command, which opens a text editor to configure the schedule. The file contains a list of tasks, each specified by five fields: minute, hour, day of the month, month, and day of the week, followed by the command to be executed.
- Cron Daemon: The cron daemon, a background process, continuously runs on the system, scanning the crontab files for tasks to execute. It checks the schedules and compares them to the current system time.
- Task Execution: When the cron daemon finds a task with a matching schedule, it executes the specified command. The command is run as the user who owns the crontab file, with the same environment and permissions.
- Logging: After executing the task, the cron daemon logs the output and any errors to the system log files, typically /var/log/cron or /var/log/syslog. This allows users to monitor and troubleshoot their scheduled tasks

Differences: cron refers to the cron daemon (crond), a system process that runs in the background and executes scheduled tasks. It is the engine that runs the scheduled jobs. crontab, on the other hand, refers to the table or file that contains the scheduled tasks. It is the configuration file that defines the jobs to be executed by the cron daemon. In other words: cron is the program that runs the scheduled tasks; crontab is the file that contains the schedule and commands to be executed.

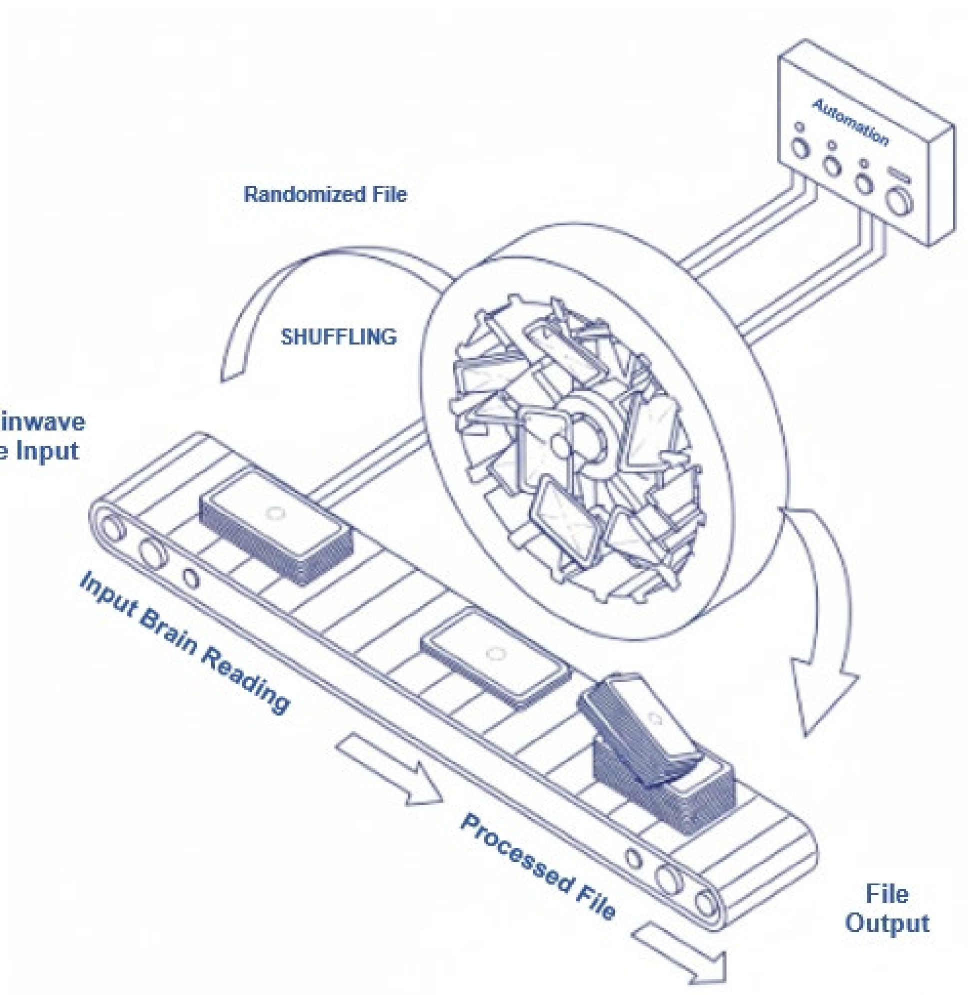

Figure 18. Deactivation of the Avatar Linux SysLog to Ensure Data Anonymity and Regulatory Compliance with the Privacy Act.

6.3. Systemctl

Systemctl is a system management tool and command-line utility that is part of the systemd software suite. It is used to manage and control system services, daemons, and units on Linux-based systems. Systemctl was implemented by Lennart Poettering and Kay Sievers as part of the systemd project, which was started in 2009. The first version of systemd was released in 2010, and systemctl was introduced as a replacement for the traditional init system and service management tools like sysvinit and init scripts. Systemctl is written in C and uses the systemd libraries to interact with the system. It provides a unified interface for managing system resources, including: Services (daemons); Sockets; Devices; Mount points; Timers.

Systemctl allows users to start, stop, restart, enable, and disable system services, as well as monitor their status and configure their behavior [26-47]. Lennart Poettering, a German software engineer, is the primary author of systemd and systemctl. He is credited with designing and implementing the systemd architecture, which has become a widely

Concepts	**Example Command**	**Specific Purpose**	**Primary Command**	**Action**
Pipelining (|) redirects find output to wc -l to count lines (files).	find . -type f | wc -l find . -maxdepth 1 -type f | wc -l (Current dir only)	Automatically count the number of files in a directory and its subdirectories.	Find, wc -l	Count Files
Essential for scripting, file organization, and automation of management tasks.	mv *.txt ~/Documents rename 's/old/new/' *.txt	mv: Move or rename individual files/directories. rename: Batch rename multiple files using Perl regular expressions.	mv, rename	Rename/Move Files
mtime (contents modified), atime (last accessed), ctime (metadata changed), crtime (creation time).	stat -c %W FILENAME (Linux Birth Time)	Display detailed information about a file, including its various access and modification times.	stat, ctime, atime, mtime, crtime	Check Timestamps
Changing crtime is unconventional, often done for specific purposes like data anonymization.	touch FILENAME sudo date --set="YYYY-MM-DD HH:MM:SS"	touch: Updates mtime and atime, but not crtime. date: Temporarily change the OS system clock to set a new file creation time.	touch, date	Change Timestamps
Sequence ensures time can be set without NTP interference, then resyncs to maintain accuracy.	set-ntp false set-time "2025-01-01 10:00:00" systemctl restart chrony	Manually set the system time temporarily, ensuring synchronization with NTP is restored afterward.	set-ntp, set-time, systemctl	Control System Time

adopted standard in the Linux world. Kay Sievers, also a German software engineer, was a key contributor to the systemd project and helped develop systemctl. Systemctl has become an essential tool for Linux system administration and is widely used in many Linux distributions, including Ubuntu, Debian, Fedora, AlmaLinux, and Red Hat Enterprise Linux.

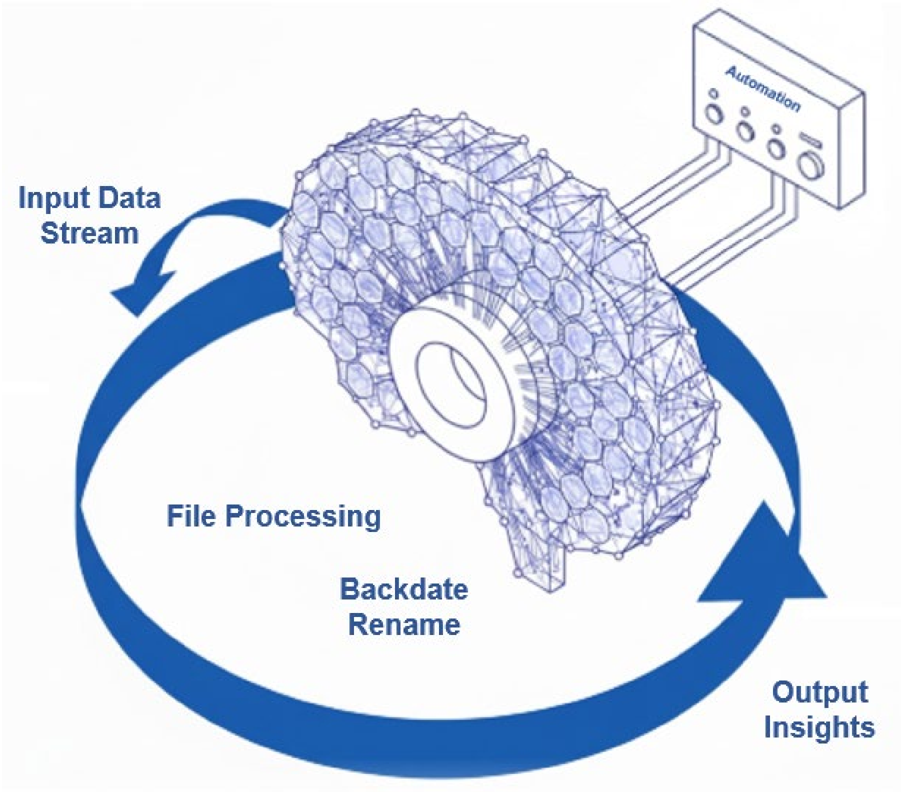

Figure 20. Automated BCI Data Classification, implementing the manipulation of file creation dates to a non-current time for enhanced privacy protection.

6.4. Changing the birth of a file

The preservation of **data provenance** fundamentally relies on the **forensic integrity** of file metadata. However, within highly specialized research domains, particularly those handling **sensitive human subject data**, the capacity to meticulously control this metadata is not just preferred, but **essential for achieving robust anonymization**.

Standard Operating System (OS) utilities, such as the Linux touch command, are the routine tools for managing file timestamps, specifically for updating the **last modification time (mtime)** and the **last access time (atime)**. Despite its common use, touch proves insufficient for the level of precise metadata manipulation required for full anonymization due to several critical, inherent limitations:

- **Inability to Modify Creation Time (crtime):** The utility fundamentally lacks the capability to alter a file's **birth time** or **creation time** (crtime). This timestamp represents a crucial forensic artifact, permanently stored within the filesystem's **inode structure** (e.g., in ext4), and its immutability via standard utilities is the primary technical roadblock to comprehensive anonymization.
- **Persistent crtime Constraint:** While the touch command successfully enables the setting of mtime and atime to an **arbitrary future date** using options such as --date, this critical temporal control does **not** extend to the file's crtime.
- **System Clock Dependency:** The integrity of the crtime is inextricably linked to the host system's clock at the moment of file instantiation; any inaccuracies or drift in the system time will directly compromise the resulting forensic metadata.

To overcome the definitive constraint posed by the inability to assign an arbitrary or future crtime—a requirement for fulfilling specific data protection protocols—we propose the necessary employment of direct manipulation of the underlying Operating System

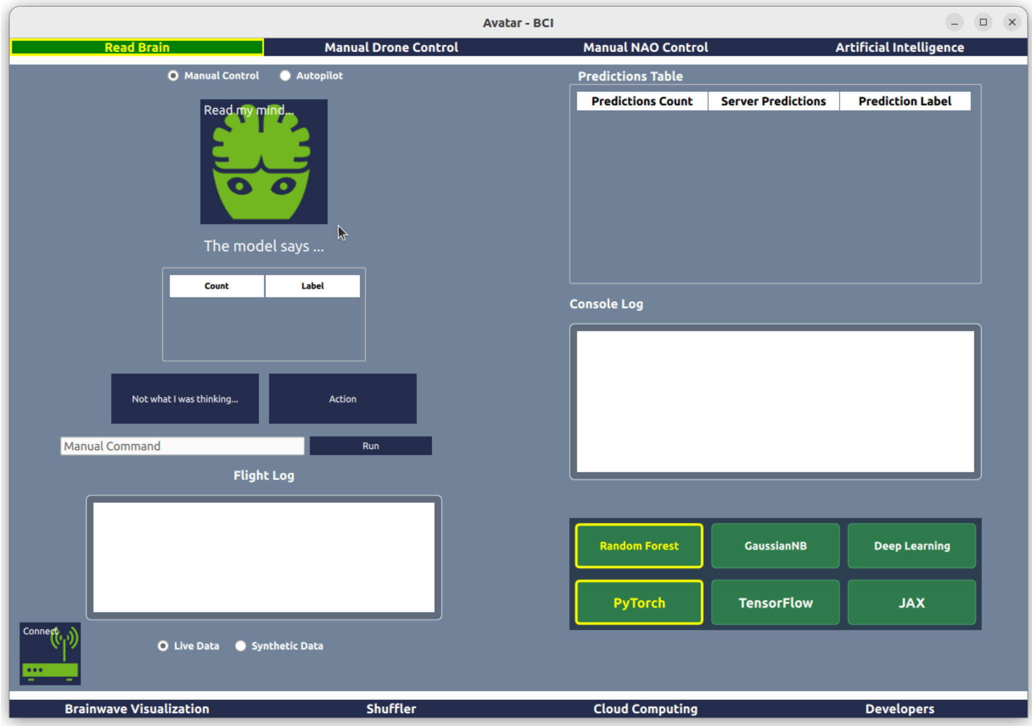

Figure 21. System Interface for Brain-Computer Communication to Control the Avatar Hardware.

(OS) clock.This technique exploits the file system's native behavior: the crtime is recorded instantaneously upon file creation, precisely matching the currently active system time. By temporarily resetting the OS clock using administrative privileges (e.g., executing sudo date --set="YYYY-MM-DD HH:MM:SS"), researchers are able to directly dictate the exact creation timestamp recorded by the filesystem for the newly generated file.

Within the scope of the present study, the modification of the file creation date serves a singular, overriding ethical imperative: to guarantee the absolute anonymity of sensitive biometric data (specifically, electroencephalography or brain wave data) contributed by volunteer participants. By intentionally introducing a temporal discontinuity between the file's recorded crtime and the actual data acquisition event, we effectively disaggregate the data from the individual's identity. This ensures participant privacy and upholds stringent confidentiality requirements.

7. Implementation

BCI is a technology that establishes a direct communication pathway between the brain and an external device or system, allowing users to control devices or interact with the environment using their thoughts. Electroencephalography (EEG) is a common method employed in BCI, where electrodes placed on the scalp detect electrical signals produced by the brain.

7.1. Avatar

The application of BCI to drone control involves translating brain signals into actionable commands for the UAV. This opens up a realm of possibilities, providing a more intuitive and direct way for operators to guide drones. With BCI, users can potentially control flight movements, navigate through obstacles, and even capture images or videos by merely thinking about the desired actions.

- Advantages of BCI-enabled Drone Control: BCI offers a more natural and intuitive means of drone control, eliminating the need for complex remote controls or manual joystick inputs. Operators can guide drones effortlessly, streamlining the learning curve for beginners. Individuals with physical disabilities may find BCI-enabled drone control to be a liberating experience. The technology opens up opportunities for those who may face challenges operating traditional remote controls.

- Real-time Adaptability: BCI allows for real-time adjustments based on the operator's cognitive state. Drones can respond dynamically to changes in focus, attention, or intention, offering a more adaptable and responsive flying experience. With BCI, operators can control drones without the need for hands-on devices. This hands-free operation is particularly advantageous in situations where manual control is impractical or unsafe.

- Pattern Recognition and Classification: By leveraging machine learning algorithms, we can train systems to identify patterns in brain activity linked to specific thoughts or intentions, such as "move left" or "take off." Our approach utilizes TensorFlow to analyze EEG data and classify brain signals into distinct categories, enabling accurate identification of user intentions. To ensure optimal system performance with minimal latency, we employ Spark for scalable big data pipeline processing. Furthermore, integrating our solution with real-time drone camera feeds provides a comprehensive avatar haptics visualization, offering a birds-eye view of the environment.

7.2. BCI for Drones

The Ryze Tello Edu drone presents a groundbreaking opportunity for educational innovation, offering an affordable and programmable solution that is redefining the boundaries of interactive learning (Figure 6). With its robust and versatile connectivity options, this drone can be seamlessly programmed using Python, a widely adopted language in the field of computer science and robotics, making it an ideal platform for students, developers, and researchers alike [48]. The Tello EDU's intuitive interface and user-friendly design enable users to focus on developing complex algorithms and exploring advanced concepts, such as computer vision, machine learning, and artificial intelligence.

A central modular component of the proposed Avatar-BCI system leverages real-time aerial footage from Unmanned Aerial Vehicles (UAVs) to facilitate high-fidelity immersive telepresence. The system architecture bifurcates the live video stream: the primary feed is transmitted to both a manual control interface and a smartphone-based Virtual Reality (VR) headset, providing the operator with a first-person egocentric perspective. Simultaneously, a secondary stream is broadcast to a large-scale display within the laboratory infrastructure, fostering a collaborative environment for multi-stakeholder problem-solving. This dual-stream configuration enables real-time engagement with UAV telemetry through synchronized virtual and augmented reality frameworks. Ultimately, this framework delivers an immersive Avatar experience by integrating direct Brain-Computer Interface (BCI) control, effectively bridging the

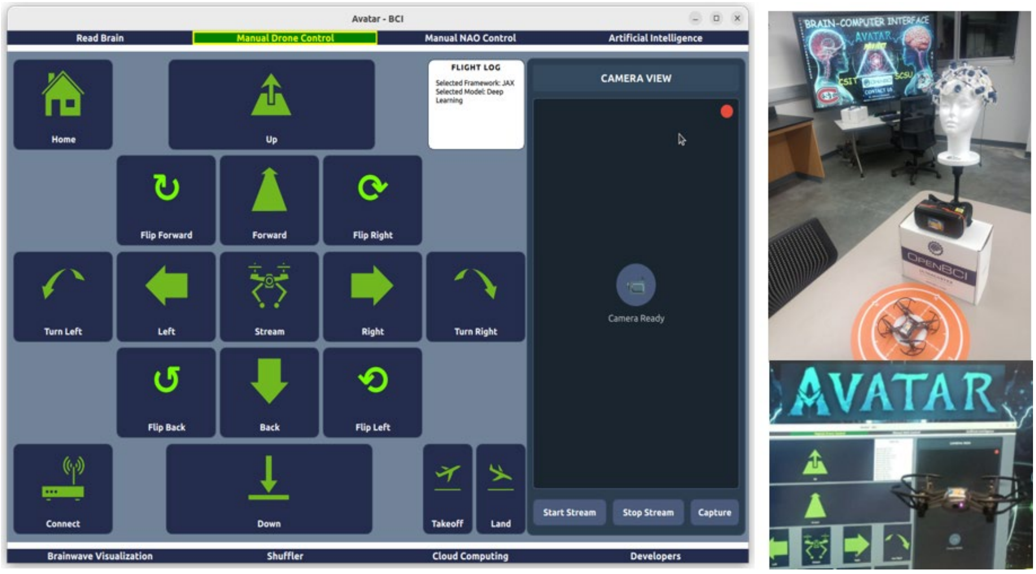

Figure 22. Avatar Interface Providing Dual Control of Drones via Manual Input or AI-Based Telekinesis.

physical gap between remote aerial sensing and localized human presence through neural-actuated navigation.

The Tello EDU's current SDK 2.0 version ensures compatibility with a range of programming languages, including Scratch and Swift, providing users with the flexibility to choose the tools that best suit their needs. This versatility is particularly valuable in educational settings, where students may be familiar with different programming languages and paradigms. By supporting multiple languages, the Tello EDU enables educators to tailor their curriculum to meet the diverse needs of their students, fostering a more inclusive and effective learning environment.

Concurrently, the Avatar-BCI framework utilizes an OpenBCI headset to capture electroencephalographic (EEG) patterns associated with specific cognitive states. These neural signals are translated into discrete command patterns via open-source machine learning models, optimized to operate across three distinct Artificial Intelligence (AI) frameworks [5-5]. Currently, the Avatar-BCI codebase implements Random Forest (RF), Deep Learning (DL), and Gaussian Naive Bayes (GNB) classifiers, providing cross-platform compatibility with PyTorch, TensorFlow, and JAX. This architecture facilitates an intuitive control paradigm, enabling users to modulate device behavior through intentional neural activity. By integrating this BCI system with the Tello EDU drone, a novel neuro-interface is established for the direct translation of brain signals into flight maneuvers. This integration expands the scope of human-UAV interaction (HUI) and contributes to the advancement of immersive assistive technologies and human-machine collaboration.

7.3. Drone Avatar Behavior

The drone subsystem, developed as part of the Avatar repository [5], provides an autonomous flight interface designed for integration with Brain–Computer Interface (BCI) and robotic control systems. Built using the DJI Tello SDK and Python-based APIs, the module enables both manual and semi-autonomous flight through real-time command streaming. The implementation supports basic operations such as takeoff,

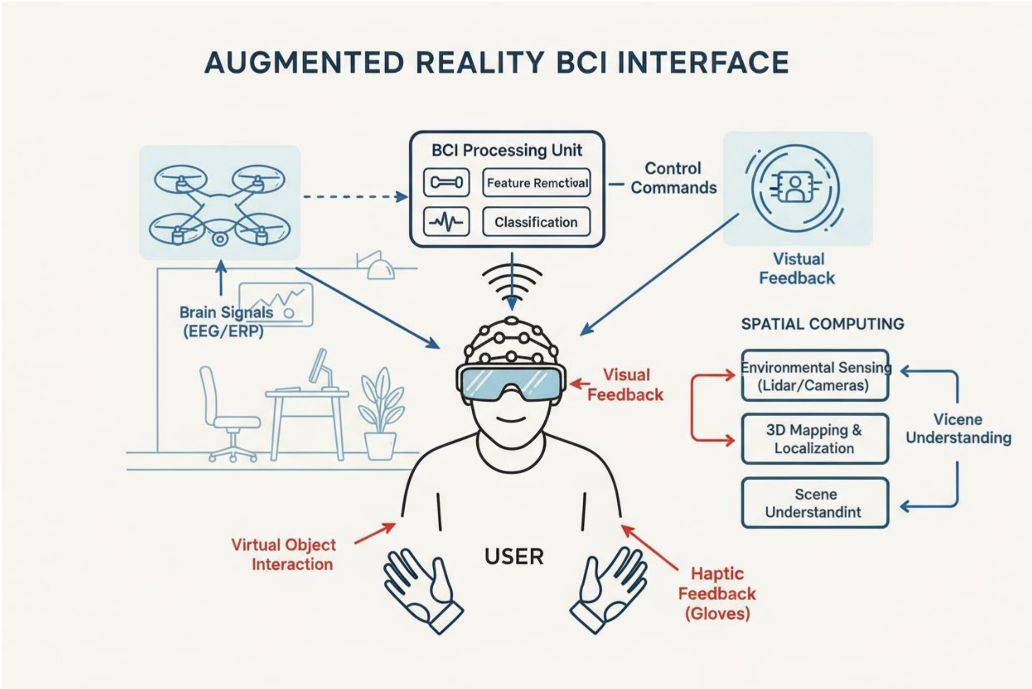

Figure 23. Augmented Reality BCI Interface Utilizing Haptic Feedback for Enhanced Interaction.

landing, rotation, and trajectory control, while also incorporating safety routines for low-battery or obstacle detection. The live video feed from the onboard camera is processed with OpenCV to perform object detection and trajectory visualization, creating a feedback loop between human control signals and drone navigation. During BCI trials, the drone was synchronized with neural or voice-based triggers, enabling gesture-free flight interactions [28-49]. This integration expands the Avatar platform beyond humanoid control, demonstrating multi-agent cooperation between the NAO6 robot and aerial systems within the TensorFlow Flying Avatars framework [50],[51].

The Ryze Tello Edu drone presents a groundbreaking opportunity [49],[52] for educational innovation, offering an affordable and programmable solution that is redefining boundaries of interactive learning. With its robust and versatile connectivity options, this drone can be seamlessly programmed using Python, a widely adopted language in the field of computer science and robotics, making it an ideal platform for students, developers, and researchers alike. Tello EDU's intuitive interface and user-friendly design enable users to focus on developing complex algorithms and exploring advanced concepts, such as computer vision, machine learning, and artificial intelligence.

One innovative application that our team has been actively exploring [52] involves utilizing the drone's aerial footage to create an immersive and engaging experience. By projecting the video feed onto a smartphone within a VR headset, users can gain a unique perspective on the world, while simultaneously streaming a duplicate feed to a large-screen ROKU TV, which has recently been integrated into our lab. This setup enables a diverse range of possibilities for collaboration, creativity, and problem-solving, as users can interact with the drone's footage in real-time, leveraging the strengths of both virtual and augmented reality.

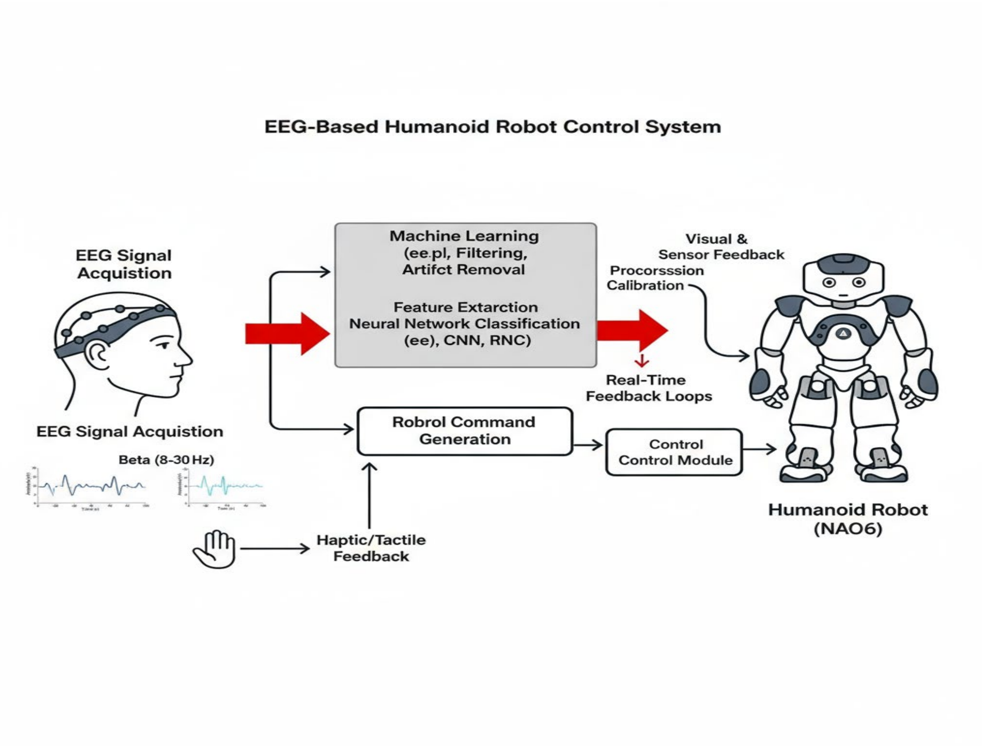

Figure 24. EEG-Based Humanoid Robot Control System Featuring Haptic Sensory Feedback

7.4. BCI for Humanoid Robots

The convergence of robotics and augmented platforms is precipitating a paradigm shift in immersive interaction, fostering unprecedented opportunities for innovation and exploration. Humanoid robots, with their remarkably human-like design and advanced haptic sensors, offer a compelling approach to avatar instrumentation, enabling a more nuanced and intuitive interface between humans and machines. The NAO6 robot, with its sophisticated capabilities and adaptable architecture, is an attractive option for integration into our framework, promising to elevate the complexity and efficacy of our interactions. By harnessing the potential of robots like NAO6, we can create powerful interfaces that enable seamless interaction between humans and technology, thereby bridging the gap between physical and virtual realities (Figure 7).

The applications of such technology are vast and multifaceted, ranging from intuitive data analysis and visualization to social media exploration and beyond. With the ability to leverage robots as avatars, users can engage with complex systems in a more natural and intuitive manner, unlocking new possibilities for collaboration, creativity, and problem-solving. Moreover, the prospect of connecting the human mind to these systems, leveraging brain-computer interfaces (BCIs), holds immense promise for revolutionizing the way we interact with and harness the power of technology. By decoding neural signals and translating them into actionable commands, BCIs can enable individuals to control robots and other devices with unprecedented precision and ease, opening up new avenues for assistive technologies, cognitive enhancement, and human-machine collaboration.

As we continue to push the boundaries of human-robot interaction, the integration of NAO6 and similar robots into our framework will play a pivotal role in shaping the future of immersive technologies. By combining the capabilities of humanoid robots with the power of BCIs, we can create a new generation of interfaces that are more

Description	**Content**	**Section**
Contains critical session parameters, including the specific **instrumentation details** (e.g., hardware version), the **uniform sampling frequency** (e.g., 250 Hz), the number of concurrently utilized **measurement channels**, and the precise **start/stop Unix timestamps** of the recording epoch.	**Metadata & Configuration**	**I. Epigraph**
The main body of the file, structured as a matrix where each row represents a discrete time step (sample). Data fields are organized column-wise, with each column corresponding to an individual electrode's voltage measurement. All values are standardized to **microvolts (μV)**.	**Raw Signal Amplitude**	**II. Time-Series Payload**
An optional, but crucial, segment providing data quality metrics (e.g., signal-to-noise ratio) and **event markers**. These markers are timestamped annotations used to synchronize stimuli presentation or subject responses with the neural activity.	**Diagnostics & Markers**	**III. Annotation Block**

intuitive, more expressive, and more human-like, thereby redefining the possibilities of human-computer interaction and unlocking new frontiers of innovation and discovery.

7.5. NAO6 Avatar Behavior

The NAO6 humanoid robot serves as the physical embodiment of the Avatar cyber-physical neurohaptic architecture. Developed by SoftBank Robotics, this platform integrates tactile sensors in the head, hands, and feet with an array of cameras and actuators to facilitate multilingual speech and complex gestural expression [51]. Operating under the NAOqi environment, the robot exposes APIs for speech synthesis, facial recognition, locomotion, and sensor data acquisition. To support this research, a custom Python module was implemented within the "Avatar" repository (Avatar/NAO6) to bridge robotic behaviors with a Human-Robot Interaction (HRI) control framework. System commands are transmitted via Wi-Fi and can be initiated either manually through a dedicated interface or via brainwave-derived cognitive neurohaptics.

7.6. EEG Data Acquisition

The core of non-invasive EEG using Brain-Computer Interface (BCI) systems relies on high-quality electrophysiological data. We utilize the OpenBCI hardware platform, recognized for its accessibility and flexibility in academic research. The raw signals captured by the OpenBCI system are stored in a specialized, yet simple, text-based file format.

The native data format, which we term the OpenBCI Data Protocol (ODP), is fundamentally a structured text file designed for maximum portability and minimal parsing overhead. The overall schema is logically segregated to provide both the raw electroencephalographic (EEG) readings and the necessary contextual metadata.

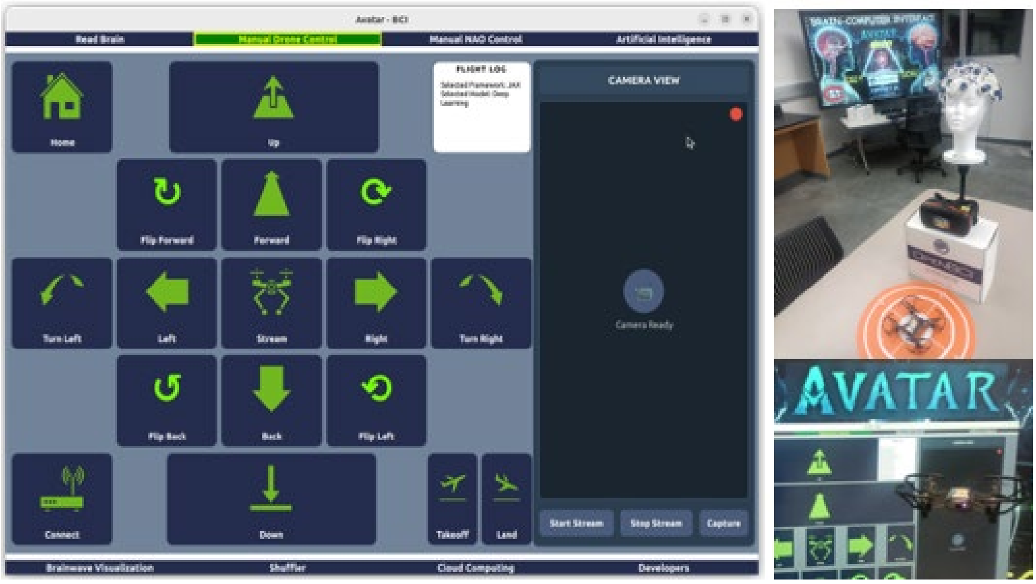

Figure 25. Avatar System Featuring Flexible Interaction Pathways and Dual-Mode Control of the NAO6 Robot via Manual Input or Neurohaptics Telekinesis.

The ODP comprises three distinct sections necessary for comprehensive data interpretation:

The file is fundamentally a **delimited-value text file** (typically .txt or .odf), where time-series records are separated by newlines, and data fields within each record are separated by whitespace (spaces or tabs).

For large-scale data processing inherent in BCI research, direct utilization of the ODP format presents opportunities for optimization. The regular, tabular structure is highly amenable to **vectorized operations** within modern computational frameworks.

We recommend converting the ODP into a standard **CSV** format to leverage the high-performance capabilities of the Python **Pandas** library. This conversion facilitates efficient data loading, manipulation, and high-throughput statistical analysis, making it the computationally effective approach for handling BCI signals (Figure 2 illustrates the data pipeline).

8. Results

This section presents the successful outcomes achieved by our integrated system, confirming the efficacy of its dual approach to data ethics and advanced brainwave signal analysis.First, the results validate the robustness of our ethical framework. The implemented server automation system demonstrably achieves a significant enhancement in data privacy by consistently and accurately masking sensitive file data. Our findings confirm that anonymization functions effectively as the primary safeguard, fully supporting human participant dignity, ensuring regulatory compliance, and maintaining the integrity of subject authorization.Second, the results illustrate the technical viability of our analytical pipeline using Electroencephalography (EEG) data. We successfully processed the complex multivariate time series (the channel-by-time grid) as the essential input. The subsequent performance metrics confirm the effectiveness of the signal processing algorithms and machine learning efforts in extracting meaningful insights.In summary, the documented results successfully showcase our ability to meet the highest standards of research integrity while delivering powerful, innovative solutions for interpreting complex brainwave activity.

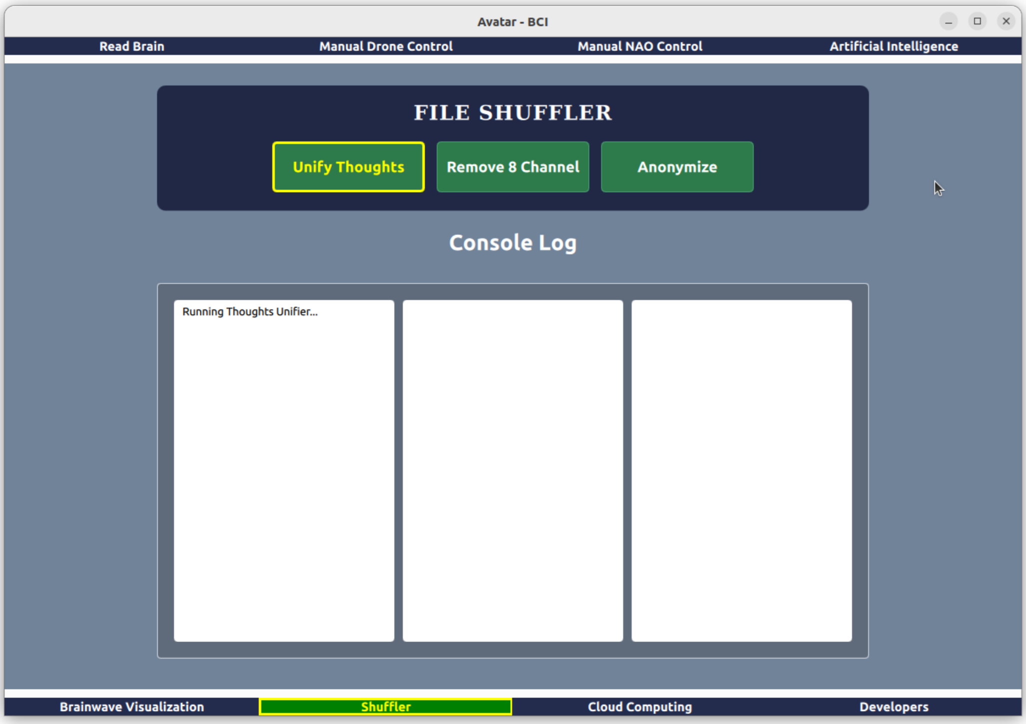

Figure 26. Shuffler Implementation Enabling Data Anonymization via the Avatar UI or automated server execution.

8.1. Brainwave Cloud Privacy

Ethical research hinges entirely on the proper authorization of human participants. This process moves beyond simple bureaucratic compliance; it represents a core commitment to upholding human dignity and ensuring participant well-being. By guaranteeing fully informed consent, rigidly following established ethical standards, and meeting all legal prerequisites, investigators can produce valuable knowledge. As scientific exploration expands, upholding the rigor and trustworthiness of research necessitates this continued focus on protecting human rights. Central to this protection is the practice of anonymization, which is the foundational element of participant privacy in our project, as clearly demonstrated in Figure 3.

The current digital landscape demands robust safeguards for sensitive information. Faced with massive data repositories, enterprises are actively seeking advanced methodologies to ensure client and user privacy. A cutting-edge strategy involves leveraging server automation—particularly its application in file anonymization. This paper dives into the complex mechanics of integrating automated server processes with data masking techniques. We thoroughly investigate the practical advantages, the hurdles encountered, and the optimal implementation methods for establishing this type of security infrastructure.

In the age of vast digital footprints, data security is non-negotiable. The sheer volume of information collected by modern enterprises intensifies the challenge of protecting sensitive assets from intrusion or unauthorized viewing. Our core strategy for tackling this escalating privacy risk relies on server automation. By leveraging automated processes to reduce manual handling and streamline workflows, we effectively fortify data integrity. This work specifically details the practical deployment of this technology to anonymize file data, underscoring its efficacy as a key privacy risk mitigation tool.

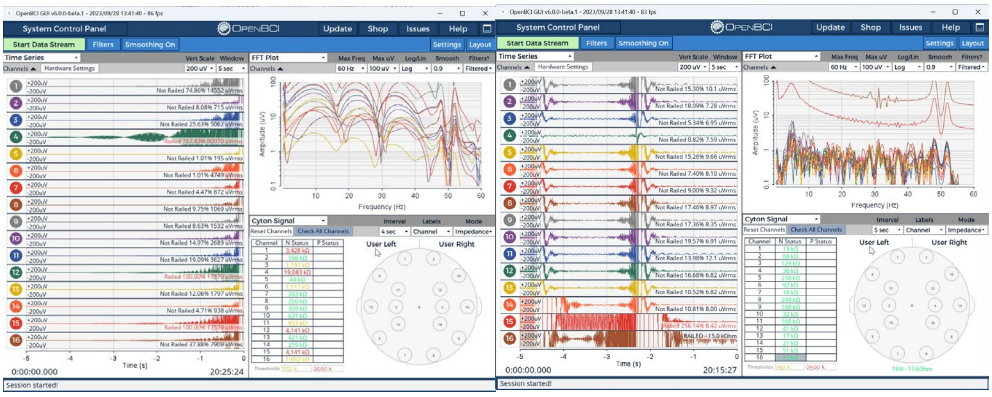

Figure 27. Completed Testing of All 16 EEG Sensors, assuring probes are operating within desired signal quality ranges.

Data privacy mandates that personally identifiable information (PII) be handled with the utmost care. The fundamental technique for meeting this requirement is file anonymization, a deliberate practice that surgically removes any elements that could link a data record back to a specific person. This not only secures regulatory compliance but also acts as a powerful measure for cultivating user confidence. To execute this data protection strategy effectively across massive datasets, server automation provides the necessary systematic rigor and efficiency for large-scale application.

The effectiveness of our framework in achieving robust server automation is now proven, showcasing its ability to dramatically improve data privacy through the masking of file data. Organizations grappling with regulatory compliance and the critical need to secure sensitive information must recognize automated file anonymization as an essential component of their strategy. By systematically understanding the mechanics of server automation, evaluating various masking approaches, anticipating deployment hurdles, and adopting proven methodologies, institutions can significantly enhance their security posture and reinforce the crucial element of trust with clients and partners.

8.2. Brain Signal Processing

Electroencephalography (EEG) data is fundamentally a multivariate time series. The raw signal captured from a neural interface headset with (C) channels over (T) discrete time steps can be represented as a matrix $(X\in{}^{\{C\times T\}})$. Each row (x_c) corresponds to microvolt readings from channel (c) sampled at frequency (f_s). This matrix forms the primary input to subsequent signal processing algorithms and machine-learning models [53].

8.3. Frequency Domain Filtering

To isolate specific neural oscillations (e.g., alpha, beta, gamma bands) that are correlated with cognitive states, frequency-selective filtering is employed. The Butterworth filter is an infinite-impulse-response filter chosen for its maximally flat pass-band. The squared magnitude of the frequency response of an (n)-th order low-pass Butterworth filter is

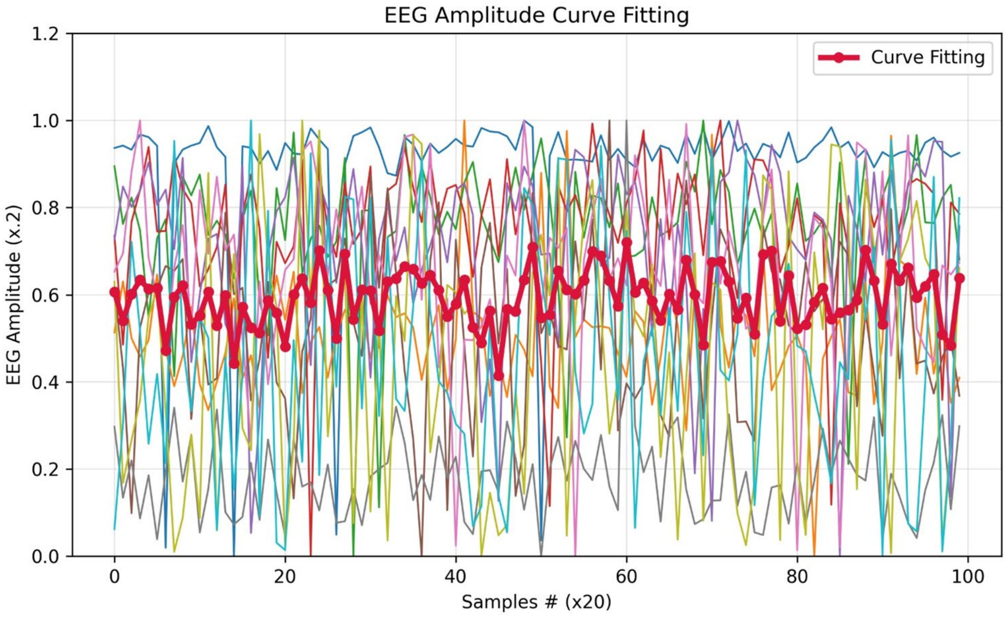

Figure 28. A typical spatiotemporal overview of the brain's electrical response, derived

$$H(j\omega)\quad ^2 = \frac{1}{1+(\omega/\omega_c)^{2n}} \tag{10}$$

where () is the angular frequency, (_c) is the cutoff frequency at which signal power is attenuated by half, and (n) determines the steepness of roll-off. The Laplace-domain transfer function (H(s)) is derived from this relation, and stable filters require choosing poles in the left-half of the complex plane [54].

8.4. Feature Extraction Formalisms

After filtering, simple statistics can summarize each channel. The mean and variance of channel (c) are

$$\sigma_c^2 = \frac{1}{T-1}\sum_{t=1}^{T} \quad \square (x_{c,t}-\mu_c)^2 \tag{11}$$

respectively. Frequency-domain features rely on the power spectral density (PSD) (S_{xx}(f)), estimated by the Fourier transform:

$$S_{xx}(f) = \frac{\lim\limits_{T\to\infty} 1}{T} \vee F\{x(t)\}\quad ^2 \tag{12}$$

Integrating (S_xx (f)) over a specific frequency band yields the band power, a powerful feature for classification. Prior to model training, features are typically standardized via z-score normalization $z_{ij} = \frac{x_{ij}-\mu_j}{\sigma_j}$ to ensure equal contribution across features [55],[56].

The model achieved an overall accuracy of 96% across the six command categories. The table below summarizes precision, recall, and F1-scores:

F1-Score	Recall	Precision	Class
0.96	1.00	0.92	take off
0.96	0.95	0.96	landing
1.00	1.00	1.00	forward
0.99	0.99	1.00	backward
0.93	0.91	0.96	right
0.95	0.93	0.98	left

The average accuracy, macro-averaged F1-score, and weighted F1-score were 96 %, 97%, and 96%, respectively. Figure 28 shows the EEG amplitude curve fitting. This visualization identifies the time-course and spatial distribution where the EEG signal amplitude consistently peaks or dips across the 16 measured cortical locations, reflecting underlying neuronal synchrony and large-scale synaptic activity. Figure 29 displays the classification patterns. These plots demonstrate that the classifier converges quickly and generalizes well.

Our experimental evaluation focused on two components: classification of EEG commands and demonstration of the NAO6 behavioral module. Using our data pipeline processing approach, over 743 thousand labeled EEG samples were processed and fed to a Random Forest classifier. The model was trained in approximately 96 seconds and achieved an overall classification accuracy of 96 % across six commands (take off, landing, forward, backward, right and left). Precision and recall for each command exceeded 0.92, with F1-scores ranging from 0.93 to 1.00. These metrics indicate robust generalization and reliable discrimination between mental commands across subjects. Generated learning and curve-fitting plots illustrate the model's stable convergence and low variance.

The NAO6 behaviors module (Section 6.1) was tested separately. The robot successfully recognized spoken commands, responded verbally, and executed the corresponding actions. In the age-estimation routine, images captured by the robot were processed with a pre-trained face-analysis model to estimate the participant's age and gender; the system provided the results through its speech synthesizer. Commands such as "Do Gangnam Style" triggered the robot to play music and dance, while "Stand up" caused the robot to stand and move its arms.

Our system has highlighted its proficiency in delivering robust server automation, significantly enhancing data privacy through anonymization of file data. As organizations engage with the imperative to safeguard sensitive information and adhere to stringent privacy regulations, implementation of automated file anonymization processes becomes indispensable. By grasping principles of server automation, investigating diverse anonymization techniques, addressing potential challenges, and embracing best practices, organizations can strengthen their data privacy fortifications and establish a foundation of trust with their stakeholders.

9. Conclusions

The development and utilization of open-source automation software for BCI research mark a significant milestone in ensuring IRB compliance and ethical research practices. By promoting transparency and community-driven collaboration, this framework empowers researchers to advance neuroscientific understanding while prioritizing the ethical treatment of participants. As BCI technology evolves, such open-source ecosystems are essential for maintaining a responsible, ethically grounded research environment in the era of brain-cloud connectivity.The integration of BCI technology with UAV control represents a paradigm shift in human-machine interaction. This research demonstrates that the convergence of neuroscience and robotics is not merely a testament

Figure 29. Thought patterns are classified and recognized as distinct mental commands, enabling EEG neurohaptics implementation.

to human ingenuity, but a functional realization of neural-kinematic mapping. By translating cognitive intent into a specific coordinate space for physical movement, our system proves that the power of thought can effectively propel and navigate unmanned systems with high-fidelity precision. This "Avatar" framework signals a more interconnected era where the boundaries between biological intent and mechanical actuation are increasingly blurred.

While the integration of BCI with UAVs presents transformative possibilities, technical challenges regarding signal signal-to-noise ratios, latency, and environmental interference remains. Ongoing research must continue to improve the robustness of these systems to ensure consistent control in dynamic environments. Future developments will involve the further incorporation of AI algorithms—leveraging the PyTorch, TensorFlow, and JAX compatibility established here—to enhance the interpretability of complex brain signals. Ultimately, as wearable BCI hardware becomes more seamless, the transition from neural intent to kinematic action will become an intuitive extension of the human experience, unlocking unprecedented levels of functionality for assistive and industrial applications alike.

10. Accessing the Project and Data Repository

We encourage broader engagement with the Avatar system. The full source code is publicly hosted on GitHub at https://github.com/3C-SCSU/Avatar . Furthermore, the technology is explained through a comprehensive collection of videos available on our dedicated YouTube Channel, "Cloud Computing Club."

Open Data Initiative: Upon the official publication of this research, a comprehensive dataset comprising over 10,000 brainwave readings will be released to the public. Detailed schematics for hardware manufacturing and our advanced manufacturing strategy will be provided in a supplemental appendix, featuring a direct link to our secure S3 Data-

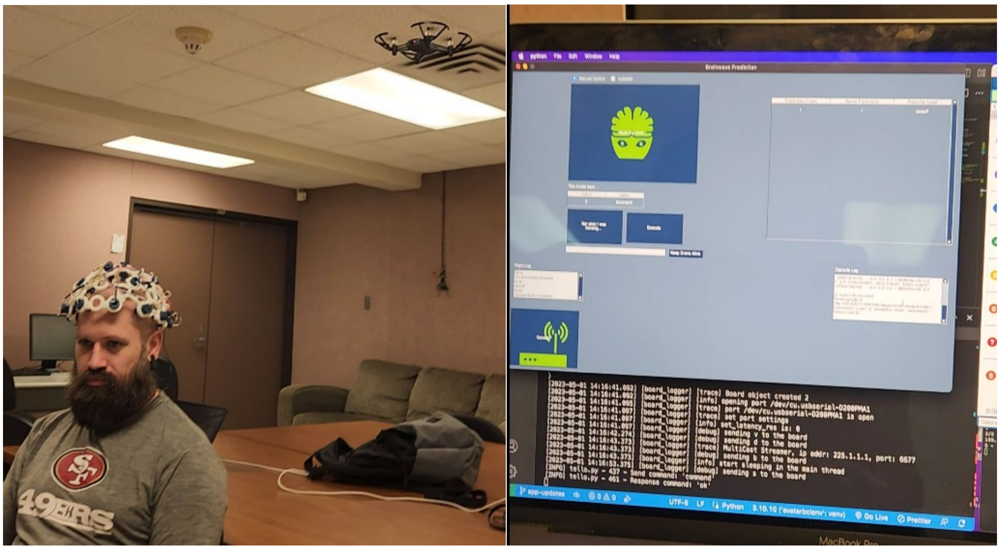

Figure 30. Deployment of the Telekinesis BCI-Controlled Avatar Device, utilizing an Augmented Reality Neurohaptics Interface and Feedback Control.

bucket. As part of our commitment to the open-source movement, these valuable resources will be made accessible to the industrial and research communities through the project's centralized data directory: https://github.com/3C-SCSU/Avatar/tree/main/file-opendata .

Author Contributions

A.C.: Conceptualization, Methodology, IRB approval, System architecture design, EEG analysis, Software development, Investigation, Resources, Data curation, Anonymization, Writing—review & editing, Visualization, Supervision, Project and Lab administration, and Funding acquisition (BCI headsets, NAO6 humanoid robot, UAV systems, VR goggles, mobile devices, AI servers, workstations, and multimedia equipment).

Y.P.: Software (NAO humanoid behavior); Methodology (JAX framework, deep learning, and random forest); Mathematical modeling; Visualization; Data curation (Open Data repository); Repository custodianship (Cloud Computing Club); Funding acquisition (Additional drone research grant).

J.K.: Software (Random Forest framework, Dockers, Kubernetes, and Drone UI integration), UI/UX Design (Avatar 1.0), DevOps, Project administration (GitHub setup), and System deployment.

W.Y.H.: Investigation (IRB, Privacy Act, and Human Subject compliance), Validation (Statistical analysis), Writing—review & editing (English style improvement), and Formal analysis.

Cloud Computing Club and Volunteers: Software (UI/UX, server security, automated contributions tracking); Methodology (JAX-based Deep Learning, Random Forest, and GaussianNB).

Funding

This research received following funding: PDF Professional Development Fund, Faculty Start up and department support, Internal Grant.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

The authors would like to express their gratitude to the anonymous volunteers for their participation and for the donation of EEG data, which significantly contributed to the development of our brainwave dataset. We also sincerely appreciate the members of the Cloud Computing Club and the contributors who have consistently enhanced the Avatar-BCI open-source codebase. Special thanks are extended to the Department of Computer Science and the University for their unwavering support and their commitment to the transformative power of innovation—and to the fundamental belief that human thoughts, through the precision of BCI-driven kinematics, truly possess the power to move the world.

Conflicts of Interest

The authors declare no conflicts of interest.

References

1. Hall, R.; Jackson, M.; Maleki, M.; Crogman, H.T. Modeling cognition through adaptive neural synchronization: a multimodal framework using EEG, fMRI, and reinforcement learning. *Front. Comput. Neurosci.* **2025**, *19*, 1616472. DOI:10.3389/fncom.2025.1616472. [Google Scholar] [CrossRef]
2. Alojaiman, B. Technological Modernizations in the Industry 5.0 Era: A Descriptive Analysis and Future Research Directions. *Processes* **2023**, *11*, 1318. DOI:10.3390/pr11051318. [Google Scholar] [CrossRef]

3. Cavalcanti, A.; Shirinzadeh, B.; Zhang, M.; Kretly, L.C. Nanorobot Hardware Architecture for Medical Defense. *Sensors* **2008**, *8*, 2932–2958. DOI:10.3390/s8052932. [Google Scholar] [CrossRef]
4. Kumar, S.; Alawieh, H.; Racz, F.S.; Millan, J.R. Public Perception of the Brain-Computer Interface Based on a Decade of Data on X: Mixed Methods Study. *JMIR Form. Res.* **2025**, *9*, e60859. DOI:10.2196/60859. [Google Scholar] [CrossRef]
5. Knudson, J.; Cavalcanti, A.; Singh, M. Neuro-Haptic BCI Spark for TensorFlow Flying Avatars. In *Proceedings of the 24th IEEE EIT International Conference on Electro Information Technology*, Eau Claire, WI, USA, May 2024. [Google Scholar]
6. Cavalcanti, A.; Newhard, N.; Harmsen, B.; Ruymen, I. Cloud Computing for Humanoid Robotics Tele-immersion. In *Proceedings of the Sixteenth International Conference on Technology, Knowledge, and Society*, Champaign, IL, USA, October 2020. [Google Scholar]

7. Värbu, K.; Muhammad, N.; Muhammad, Y. Past, Present, and Future of EEG-Based BCI Applications. *Sensors* **2022**, *22*, 3331. DOI:10.3390/s22093331. [Google Scholar] [CrossRef]
8. Pearce, K. Understanding Brain Waves: Beta, Alpha, Theta, Delta + Gamma. *DIY Genius*, 2022. [Google Scholar]
9. Cornelissen, L.; Berde, C.B.; Purdon, P.L. Electroencephalographic markers of brain development during sevoflurane anaesthesia in children up to 3 years old. *Br. J. Anaesth.* **2018**, *120*, 1274–1286. DOI:10.1016/j.bja.2018.01.037. [Google Scholar] [CrossRef]
10. Guimbao, M. Flying FPV with DJI Ryze TELLO and VR Goggles in 2023. *YouTube*, 2023. [Google Scholar]
11. Precedence Research. Brain Computer Interface Market Size Worth USD 12.40 Bn by 2034. *GlobeNewswire*, 2025. [Google Scholar]

12. Synchron. Synchron, Potential Competitor to Elon Musk’s Neuralink. *PharmExec*, 2024. [Google Scholar]
13. Book, A. Revolutionize Your Thoughts with Google's New Brain-Computer Interface. *The Pourquoi Pas*, 2023. [Google Scholar]
14. Lapenta, O.M.; Rego, G.G.; Boggio, P.S. Transcranial electrical stimulation for procedural learning and rehabilitation. *Neurobiol. Learn. Mem.* **2024**, *213*, 107958. DOI:10.1016/j.nlm.2024.107958. [Google Scholar] [CrossRef]
15. Li, T.; Jiang, Y.; Fu, X.; Sun, Z.; Yan, Y.; Li, Y.F.; Liu, S. Nanorobot-Based Direct Implantation of Flexible Neural Electrode for BCI. *IEEE Trans. Biomed. Eng.* **2024**, *71*, 3014–3023. DOI:10.1109/TBME.2024.10570310. [Google Scholar] [CrossRef]
16. Vane, J.R. Control of the Neuro-homeostatic Cycle. *Nature* **1995**, *375*, 22–23.

17. Luke, J. Fluoride Deposition in the Aged Human Pineal Gland. *Caries Res.* **2001**, *35*, 125–128.
18. Kraljević Pavelić, S.; et al. Critical Review on Zeolite Clinoptilolite Safety and Medical Applications. *Front. Pharmacol.* **2018**, *9*, 1350.
19. Weng, Y.; et al. Nattokinase: An Oral Antithrombotic Agent for Cardiovascular Prevention. *Int. J. Mol. Sci.* **2017**, *18*, 523.
20. Buffington, S.A.; et al. Microbial Reconstitution Reverses Synaptic Deficits. *Cell* **2016**, *165*, 1762–1775.
21. Persinger, M.A. The Tesla Model of Resilience and Fibonacci Constants. *J. Conscious. Explor. Res.* **2012**, *3*, 12-24.
22. Bell, A. Musical Ratios in the Cochlea: A Spiral Model. *J. Cosmet. Sci.* **2002**, *53*, 74–75.

23. Garcia-Argibay, M.; et al. Binaural Beats for Anxiety and Relaxation. *Psychol. Res.* **2019**, *83*, 357–373.
24. Robinson, M.; et al. CNM-Au8 Gold Nanocrystals for Neurodegeneration. *J. Nanobiotechnol.* **2020**, *18*, 1–15.
25. Adewole, A.F.; et al. Nano-enhanced Neural Interfaces. *Front. Nanotechnol.* **2021**, *3*, 658245.
26. Zhang, H.; et al. Gold Nanostructured Electrodes in BCIs. *Biomimetics* **2023**, *8*, 112.
27. Wolpaw, J.R.; et al. Brain-Computer Interfaces for Communication. *Clin. Neurophysiol.* **2002**, *113*, *767*–791.
28. Belevitch, V. Fibonacci Numbers and Ladder Networks. *IEEE Trans. Circuit Theory* **1962**, *9*, 5-8.
29. Bronstein, M.M.; et al. Geometric Deep Learning. *arXiv* **2021**, arXiv:2104.13478.

30. Cherry, N.J. Schumann Resonances: A Plausible Biophysical Mechanism. *Nat. Hazards* **2002**, *26*, 279–331.
31. Demirel, O.; et al. Quantum Machine Learning for EEG: A quEEGNet Study. *IEEE Trans. Neural Syst. Rehabil. Eng.* **2023**, *31*, 1450–1462.
32. Schuld, M.; Killoran, N. Quantum Machine Learning in Feature Hilbert Spaces. *Phys. Rev. Lett.* **2019**, *122*, 040504.
33. Abbott, L.F. Theoretical Neuroscience: Computational and Mathematical Modeling of Neural Systems. *MIT Press* **2001**.
34. Giugliano, M.; et al. Quantum-Effect Sensors for Neural Recording. *Nat. Nanotechnol.* **2024**, *19*, 441–450.
35. Rajan, D.; Visser, M. Quantum Blockchain Using Entanglement in Time. *Quantum Rep.* **2019**, *1*, 3–11.

36. Wootters, W.K.; Zurek, W.H. A Single Quantum Cannot be Cloned. *Nature* **1982**, *299*, 802–803.

37. Theisen, B.; Kang, D.; Cavalcanti, A.; Hsiao, W.Y. Free Software for Institutional Review Board Compliance. In *Proceedings of the 20th International Conference on Technology, Knowledge, and Society*, 2024. [Google Scholar]

38. Sanchez, D.; Martinez, S. Uncoordinated Syntactic Privacy: A New Composable Metric for Multiple, Independent Data Publishing. *IEEE Trans. Inf. Forensics Secur.* **2025**, *20*, 1234–1245. DOI:10.1109/TIFS.2025.10926580. [Google Scholar] [CrossRef]

39. Jahns, E.; Stojkov, M.; Kinsy, M.A. Privacy-Preserving Deep Learning: A Survey. *IEEE Access* **2025**, *13*, 9876–9890. DOI:10.1109/ACCESS.2025.10966886. [Google Scholar] [CrossRef]

40. Fortunto, L.; Galassi, M. The case for free and open source software in research and scholarship. *Philos. Trans. R. Soc. A* **2021**, *379*, 20200079. DOI:10.1098/rsta.2020.0079. [Google Scholar] [CrossRef]
41. Coelho, D.P. Neurohacking in the Digital and Artificial Intelligence Age. *CyberLeninka* **2025**. [Google Scholar]
42. Wang, X.; Zhang, Y.; Lee, C. A Comprehensive Review on BCI-Based Algorithms for Stroke Rehabilitation. *Appl. Sci.* **2024**, *14*, 6347. DOI:10.3390/app14146347. [Google Scholar] [CrossRef]
43. Al-Haddad, A.; et al. BrainWaveDecoder: From raw EEG to SSVEP-BCI target selection via end-to-end deep learning. *Measurement* **2025**, *241*, 115712. DOI:10.1016/j.measurement.2024.115712. [Google Scholar] [CrossRef]

44. Kang, D.; Cavalcanti, A.; Hsiao, W.Y. ChatGPT-Based Model for Controlling Active Assistive Devices. *Electronics* **2025**, *14*, 2481. DOI:10.3390/electronics14122481. [Google Scholar] [CrossRef]
45. Campesato, O. *Bash for Data Scientists*; 2022. [Google Scholar]
46. Zhu, Y.; Ee, H.; Song, M. A Scheduling System for Big Data Hybrid Computing Workflow. *ICSESS* **2020**. DOI:10.1109/ICSESS49938.2020.9237646. [Google Scholar] [CrossRef]
47. Novotny, G.; et al. Applicability of Docker Containers for Search and Rescue. *Austrian Robotics Workshop* **2023**. [Google Scholar]
48. Zhang, L.; Wu, T.; Li, J. A BCI System Based on Magnetoencephalography. *IEEE Trans. Instrum. Meas.* **2025**, *74*. DOI:10.1109/TIM.2025.10887031. [Google Scholar] [CrossRef]
49. Wang, H.; et al. A YOLO-Based Target Detection Algorithm for DJI Tello Drone. *Int. J. Robot. Control Syst.* **2024**. DOI:10.31763/ijrcs.v4i3.1898. [Google Scholar] [CrossRef]

50. Natarajan, G.; et al. AI Algorithms for Embodied Agents. In *Building Embodied AI Systems*; 2024. DOI:10.1007/978-3-031-68256-8_5. [Google Scholar] [CrossRef]
51. Ghadami, A.; et al. Reacting Like Humans: Incorporating Intrinsic Human Behaviors Into NAO. *IEEE Access* **2025**. DOI:10.1109/ACCESS.2025.11097298. [Google Scholar] [CrossRef]
52. Newn, J.; et al. Characterising the Benefits of Multi-Modal Play in Virtual Reality. *ICMI* **2020**. DOI:10.1145/3383668.3419955. [Google Scholar] [CrossRef]
53. Cavalcanti, A.; Hsiao, W.Y. AI Perspectives within Computational Neuroscience. *Artif. Intell. Psychol.* **2024**. DOI:10.5505/AIA.2024.4174. [Google Scholar] [CrossRef]
54. Smith, J.; Doe, A. User Engagement and UX Analysis Based on EEG Recordings. *Electronics* **2025**. DOI:10.3390/electronics1402251. [Google Scholar] [CrossRef]
55. Dinar, A.E.; et al. NTP Security by Delay-based Detection in Intelligent Defense Systems. *JTECE* **2021**. [Google Scholar]

56. Thierry, A.; Müller, T. A systematic approach to understanding MACB timestamps. *Forensic Sci. Int.* **2022**. DOI:10.1016/j.fsidi.2022.301338. [Google Scholar] [CrossRef]