

No Brain, No Gain

The Next Frontier in IoT/ICS Authentication

Presented by:

Mehmet Önder Key, Temel Demir

Event: *August 2025*, *DEFCON33 IoT Village*

AGENDA

01 Introduction & The Evolving Threat Landscape

02 Foundations & Unique Advantages of EEG Biometrics

03 Comparative Analysis & Technical Architecture

04 GMM Training & Utilization for EEG Authentication

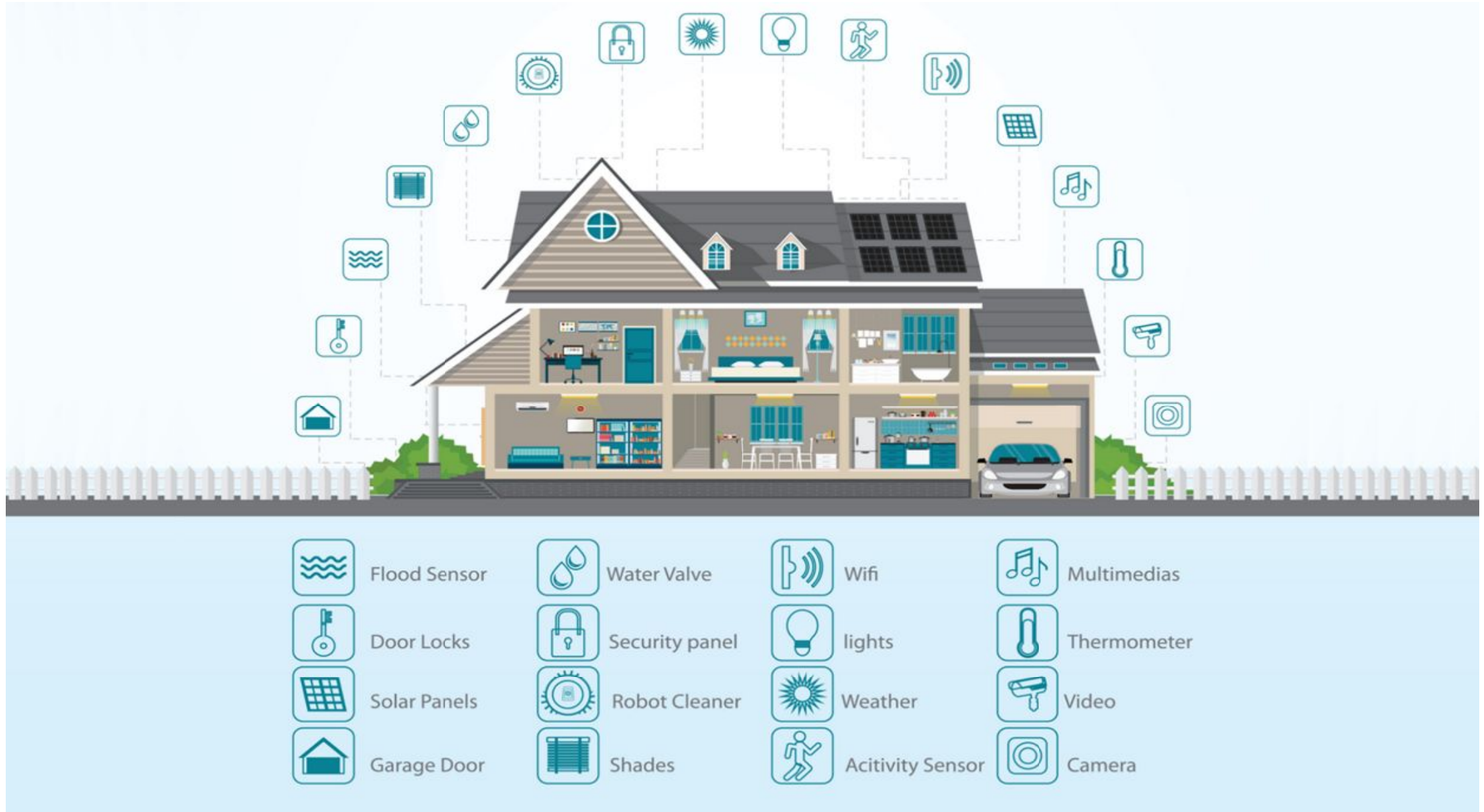
05 Demonstration



Introduction & The Evolving Threat Landscape

Strategic Advantage:

- **Converging Risks:** IoT/ICS convergence expands attack surface, creating severe cyber-physical threats with real-world consequences.
- **Inadequate Defenses:** Traditional authentication methods are fundamentally insufficient against sophisticated, evolving attacks (e.g., deepfakes, quantum threats, social engineering).
- **EEG, The Next Frontier:** Electroencephalography (EEG) biometrics offer intrinsic liveness detection, robust resistance to spoofing and coercion, and continuous authentication capabilities.
- **Probabilistic Modeling:** Gaussian Mixture Models (GMMs) are central to accurately modeling the complex, unique patterns of brain activity for reliable authentication.
- **Critical Necessity:** Adopting EEG-based authentication is a strategic imperative for maintaining operational continuity, safeguarding national security, and protecting public safety in critical infrastructure.

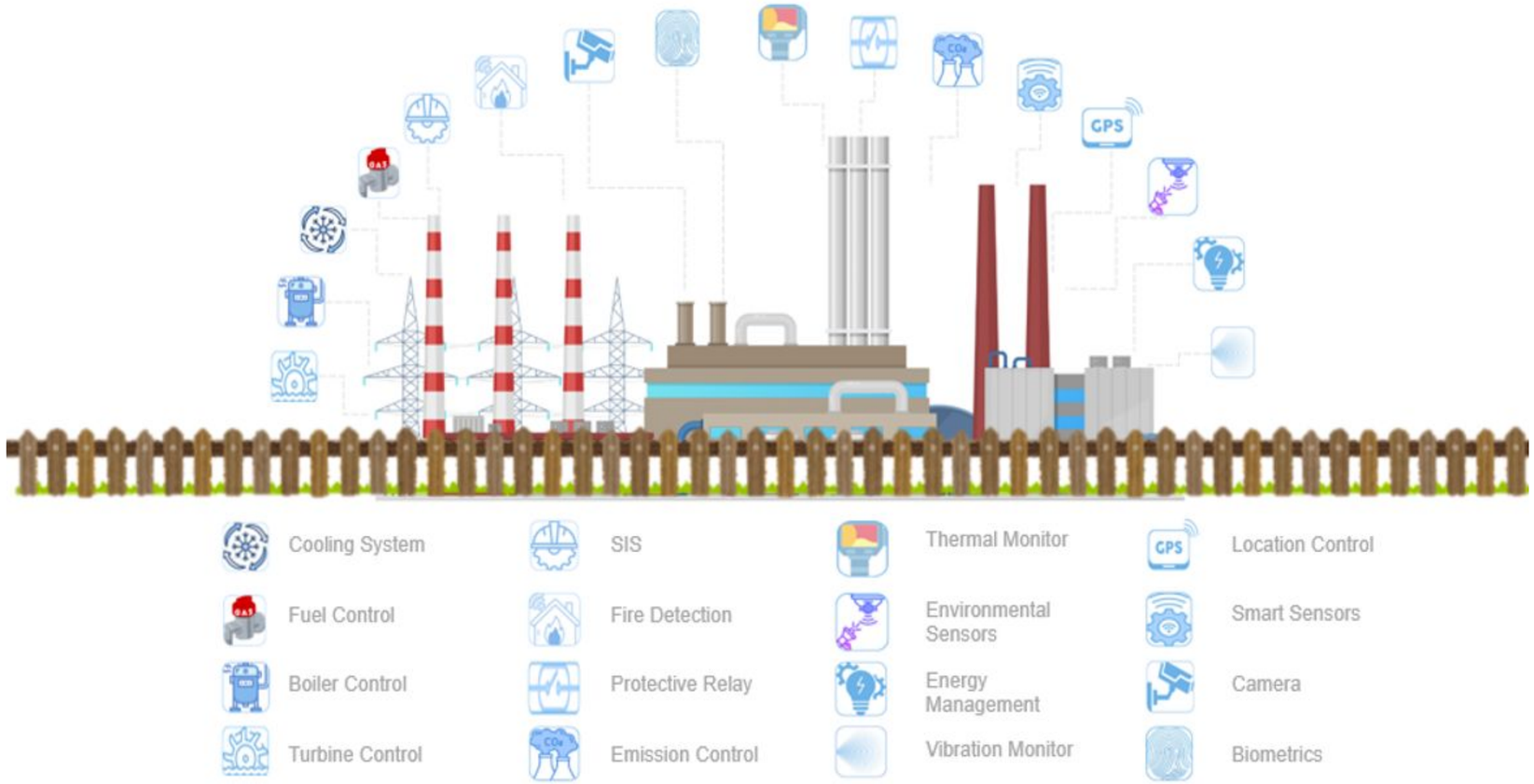


Criticality:

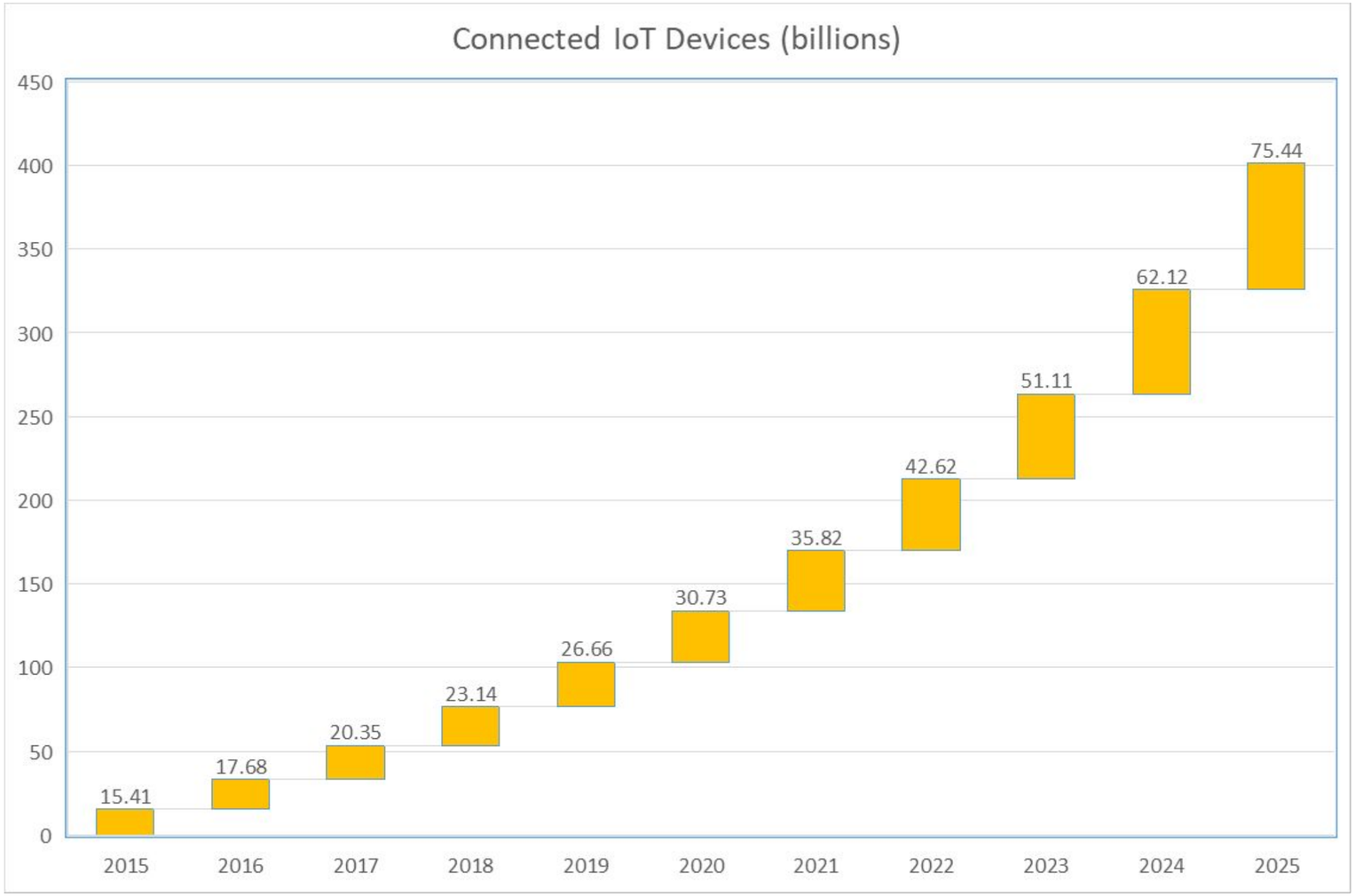
- Backbone of essential services: energy grids, water treatment, manufacturing, healthcare, defense.
- Cyber vulnerabilities directly impact physical processes, human safety, and national security.
- Compromise can lead to widespread operational failures, physical damage, and even loss of life (e.g., water treatment plant hack leading to chemical overdoses).

Inherent Vulnerabilities:

- **Systemic Weaknesses:** Pervasive use of weak/default passwords, insecure network services, outdated firmware, and lack of encryption.
- **Alarming Statistics:** An alarming 98% of IoT device traffic is unencrypted, making nearly all data could be intercepted.
- **Design Philosophy:** Many ICS components deployed before modern cyber threats, prioritizing longevity and operational functionality over security, often omitting encryption to reduce costs.



Connected IoT Devices



Source: https://www.mdpi.com/2078-2489/12/4/154

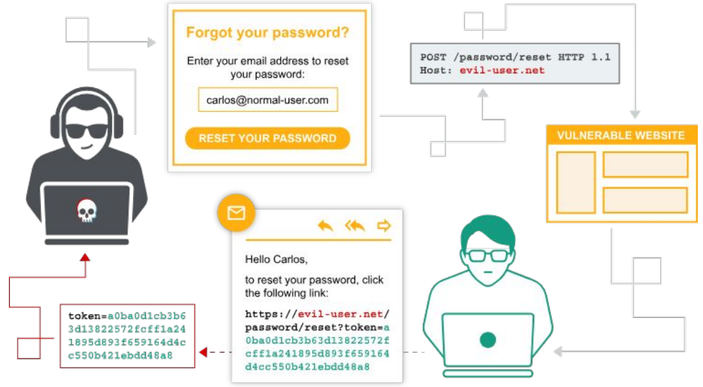
Traditional Methods (Passwords, PINs, Tokens, Fingerprints, Face)

- **Susceptibility:** Inherently susceptible to theft, loss, forgery, brute-force attempts, and social engineering.
- **Replicability:** Fingerprints and faces, while unique, can be easily obtained and replicated (e.g., from images, deepfakes), and even used post-mortem.
- **Lack of Liveness:** Many lack intrinsic liveness detection, failing to verify if the authenticating entity is a live human.



Fundamental Flaw

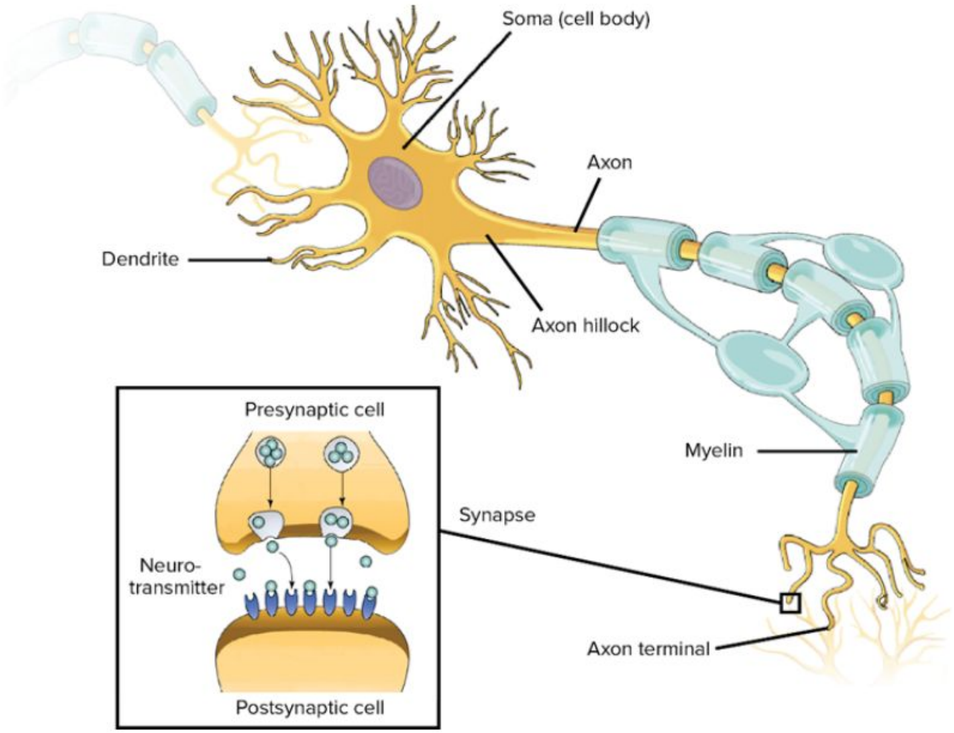
- **Remote Access Exploitation:** Adversaries target remote access points, mimicking authorized users to establish persistent access.
- **Supply Chain Attacks:** Vulnerabilities introduced during manufacturing or distribution (e.g., malicious firmware updates).
- **Man-in-the-Middle (MITM):** Exploiting unencrypted communications to inject malicious payloads or steal credentials.
- **Phishing & Malware**: Remain prevalent tactics to compromise system integrity.

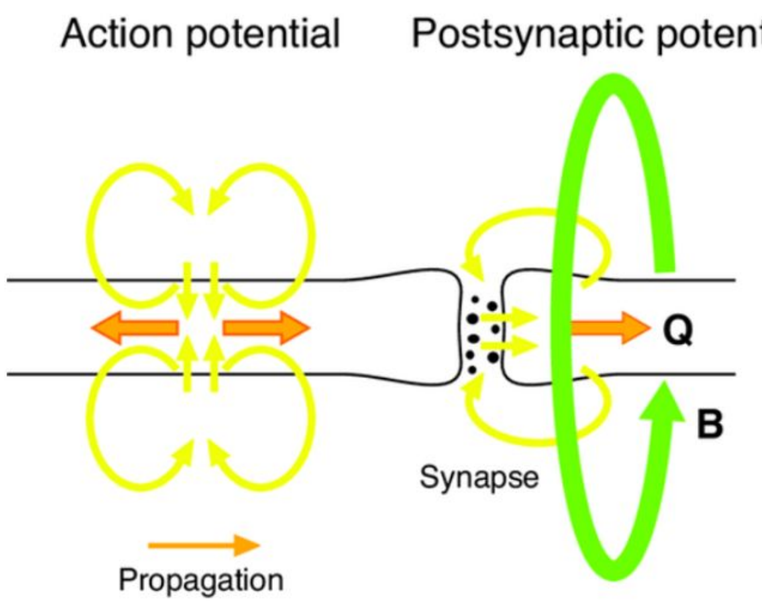


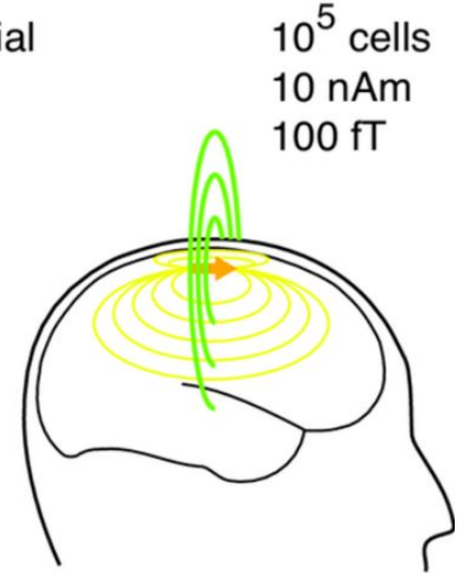
Source: https://portswigger.net/web-security/authentication

Neurons

- Neurons in the brain are electrically excitable cells. The human brain has approximately 55 to 70 billion neurons. Neurons communicate through unique connections called axons and using a structure called synapsis. Axon terminal uses Synapse points to communicate with another neuron. The presynaptic cell forms the connection with the Neurotransmitter. The postsynaptic cell is located on the receiving side, not the connecting side, and determines the propagation direction.

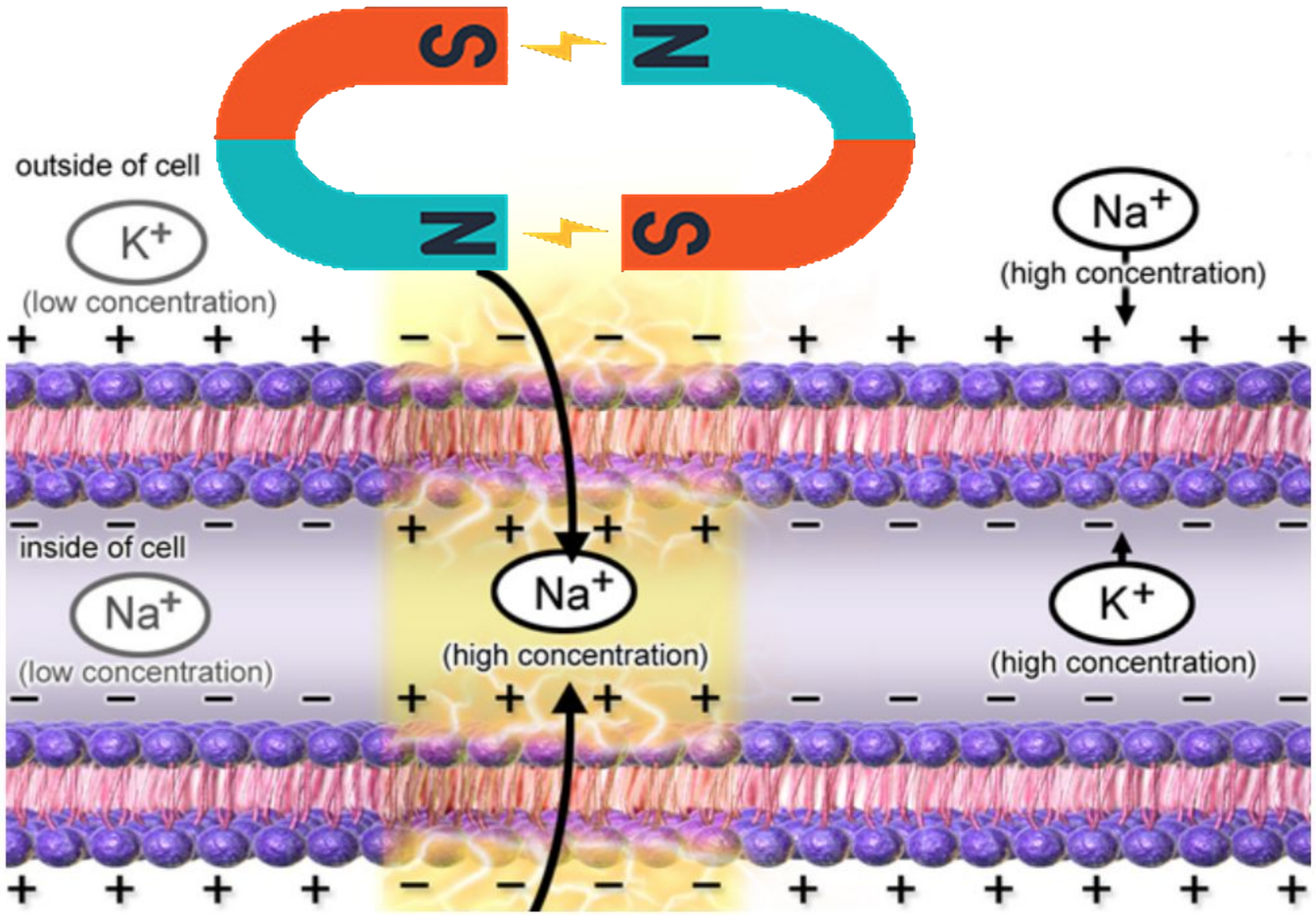


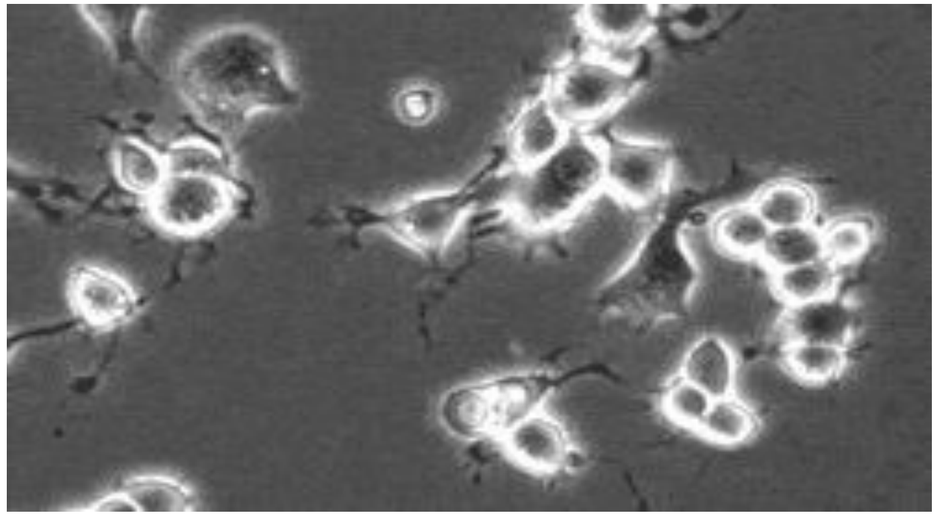




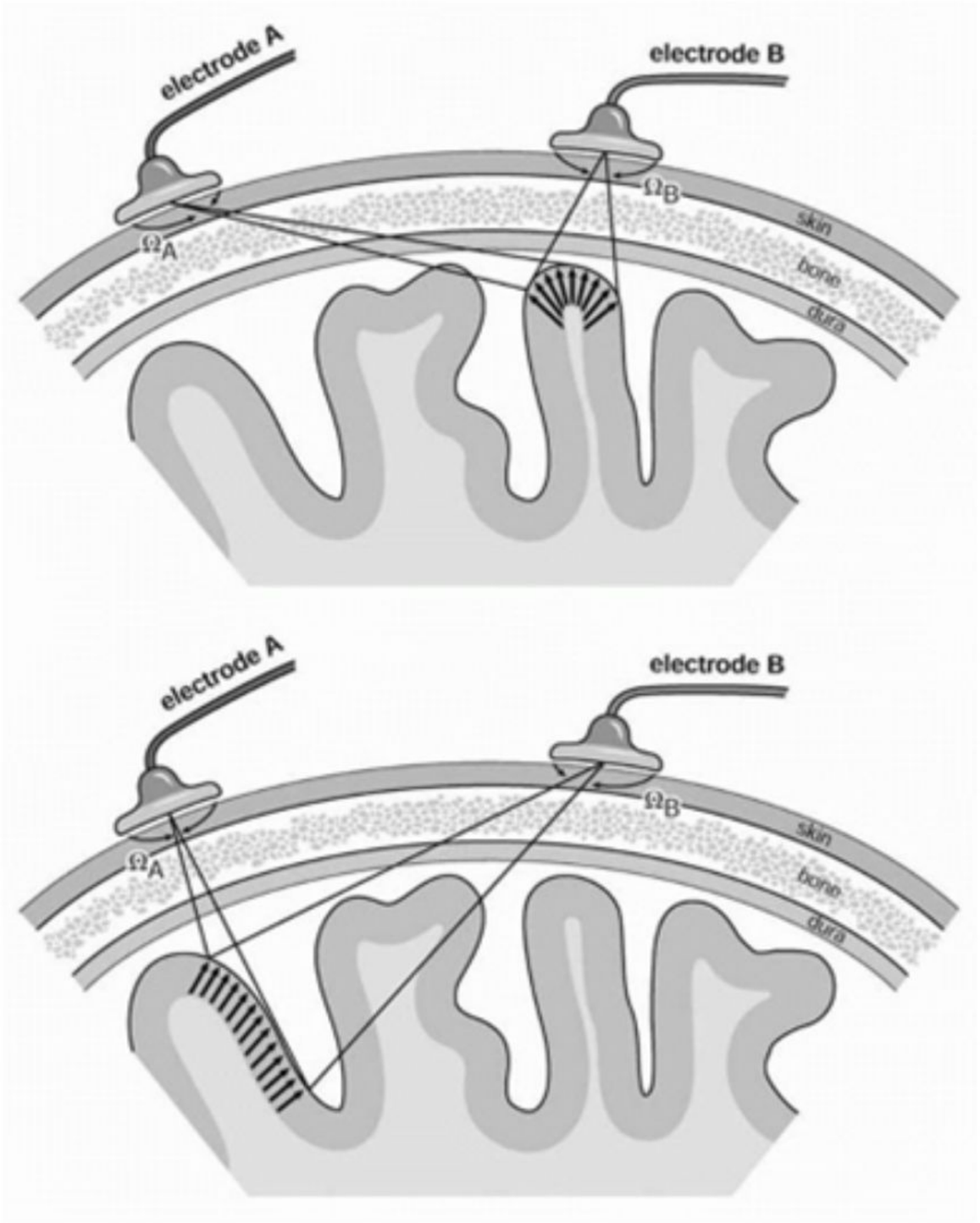
The Chemical Foundation of Brain Signals

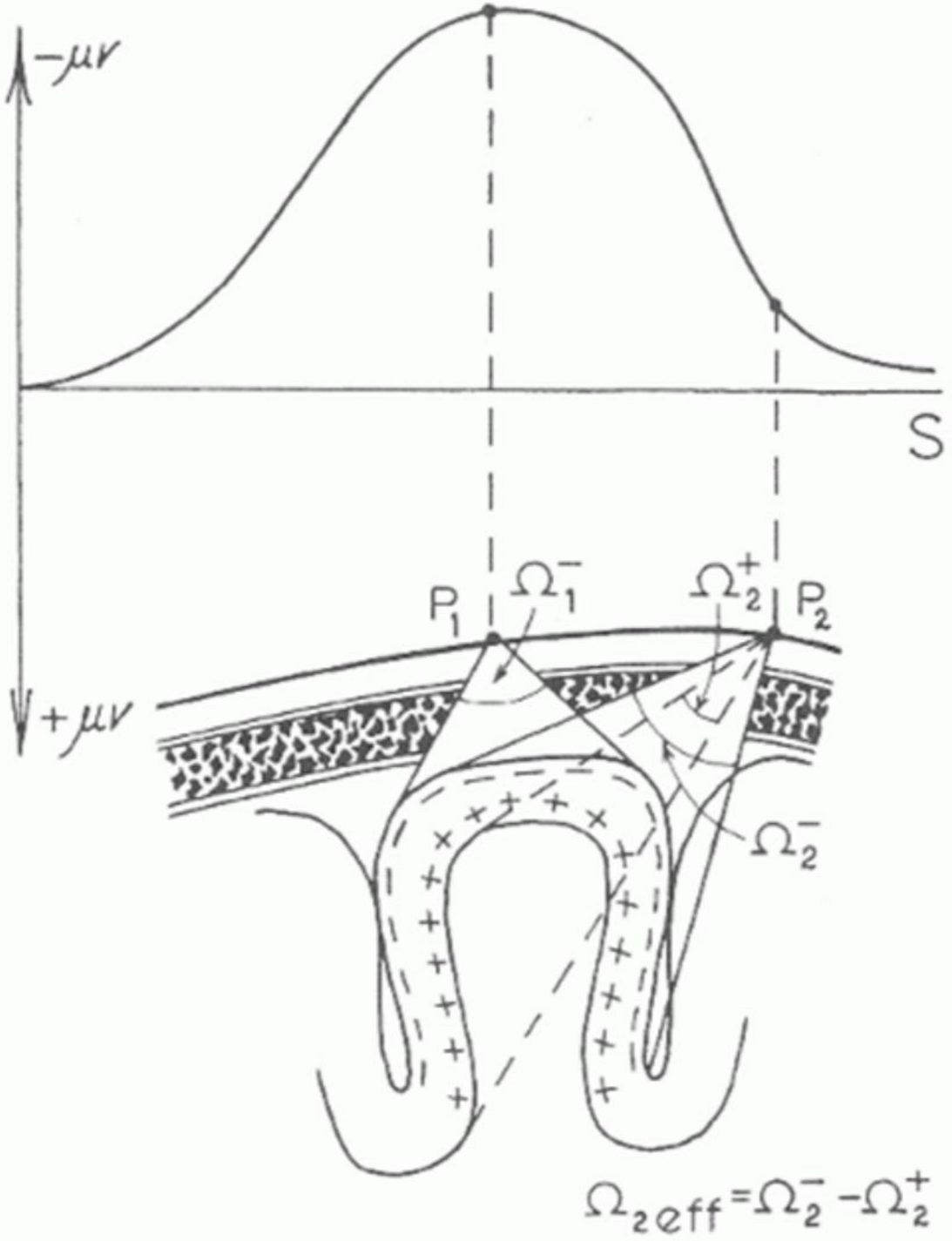
- The content of the two-neuron transmission consists of chemical substances. These chemicals are listed as Potassium, Sodium, Chloride, and Calcium. As ionized substances in the environment pass through the neuron membrane, action potentials cause the opening of sodium channels. Sodium is found in abundance outside of communication channels. For this reason, since the inside of the neuron is negative relative to the outside, sodium is instantly transferred to the other neuron.





Foundations & Unique Advantages of EEG Biometrics

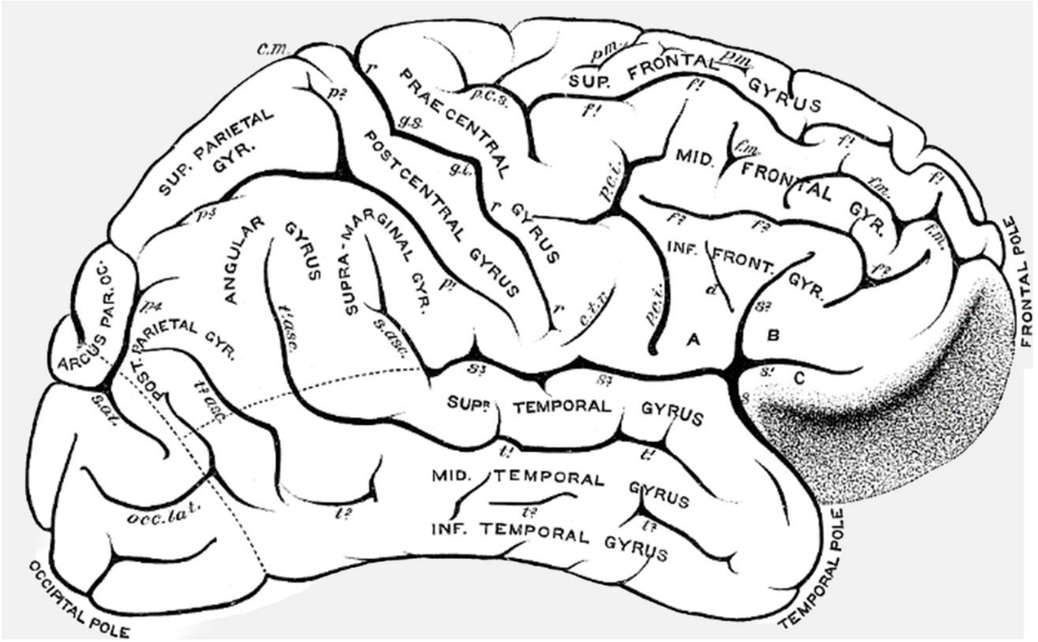




Foundations & Unique Advantages of EEG Biometrics

What is EEG?

- Non-invasive neurophysiological method that records the spontaneous electrical activity of the brain from electrodes placed on the scalp.
- Offers a unique window into brain function, capturing macroscopic electrical activity generated by neuronal populations.



Signal Generation

- Primarily stems from postsynaptic potentials (PSPs): voltage changes across neuronal membranes caused by synaptic activity.
- These individual potentials are amplified through spatial and temporal summation, largely contributed by the parallel alignment of cortical pyramidal neurons.
- Volume Conduction: Electrical fields propagate through various brain tissues (gray matter, white matter, CSF), influencing signal transmission, attenuation, and distortion.
- Neural Synchronization: Synchronized firing of neuronal populations creates detectable rhythmic patterns (coherent oscillations), modulated by thalamocortical circuits and neurotransmitter systems.
- High temporal resolution, captures dynamic, real-time brain activity.

Understanding Brainwave Frequencies

Key Takeaway: Distinct patterns, amplitudes, and frequencies are unique to each individual, forming "mental signatures". This individuality allows EEG-based systems to determine identity by evaluating the brain's electrical activity.

Frequency Band	Frequency Range (Hz)	Associated Mental State/Cognitive Process	Relevance for Authentication
Delta	0.5 - 4 Hz	Deep Sleep, Unconsciousness, Body Recovery	Not actively used for authentication; associated with non-alert states
Theta	4 - 8 Hz	Drowsiness, Creativity, REM Sleep, Memory Processing	Helps recognize distinctive patterns during focus or visualization tasks
Alpha	8 - 14 Hz	Relaxed Wakefulness, Meditation, Eyes Closed	Provides unique brainwave patterns in calm, alert states
Beta	14 - 38 Hz	Active Thinking, Focus, Concentration, Alertness, Problem-Solving	Used for verification during active thought and concentration tasks
Gamma	38 - 80 Hz	Higher Cognitive Functions, Decision-Making, Conscious Awareness	Reliable indicator for complex mental processes and deep thought

Foundations & Unique Advantages of EEG Biometrics

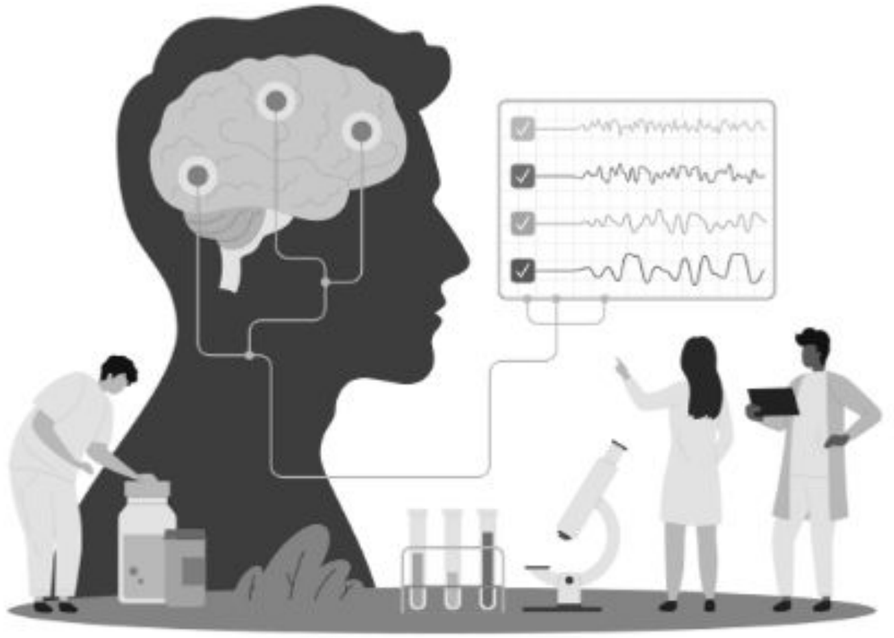
Uniqueness

- Individual brainwave patterns exhibit distinct characteristics across different people, even under similar stimuli or resting states.
- Relatively stable and difficult to replicate, unlike traditional biometric features which are susceptible to external factors or environmental conditions.



Intrinsic Liveness Detection

- EG signals can only be generated by a living body; they cease to exist once an individual dies
- This intrinsic property makes EEG highly resistant to post-mortem acquisition attempts; a critical vulnerability present in other biometric modalities where a dead (and warm) body could potentially be used for authorization.
- This inherent liveness check is a critical security feature that traditional biometrics often lack.



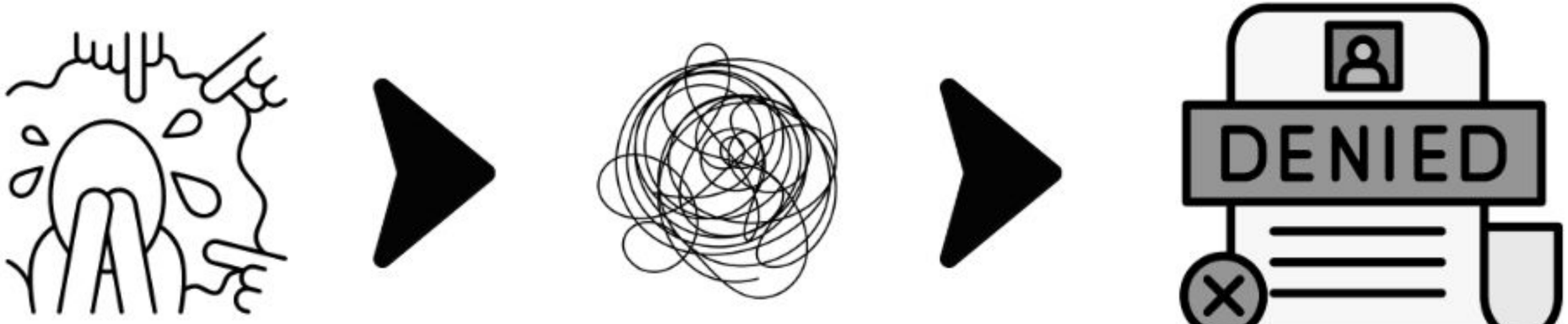
Foundations & Unique Advantages of EEG Biometrics

Spoof Resistance

- The brain's electrical activity is highly sensitive to an individual's emotional and cognitive state, making it difficult to forge or imitate.
- Brainwaves are not exposed to an intruder, making them uncapturable and hard to replicate, unlike external biometric factors.

Coercion Resistance

- Studies have shown that stress, fear, or a 'compulsion state' significantly alter normal brainwave patterns, making it impossible to produce the expected EEG signals for authentication under duress.
- This means that an attacker cannot force a user to authenticate via EEG because the brain's activity under duress would produce abnormal or no recognizable patterns, leading to authentication denial.
- This physiological barrier to coercion provides an unparalleled layer of security, directly addressing a major vulnerability in other biometric systems where individuals can be compelled to provide their biometric traits.



Coercion *EEG Data* *Denied Access*

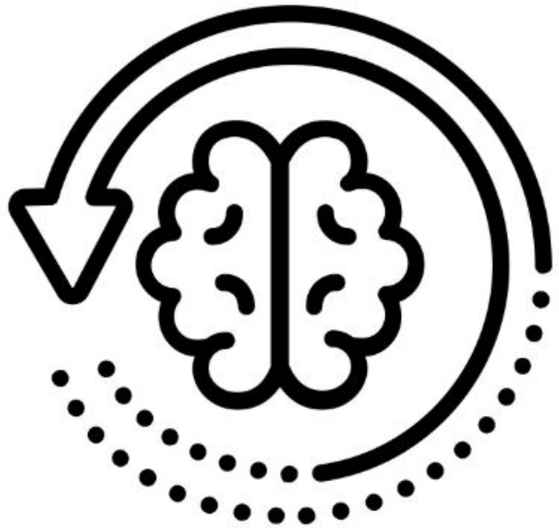
Foundations & Unique Advantages of EEG Biometrics

Revocability

- Unlike immutable traditional physiological biometrics (fingerprints, iris, DNA), EEG-based authentication offers a unique form of revocability.
- This revocability is linked to the task-dependent nature of EEG signals; different cognitive tasks elicit distinct brainwave patterns.
- If a specific task-dependent EEG characteristic used for authentication were compromised, it could theoretically be 'revoked' by switching to a different task or modifying the authentication paradigm.
- Provides an adaptive security response that traditional biometrics simply cannot offer.

Strategic Advantage

Task-dependent revocability offers an adaptive security response to compromised credentials; a unique layer of security not found in many traditional biometric modalities.



Comparative Analysis & Technical Architecture

EEG vs. Traditional Authentication Methods

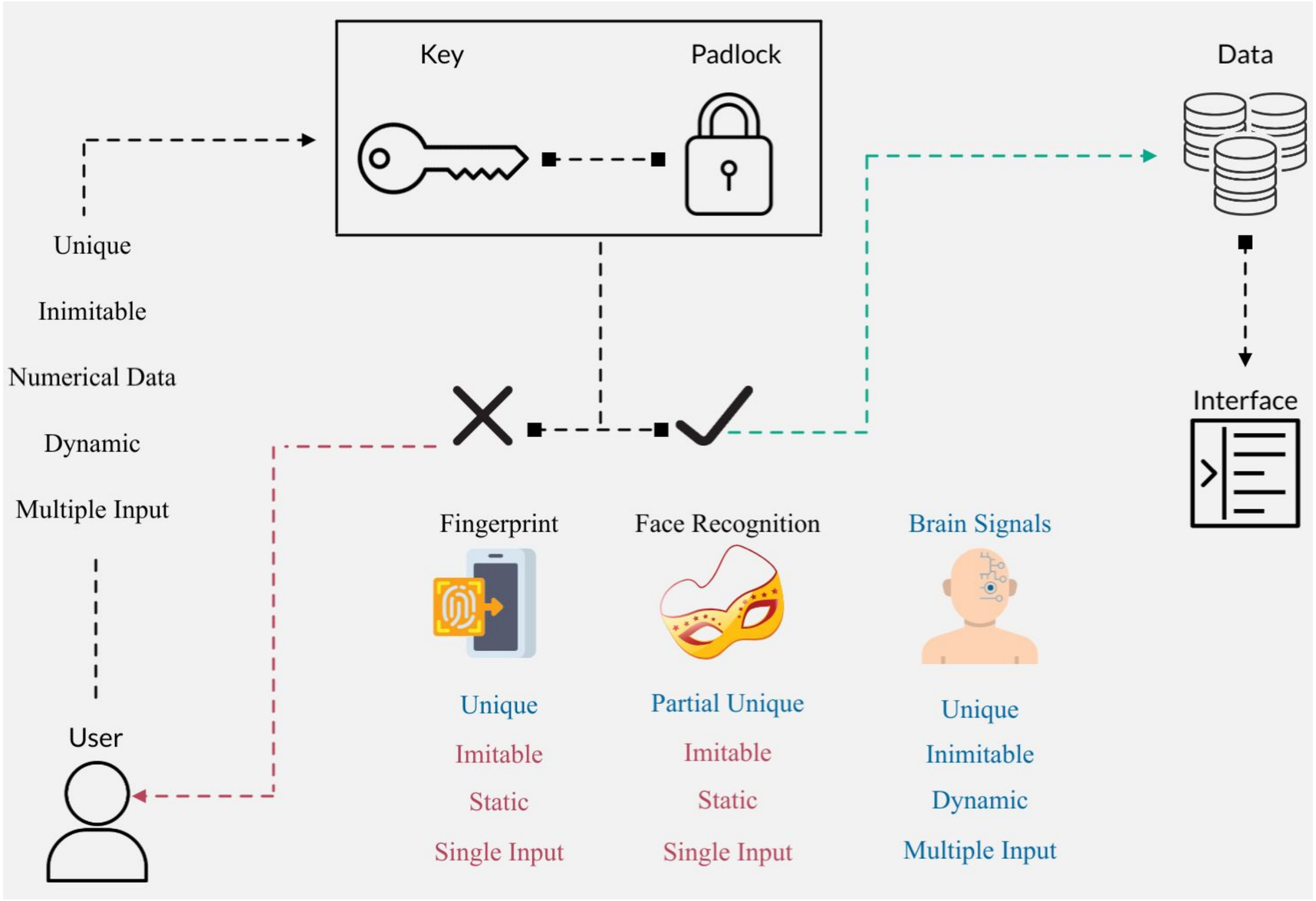
Feature/Method	Passwords	Physical Tokens	Fingerprint	Face	Iris	EEG
Security against Spoofing/Forgery	Low (easily guessed, stolen)	Medium (can be lost/stolen)	Medium (can be forged from images)	Medium (can be spoofed with photos/masks)	Medium-High (difficult to forge)	High (brainwaves difficult to imitate/capture)
Liveness Detection	None	None	Limited (vulnerable to dead body use)	Limited (vulnerable to deepfakes/masks)	Limited	High/Intrinsic (requires live brain activity)
Coercion Resistance	Low (can be forced)	Low (can be forced)	Low (can be forced)	Low (can be forced)	Low (can be forced)	High (stress alters signals, cannot be forced)

Comparative Analysis & Technical Architecture

EEG vs. Traditional Authentication Methods

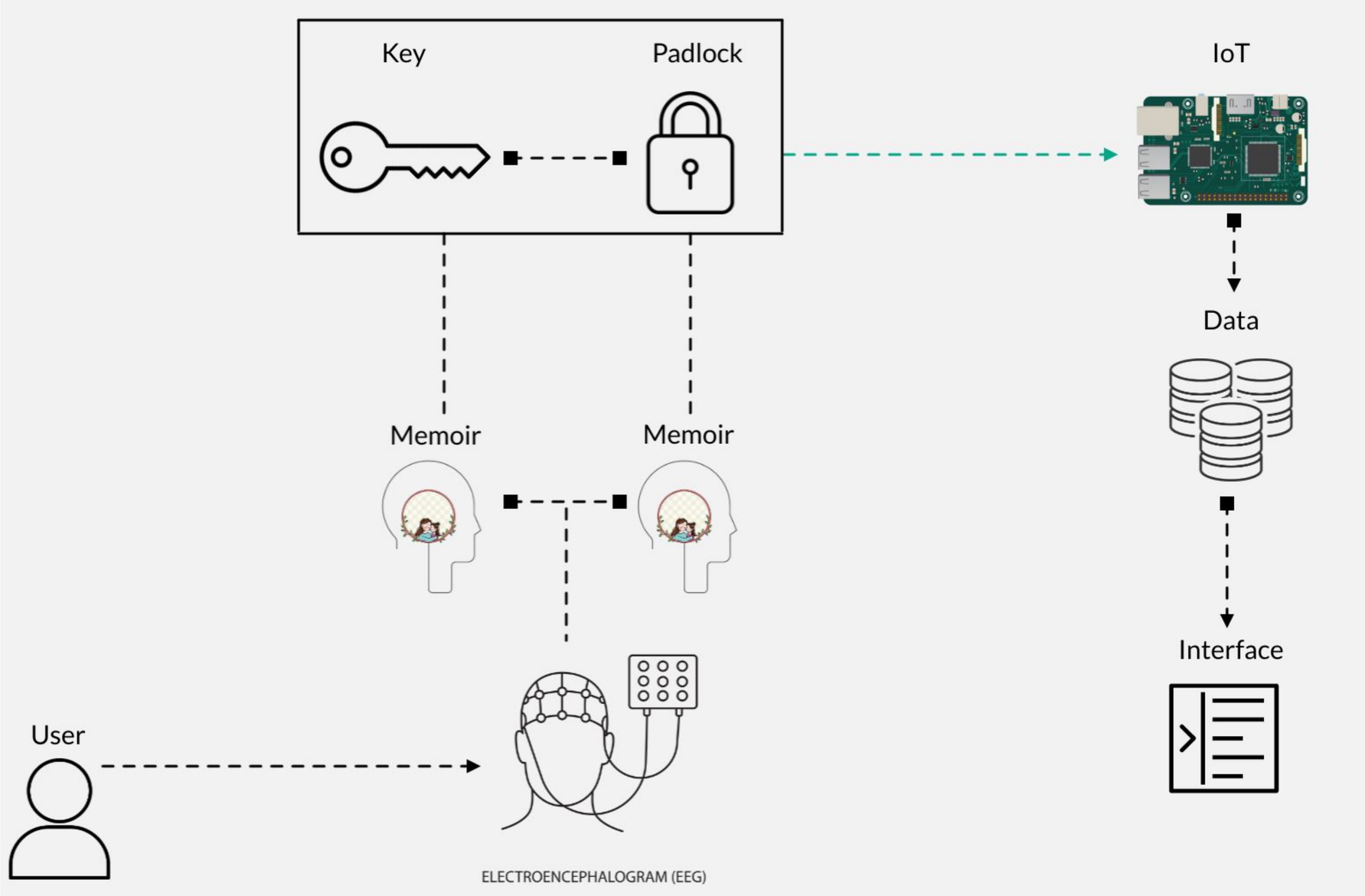
Feature/Method	Passwords	Physical Tokens	Fingerprint	Face	Iris	EEG
Continuous Authentication Potential	No	No	Limited (requires repeated action)	Limited (requires repeated action)	Limited	High (dynamic, unconscious data collection possible)
Revocability	Yes (can be changed)	Yes (can be replaced)	No (immutable)	No (immutable)	No (immutable)	Yes (task-dependent, can be reset)
User Comfort/Ease of Use	High	Medium	High	High	Medium	Medium (improving with semi-dry sensors)
Privacy Concerns	Low	Low	High	High	High	High (sensitive neural data)
Technical Complexity/Cost	Low	Medium	Low	Medium	High	Medium-High (decreasing with portable devices)

Comparison of required features with existing biometric systems



Comparative Analysis & Technical Architecture

Model



Essential Preprocessing of EEG Signals

Challenge: Raw EEG signals are inherently noisy and complex.

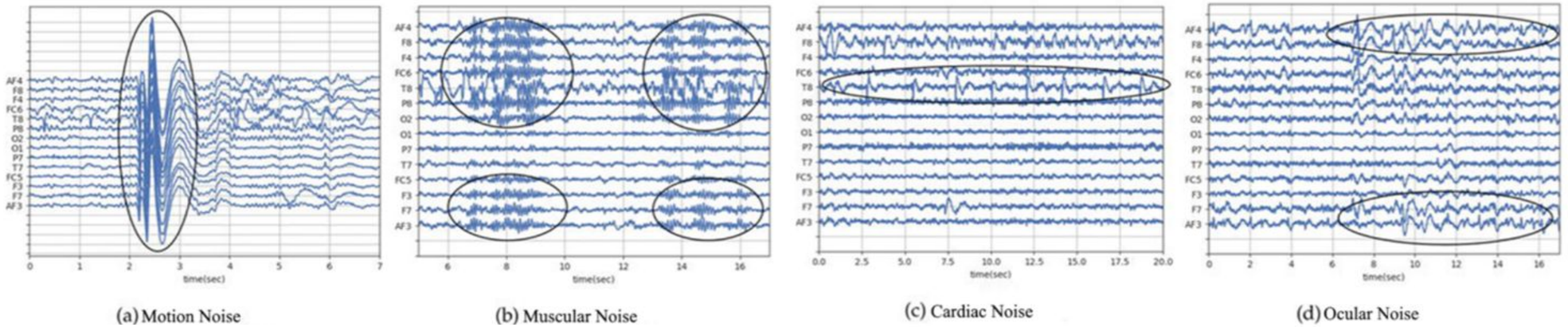
Imperative: Preprocessing is indispensable for reliable GMM training.

Core Steps:

- **Filtering:** Isolating relevant brainwaves and removing interference.
- **Denoising & Artifact Removal:** Eliminating biological and environmental noise.
- **Segmentation:** Preparing data into manageable segments.

Impact

Ensures GMMs learn from clean, accurate brain activity, preventing model degradation.



(a) Motion Noise (b) Muscular Noise (c) Cardiac Noise (d) Ocular Noise

GMM Training & Utilization

Feature Extraction for EEG Data

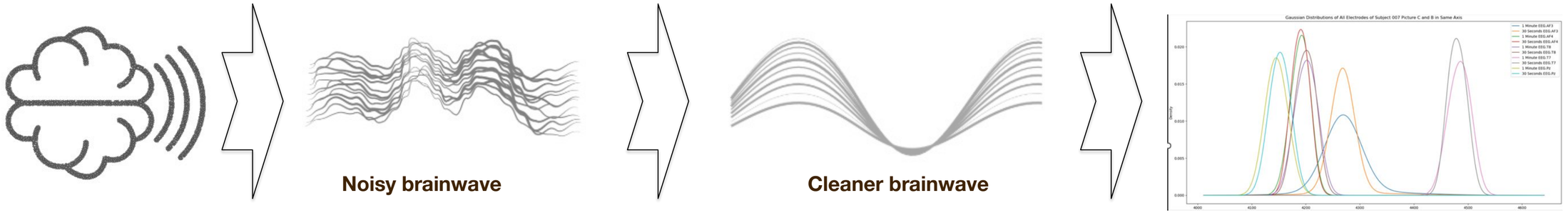
Key Feature Categories:

- Frequency Domain (e.g., Power Spectral Density)
- Time Domain (e.g., Autoregressive Coefficients)
- Non-Linear/Complexity (e.g., Entropy-based measures)
- Event-Related Potentials (ERPs)
- Spatial Domain (e.g., Common Spatial Patterns)

Feature Selection: Optimizing the feature set for model performance.

Impact

Enables robust, task-independent authentication by capturing holistic brain signatures
enables robust, task-independent authentication by capturing holistic brain signatures



The Expectation-Maximization Algorithm

Gaussian Mixture Model (GMM): A probabilistic model representing data as a blend of multiple Gaussian distributions.

Objective: Estimate GMM parameters (Mean, Covariance, Weight) from EEG features.

Expectation-Maximization (EM) Algorithm: The standard iterative method for GMM parameter estimation when component assignments are unobserved.

Core EM Steps

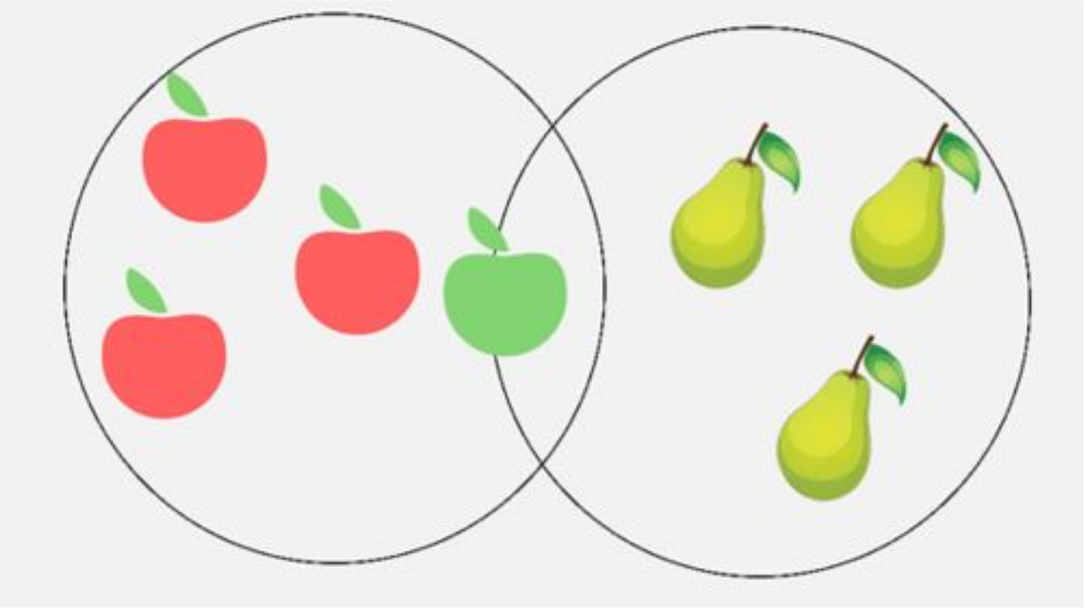
Initialization: Setting starting parameters.
E-step (Expectation): Probabilistically assigning data points to components.

M-step (Maximization): Updating component parameters based on assignments.

Convergence Check: Repeating steps until the model stabilizes.
EEG Suitability: EM's 'soft assignment' handles the nuanced and overlapping nature of brain activity, crucial for robust modeling.

Impact

A conceptual diagram of the EM algorithm: perhaps a scatter plot of data points with evolving Gaussian ellipses representing components, showing the iterative refinement. A flowchart of the EM algorithm could also be effective.



GMM for EEG-Based Authentication and Classification

GMM Training & Utilization

GMM as Biometric Template: Each trained GMM serves as a unique 'biometric signature' for an individual.

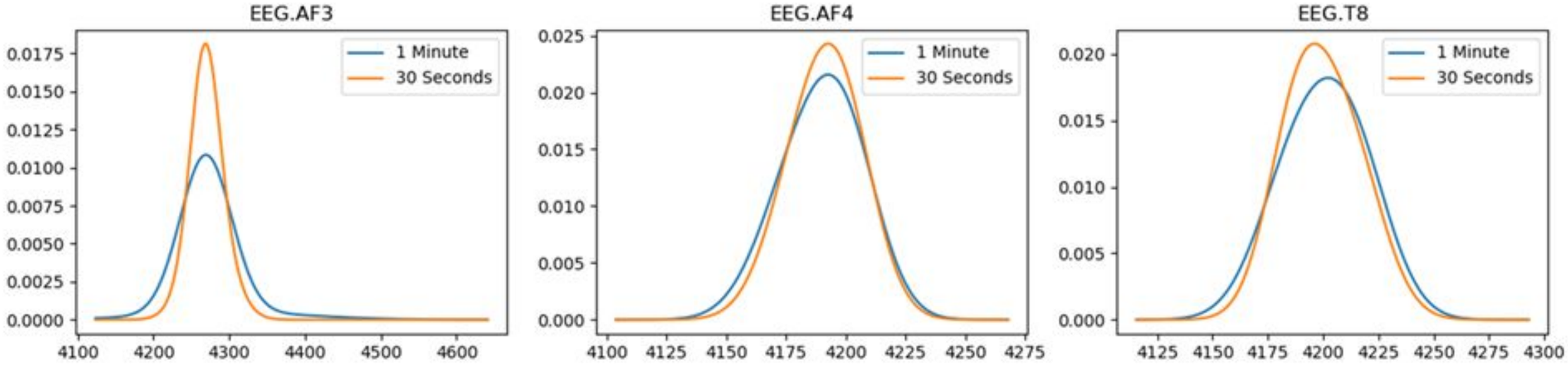
Modes of Operation

Identification (One-to-Many): Determining who a user is.

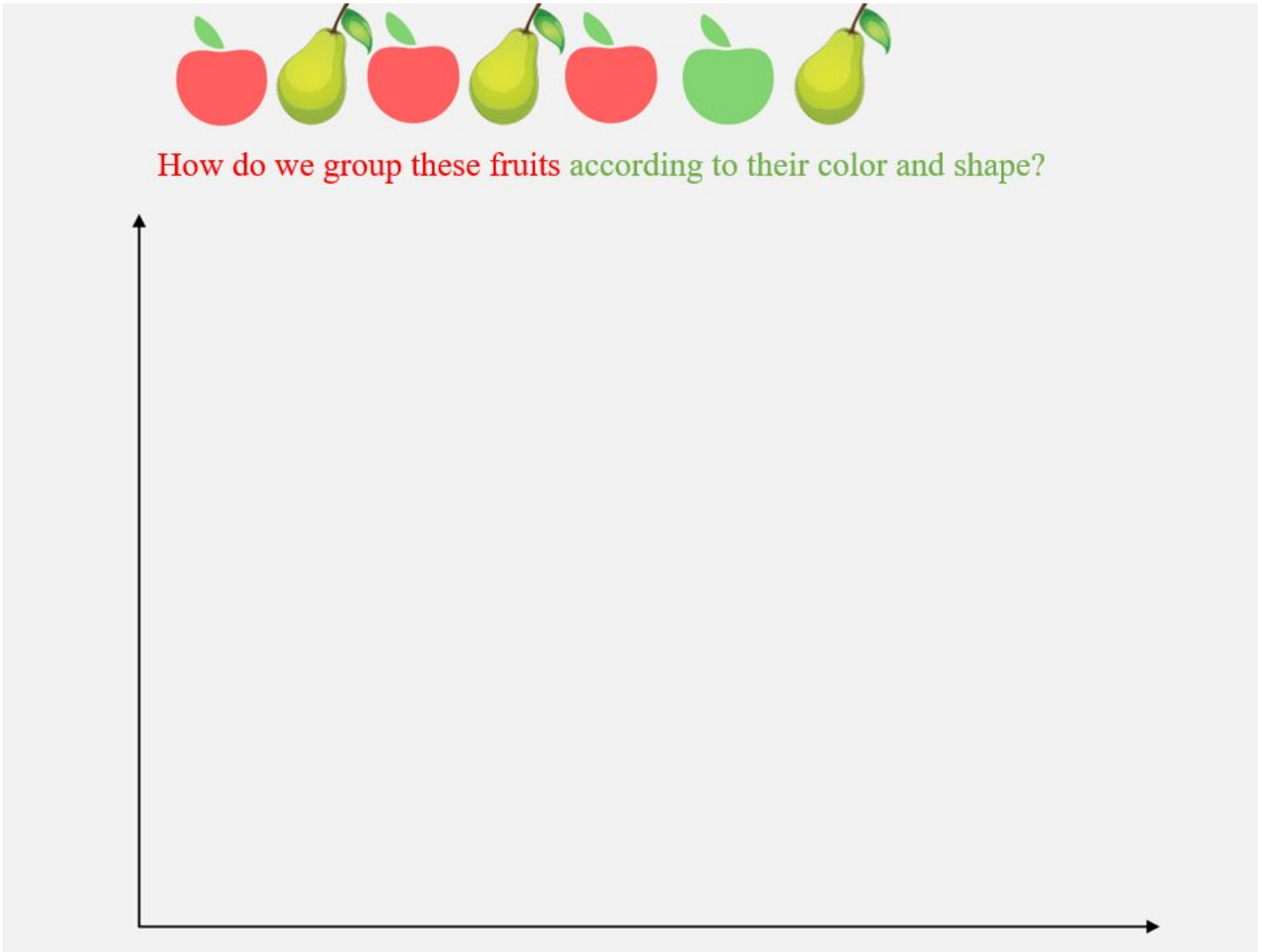
Verification (One-to-One): Confirming if a claimed identity is genuine.

Performance: High reported accuracies (80-95%+), evaluated by metrics like Equal Error Rate (EER).

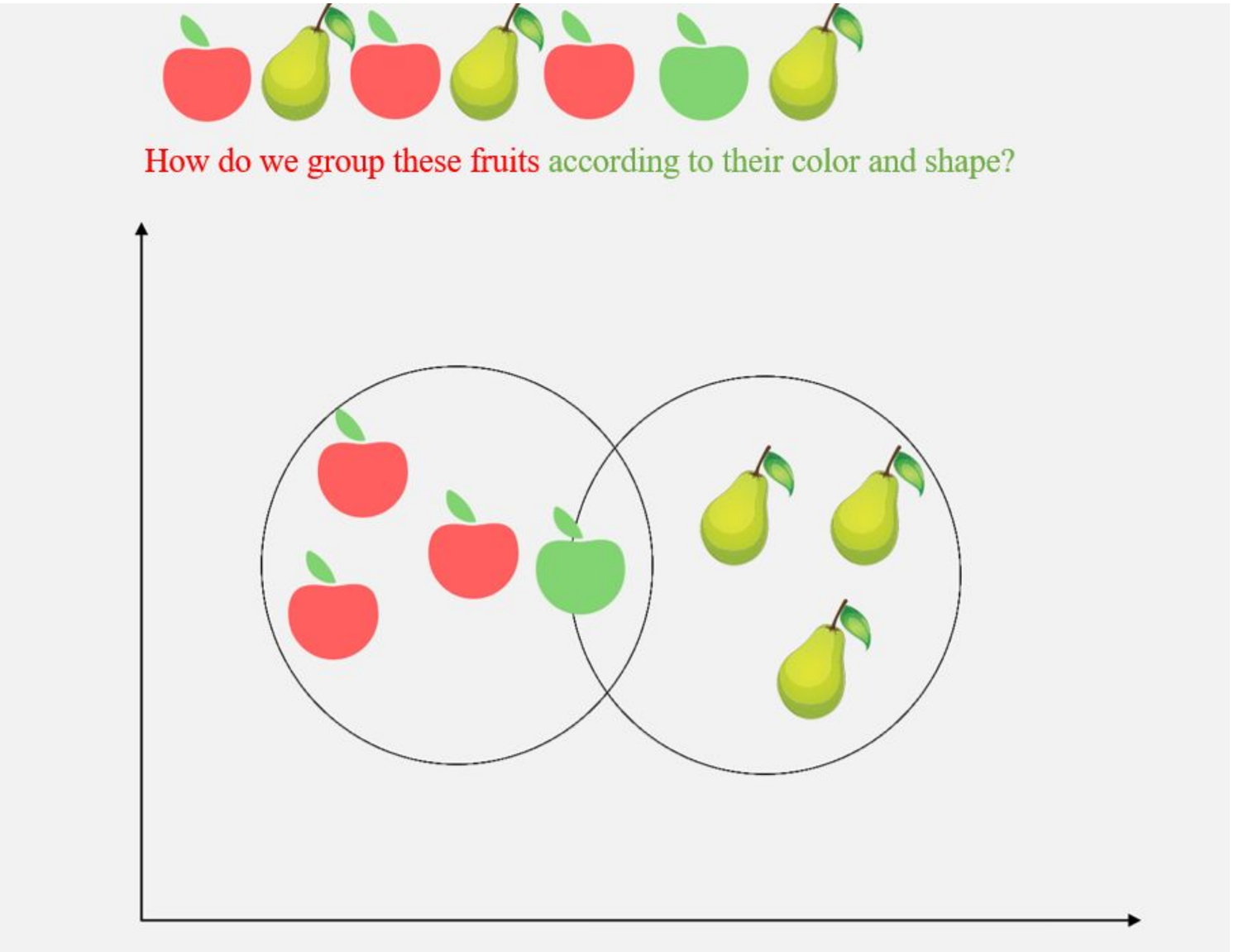
Challenges: Intra-subject variability, dataset size limitations, persistent noise.



Clustering Algorithms



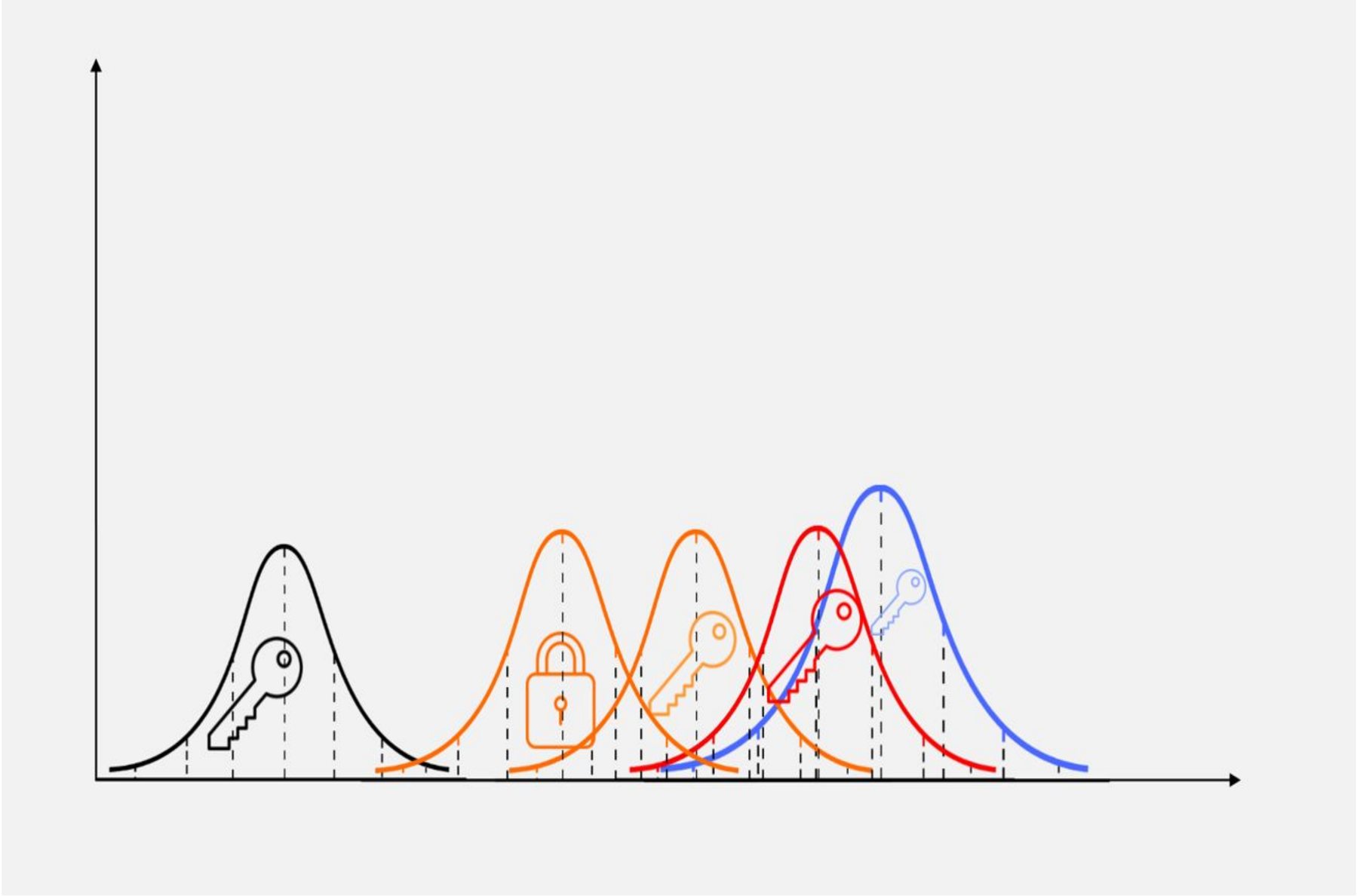
Clustering Algorithms



Clustering Algorithms

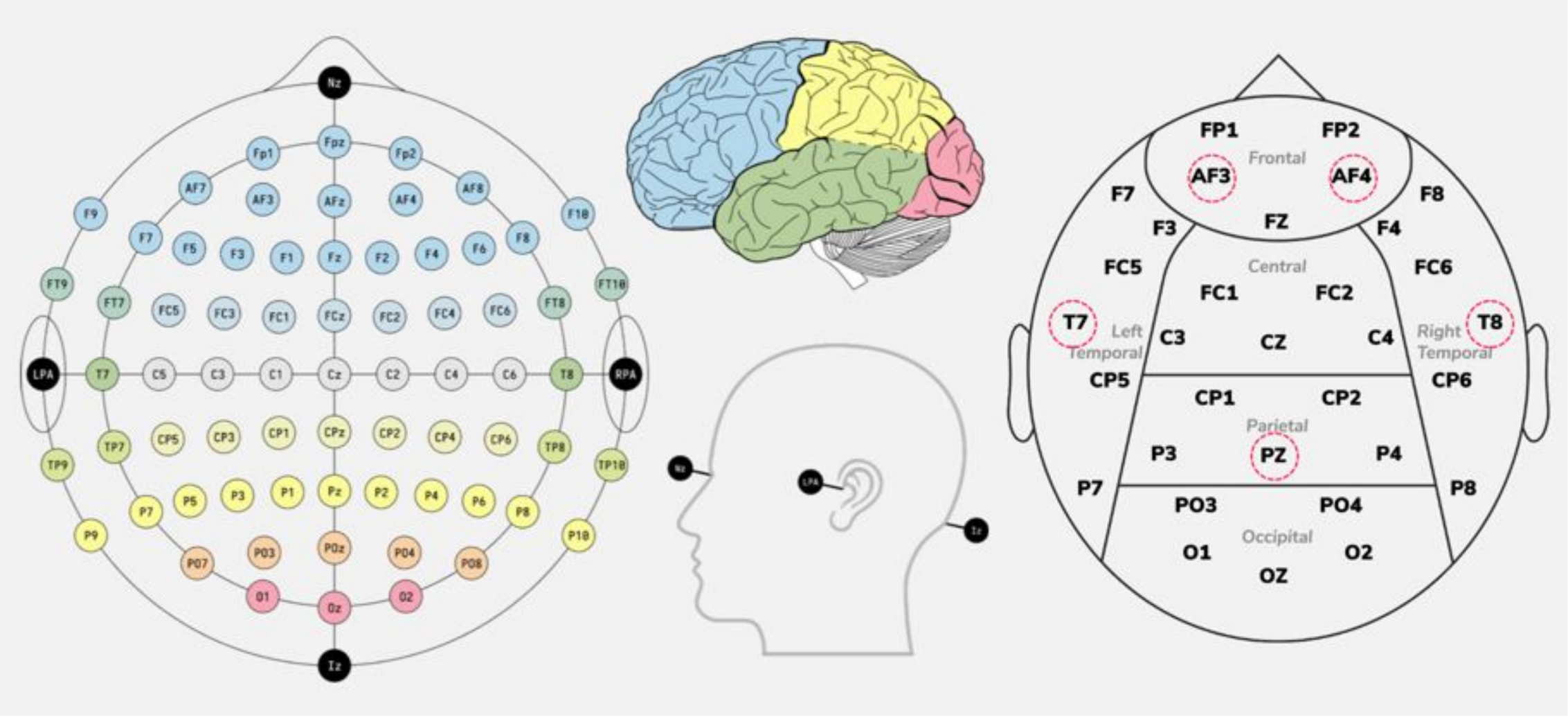


Clustering Algorithms



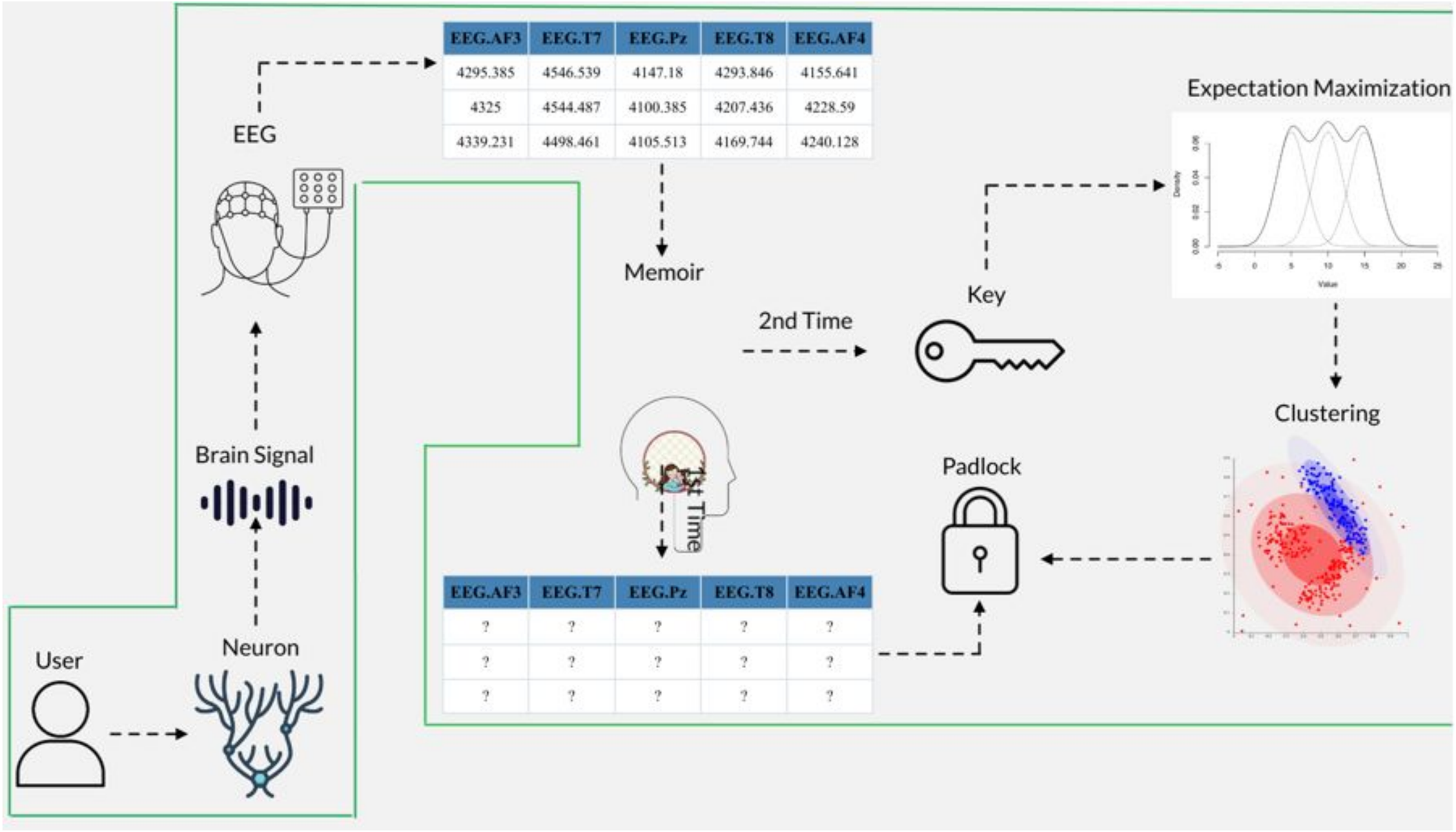
DEMONSTRATION

EEG Devices



DEMONSTRATION

More on model



DEMONSTRATION

Experiments

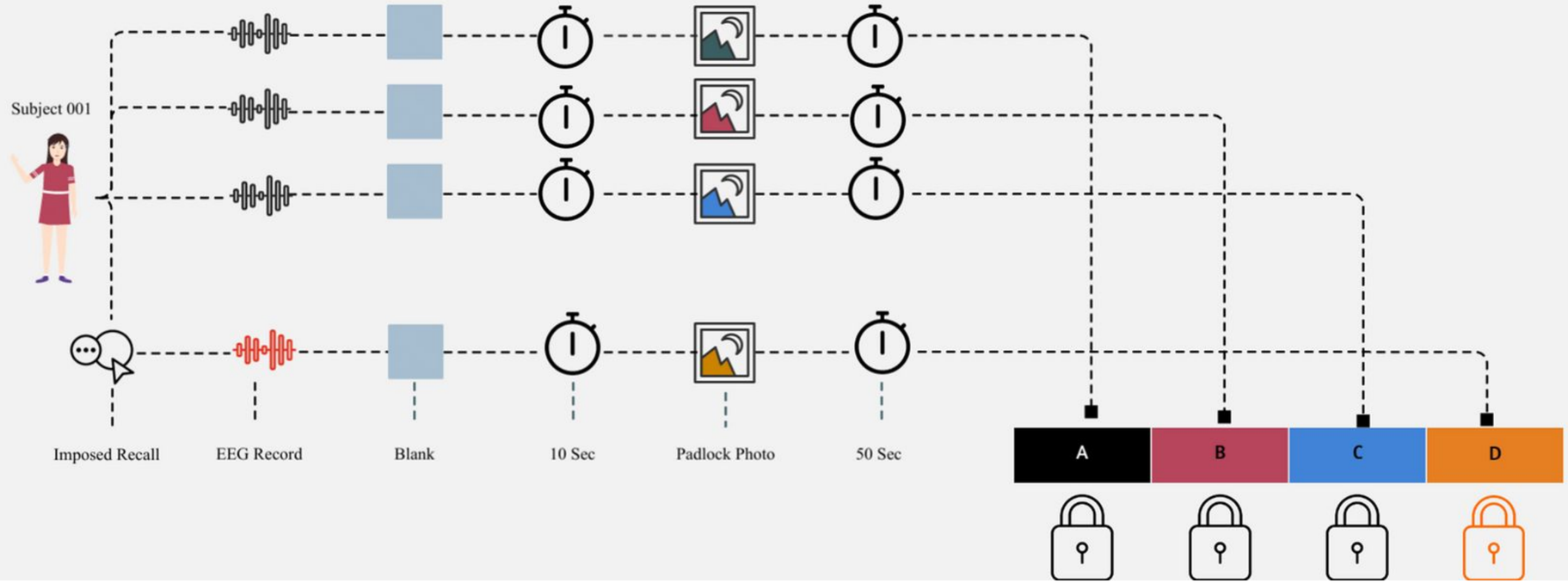
Phase 1

First Phase : Padlock Generation.

- Imposed Recall : The next photo will be your padlock. Think that you have an imaginary wallet and you hide it somewhere in the photo.



- Blank : 10 seconds of blank screen. Eliminating the preparation period where most data noise occurs.



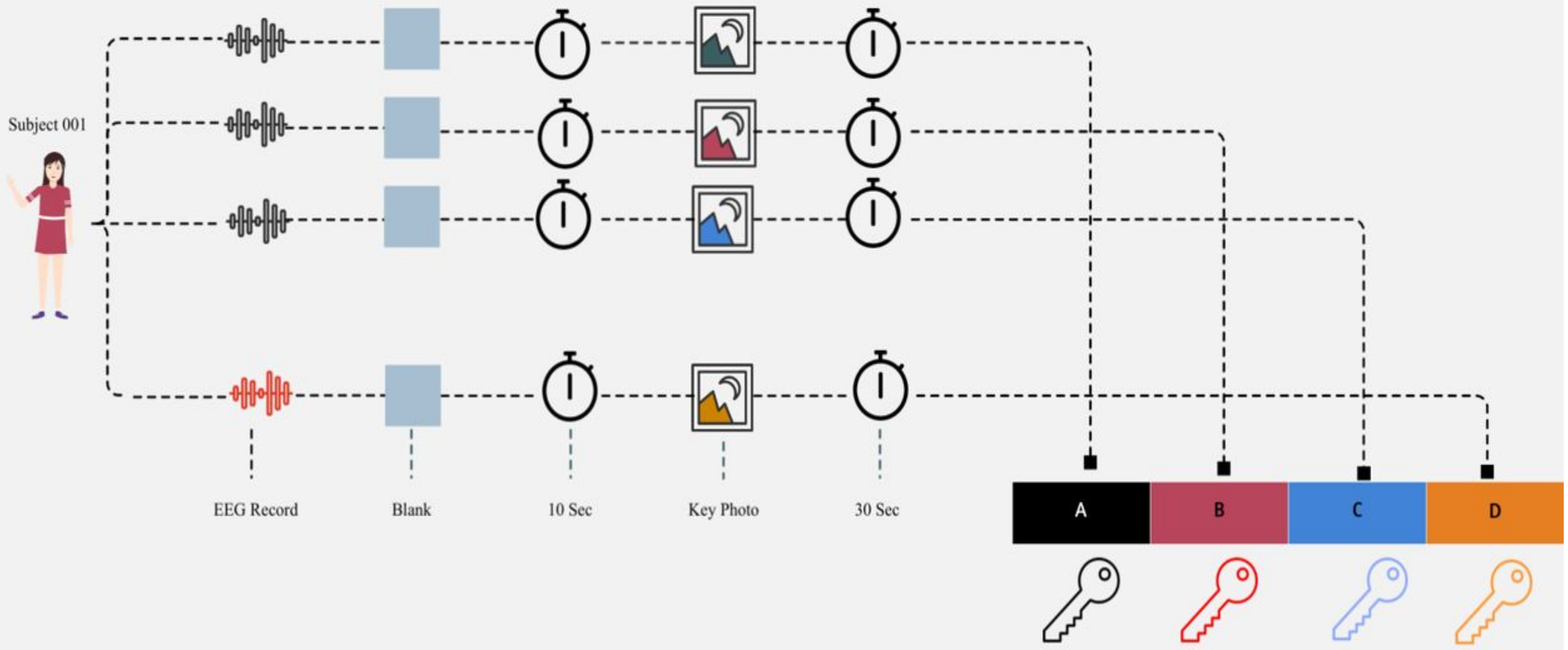
DEMONSTRATION

Experiments

Phase 2

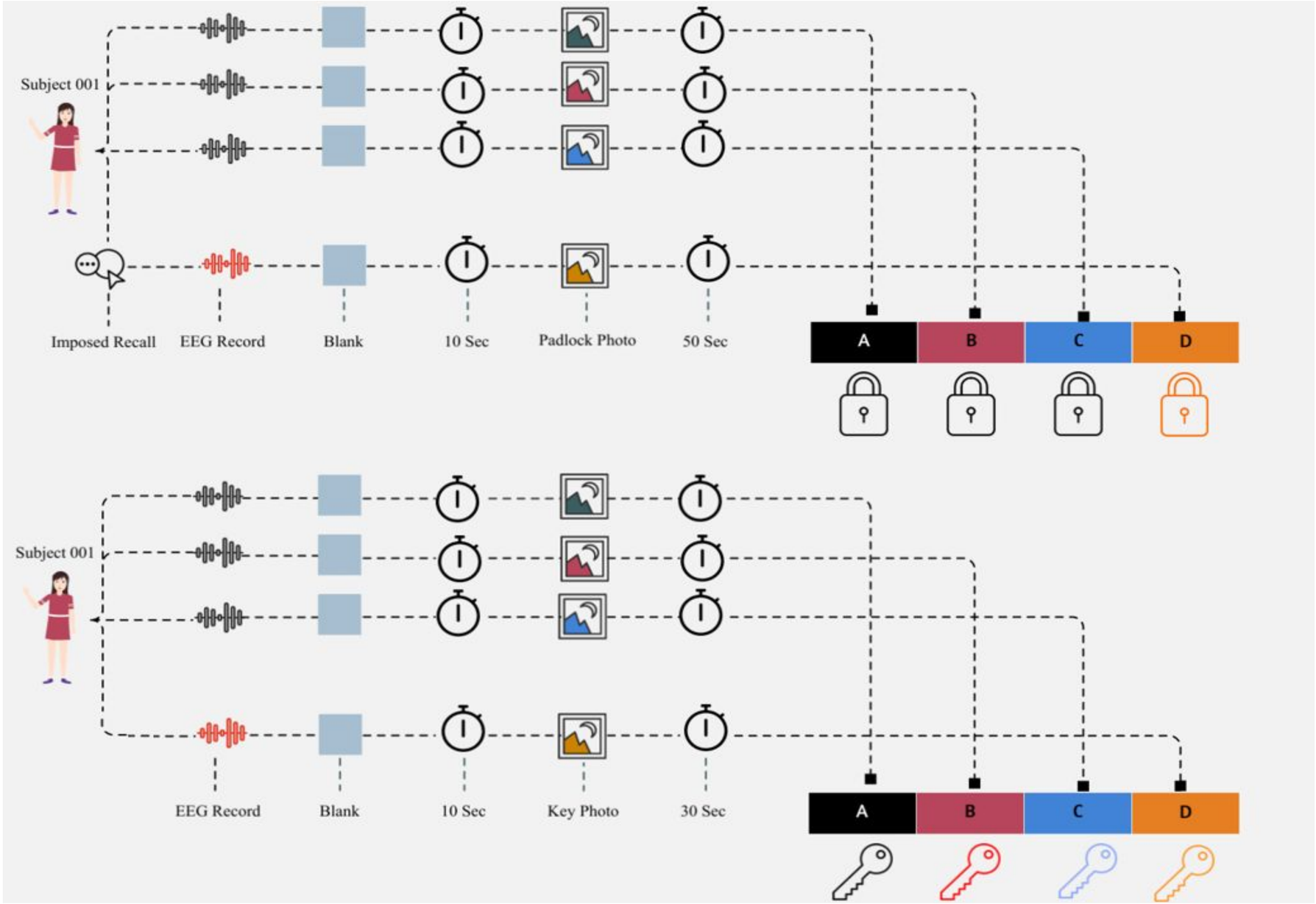
Second Phase : Key Generation.

- Blank : 10 seconds of blank screen. Eliminating the preparation period, where most data noise occurs.

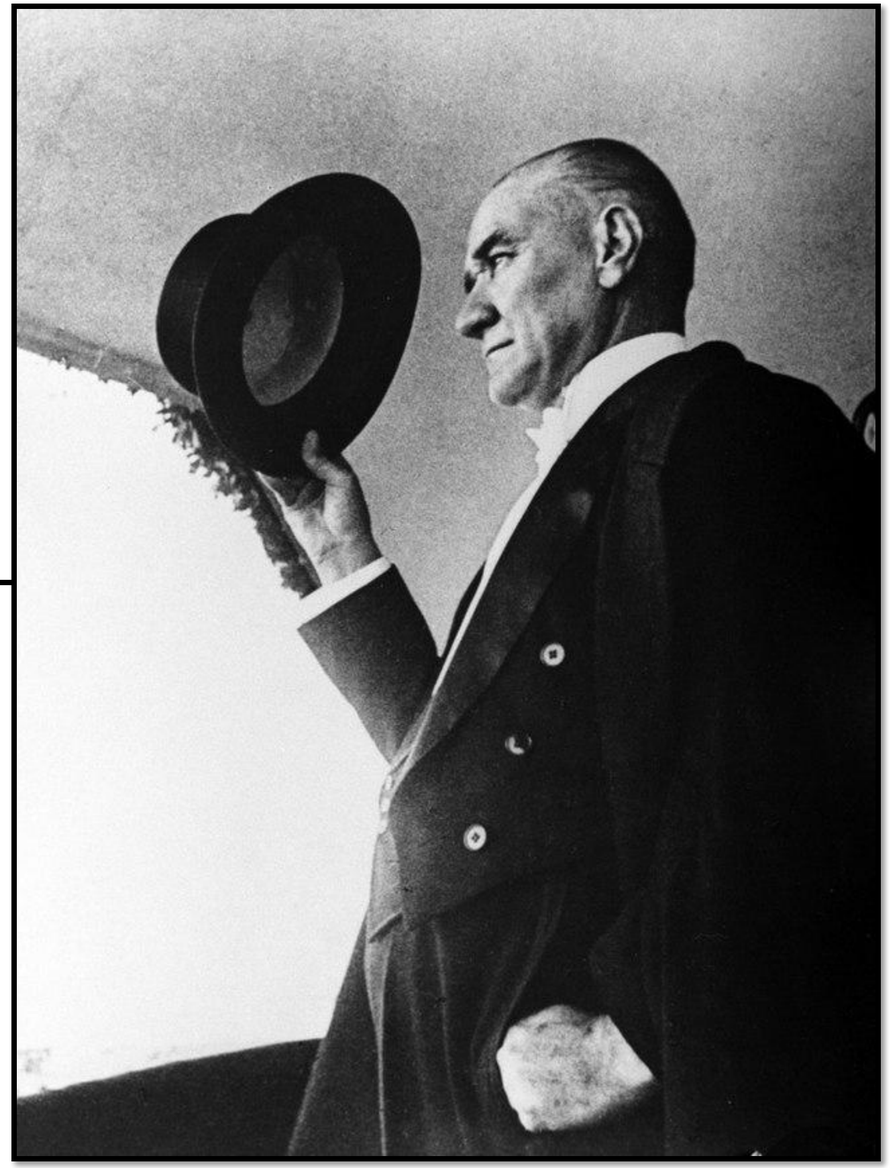


DEMONSTRATION

SUMMARY

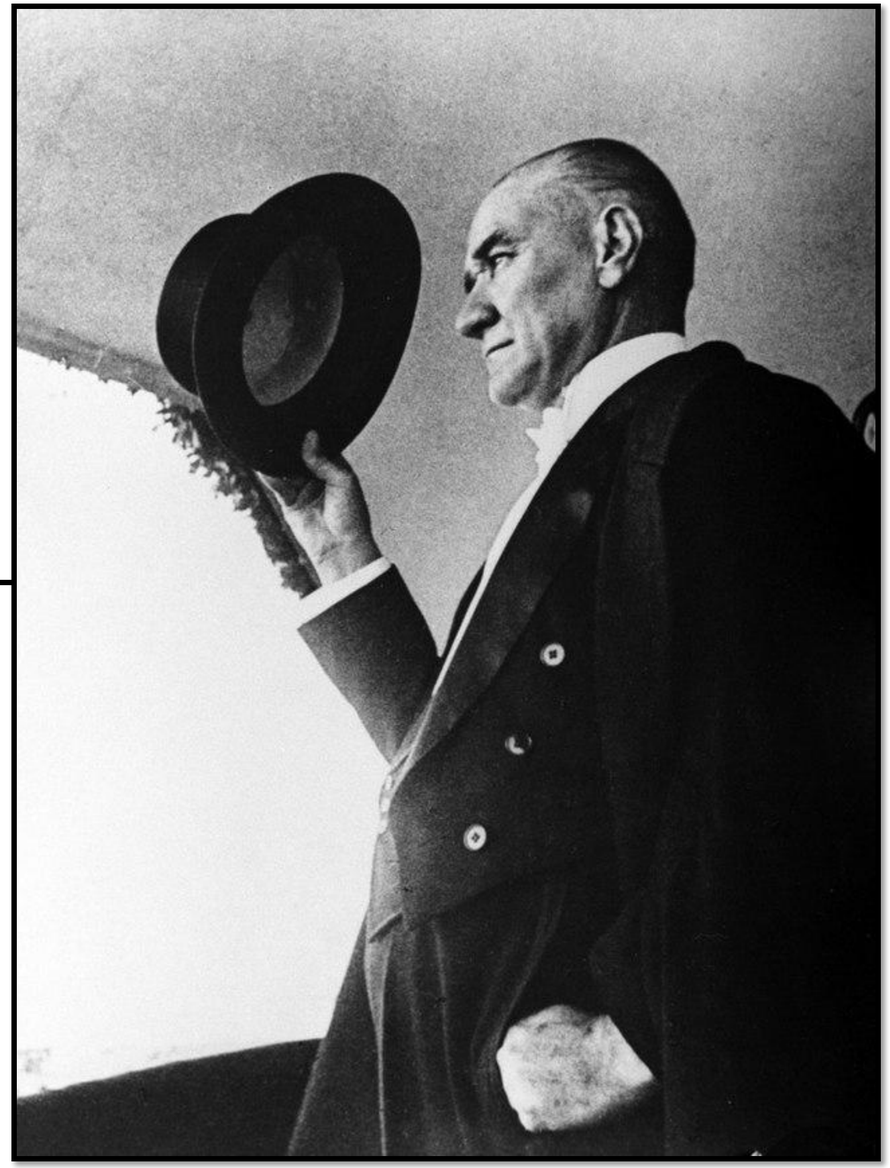


DEMONSTRATION



"Peace at home, peace in the world."

"There is no defense line, but defense territory. This territory is the whole of the motherland!"



"Peace at home, peace in the world."

"There is no defense line, but defense territory. This territory is the whole of the whole world!"

THANK YOU

For your Attention!

Contact at:
nobrainnogainatdefcon@gmail.com