



International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.935

Volume 15, Issue 10, October 2026

BrainLock: A Machine Learning-Based EEG Identity Verification System for Secure Authentication

Harshitha H V¹, Rithu G S², Spandana B³, Srujana S⁴, Yashaswini I A⁵

Assistant Professor, Department of Computer Science and Engineering, G M Institute of Technology, Davanagere,
Karnataka, India¹

UG Student, Department of Computer Science and Engineering, G M Institute of Technology, Davanagere,
Karnataka, India²

UG Student, Department of Computer Science and Engineering, G M Institute of Technology, Davanagere,
Karnataka, India³

UG Student, Department of Computer Science and Engineering, G M Institute of Technology, Davanagere,
Karnataka, India⁴

UG Student, Department of Computer Science and Engineering, G M Institute of Technology, Davanagere,
Karnataka, India⁵

ABSTRACT: Passwords and PINs remain the most common means of authentication, yet they can be stolen, guessed, phished or shared. Biometric methods offer an alternative, and electroencephalography (EEG), which records the electrical activity of the brain, has emerged as a research direction for identity verification. This paper presents BrainLock, a web-based research prototype that combines password authentication with machine learning-based EEG identity verification. The system accepts prerecorded EEG recordings in EDF, BDF and CSV formats, validates and preprocesses them through filtering, resampling and epoching, and extracts time-domain, Hjorth and spectral features. Four classifiers, Support Vector Machine (SVM), Random Forest, Logistic Regression and Linear Discriminant Analysis (LDA), are trained and compared using recording-grouped validation to limit data leakage. For a claimed identity, the system returns an explicit decision of Verified, Rejected or Inconclusive, and separately reports invalid samples and unavailable models. The platform is built with React, TypeScript, FastAPI, MNE-Python, scikit-learn and SQLAlchemy, and includes role-based access control, Argon2id password hashing, CSRF-protected sessions, rate limiting, audit logging and a personal workspace that demands fresh EEG re-verification for sensitive operations. Experiments on 20 motor-imagery recordings of five participants from the PhysioNet EEG Motor Movement/Imagery Dataset, with 1,536 features per 2-second window and a recording-grouped split, gave held-out test accuracies of 99.4% to 100% for all four models, with LDA reaching the lowest validation Equal Error Rate of 1.7%. In verification, all 4 genuine claims were accepted and all 16 impostor claims were rejected. The work provides an integrated, reproducible environment for studying EEG biometrics while clearly documenting its limitations, including the absence of live acquisition and replay protection.

KEYWORDS: EEG biometrics, identity verification, machine learning, signal processing, Hjorth parameters, SVM, Random Forest, authentication, FAR, FRR, EER

I. INTRODUCTION

Authentication is a fundamental requirement of every secure computing system. Conventional schemes rely on knowledge factors such as passwords and PINs, which are vulnerable to theft, guessing, phishing and credential sharing. Biometric techniques such as fingerprint, face and iris recognition reduce some of these risks by relying on characteristics of the individual rather than something the user remembers.

Electroencephalography (EEG) records the electrical activity of the brain through electrodes placed on the scalp. Prior research suggests that EEG signals carry individual-specific patterns, which makes them a candidate for biometric identification. Unlike external traits, brain signals are difficult to observe or copy casually. However, EEG is complex and sensitive to noise, recording session, task, equipment and the condition of the individual, so reliable verification demands careful preprocessing, feature engineering and evaluation on data not used for training.

In practice, EEG biometric research is often carried out with separate tools for signal processing, feature extraction, model training and evaluation, which makes experiments hard to reproduce and compare. To address this, we developed BrainLock, an integrated web platform that brings EEG data management, preprocessing, feature extraction, model comparison, claimed-identity verification and application security together in one workflow.

The main contributions of this work are:

- An end-to-end platform for uploading, validating, processing and managing prerecorded EEG recordings.
- A feature pipeline combining time-domain, Hjorth and spectral features with a consistent schema for training and inference.
- A comparative evaluation framework for SVM, Random Forest, Logistic Regression and LDA using recording-grouped validation.
- A verification workflow that separates identification from claimed-identity verification and supports explicit Inconclusive decisions.
- Security features including role-based access control, session management, audit logging and EEG re-verification for sensitive actions.

The rest of the paper is organised as follows. Section II reviews related work. Section III describes the proposed system architecture. Section IV presents the methodology. Section V covers implementation, Section VI discusses testing and results, and Section VII concludes with future directions.

II. LITERATURE SURVEY

A. EEG-Based Biometric Identification

EEG has long been used in neurological research, brain-computer interfaces (BCI) and motor imagery studies. Researchers have examined whether EEG contains person-specific characteristics suitable for biometrics. The usual pipeline consists of recording collection, preprocessing, feature extraction and classification. A recurring finding is that EEG patterns vary across sessions and tasks, which makes cross-session generalisation a central challenge. Public datasets such as the PhysioNet EEG Motor Movement/Imagery Dataset [1], [2], recorded with the BCI2000 system, are frequently used for such studies even though they were not designed for biometrics.

B. EEG Signal Preprocessing

Raw EEG is contaminated by eye movements, muscle activity and power-line interference. Standard remedies include band-pass filtering to retain the band of interest, notch filtering to suppress line noise, resampling, epoch segmentation, baseline correction and signal-quality assessment. MNE-Python [5] provides a widely adopted open-source toolkit for these operations.

C. EEG Feature Extraction

Feature extraction converts signals into numerical descriptors. Time-domain features capture amplitude and statistical properties. Hjorth parameters [6], namely activity, mobility and complexity, summarise the variance and rate of change of a signal at low computational cost. Frequency-domain and spectral features describe how power is distributed across the delta, theta, alpha, beta and gamma bands. Deep-learning models such as EEGNet [3] learn features directly from data but require larger datasets.

D. Machine Learning for EEG Classification

Classical supervised classifiers remain strong baselines for EEG. SVM learns a maximum-margin boundary and can model nonlinearity with kernels. Random Forest aggregates many decision trees and handles feature interactions. Logistic Regression offers a simple probabilistic baseline, and LDA finds linear projections that separate classes [7], [8]. Their relative performance depends on the data, features and validation protocol, so the best model must be found experimentally. scikit-learn [4] provides consistent implementations of all four.

E. Biometric Verification and Evaluation

Identification asks which enrolled identity best matches a sample, whereas verification asks whether a sample supports a specific claimed identity. Verification systems compare a score with a threshold and are evaluated using the False Acceptance Rate (FAR), the False Rejection Rate (FRR) and the Equal Error Rate (EER). The literature also warns that placing epochs from the same recording in both training and test sets inflates accuracy; grouping by recording reduces this leakage.

F. Secure Authentication and Access Control

Modern authentication combines credential checks with session management, access control, logging and monitoring. Role-based access control (RBAC) restricts operations according to user roles, session expiry limits how long an authenticated session remains valid, and audit logging records important events for later review. Rate limiting reduces brute-force and automated attempts. Guidelines such as the OWASP Application Security Verification Standard [9] describe these controls in detail. For systems that hold biometric data, privacy is especially important, because EEG recordings linked to participants may reveal sensitive health information.

G. Multi-Factor and Biometric Fusion

Many practical systems combine a knowledge factor such as a password with an inherence factor such as a biometric. This multi-factor approach means that compromising one factor alone is not enough to gain access. EEG is attractive as a second factor because it is internal to the body and cannot be captured from a distance in the way a face or fingerprint can. BrainLock adopts this design by requiring password authentication followed by EEG verification.

H. Research Gap

From the survey it is clear that existing work tends to focus on a single stage, such as feature design or classifier choice, and rarely combines rigorous evaluation with a secure, usable application. BrainLock addresses this gap by integrating the full EEG pipeline with authentication, access control and auditing, while keeping verification outcomes explicit and limitations documented.

A further gap is the handling of uncertain cases. Many prototypes force every attempt into accept or reject, even when the evidence is weak. BrainLock introduces an explicit Inconclusive outcome so that low-confidence decisions are surfaced rather than hidden. Table I summarises how each research area informs the design of BrainLock.

Table I. Summary of Literature and its Use in BrainLock

Research area	Main contribution	Use in BrainLock
EEG biometrics	EEG patterns can distinguish individuals	Participant identity research
Preprocessing	Improves usability of recordings	Filtering, epoching, quality checks
Feature extraction	Numerical signal representation	Time-domain, Hjorth, spectral
Machine learning	Learns patterns from labelled data	SVM, RF, LR, LDA
Biometric evaluation	Measures verification errors	FAR, FRR, EER, grouped validation
Application security	Controls access, records events	RBAC, sessions, audit logs

III. PROPOSED SYSTEM

A. Existing System

Conventional systems rely on passwords, PINs or external biometrics such as fingerprints and faces. Passwords can be stolen or shared, and external biometrics can be observed or spoofed. In EEG research, workflows are typically split across separate scripts and tools for loading data, filtering, feature computation, training and evaluation. This fragmentation leads to inconsistent preprocessing, non-comparable data splits and results that are hard to reproduce. A classifier output on its own also does not form a complete authentication workflow, because it lacks sessions, permissions and auditing.

B. Proposed System

BrainLock is proposed as a single web application that covers the complete path from EEG upload to verification decision, together with the security controls required by an authentication system. Its advantages are an integrated workflow, multiple comparable classifiers, recording-grouped evaluation to reduce leakage, explicit verification outcomes, versioned and integrity-checked models, role-specific interfaces, server-side privacy checks and cost-effective operation on open-source software without dedicated EEG hardware.

C. System Architecture

BrainLock follows a layered architecture that separates responsibilities so that each part can be tested and updated independently. The presentation layer, built with React, Vite and TypeScript, lets participants, researchers and administrators log in, upload EEG files, view results and manage their workspace. The backend layer, built with FastAPI, handles API requests, authentication, sessions, authorisation, EEG processing orchestration and audit logging. The machine-learning layer validates and preprocesses signals, extracts features and evaluates them with the registered model. The data layer stores structured records in SQLite (default) or PostgreSQL through SQLAlchemy, while recordings, processing artifacts and model files are kept in local file storage.

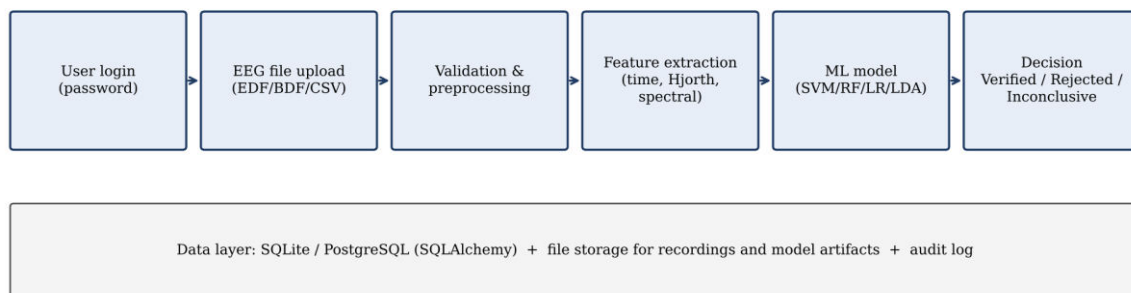


Fig.1. Workflow and architecture of BrainLock

D. Main Modules

- **EEG Signal Processing Module:** validates recordings, filters and epochs signals, and provides visualisation and quality assessment.
- **Feature Extraction Module:** computes the documented time-domain, Hjorth and spectral features.
- **Machine Learning Module:** trains and compares classifiers under defined validation strategies.
- **Model Registry:** stores versioned model artifacts with checksums and verification configuration.
- **Identity Verification Module:** evaluates a claimed identity and returns a decision with its score, threshold and reason.
- **User, Admin and Security Module:** provides role-based interfaces, session control, audit logs and rule-based alerts.
- **Personal Workspace:** a browser-based desktop with files, notes and authentication history that locks after five minutes of inactivity.

E. User Roles

Administrators manage accounts, permissions, models and security monitoring. Researchers upload and process EEG data, run experiments and compare models. Participants sign in, complete EEG verification and use their personal workspace. All permissions are enforced on the server, not only in the interface.

F. Activity Flow

Fig. 2 shows the activity flow of a verification attempt. The flow makes the decision points explicit: credentials are checked first, the EEG file is validated next, model availability is confirmed, and only then is a verification decision produced. Each failure path ends in a clearly named state rather than a generic error.

G. Database Design

The relational database organises information into related entities rather than a single table. Passwords are never stored in plain text, file references are protected against unauthorised access, and audit records hold only the information needed for operation and research. The principal entities are listed in Table II.

Table II. Principal Database Entities

Entity	Purpose
USER	Account with username, password hash and role
PARTICIPANT	EEG identity linked to a user account
EEG_RECORDING	Uploaded file with path and SHA-256 hash
PROCESSING_RUN	Processing status and generated feature artifacts
MODEL_VERSION	Model type, version, status and threshold
AUTH_ATTEMPT	Verification attempt with decision and score
JOB	Background task type and execution status
AUDIT_EVENT	Security and application event record

A participant can own many recordings, a recording can have many processing runs, a model version can be referenced by many verification attempts, and a user can generate many audit events and background jobs.

IV. METHODOLOGY**A. Dataset**

The experiments use the PhysioNet EEG Motor Movement/Imagery Dataset (EEGMMIDB) [1], [2], which contains 64-channel recordings from 109 volunteers performing motor movement and imagery tasks. For this study, five participants (S001 to S005) were selected, with four motor-imagery runs each, giving 20 recordings in which the volunteer imagined moving a hand or foot. Participant identifiers are used as identity labels. Because the dataset was collected for motor research rather than biometrics, this labelling is an experimental choice, and results should be read in that light.

Each EDF file has 64 channels sampled at 160 Hz; a typical run such as S001R04 lasts 125 s, or 20,000 readings per channel. Recordings are organised by participant identifier, checked for readability, and confirmed to contain the channels required by the processing pipeline before any experiment begins. Careful preparation matters because incorrect labels or unreadable files directly distort training and evaluation.

B. Validation and Preprocessing

Each uploaded file is checked for supported format (EDF, BDF or CSV) and readability, and duplicates are detected with SHA-256 checksums. Valid recordings are band-pass filtered between 1 and 40 Hz and cut into non-overlapping 2-second windows of 320 readings per channel. A window is discarded if any channel shows a peak-to-peak swing above 1,000 μV , which indicates an artefact such as a blink, or is flatter than 0.1 μV , which indicates a disconnected electrode. After rejection, 894 windows were kept from the 20 recordings. Recording S003R01 lost 17 of its 30 windows and S003R03 lost 3 of 62, while S001R04 kept all 62. Recordings that fail any check are rejected with an INVALID_SAMPLE status before reaching the model.

The 1 Hz lower cut removes slow drift from sweat and movement while keeping the delta rhythm, and the 40 Hz upper cut removes muscle activity and 50/60 Hz mains hum. A sample is considered usable only if it yields at least 3 good windows and no more than 50% of its windows are rejected; S003R01 (56.7% rejected) fails this rule and is never scored. Epoching divides a continuous recording into shorter windows, which multiplies the number of training samples and allows features to capture short-term signal behaviour. Users can compare raw and processed signals and inspect the power spectral density in the interface.

C. Feature Extraction

For every window, 24 features are computed on each of the 64 channels, giving a vector of $24 \times 64 = 1,536$ numbers. They comprise nine signal statistics (mean, minimum, maximum, standard deviation, variance, RMS, peak-to-peak, energy and zero-crossing rate), the Hjorth mobility and complexity, log band power and relative band power in five bands, and three spectral-shape measures (dominant frequency, spectral entropy and spectral centroid). The final dataset is a table of $894 \text{ windows} \times 1,536 \text{ features}$ with a participant label. Hjorth parameters are computed for a signal $x(t)$ as:

$$\text{Activity} = \text{var}(x(t))$$

$$\text{Mobility} = \sqrt{\text{var}(x'(t)) / \text{var}(x(t))}$$

$$\text{Complexity} = \text{Mobility}(x'(t)) / \text{Mobility}(x(t))$$

Band powers are estimated from the power spectral density in the delta (1–4 Hz), theta (4–8 Hz), alpha (8–13 Hz), beta (13–30 Hz) and gamma (30–40 Hz) bands. For example, at electrode Cz in the first window of S001R04 the relative band powers are 48%, 24%, 12%, 11% and 5%, the dominant frequency is 1.0 Hz and the spectral centroid is 6.5 Hz. The same feature schema is used during training and verification to guarantee compatibility.

D. Model Training

SVM, Random Forest, Logistic Regression and LDA are trained on the feature vectors. The data are split by whole recording: 15 recordings (636 windows) form the development set and 5 recordings, one per participant (258 windows), form the held-out test set. Model performance on the development set is estimated with 3-fold grouped cross-validation using balanced accuracy. Each feature is standardised to zero mean and unit variance using statistics learned from training rows only. All models share the same split, scaling and random seed (42). The SVM uses an RBF kernel with $C = 1$ and Platt scaling for probabilities (315 of 636 training windows became support vectors). Logistic Regression is the registered model in BrainLock.

Recording-grouped validation is essential for honest results. If closely related epochs from the same recording appear in both the training and the test sets, the model can memorise recording-specific artefacts and report misleadingly high accuracy. Grouping by recording ensures that the test set measures how the model performs on recordings it has never seen.

E. Verification Workflow

A participant first passes password authentication, then submits a prerecorded EEG file along with a claimed identity. The backend validates and processes the file, extracts features and scores them with the registered model. The score for a recording is the claimed participant's probability averaged over all its windows. The decision threshold is set at the EER point on validation data (0.154 for Logistic Regression), and the threshold is recomputed on 1,000 bootstrap resamples to obtain a 95% uncertainty band. Scores below the band are Rejected, scores above it are Verified, and scores inside it are Inconclusive. For Logistic Regression the bands are: Rejected at or below 0.081, Inconclusive between 0.081 and 0.500, and Verified at or above 0.500. The system returns one of five outcomes: VERIFIED, REJECTED, INCONCLUSIVE, INVALID_SAMPLE or MODEL_UNAVAILABLE. Separating these outcomes prevents a technical failure from being mistaken for a genuine decision.

A successful password check alone never completes the EEG stage, and the display of a result in the interface never replaces server-side permission checks. Every attempt, including failed and inconclusive ones, is recorded in the audit log.

F. Evaluation Metrics

Classification performance is measured with accuracy, precision, recall and F1-score. Verification performance is measured with:

$$\text{FAR} = \text{False Acceptances} / \text{Total Impostor Attempts}$$

$$\text{FRR} = \text{False Rejections} / \text{Total Genuine Attempts}$$

The EER is the operating point where FAR and FRR are equal, estimated by sweeping the decision threshold.

V. IMPLEMENTATION

The system is implemented with open-source technologies, summarised in Table III. Security is built into every layer: passwords are hashed with Argon2id; sessions use HTTP-only cookies with CSRF protection and expiry; requests are rate-limited; role-based access control and ownership checks are enforced on the server; and authentication attempts, sessions and security events are written to an audit log. Sensitive workspace operations require an EEG verification no older than 2 minutes, and five failed EEG checks within 15 minutes block further attempts.

Table III. Technology Stack

Component	Technology
Frontend	React 18, Vite 5, TypeScript, Tailwind CSS
Backend	FastAPI, Python 3.11
EEG processing	MNE-Python, NumPy, SciPy, pandas
Machine learning	scikit-learn
Database	SQLAlchemy 2, Alembic, SQLite / PostgreSQL
Security	Argon2id, HTTP-only cookies, CSRF tokens
Visualisation	Recharts, Matplotlib
Testing	pytest, HTTPX, Vitest, Testing Library

A. Frontend

The React interface provides the login page, EEG upload page, signal viewer, feature and model information pages, verification result screens, administrator dashboard, user management, audit log viewer and the personal workspace. The frontend handles interaction only; every authentication and authorisation decision is enforced by the backend.

B. Backend and Processing

FastAPI exposes REST endpoints for authentication, recordings, processing, experiments, models, verification and administration. Long-running tasks such as feature extraction and model training run as background jobs so that the interface remains responsive. MNE-Python loads and filters EEG, NumPy and SciPy compute features, and scikit-learn trains and serves the models. Each registered model is stored with a checksum that is verified before use.

C. Security Controls

The workspace locks automatically after five minutes of inactivity, and operations such as deleting or downloading files require fresh EEG re-verification. These controls strengthen the application but do not eliminate every attack; in particular, prerecorded files cannot prove liveness or prevent replay.

VI. TESTING AND RESULTS

Functional testing covered login with valid and invalid credentials, upload of supported, unsupported, corrupted and duplicate files, model availability, all verification outcomes and backend permission enforcement. Security tests confirmed hashed password storage, blocking of unauthenticated requests, session expiry, CSRF checks, rate limiting and audit recording.

Table IV. Functional Test Cases

Test ID	Scenario	Expected result
TC01	Open the application	Login page displayed
TC02	Submit valid credentials	Session established
TC03	Submit invalid credentials	Login error shown
TC04	Upload supported EEG file	File validated and processed
TC05	Upload invalid EEG file	INVALID_SAMPLE returned
TC06	Required model missing	MODEL_UNAVAILABLE returned
TC07	Genuine claim, high score	VERIFIED returned
TC08	Impostor claim, low score	REJECTED returned
TC09	Score near threshold	INCONCLUSIVE returned
TC10	Access restricted operation	Backend denies access

The machine-learning evaluation compares the four classifiers using identical recording-grouped splits and the same feature set. Table V lists the metrics to be reported for each model.

Table V. Classifier Performance (Test Set: 258 Unseen Windows, 5 Participants)

Model	CV balanced accuracy (mean $\pm$ SD)	Test accuracy	Validation EER	Train time	Time per window
Logistic Regression	88.6% $\pm$ 4.8%	100%	6.7%	0.07 s	0.02 ms
SVM (RBF)	82.2% $\pm$ 9.3%	100%	6.7%	0.37 s	0.55 ms
Random Forest	80.4% $\pm$ 9.6%	99.4% (2 of 258 wrong)	6.7%	1.14 s	0.09 ms
LDA	92.1% $\pm$ 7.4%	100%	1.7%	0.18 s	0.02 ms

Individual cross-validation folds were 90.7%, 93.3% and 82.0% for Logistic Regression; 69.4%, 91.2% and 86.1% for SVM; 68.7%, 92.2% and 80.4% for Random Forest; and 81.7%, 98.3% and 96.3% for LDA. LDA achieved the highest mean cross-validation score and the lowest validation EER, while Logistic Regression was the most consistent across folds and, together with LDA, the fastest at 0.02 ms per window. Random Forest fitted the training data perfectly but generalised least well, misclassifying 2 of the 62 windows of S001R04 as S003. Because the test set is small and the $\pm$ ranges overlap, no single model can be declared statistically superior.

Table VI. Verification Example for Recording S001R04

Model	Genuine claim (S001): score vs. Verified threshold	Impostor claim (S002): score vs. Rejected threshold
Logistic Regression	0.991 $\geq$ 0.500 $\rightarrow$ Verified	0.0002 $\leq$ 0.081 $\rightarrow$ Rejected
SVM	0.978 $\geq$ 0.481 $\rightarrow$ Verified	0.004 $\leq$ 0.176 $\rightarrow$ Rejected
Random Forest	0.850 $\geq$ 0.492 $\rightarrow$ Verified	0.014 $\leq$ 0.237 $\rightarrow$ Rejected
LDA	1.000 $\geq$ 0.500 $\rightarrow$ Verified	0.000 $\leq$ 0.084 $\rightarrow$ Rejected

Across the test set, every model accepted all 4 usable genuine test recordings and rejected all 16 impostor claims, giving an observed FAR and FRR of 0%. With only 20 trials, however, the 95% confidence upper bounds are 52.7% for FRR and 17.1% for FAR, so this outcome is promising but not proof of real-world reliability. The most informative features for Logistic Regression and Random Forest lay at the temporal electrodes (T10, TP8, TP7, T7) and Iz, particularly in the alpha, beta and gamma bands.

The comparison highlights that classifier choice, feature set and validation strategy all affect results, and that recording-grouped splits give more realistic figures than random epoch-level splits. Classification accuracy alone does not establish biometric security; FAR, FRR and EER must be reported alongside it, as done here.

VII. CONCLUSION AND FUTURE WORK

This paper presented BrainLock, an integrated web platform for machine learning-based EEG identity verification. It unifies EEG data management, preprocessing, feature extraction, model comparison and claimed-identity verification with strong application security, and it reports explicit outcomes including Inconclusive decisions. On five participants from EEGMMIDB, all four classifiers reached 99.4% to 100% test accuracy, LDA achieved the lowest validation EER of 1.7%, and all genuine and impostor claims in the test set were decided correctly. The platform offers a structured, reproducible environment for studying EEG biometrics and for understanding both their potential and their limits.

Future work includes integrating live EEG acquisition hardware, investigating liveness detection and replay protection, evaluating deep-learning models such as EEGNet, testing on larger, multi-session and participant-independent datasets, performing fuller FAR/FRR/EER analysis, enabling real-time verification, and deploying the system securely in the cloud.

ACKNOWLEDGEMENT

The authors thank the Department of Computer Science and Engineering, G M Institute of Technology, Davanagere, for its guidance and support, and the PhysioNet team for making the EEG dataset publicly available.

REFERENCES

1. A. L. Goldberger et al., "PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals," *Circulation*, vol. 101, no. 23, pp. e215–e220, 2000.
2. G. Schalk, D. J. McFarland, T. Hinterberger, N. Birbaumer, and J. R. Wolpaw, "BCI2000: A general-purpose brain-computer interface (BCI) system," *IEEE Trans. Biomed. Eng.*, vol. 51, no. 6, pp. 1034–1043, 2004.
3. V. J. Lawhern et al., "EEGNet: A compact convolutional neural network for EEG-based brain-computer interfaces," *J. Neural Eng.*, vol. 15, no. 5, 056013, 2018.
4. F. Pedregosa et al., "Scikit-learn: Machine learning in Python," *J. Mach. Learn. Res.*, vol. 12, pp. 2825–2830, 2011.
5. A. Gramfort et al., "MEG and EEG data analysis with MNE-Python," *Front. Neurosci.*, vol. 7, art. 267, 2013.
6. B. Hjorth, "EEG analysis based on time domain properties," *Electroencephalogr. Clin. Neurophysiol.*, vol. 29, no. 3, pp. 306–310, 1970.
7. C. M. Bishop, *Pattern Recognition and Machine Learning*. New York, NY, USA: Springer, 2006.
8. A. Géron, *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow*, 3rd ed. Sebastopol, CA, USA: O'Reilly Media, 2022.
9. OWASP Foundation, "Application Security Verification Standard (ASVS)." [Online]. Available: <https://owasp.org/www-project-application-security-verification-standard/>



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details