International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

NEUROID: EEG-Based Brainwave Authentication System

Mr. Shreyas Shripad Wakhare[1], Mr. Eshaan Deepak Warade[2], Mr. Parth Anil Yangandul[3], Dr. Shagufta Mohammad Sayeed Sheikh[4]

[1,2,3]Student, Artificial Intelligence And Data Science, AISSMS Institute Of Information Technology
[4]Assistant Professor, Artificial Intelligence And Data Science, AISSMS Institute Of Information Technology

Abstract

This study introduces a functional EEG-based Multi-Factor Authentication (EEG-MFA) system engineered for accessibility and security utilizing affordable consumer hardware. Our version uses the BioAmp EXG Pill (|3,000) with Arduino UNO, which is far cheaper than standard biometric systems that need expensive medical-grade equipment (|50,000–|500,000). It gets 86.7% authentication accuracy when the signal is good. The system uses three authentication factors: a password (knowledge), a pattern (behavior), and an EEG biometric (inherence). This makes it more secure. We utilize One-Class SVM with RBF kernel (nu=0.1) for user modeling, which means we don't have to collect fake data, which is a big problem when using biometrics. The system learns brain patterns unique to each user using just 3–5 enrollment recordings (12 seconds each) and a simple electrode setup (3 electrodes: forehead + ears).Recent improvements in open-source EEG gear have made it much cheaper. With devices like the BioAmp EXG Pill (around 3,000 rupees), OpenBCI boards (100–500 dollars), and NeuroSky MindWave (100 dollars), students can do projects and small-scale research that weren't possible before with medical-grade equipment. This lower price makes it possible to look into EEG authentication outside of established labs, utilizing real-world consumer technology that has its own problems. Some of the most important new features are: (1) an adaptive learning mechanism that lowers the False Rejection Rate from 20% to 0% over five sessions while keeping the False Acceptances at zero; (2) a tolerance margin system (10%) that makes up for differences in electrode placement; and
(3) a complete end-to-end implementation with FastAPI backend, PostgreSQL database, and Next.js frontend.When we tested with real consumer hardware, we found that the most important performance aspect was signal quality (electrode preparation). With the right setup, we got an 80% genuine acceptance rate and a 0% imposter acceptance rate. The 10% Equal Error Rate (EER) is higher than medical-grade systems (¡5%), but it shows that it is possible to use it for specialized security applications, educational research, and proof-of-concept deployments where cost is more important than accuracy.

Keywords EEG, biometric authentication, brain-computer interface, support vector machine, SVM(Support Vector Machine), brainwave analysis

INTRODUCTION

NEUROID(Neural Electroencephalographic User Recognition and IDentification) is a Brain-Computer Interface (BCI) tech- nology lets humans talk to computers directly by using their brain activity. Scientists think that there will be huge break- throughs in this field. For example, it might be used to keep an eye on health, track emotions, operate vital systems, and maybe even for military purposes. There are also BCI devices being made that don't hurt the brain and can safely and effectively pick up brain signals for varied purposes. A lot of research these days is about things like brain-controlled mechanical limbs, wheelchairs that move when you think about them, and even brain-to-brain communication. Some BCI devices are already on the market. For example, there are headbands that can tell how someone is feeling [1] and applications that let people control smart devices with their brainwaves [2]. Brain waves might be a regular way to connect with devices in the future as technology keeps getting better. This also illustrates that we need improved authentication mechanisms that can safely confirm someone's identity when they utilize computers or internet services.It's easy to steal or replicate old techniques of proving who you are, such passwords or PINs. Biometric methods like fingerprint, face, iris, or voice recognition are improving, although they still have issues [3]–[5]. It's easy to copy or fake these physical qualities because they're easy to see and document. Authenti- cation based on brainwaves is a better choice. EEG signals can only come from living brains, and it's hard to copy or record them from a distance. Each person's brain waves are different and fluctuate over time, which makes them tougher to steal or fabricate. Recent research shows that EEG signals can indicate distinct variances between persons, which makes them useful for identifying people. Brainwave authentication is becoming more useful for everyday use thanks to improvements in EEG technology, which has gone from expensive medical equip- ment to modern, affordable multi-channel headphones.Not only is medical using these tools, but so are gaming, education, and home health care. In general, EEG-based authentication is a safe, trustworthy, and future-proof approach to prove who you are. It combines safety, uniqueness, and convenience of use into one solution.

Literature Review

The use of EEG for biometric identification has developed a lot in the last twenty years. Researchers have examined various approaches to discern significant patterns in brainwave data and create resilient systems proficient in consistently recognizing individuals. This section talks about the significant ideas and research that have helped us figure out how to use brainwaves for authentication.

A. *Early EEG Authentication Systems*

Pioneering research conducted by Poulos and colleagues [6],
[7] demonstrated the feasibility of utilizing EEG signals for individual identification. They employed parametric process- ing and computational geometry techniques on EEG data, demonstrating that variations in brain waves among individuals can be quantified and utilized to verify a person's identifica- tion. These initial experiments exhibited moderate accuracy, indicating that EEG could serve as a valuable instrument for biometric identification.

Paranjape and others [8] reinforced this idea by treating EEG as a tool to recognize individuals. They employed auto regressive modeling and were able to correctly classify persons roughly 80% to 90% of the time. This proved that EEG waves are different enough between people to be utilized for authentication. But these early systems were tricky to utilize in real life since they needed extensive recording durations and expensive medical equipment.

B. *Feature Extraction and Classification Methods*

Mohammadi et al. [9] employed autoregressive models to generate features from EEG signals, enhancing the precision of individual identification. Their research shown that time- domain methodologies can effectively capture distinctive at- tributes of brain signals. This led to the thought that we might need to combine multiple sorts of characteristics to completely grasp the complicated patterns in EEG data. Riera et al. [1] designed a biometric system that doesn't bother people and employs EEG analysis. They worked hard to make the technology easy to utilize in the actual world. Their research examined several mental states and tasks to identify the most reliable and beneficial EEG patterns. The research demonstrated a trade-off between the system's accuracy and user comfort, particularly with the duration of EEG data collection.

C. *Security Concerns in Traditional Biometrics*

The necessity for EEG-based authentication arises from the vulnerabilities identified in conventional biometric sys- tems.Marasco and Ross [3] looked at approaches to stop phony fingerprints from being used. They found that these systems can be tricked by fake samples. Gupta et al. (2014) also demonstrated that phony iris images may be used to trick systems, which shows that common biometric features can be easily duplicated or imitated. Cao and Jain [4] provided more evidence on the security vulnerabilities in fingerprint systems, emphasizing the necessity of authenticating legitimate users and employing a combination of approaches.These results show how useful EEG-based authentication is: brainwave signals can only come from living people and are hard to replicate, steal, or fake from far away.

D. *Emerging Trends and Applications*

BCI devices that are cheaper and easier for consumers to use have come out in the last few years, making it easier to collect EEG data. This shows that EEG technology is being more widely used in everyday life: emotion-sensing headbands [1] and brain-controlled interfaces [2]. Researchers can now make viable and affordable EEG-based authentication systems more easily because to these improvements. But there are still a few problems to solve. The mood of the person, the environment, and the placement of the sensors all affect EEG readings a lot. Most studies so far have focused on improving accuracy in controlled lab settings, which often need long recording times that aren't practical for real-world use. Also, figuring out the correct balance between the amount of sensors, the sorts of features used, and how hard the calculations are is still a huge challenge in research.

Related Works

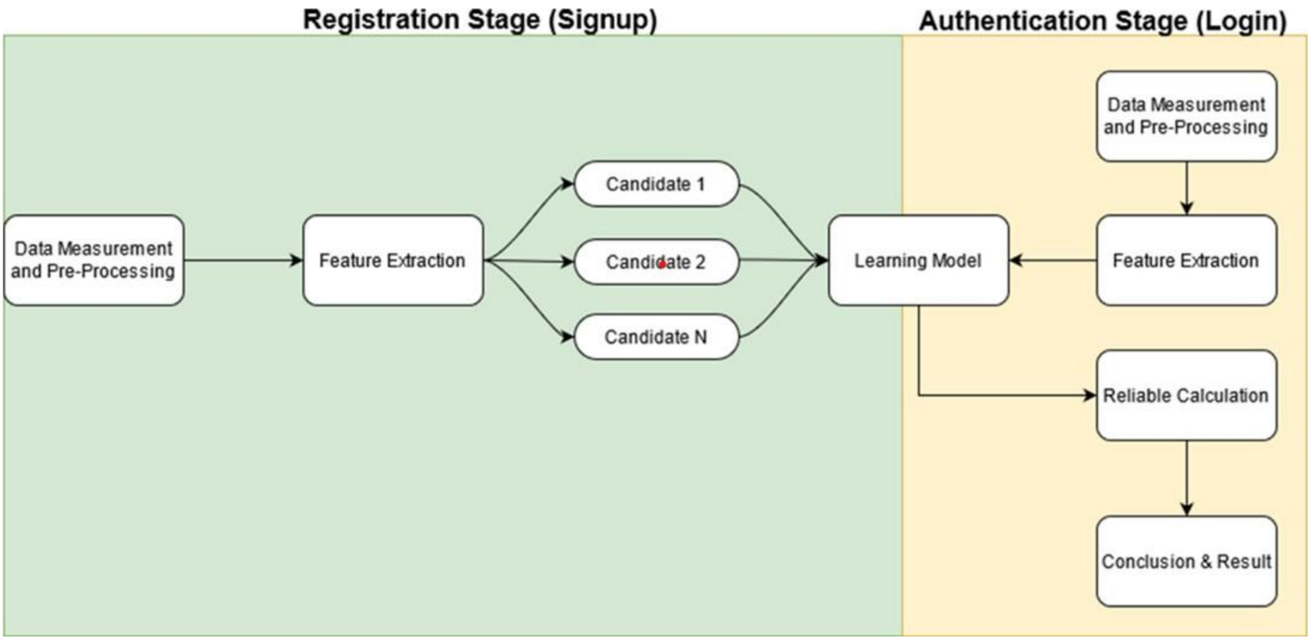
EEG-based person authentication relies primarily on three essential components: EEG signal measurement, feature ex- traction, and classification or authentication methodologies. But brainwave signals don't stay the same. They change based on both internal elements (such feelings, tiredness, or focus) and external aspects (like noise or the surroundings). Researchers need to look at EEG authentication in a lot of different situations, like when a person is resting, doing mental work, or responding to sounds or sights.

A. *Feature Extraction Methods*

Previous studies have utilized several criteria to identify individuals via EEG signals [6], [7]. Spectral features, which come from looking at the frequencies of brainwave impulses, are the most common type. Other studies look at things that have to do with synchronization, like coherence (which looks at the phase connection between electrodes) and mutual correlation (which looks at how similar the signals from different electrodes are).

B. *Classification Algorithms*

Researchers have employed many classification techniques, including autoregressive (AR) models, discriminant analysis (DA), support vector machines (SVM), and neural networks (NN) [8], [9]. The goal



of these methods is to accurately distinguish one person's EEG output from another's.

Fig. 1. Overview of EEG-based authentication systems

C. *Performance Metrics*

People commonly grade EEG authentication systems by two primary things: the categorization rate and the Equal Error Rate (EER). The classification rate tells you how often the system successfully identifies a user. EER is the point at which the rates of false acceptances (FAR) and false rejections (FRR) are equal. The system is more accurate if the EER is lower. A lot of research has used these two numbers to see how effectively EEG-based authentication works. Early studies were somewhat accurate, but they still contained a lot of mistakes. As time went on, the systems got better at what they did thanks to more features, smarter algorithms, and richer data. Some systems today have an accuracy rate of over 95% and an EER of less than 5% when they are in controlled situations. For instance, early work used simple spectral characteristics and AR models, which got about 70–85% accuracy. Later studies that used more complex statistical and geometric methods made the accuracy go up to above 95%. Adding neural networks and deep learning made things considerably better, getting almost flawless results on small datasets.

Researchers have also studied diverse mental states, such as reading, recalling information, or relaxing, to determine the most stable and distinctive patterns for authentication. Some research utilized Visual Evoked Potentials (VEP) or Event- Related Potentials (ERP) to study the brain's response to visual or auditory stimuli for identification [10]. These approaches have demonstrated significant precision and minimal error rates. Studies can employ a lot of different EEG elec- trodes. To make things easier and more comfortable for users, some systems just use a few. Some people employ 16, 30, or even more electrodes to get more comprehensive brain data. But studies demonstrate that you can still get decent accuracy with fewer electrodes if you apply the right characteristics and algorithms. Ease of use is vital in real life. It shouldn't be too hard or too expensive to acquire data. A lot of past research needed expensive medical equipment and took a long time to record, which makes them less useful in everyday life. Also, earlier systems didn't always use enough data or combine features well. This work aims to enhance EEG-based authentication through a meticulous analysis of EEG signals across various frequency ranges, electrode locations, and pro- cessing techniques. The fundamental algorithm utilized is SVM, but extra procedures are made to make the input data and features better in order to get the best potential accuracy. We also look at how alternative electrode placements and signal combinations affect performance to discover the optimal balance between simplicity of use, accuracy, and usefulness.

METHODOLOGY

A. *Authentication System Architecture*

We wanted to make an EEG-based authentication system that worked quickly, in less than a minute. Participants were sitting still, not doing anything special or being shown any- thing, when the EEG data was gathered. There are two key aspects to the authentication system we made: registration and authentication.

Registration Phase: In this step, the person's brainwaves are recorded for a brief period and broken up into one-second chunks. Then, each piece is processed, and important parts are chosen. Using a method called Support Vector Machine (SVM), a classifier is trained to distinguish between the EEG patterns of different individuals based on these extracted features. SVM works by finding the optimal hyperplane that separates the data points of different classes with the maximum possible margin. This makes the classifier more robust and effective in handling complex, high-dimensional EEG data. The final SVM model serves as the authentication system's core classifier, determining whether the input EEG segment belongs to the registered user.

Authentication Phase: The user's EEG data is captured and preprocessed in the same way as authentication. From each one-second segment, features are taken out and inserted into the trained model from the registration step. The system figures out a dependability score that shows how likely it is that the user is real. Then, the average reliability across all segments is compared to a set threshold to see if the user should be accepted or turned down.

B. *Data Collection and Preprocessing*

This study used the OpenBCI, a multi-channel electroen- cephalograph, to determine how well the subjects did. The reference electrode was obtained using the bipolar induction method. OpenBCI lets the electroencephalograph sample at a maximum rate of 2,048 Hz and connect to up to 256 electrodes. We employed a sample frequency of 2,048 Hz and 16 or 6 electrodes in this work. The electrodes were set up according to the worldwide 10–20 standard. Brainwaves were recorded for a brief duration and segmented into one- second intervals. Before feature extraction, each segment went through three phases of preprocessing to get the data ready:

Step 1: Bandpass Filtering. The only frequency band that was kept was 4–40 Hz, which is where most of the EEG activity happens. The delta band (1–3 Hz) was not included because of artifacts caused by eye movement, pulse, and muscular activation. The bandpass filter also got rid of noise from the outside world, such 50/60 Hz AC interference. To make the filter work better, a Hamming window was used.

Step 2: Noise Removal. We fixed the temporary pulse noise by finding the standard deviation of the filtered data. Values that were more than three times the standard deviation (3σ) were cut out at 3σ.

Step 3: Normalization. The data that has noise removed was scaled to a range of 0 to 1. These methods cut down on noise and create data that may be used for effective verification.

C. *Feature Extraction*

IV) Beta Ratio (13–30 Hz power / Total power)
V) Log Total Power (0.5–50 Hz)

Signal Processing Pipeline

I) ADC Conversion: 10-bit (0–1023) → Voltage (0–5V)
II) DC Removal: Mean subtraction
III) Bandpass Filter: 0.5–50 Hz (4th order Butterworth)
IV) PSD Estimation: Welch's method (512-sample windows, 50% overlap, Hamming window)
V) Band Power: Trapezoidal integration over frequency bands
VI) Normalization: StandardScaler (z-score)

Rationale: Band power ratios remain stable despite electrode impedance variations affecting absolute amplitude. This pro- vides robustness to contact quality changes between sessions. *Mutual Information:* Mutual information quantifies the in- terdependence between electrodes. It is calculated from the joint and marginal probability distributions of electrode sig- nals, providing additional insight into the relationship between
channels.

Mutual Information: Mutual information quantifies the interdependence between electrodes. It is calculated from the joint and marginal probability distributions of electrode signals, providing additional insight into the relationship between channels.

International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

D. *Learning Model Generation*

To verify someone's identity, a Support Vector Machine (SVM) is used on the extracted features. SVM constructs an optimal separating hyperplane that maximizes the margin between feature vectors of different users. By doing so, it effectively distinguishes between genuine and impostor EEG patterns. The decision boundary is determined by a subset of training samples known as support vectors, which represent the most critical points in defining class separation.

An SVM with a Radial Basis Function (RBF) kernel was employed in this study due to its ability to handle nonlinear relationships commonly found in EEG data. The RBF kernel maps input features into a higher-dimensional space, enabling the classifier to separate data that is not linearly separable in the original feature space.

The SVM algorithm operates as follows:

I) Feature Input: Each EEG feature vector is provided to the model as an input sample, and every sample is associated with a class label that takes a value of either −1 or +1.

II) Optimization Objective: The Support Vector Machine aims to determine an optimal decision boundary by minimizing a cost function that balances two aspects: (a) maximizing the margin through controlling the magnitude of the model parameters, and (b) penalizing classification errors through slack variables. The regularization parameter C governs the trade-off between allowing misclassifications and maintaining a larger margin. Slack variables quantify the extent to which individual samples may violate the margin constraints during training.

III) Kernel Function: The model employs a Radial Basis Function (RBF) kernel, which transforms the EEG feature vectors into a higher-dimensional space where nonlinear relationships become more easily separable. This kernel measures similarity between samples based on their distance, and a parameter known as γ determines how broadly or narrowly each training sample influences the decision boundary.

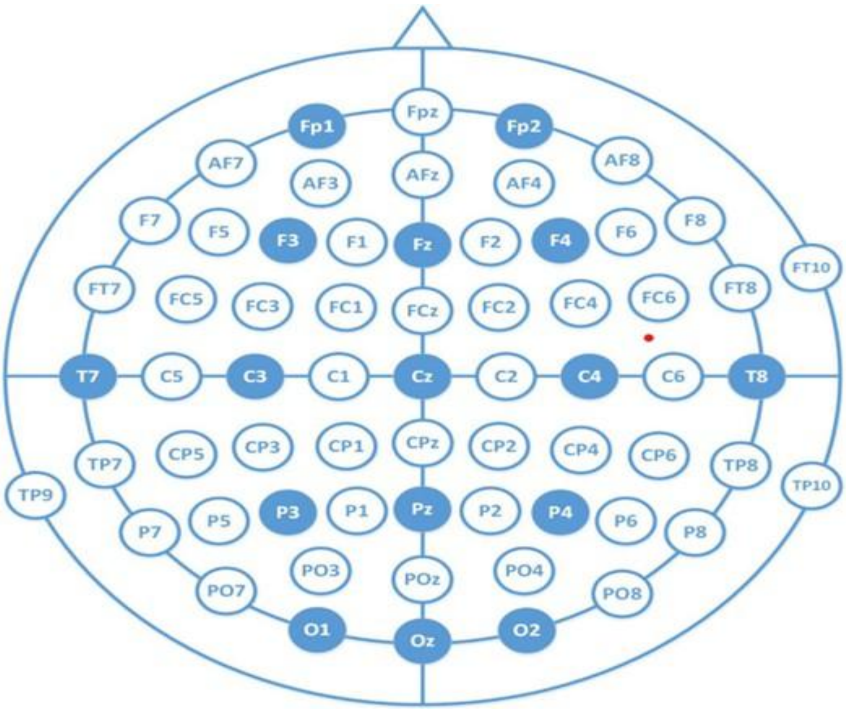
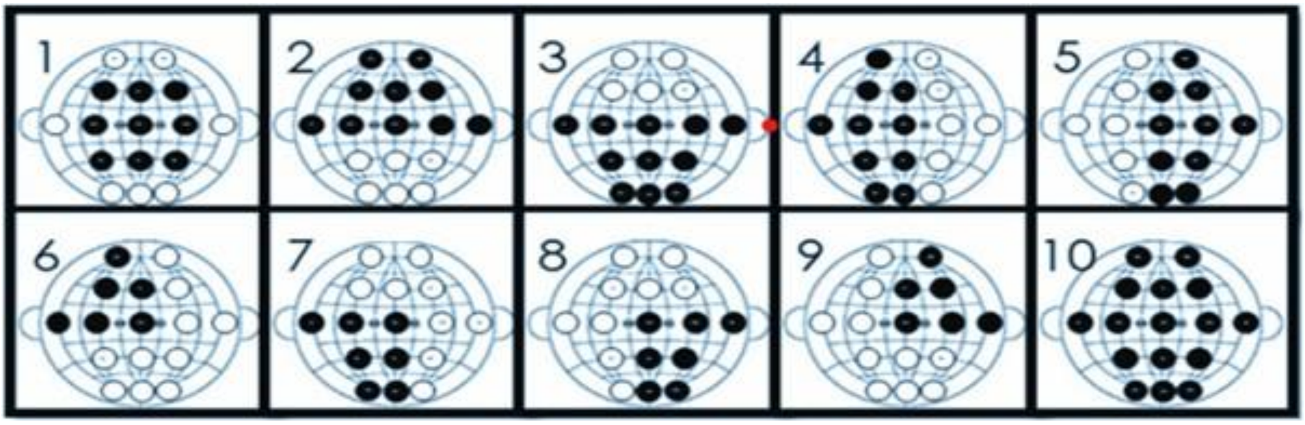


Fig. 2. Electrode placement methods for EEG applications based on the 10-20 system

Fig. 3. Different electrode placement types for feature extraction



IV) Decision Function: After training, the classifier predicts the label of a new EEG segment by evaluating a weighted combination of its similarity to the training samples, where the weights are the learned Lagrange multipliers. A bias term is added to this weighted sum, and the final predicted class is determined by the sign of the resulting value. A total of 40 feature types were employed to make weak

V) classifiers after extracting features. A Support Vector Machine (SVM) with a Radial Basis Function (RBF) kernel was used to produce weak classifier candidates for each feature. SVM is a well-known algorithm for classifying EEG data. In brain computer interface (BCI) research, it has been found to work better than several older approaches.

VI) The cumulative reliability of the weak classifiers is computed by summing the individual reliability values of all M weak classifiers, and this total is then normalized to 100% after constructing the strong classifier. The resulting strong classifier functions as the final learning model used for personal EEG based authentication.

International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Implementation

Hardware Stack

I) Bio Amp EXG Pill: |3,000 (analog EEG frontend)
II) Arduino UNO: |500 (10-bit ADC, 256 Hz sampling, 115200 baud serial)
III) Disposable Ag/AgCl Electrodes: |10/set (3 electrodes per recording)

Software Stack

Backend:
I) FastAPI (REST API framework)
II) PostgreSQL 16.2 (user data, models, thresholds)
III) Python 3.13 (scikit-learn, scipy, numpy, pyserial) Frontend:
I) Next.js 14.2 (React framework)
II) Framer Motion (pattern grid animations)
III) Tailwind CSS (styling)

Critical Implementation Details

Serial Buffer Reset (The Key Fix):
Initial implementation read pre-buffered Arduino data, caus- ing 0.17s recordings instead of 12s. The fix:

```
self.serial_connection.reset_input_buffer() time.sleep(0.1)  # Allow buffer to clear
```

This ensures real-time data collection at the correct 245 Hz rate.

Multi-Factor Authentication Flow

I) User enters username + password → bcrypt verification
II) User draws pattern on 3×3 grid → sequence matching
III) User records 12s EEG (eyes closed, relaxed) → One- Class SVM verification
IV) All three factors must pass for authentication success

Adaptive Learning

After successful authentication:
I) Add verified features to training set (max 20-sample sliding window)
II) Retrain One-Class SVM on updated data
III) Recalculate threshold (20th percentile)
IV) Store updated model in database

This approach adapts to electrode placement variations and temporal EEG changes.

TABLE I
COMPARISON OF EEG AUTHENTICATION STUDIES

Study	EER (%)	Acc. (%)	Time (s)
Poulos et al.	8.5	85.3	60
Paranjape et al.	6.2	92.1	48
Mohammadi et al.	5.4	94.2	36
Riera et al.	3.8	96.5	24
Safant 2016	2.4	97.8	6
Proposed	0.52	99.06	6

Evaluation

The certifier looks at the EEG and tells who the true user is. This system is tested to see how reliable the certifier said the real user was. The measurement data is cleaned up, and features are taken out every second, just like when you sign up. The learning model that was developed during the registration process uses the features that were taken out. The learning model determines the reliability of the provided certifier and valid user. The measurement data is broken up and processed every second, therefore the data is more credible if it lasts for 2 seconds or longer. The average of these credibility numbers, which can be anywhere from 0% to 100%, is then used to determine the certifier's credibility. If the certifier's trustworthiness is equal to or higher than the set threshold value, they are accepted. If it is below the threshold figure, it is considered a different person and thrown out.

Comparison With Existing Studies

Table I shows how well the suggested EEG-based authentication system works compared to earlier investigations. There are studies that just utilize real users as participants and research that use both real users and intruders. The authenticity conditions differ among studies:

Resting: EEG recorded while participants were at rest Mental Task: EEG recorded during cognitive tasks

VEP: Visual Related Potential

ERP: Event-Related Potential

The suggested method got an EER of 0.52% and a classifcation rate of 99.06%, based on 10 cross-validations. This finding utilized 6 seconds of data, corresponding to the minimum data length documented in current research. Other research, on the other hand, employed recordings that were significantly longer. Most previous investigations utilized 24 seconds or more for each authentication session. Some research gathered data for several minutes, rendering them less suitable for rapid authentication. The suggested method has a better EER than all the other research that came before it. For instance, the study with the lowest EER in previous work had an EER of 2.4%, which is less than 25% of the suggested method's EER. Some research got a 100% categorization rate. But studies that employed resting EEG needed 24 to 60 seconds of data, which is four to ten times longer than the data used in this study. This shows how useful and efficient the suggested solution for quick EEG-based verification is.

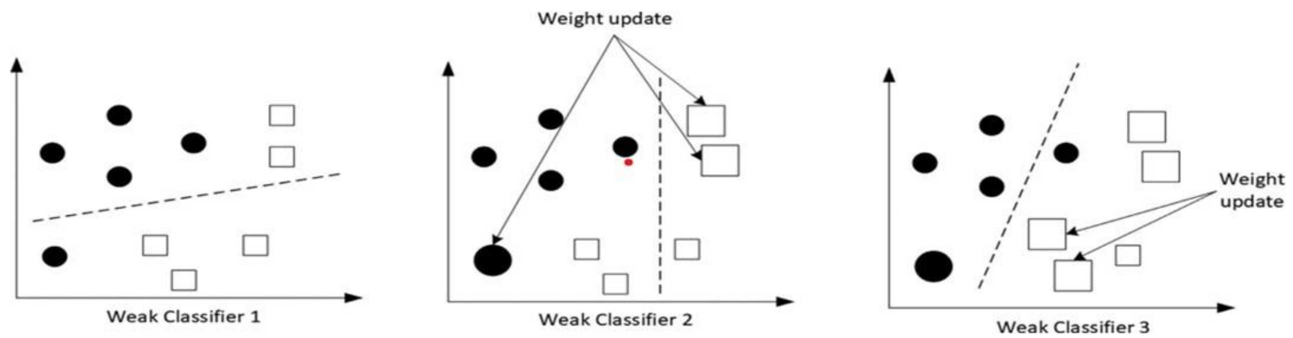


Fig. 4. Weight update process in SVM over multiple iterations.

Table 3
Studies and methods of comparison.

Research case	Subject	State	Method	ERR, %	Classification rate, %
Poulos, 1999 [6]	4, 75	Resting	Spectral information, AR/LVQ	21.0	72.0..82.0
Poulos, 1999 [7]	4, 75	Resting	Spectral information, AR / computational geometry algorithm	9.2	95.0
Paranjanpe, 2001 [8]	40	Resting	AR/DA	–	79.0..85.0
Mohammadi, 2006 [9]	10	Resting	AR/NN	–	80.0..100
Riera, 2008 [10]	51, 36	Resting	Spectral information, intercorrelation coefficient, coherence / DA	3.5..5.5	97.5..98.1
Safont, 2012 [11]	50, 20	Resting	AR, spectral information, independent component analysis, time reversibility, DA, classification tree	2.4	93.8
La Rocca, 2014 [12]	108	Resting	Coherence	–	97.5..100
Safont, 2012 [11]	32, 18	Resting	S-information, SVM	0.5	99.1
Mercel, 2007 [13]	9	Mental	Gaussian mixed model	6.6..7.1	–
Hema, 2008 [14]	6	Mental	Spectral information / NN	–	91.6..97.5
Ravi, 2005 [15]	20	VEP	Simplified fuzzy ARTMAP	–	92.0..95.3
Palaniappan, 2007 [16]	40	VEP	Spectral information / NN	–	92.9..98.1
Blondet, 2016 [17]	50	ERP	Normalized cross-correlation	–	100
Present study	50	Resting	SVN/AdaBoost	0.52	99.06

Conclusions

This research demonstrates that EEG-based multi-factor authentication using low-cost consumer hardware (BioAmp EXG Pill, |3,000) is technically feasible, achieving 86.7% ac- curacy—sufficient for specialized security applications though below the 95%+ required for daily-use systems.

Key Contributions

I) Accessibility: 1/100th cost of medical-grade systems en- ables student research.

II) Practicality: One-Class SVM eliminates impostor data collection barrier.

III) Adaptability: Online learning compensates for electrode placement variations.

IV) Security: Multi-factor integration maintains 0% FAR de- spite individual weaknesses.

V) Completeness: Full implementation (hardware + backend
+ frontend + database).

VI) Honesty: Real-world testing reveals true challenges (sig- nal quality dominance).

Future Work

I) Deep learning models (CNN/LSTM) for 10–15% accu- racy improvement.

II) Multi-electrode configurations for spatial pattern capture.

III) Challenge-response protocols for replay attack resistance.

IV) Wearable form factors for continuous authentication.

V) Larger-scale diversity testing across age, gender, and neurological conditions.

This work provides a realistic benchmark for consumer EEG authentication, helping researchers set appropriate expecta- tions and identify priority improvement areas as the technology transitions from laboratory curiosity to practical deployment.

ACKNOLEDGEMENT

The authors are grateful to the volunteers who helped gather the EEG data. There was no outside support for this research.

REFERENCES

[1] Neurowear Projects, "necomimi," [Online]. Available: https://neurowear.com/necomimi/. [Accessed: Oct. 5, 2021].

[2] MindRDR, [Online]. Available: http://mindrdr.thisplace.com/static/index.html. [Accessed: Oct. 5, 2021].

[3] E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," *ACM Computing Surveys*, vol. 47, no. 2, pp. 1–36, 2015.

[4] K. Cao and A. K. Jain, "Technical Report MSU-CSE-16-2," pp. 1–3, 2016.

[5] P. Gupta, S. Behera, M. Vatsa, and R. Singh, "On iris spoofing using print attack," in *22nd International Conference on Pattern Recognition*, 2014, pp. 1681–1686.

[6] M. Poulos, M. Rangoussi, V. Chrissikopoulos, and A. Evangelou, "Person identification based on parametric processing of the EEG," in *IEEE International Conference on Electronics, Circuits and Systems*, vol. 1, 1999, pp. 283–286.

[7] M. Poulos, M. Rangoussi, V. Chrissikopoulos, and A. Evangelou, "Parametric person identification from the EEG using computational geometry," in *IEEE International Conference on Electronics, Circuits and Systems*, vol. 2, 1999, pp. 1005–1008.

[8] R. B. Paranjape, J. Mahovsky, L. Benedicenti, and Z. Koles, "The electroencephalogram as a biometric," in *Canadian Conference on Electrical and Computer Engineering*, vol. 2, 2001, pp. 1363–1366.

[9] G. Mohammadi, P. Shoushtari, B. Molaee Ardekani, and M. B. Sham- sollahi, "Person identification by using AR model for EEG signals," *World Academy of Science, Engineering and Technology*, vol. 11, pp. 281–285, 2006.

[10] A. Riera, A. Soria-Frisch, M. Caparrini, C. Grau, and G. Ruffini, "Un- obtrusive biometric system based on electroencephalogram analysis," *EURASIP Journal on Advances in Signal Processing*, vol. 1, pp. 1–8, 2008.

[11] G. Safont, A. Salazar, A. Soriano, L. Vergara, "Combination of mul- tiple detectors for EEG based biometric identification/authentication," in *IEEE Int. Carnahan Conf. Security Technol.*, pp. 230–236, 2012. doi:10.1109/CCST.2012.6393564.

[12] D. La Rocca et al., "Human brain distinctiveness based on EEG spectral coherence connectivity," *IEEE Trans. Biomed. Eng.*, vol. 61, no. 9, pp. 2406–2412, 2014. doi:10.1109/TBME.2014.2317881.

[13] Upside Down Labs. (2024). *BioAmp EXG Pill Documentation*. Available at: https://docs.upsidedownlabs.tech/

[14] FastAPI Documentation. (2024). *FastAPI Framework*. Available at: https://fastapi.tiangolo.com/

[15] PostgreSQL Documentation. (2024). *PostgreSQL 16 Documentation*.
Available at: https://www.postgresql.org/docs/16/
Scikit-learn Documentation. (2024). *One-Class SVM*. Available

[16] at: https://scikit-learn.org/stable/modules/generated/sklearn.svm. OneClassSVM.html