e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

AN EEG BASED BIOMETRIC SYSTEM: A REVIEW

Ms. Ranaware Purva[*1], Ms. Lavale Abhilasha[*2], Ms. Jagtap Vaishnavi[*3], Mr. S.D. Biradar[*4]

[*1,2,3,4]Department Of Electronics And Telecommunication VPKBIET Baramati Savitribai Phule Pune University, Maharashtra, India.

DOI: https://www.doi.org/10.56726/IRJMETS63316

ABSTRACT

Traditional biometric systems like fingerprint, facial recognition, iris, retina, and voice recognition have long been utilized for identification and authentication due to their unique, personal characteristics. These technologies provide several security benefits, ranging from controlling entry to device unlocking. However, they are not without some disadvantages, especially concerning misuse and ethical concerns. The possibility that these biometrics can be compelled to be used for identification without the subject's permission is one of the most urgent problems. In fact, traditional biometrics like fingerprints, irises, and retinas remain usable even after death, which raises serious concerns about privacy and security, as these identifiers can be exploited. This is where our proposed system comes it EEG based biometric system which evaluates the brain's electrical activity to determine identity. EEG uses electrodes applied to the scalp to record electrical impulses produced by brain neurons. And it cannot be forcefully used as the signals vary on different state and conditions, it cannot be forcefully verified.

Keywords: EEG (Electroencephalography), Authentication, Machine Learning.

I. INTRODUCTION

Data protection and individual privacy maintenance are more important than ever in today's digital environment, especially as technology develops further. Robust security protocols are needed to protect confidential data and individual possessions. Conventional techniques for identification include passwords, tokens, and biometrics. These identification techniques are not without limitations as passwords can be easily hacked or manipulated, tokens like keys, cards can be stolen or duplicated and biometrics, which use distinctive biological traits like voice, face, and iris identification to provide more secure alternatives, have their own limitations as they can be used in coercive ways, enabling authentication without the explicit consent of the user, which poses significant risks for privacy and misuse of personal data.

To address these concerns and enhance security, advanced biometrics, like EEG (Electroencephalography), has been introduced. EEG-based biometric systems use brainwave patterns for user identification, which are unique to each individual and difficult to replicate.

Brainwave patterns are a more secure alternative than traditional biometrics since they are practically hard to duplicate and can be affected by various situations. This development provides a more advanced layer of privacy protection, which not only increases data protection but also reduces various ethical difficulties. EEG biometrics safeguards personal data which is only used when users provide authorisation to use it.

User Identification Vs Access Authentication

User authentication is the process of identifying or recognising a user by obtaining personal data about them, such as their email address, username, or user ID. Because many unauthorised users may readily access the data, identification identifies but is unable to verify whether the person is authorised. As a result, access authentication is necessary. The technique of identifying users based on their unique biometrics is known as access authentication. Through authentication, users' validity is verified and access is granted. Identification is who the person is while Authentication confirms if it is the right person.

EEG (Electroencephalography)

The method used to assess and record the electrical activity of the brain is called electroencephalography (EEG). This method provides a secure way to authenticate users, as it relies on the unique neurological signals generated by their brains, adding an extra layer of security compared to traditional methods like passwords or fingerprints. It entails applying small non-invasive electrodes to the scalp to pick up electrical signals that

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

neurones send out as they transfer data. These signals, known as brainwaves, can provide information about different mental states, including focus, relaxation, and sleep.The recorded brainwaves are divided into five frequency bands: beta, gamma, alpha, theta, and beta. Each of these bands is linked to a certain function of the brain.

Table 1: Different EEG headsets

Device name	Channels	Electrodes
Emotiv Epoc+	14	Wet
Neurosky MindWave	1	Dry
Muse 2	4	Dry
OpenBCI Ultracortex	Configurable (Upto 16)	Wet/Dry
BrainCo FocusCalm	4	Dry
g.tec g.Nautilus	5	Dry
InteraXon Muse S	Configurable (Upto 16)	Wet/Dry

Wet and dry electrodes are the two primary electrode types used by EEG devices to record brain electrical activity. Wet electrodes are perfect for clinical situations where great precision is required, however they do need a conductive gel or saline solution to improve the signal quality. While these devices can identify minute brainwave patterns, they need to be prepared and maintained, which may be difficult. On the contrary, dry electrodes require no gel, which makes them ideal for wearable and portable electronics. They could, however, yield signals of less quality than wet electrodes. EEG devices use various electrode kinds to capture distinct brainwave patterns related to different mental states during certain tasks, which is used in the process of authentication. The device can successfully verify a user's identity by looking at their brain activity. through analysing these patterns.

Electroencephalogram (EEG) results are commonly explained in terms of brain wave rhythmic activity. Five crucial frequency ranges have been identified in growing order of frequency at which signals' amplitudes and frequencies change between states [8.]

The five brainwave types—delta, theta, alpha, beta, and gamma—play a crucial role in EEG-based authentication by producing distinct mental "signatures" for every user. Although the brain's normal condition is confirmed by delta waves, which are linked to profound sleep, they are not actively used for authentication. When performing calm activities, theta waves—which are associated with creativity and relaxation—help systems recognise distinctive patterns when focussing or visualising. When a person is relaxed but alert, like when they are meditating quietly, alpha waves arise. These calm situations provide unique brainwave patterns that are used for authentication. When doing problem-solving or focus-based tasks, users can verify themselves with the use of beta waves, which are produced during active thought and concentration. Considering how they relate to higher order cognitive functions, gamma waves serve as a reliable indicator when engaging in complex mental processes and deep thought. EEG devices provide a highly secure and individualised authentication approach by utilising the brain's natural reactions to authenticate an individual's identity.

Table 2: Types Of Brainwaves

Brainwave Type	Frequency Range (Hz)	Brain State
Delta	0.5-4	Deep Sleep
Theta	4-8	Light sleep, relaxation
Alpha	8-12	Calm, restful awake state
Beta	12-30	Active thinking, alertness
Gamma	30 and above	Higher mental activity, perception

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

II. LITERATURE REVIEW

Table 3: Summary of Various Studies on EEG Authentication in decreasing order of accuracy

Author(s)	Channels	No. of Subjects	Task	Derived or Extracted Features	Classifier	Avg. accuracy
Ruiz-Blondet et al. [11]	3	50	visual stimulation of 400 images	Event-Related Petentials (ERP)	normalized cross-correlation	100%
La Rocca et al. [14]	64	108	relaxation with opened eyes and closed eyes	Power Spectral Density (PSD), Spectral Coherence (COH)	Mahalanobis distance-based classifier and match-score fusion	100%
Chen et al. [12]	16	29	Rapid Serial Visual Representation (RSVP)	point-biserial correlation coefficients, Fisher's transformation	Linear Discriminant Analysis (LDA)	100%
Palaniappan [16]	6	6	5 tasks: relaxation, math activity, geometric figure rotation, mental letter composition, visual countings	Auto-regressive coefficients (AR), Spectral Power (SP), Inter-Hemispheric Power Difference (IHPD), Inter-Hemispheric Linear Complexity (IHLC)	LDA	100%
Ashby et al. [17]	14	5	4 tasks: relaxation, limb movement, visual counting, geometric figure rotation	AR, SP, IHPD, IHLC, PSD	Support Vector Machine (SVM)	100%
Chuang et al. [15]	1	15	7 tasks: breathing, simulated finger movement, sport activity, singing/passage recitation, audio listing, color identification, and pass-thought	Cosine similarity of the vector representation	k-Nearest Neighbour (k-NN)	99%
Palaniappan et al. [21]	61	20	drawings of common objects as visual stimulation	multiple signal classification (MUSIC)	k-NN, Elman Neural Network (ENN)	98%
Riera et al. [18]	4	-	relaxation	AR, Fast Fourier Transform (FFT), mutual information, coherence, cross correlation (EEG and ECG data)	Fisher Discriminant Analysis (FDA)	98%
Jayarathne et al. [19]	14	12	imagining four digit number as cognitive task	Common Spatial Patterns (CSP)	LDA	97%
Riera et al. [22]	2	51	relaxation with closed eyes	Higuchi fractal dimension, entropy, skewness, standard deviation, AR	LDA	97%

Key Factors Influencing EEG-Based Authentication Systems:

1. **Environmental Conditions:** The setting where EEG readings are taken can affect the quality of the signals. For example, loud noises or bright lights can interfere with the brain's electrical activity, leading to inaccurate results. A quiet and comfortable environment is essential for reliable readings.
2. **User State and Mental Condition:** How a person feels during the authentication process matters. Stress, fatigue, or distractions can alter the brain's activity, which may impact the accuracy of the authentication system. A calm and focused mental state is ideal for obtaining consistent EEG signals.
3. **Signal Processing Techniques:** The methods used to process EEG signals are crucial for their clarity. Techniques like filtering can help remove unwanted noise and artifacts from the readings. Good signal processing enhances the reliability of the data, making it easier to identify authentic users.
4. **User Training and Adaptation:** How well users are trained to use the EEG system can affect its success. If users understand how to engage with the technology and are familiar with the process, they are more likely to provide consistent signals. Adequate training can improve usability and acceptance.
5. **Age and Health Factors:** Different age groups may have varying EEG signal characteristics. Additionally, a person's health can influence brain activity patterns. For instance, neurological conditions may alter the EEG signals, making it challenging to develop a one-size-fits-all authentication system.
6. **Changeability of EEG-Based Biometrics:** Unlike traditional biometric systems, EEG patterns can change over time due to various factors like mood or cognitive tasks. This flexibility can be both an advantage and a challenge, as it may require frequent updates to the authentication model to maintain accuracy.
7. **Data Privacy and Security:** Protecting the EEG data collected during authentication is essential. Since this data is sensitive, ensuring that it is securely stored and transmitted can prevent unauthorized access and misuse. A robust security framework is necessary to build trust in EEG-based systems. These factors illustrate the complexity involved in developing effective EEG-based authentication systems, emphasizing the need for careful consideration of both technical and user-related elements.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

III. METHODS

1. Task-Specific Feature Extraction and SVM Classification.

The authentication method proposed in [13] research leverages machine learning to enhance security through biometric or behavioral data analysis. The process begins with data acquisition, where features such as fingerprints, facial recognition, or user behavior are collected. These inputs are pre-processed and supplied to a model for machine learning, typically trained using algorithms like Neural networks, decision trees, or support vector machines (SVM). The method's strength lies in the machine learning model's ability to learn and identify unique patterns in the dataset, enabling accurate user authentication. During the authentication phase, the system compares real-time input data with the trained model to verify the user's identity. While the paper claims high accuracy rates, the review highlights the importance of providing more detailed metrics, such as precision and recall, to assess the effectiveness of the approach. Additionally, the method's potential to minimize false positives and negatives is promising. However, the paper could benefit from a more comprehensive comparison with existing authentication systems to clearly illustrate the performance benefits of this machine learning-based solution.

2. Power spectral density (PSD) analysis of EEG signals and linear discriminant analysis (LDA).

In study [6], authors employed a method for EEG-based individual authentication that integrated signal processing and machine learning techniques. EEG signals were recorded from fifteen volunteers under two conditions: eyes open (EO) and eyes closed (EC). Following data acquisition, the raw EEG data underwent preprocessing, including down sampling, common average referencing (CAR), and bandpass filtering from 0.5 to 90.5 Hz. Physiological artifacts were effectively removed using fast independent component analysis (ICA). Power spectral densities (PSD) were then estimated for each condition, with differences between EO and EC calculated. The mean PSDs served as features for classification. A binary-class linear discriminant analysis (LDA) was performed with a 5x5-fold cross-validation to assess authentication accuracy. The results indicated that the EC condition achieved an impressive mean authentication accuracy of over 97%, significantly outperforming the EO and difference conditions. This highlights the potential of using resting state EEGs for robust individual authentication.

3. Wavelet Packet Decomposition.

The study [11] focuses on signal collecting, pre-processing, feature extraction, and classification in their neural network-based architecture for EEG-based identification and authentication. A visual stimulus task was used to gather EEG data from 32 individuals. The signals were subsequently denoised using a low-pass filter and ensemble averaging. Wavelet Packet Decomposition (WPD) was used to extract features across five EEG frequency bands, and the mean, standard deviation, and entropy were computed. for each band. These features were used to train a neural network for classification. Four different identification scenarios were tested: identifying all 32 subjects, improving accuracy with side-by-side identification, distinguishing a single subject from the others and a small group from the others. The performance was evaluated using classification rates, where Scenario III (identifying one subject) showed the highest accuracy (up to 99.87%), while Scenario I (identifying all subjects) had the lowest (5.75% to 10.68%). Scenario II improved accuracy through sub-models, and Scenario IV demonstrated effective group identification. The findings suggest that EEG-based authentication systems can effectively identify individuals, especially in smaller groups or single-subject scenarios, with neural networks providing high accuracy.

4. CSP and LDA.

The study [9] employs a method for user authentication using electroencephalogram (EEG) signals by combining Common Spatial Pattern (CSP) for feature extraction and Linear Discriminant Analysis (LDA) for classification. The multichannel EEG data is efficiently reduced into a lower-dimensional space via CSP, highlighting relevant patterns associated with each user. Following feature extraction, LDA classifies the data into two classes based on statistical properties, enhancing separation between users. The implementation utilizes the EMOTIV Epoch+ EEG headset, capturing brain activity while subjects visualize a four-digit PIN. The system demonstrates promising accuracy rates, achieving 81.81% for the Alpha band, 90.91% for the Beta band, and 96.97% for the combined frequency band (8–30 Hz). Despite some challenges with electrode comfort

and signal consistency, the approach shows potential for further refinement and improved accuracy in EEG-based user authentication systems.

5. Other Methods

EEG-based authentication methods include various techniques, each contributing to improved classification and accuracy. **Convolutional Neural Networks (CNN)** are effective in extracting spatial features from EEG signals through their layered structure, making them suitable for complex pattern recognition. **EEG data is classified using K-Nearest Neighbors (KNN) using the feature space's nearest training samples.**, offering simplicity and ease of implementation. **Auto-Regressive (AR) models** capture the temporal dependencies in EEG signals, providing a mathematical approach to feature extraction. **Learning Vector Quantization (LVQ)** is a type of artificial neural network that focuses on classifying patterns in EEG data by adjusting prototypes based on training samples. **Recurrent Neural Networks (RNN)** are designed to handle sequential data, making them adept at recognizing patterns in time-series EEG data. **Gaussian Mixture Models (GMM)** use statistical methods to model the probability distribution of EEG features, enhancing classification accuracy. Together, these methods leverage the unique characteristics of EEG signals to improve authentication systems.

IV. CONCLUSION

In conclusion, EEG-based authentication systems represent a promising frontier in biometric security, utilizing unique brain wave patterns for user identification. The exploration of different frequency bands highlights their significance in reflecting users' mental states during authentication tasks. Methodological advancements in data acquisition and feature extraction significantly enhance the effectiveness of these systems. While current limitations such as comfort and signal consistency exist, the potential for higher accuracy and user-friendly designs is substantial. Overall, EEG technology offers a secure, non-invasive, and efficient biometric solution for various applications. The integration of EEG in authentication has the potential to redefine security protocols across multiple domains, providing a new dimension to personal security.

V. REFERENCES

[1] H. Mou, Z. Pei ,W. Yang, F. Li , S. Zhang and X. Wu, "An Overview of Brain Fingerprint Identification Based on Various Neuroimaging Technologies," in IEEE Transactions on Cognitive and Developmental Systems, 2024.

[2] D. Lyras, and C. A. Fidas "A Review of EEG-Based User Authentication: Trends and Future Research Directions," 2023

[3] S. K. Guirguis and A. R. Elshenaway, "Adaptive Thresholds of EEG Brain Signals for IoT Devices Authentication", 2021.

[4] M. I. Husain, and J. Patel "An Approach to Developing EEG-Based Person Authentication System," 2020.

[5] J. Joy ,A. Christopherand and A. Garule "Feasibility Study on Building Practical Authentication Systems using Brain Biometrics," 2019.

[6] G. -Y. Choi et al., "Biometrics Based on Single-Trial EEG", 2019.

[7] C. A. Hewawasam Puwakpitiyage ,M. S. A. Muhammad Azizi, V. R. Paramesura Rao, M. D. Hamzah,, R. K. Murugesan and W. J. Tee, "Authentication with brainwaves: a review on the application of EEG as an authentication method,"2018,

[8] Isuru Jayarathne,Michael Cohen and Senaka Amarakeerthi ,“Survey of EEG-Based Biometric Authentication”,2017.

[9] M. Cohen ,I. Jayarathne and S. Amarakeerthi, "BrainID: Development of an EEG-based biometric authentication system," 2016.

[10] Harshit, K. P. Thomas, K. G. Smitha and A. P. Vinod, "Online Electroencephalogram (EEG) based biometric authentication using visual and audio stimuli,"2016.

[11] Qiong Gui, ,Wenyao Xu and Zhanpeng Jin. “Exploring EEG-based biometrics for user identification and authentication”,2014.

[12] Bru. Quintela , J. P. da Silva Cunha and A. Zquete ,”Biometric authentication using brain responses to visual stimuli.”, 2010.

[13] Amit Bhatia, Jacob Vogelstein ,Francesco Tenore and Corey Ashby. “Low-Cost Electroencephalogram (EEG)- Based Authentication.” 1999.