International Journal of Advanced Multidisciplinary Research and Educational Development ISSN: **3107-6513**
Volume 2, Issue 1 | January - February 2026 | www.ijamred.com

Brainwave-Based Secure Authentication Using Neural Identity Patterns

Abirami S[#1], Dr. K. Banuroopa[*2]
[#1]Student, Department of Information Technology, Dr. N.G.P Arts and Science College, Coimbatore, India
[*2]Associate Professor, Department of Information Technology, Dr. N.G.P Arts and Science College, Coimbatore, India
[1]abhiialkah@gmail.com, [2]banuroopa.k@drngpasc.ac.in

ABSTRACT
The growing pace of digital systems has led to the exposure of traditional methods of authentication, like passwords and biometric identifiers, to mounting levels of concerns of safety, privacy, and vulnerability to impersonation attacks[1]. To counter these limitations, this paper proposes a brainwave-based secure authentication mechanism that makes use of distinct neural identity sensitivity on electroencephalographic (EEG) responses[2]. The suggested model focuses on four main EEG frequency bands such as delta, theta, alpha and beta, which represent the unique cognitive and physiological features of individual subjects[3]. The features are received through signal preprocessing and feature extraction algorithms and then categorized through the use of a Gradient Boosting machine learning algorithm to provide powerful user authentication[5].
The system uses a cryptographic layer to enhance the data security by encrypting user-related information with sensitive files using the Advanced encryption Standard (AES) encryption[4]. The authentication and encryption tasks are performed in order to ensure identity verification and safe data protection[6]. The system is tested using publicly available EEG datasets, thus showing that it is possible to perform EEG-based authentication under a controlled setting[7]. The results show that a neural signal analysis, machine learning, and cryptographic method have been combined to produce a strong and multi-layered security system[8]. The paper preconditions the future real-time applications, which could utilize wearable EEG sensors and IoT-based systems with the goal of improving the usability and supporting the working implementation of the application in secure access-control settings[9].

KEYWORDS : EEG Authentication, Brainwave Signals, Neural Identity Patterns, Gradient Boosting, Secure Access Control, AES Encryption.

I. INTRODUCTION

The increased pace of the development of digital applications and online services has increased the pressure on the need to have secure and reliable authentication mechanisms[10]. Traditional credentials, such as passwords, personal identification numbers, and one-time passwords, are widely used, but still, they tend to have vulnerabilities to credential theft, brute-force attacks, and unauthorized access[11]. The modalities, which are mostly used as biometrics like facial recognition and fingerprint, are also susceptible to spoofing and privacy concerns[12]. These restrictions therefore provide impetus to the need to develop advanced authentication methods that can be used to authenticate the true identities of users with a greater level of security. The introduction of the electroencephalogram (EEG)-based authentication is the result of the peculiarities of the brainwave signals[13]. EEG records the electrophysiological activity of the cerebral cortex and is often decomposed into four major frequency bands which are: Delta, Theta, Alpha and Beta[14]. The combination of these spectral patterns results in a very personalized neural signature making EEG signals very resistant to imitation and counterfeit[15]. Based on this, EEG is an effective biometric modality of high-security authentication setting.

Reflecting on the current research, a safe authentication system based on EEG signals was realized with the help of publicly accessible EEG corpora[5]. The raw EEG signals were first preprocessed with routines that reduced noise and other extraneous artifacts and discriminative statistical and frequency-domain features of each canonical EEG band were then extracted[10]. The users were categorized using a Gradient Boosting machine-learning model, which was used to label the users according to derived features vectors[7]. To add further security to the system, a cryptographic layer was added in which an authenticated user data was encrypted through the Advanced Encryption Standard(AES)[4]. The resulting architecture demonstrates the soundness of the hybridization of EEG-based biometric authentication with modern machine-learning and cryptographic systems, which proves to provide a high-scalability platform to future real-time applications with the use of IoT-enabled wearable EEG devices[8].

II. LITERATURE REVIEW

The traditional authentication systems, such as passwords and one-time credentials, are inherently limited and have triggered the research into the biometric-based authentication systems[1]. The conventional biometric characteristics like fingerprints and facial identification, although making it easier to use, are prone to attacks by spoofing and pose a serious privacy issue[2]. In this line, the recent studies have focused on the electroencephalogram (EEG) signals as a biometric modality due to its implicit uniqueness and inability to be imitated[3].

Many research works have confirmed that EEG-based authentication is possible using publicly available EEG data, where the recording of multiple subjects are recognized as different user identities[5]. These studies are regularly using preprocessing methods that reduce the noise and artifacts, followed by deriving statistical and frequency-domain features of canonical EEG frequency bands, such as Delta, Theta, Alpha, and Beta[11]. These features capture the individual neural attributes that are friendly to authenticating the user[6].

Machine-learning systems have been implemented to categorize users according to extraction EEG characteristics[12]. It is noteworthy that ensemble learning algorithms and especially the Gradient Boosting have shown encouraging results in terms of their ability to cope with the nonlinear and noisy characteristics of the EEG data[7]. Gradient Boosting enhances the accuracy and resistance of classification by repeatedly refining weak learners making it highly applicable in EEG-based user authentication[13].

Although there is the EEG-based authentication process, most of the existing systems focus on identity verification and do not incorporate the provision of mechanisms that ensure safe protection of post authentication data[8]. Cryptography (like the Advanced Encryption Standard) provides high security levels of confidentiality to sensitive data, but is more often used without biometric systems[14]. This has been a gap that has inspired the current work, which combines EEG-based authentication using Gradient Boosting with AES-based encryption to give a more detailed and safe authentication system[9].

III. METHODOLOGY

1. Dataset Description

The EEG-based secure authentication system is suggested to be performed with publicly available EEG data sets

where participants are the representations of individual user groups. The data is multi-channel EEG recordings that were made in controlled experimental situations. In every EEG sample, there are subject identifiers, time-series values of EEG signals, channel data, sampling rate, and recording time[15]. Each subject has several EEG trials, which enables the system to gain intra-subject variability and boost the reliability of authentication[13]. The method is based on the use of datasets, enabling the use of controlled experiments without having to acquire equipment to record real-time EEG[6].

2. Data Preprocessing

The noise and the artifacts in the raw EEG signals are caused by eye blink, muscular and external electrical interferences[11]. In order to enhance the signal integrity, bandpass filtering and normalization are used as preprocessing methods. These processes reduce the frequency contents that are not relevant and normalize the amplitude of signals, thus leaving only informative information in the neural systems to be subjected to further processing[6].

3. Feature Extraction

The processed EEG signals are separated into four main frequency bands including Delta, Theta, Alpha, and Beta. Both the statistical and frequency-domain features of each band are obtained to generate discriminative neural features[10]. The resultant features consist of band-specific energy levels and spectral measures which are useful in capturing subject-specific EEG patterns[3]. These characteristics are later aggregated to create small sized feature vectors as neural identity representations of individual users.

4. Gradient Boosting user authentication. The authentication of users is performed with the help of a Gradient Boosting machine-learning algorithm[7]. Gradient Boosting is an ensemble learning method that builds a powerful classifier by sequentially combining many weak learners which makes it optimal towards capturing the nonlinear and non-stationary characteristics of the EEG data[14]. The model is trained at the stage of training and acquires the mapping between the extracted EEG feature vectors and user identities. The data is divided into training and testing to test the performance of authentication. In the authentication process, the trained model is tested on feature vectors based on test EEG patterns, and a confidence based decision level is used to reduce the false acceptance and false rejection error rates[15].

5. Cryptographic Data Protection

The successful authentication is followed by a cryptographic layer protection of sensitive user data. The encryption of the authenticated user information is done using the Advanced Encryption Standard (AES) to achieve confidentiality and prevent unauthorized access to the information[4]. Encryption is used with an identity check and thus this explicitly separates authentication and data-protection functions and makes encrypted content only available to authenticated users[12].

6. Workflow Summary

 ISSN: 3107-6513

The general design of the workflow is as follows: it is based on EEG data acquisition of a dataset, so that the noise and artifacts are removed, the standard frequency bands are decomposed and the discriminative features are extracted[11]. All these features are identified with the help of a Gradient Boosting model that helps to authenticate the user and encrypt sensitive data with the help of AES[4]. It is a software-based system with EEG datasets that allows its implementation and validation in an experimental setting with a software system, which can be verified and scaled. The unified framework indicates that it is possible to combine EEG-based biometric authentication, machine-learning, and cryptography methods into one secure and secure system[15].
The secure authentication system based on the EEG that was detailed herein was tested using the publicly available EEG datasets with the aim of testing whether the authentication was reliable, security was robust and whether the system was feasible[10]. Neural identity patterns
using features extracted at the Delta, Theta, Alpha and Beta frequency bands were stable and provided a means of effective user discrimination through a Gradient Boosting classifier[13]. The system had a high level of reliability in generating conclusive authentication decisions- permission to access or not allow access and then use secure data encryption[9].

IV. RESULTS AND DISCUSSION

1. Comparison with Existing Authentication Systems

Parameter	Existing Systems	Proposed EEG-Based System
Authentication Method	Passwords, OTPs, Biometrics	EEG Neural Patterns
Identity Verification	Credential-Based	Brainwave-Based
Spoofing Resistance	Low to Moderate	High
Replay Attack Protection	Low	High
Continuous Authentication	Not Supported	Supported
Data Security	Optional	AES-Based Encryption
User Data Protection	Partial	Strong
Hardware Dependency	Minimal	Dataset-based (Future IoT EEG)

2. Discussion of Authentication Result and Performance.

Gradient Boosting classifier was able to include nonlinear features of EEG signals and to learn personalized neural signatures during the training process. The verification consistency was maintained by basing authentication decisions on a confidence-based threshold, which reduced the false acceptances. As a result, the product of this system is binary that gives one access only when there is a match between the features of the extracted EEG and the stored neural identity[7].

3. Security and System Feasibility.

The AES encryption is only performed after a successful authentication process and thus it protects confidentiality and eliminates any possibility of unauthorized access to vital information[11]. Although the present prototype relies on fixed datasets, the results clearly indicate the high potential of real-time implementation through the IoT-enabled wearable EEG devices in future applications[5].

4. Result Summary

The findings testify to the fact that EEG-based biometric authentication, Gradient Boosting classification and AES encryption makes up a safe and reliable authentication system. This solution offers better protection functionality as compared to the traditional methodologies and highlights its potential of high security applications.

V. CONCLUSION AND FUTURE SCOPE

This paper proposes a safe authentication system based on electroencephalogram (EEG) signals, in which a machine learning and cryptographic approach will be combined to enhance the security of the system[9]. Using the unique neuro-identity patterns that are encoded in EEG frequency bands, the proposed architecture can be used to replace the traditional authentication approaches based on a credential, which are most susceptible to spoofing, and unauthorized access[12]. Using signal preprocessing and feature extraction techniques allow derivation of neural features that are discriminative, and a Gradient Boosting classifier is a good learner that classifies users by the discriminative features. Besides, the use of the Advanced Encryption standard (AES) encryption protects confidentiality of sensitive user data once authenticity is achieved. The existing system can be improved further by adding additional functionality that can monitor real-time
EEG signal acquisition with IoT-enabled wearable EEG devices. This kind of integration would allow live authentication, ease of use, and deployment in the real-world security environment[4]. Further studies may also focus on adaptive thresholding methods, lightweight authentication models to run authentication faster, and multimodal authentication systems that are more complex and integrate EEG with other biometric techniques.
The proposed system has a number of limitations in spite of its merits. The current implementation mostly uses EEG datasets that are available publicly as opposed to real-time acquisition of EEG and therefore limiting real use in real-life applications[6]. Moreover, EEG signals are highly variable and prone to noise and it is required to carefully preprocess them so as not to eliminate authentication accuracy. The general usability of EEG-based authentication also depends on the level of comfort to the user as well as the availability of EEG recording apparatuses[8]. Taken together, the suggested framework proves the practicability of using EEG-based authentication that is added with cryptographic safeguarding and provides the basis of scalable secure access systems of the next generations[7].

REFERENCES

[1] Sarah Laszlo and Zhanpeng Jin, "CEREBRE: A Novel Method for Very High Accuracy Event-Related Potential Biometric Identification," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2340–2353, 2016.

[2] N. Abo Alzahab, A. Di Iorio, M. Baldi, and L. Scalise, "Effect of Auditory Stimuli on Electroencephalography-Based Authentication," *arXiv preprint arXiv:2206.14519*, 2022.

[3] W. Alsumari, M. Hussain, L. Alshehri, and H. Aboalsamh, "EEG-Based Person Identification and Authentication Using Deep Convolutional Neural Network," *Axioms*, vol. 12, no. 1, p. 74, 2023.

[4] A. R. Hassan, S. Siuly, and Y. Zhang, "Epileptic Seizure Detection Using Statistical Features and Machine Learning Techniques," *Biomedical Signal Processing and Control*, vol. 31, pp. 365–372, 2017. *(Relevant for EEG feature extraction and classification methods)*

[5] J. Chuang, H. Nguyen, C. Wang, and B. Johnson, "I Think, Therefore I Am: Usability and Security of Authentication Using Brainwaves," *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI)*, pp. 373–382, 2013. *(Foundational EEG authentication concept, cited widely in later works)*

[6] KeyEncoder: A Secure EEG-Based Cryptographic Key Generation Mechanism, *Pattern Recognition Letters*, vol. 173, pp. 1–9, Sept. 2023.

[7] Bin Liu et al., "Research on Real-Time Security Authentication Method Based on EEG Data Features," *Applied Mathematics and Nonlinear Sciences*, vol. 10, no. 1, pp. 1–12, Jan. 2025.

[8] Abeer Al-Nafjan, L. Alahaideb, M. Aldayel, and H. Aljumah, "EEG-Based Authentication Across Various Event-Related Potentials (ERPs)," *Sensors*, vol. 25, no. 16, 2025.

[9] M. Fallahi, P. Arias-Cabarcos, and T. Strufe, "Advancing Brainwave-Based Biometrics: A Large-Scale, Multi-Session Evaluation," *arXiv preprint arXiv:2501.17866*, Jan. 2025.

[10] R. Palaniappan, "Biometric Authentication Using Brain Signals: A Review," *International Journal of Neural Systems*, vol. 25, no. 2, 2016.

[11] S. Marcel and J. Delorme, "On the Application of EEG Biometrics to User Authentication," *Pattern Recognition Letters*, vol. 82, pp. 79–85, 2016.

[12] A. Bashar, M. Bhuiyan, and I. Ahmad, "Identification of Individuals Using EEG Signals with Ensemble Learning Techniques," *Expert Systems with Applications*, vol. 165, 2021.

[13] S. Yang, Y. Wang, and J. Huang, "EEG-Based Biometric Authentication Using Frequency-Domain Features," *IEEE Access*, vol. 7, pp. 37889–37899, 2019.

[14] J. Li, X. Zhang, and Y. Li, "Secure Biometric Authentication System Based on EEG and Cryptographic Techniques," *Journal of Information Security and Applications*, vol. 58, 2021.

[15] K. Wang, Z. Li, and Q. Sun, "Security Threats and Privacy Protection in EEG-Based Biometric Systems," *Computers & Security*, vol. 124, 2023.