IJIREEICE

ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁙ Peer-reviewed & Refereed journal ⁙ Vol. 12, Issue 5, May 2024

DOI: 10.17148/IJIREEICE.2024.12530

Biometric Identification System using EEG Signals

Prathamesh Chaudhary[1], Dhanashri Mokashi[2], Ajnkya Parve[3] , Mr. S. D. Biradar[4]

Student, Department of Electronics and Telecommunication Engineering, VPKBIET, Pune, India[1]

Student, Department of Electronics and Telecommunication Engineering, VPKBIET, Pune, India[2]

Student, Department of Electronics and Telecommunication Engineering, VPKBIET, Pune, India[3]

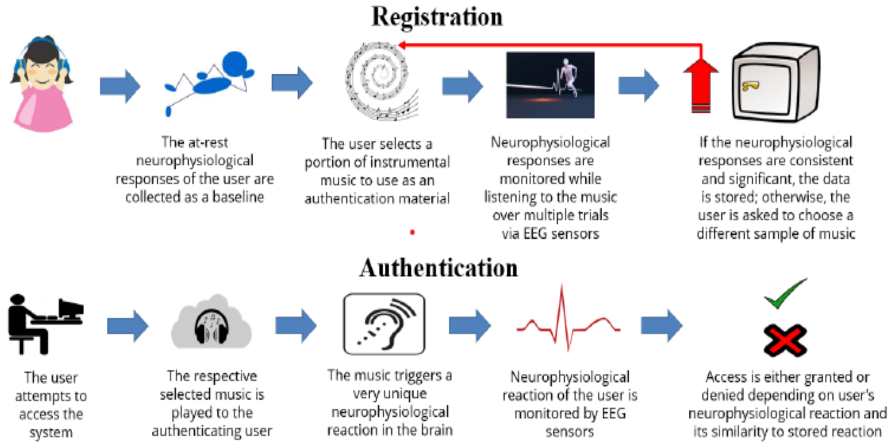
Professor, Department of Electronics and Telecommunication Engineering, VPKBIET, Pune, India[1]

Abstract: The activities of human brain- EEG signals are no doubt to furnish a most secure approach in biometric for user authentication/identification owing to the fact that they are highly sensitive, secretive and inimitable. As we can see, now-a-days the attacks against traditional biometric authentication systems are increased, hence there is the need of a robust biometric authentication which cannot be easily compromised. At present there are two biometric authentication systems: Fingerprint and Facial Recognition, which are most popular and widely used. There is one more case in which the user might be forced by an attacker or hacker to comply authentication. Hence here comes the authentication mechanism which we propose in which the attacker cannot hack, mimic, or forcefully gain access from the user. A Biometric Identification technique which is totally based on subject's neurological responses and are measured by exercising electroencephalogram (EEG).

Keywords—EEG biometrics, User identification, High accuracy, Brainwave authentication, Biometric security, Electroencephalography, User authentication, Biometric recognition, Neurotechnology, Biometric identification.

I. INTRODUCTION

Numerous technological developments have made real-time applications with remote access feasible in a wide range of industries, including banking, healthcare, retail, law enforcement, military, and enterprise. But security is a crucial component in these kinds of sensitive applications, and convenience is typically sacrificed for security[2]. Methods for identifying users are advancing quickly, and in many areas of information security, they are crucial. In order to recognise the user while interacting with computers, this technique requires the user's credentials. Biometrics has gradually arisen lately to improve the confidentiality of the user's method for identification. Utilising signal processing, machine learning, and pattern recognition techniques, they are made to extract physiological information from users and compare them to These biometric traits include voice, face, iris, gait, fingerprint or foot print, and signature technology. user's profile or template stored in database. However, there is a chance that users' biometric traits can be stolen or faked. Physical attributes, like voice recordings or pictures of faces, can be digitally recorded, duplicated, or falsified by an adversary[1].


Registration
The at-rest neurophysiological responses of the user are collected as a baseline
The user selects a portion of instrumental music to use as an authentication material
Neurophysiological responses are monitored while listening to the music over multiple trials via EEG sensors
If the neurophysiological responses are consistent and significant, the data is stored; otherwise, the user is asked to choose a different sample of music
Authentication
The user attempts to access the system
The respective selected music is played to the authenticating user
The music triggers a very unique neurophysiological reaction in the brain
Neurophysiological reaction of the user is monitored by EEG sensors
Access is either granted or denied depending on user's neurophysiological reaction and its similarity to stored reaction

Biometrics, which is a pattern-recognition technology that uses an individual's unique physiological or behavioural traits to authenticate or identify them. Among other things, these characteristics may include facial features, iris, fingerprints, and brainwaves. Unlike traditional personal recognition schemes that use rules like "something we know" or "something

DOI: 10.17148/IJIREEICE.2024.12530

we have," biometric systems rely on a more secure "something we are" policy. Examples of such policies include access cards, user identifying features, and personal identity numbers. Simple and sensible ways to establish security involves using bank cards, smart cards, security tokens, and traditional techniques including user passwords and personal information. Unfortunately, though, malicious attacks can still target them[3]. According to a study, it is possible to create master prints that an adversary may use to start a dictionary attack on a fingerprint recognition system. Furthermore, biometric systems are susceptible to external attacks, such as those carried out by people wearing contact lenses that have synthetic iris and printed artificial textures on them. New biometric identification techniques employing EEG have been designed and suggested in anticipation of these security vulnerabilities. EEG is a reasonable indication for biometrics for a number of reasons. As each person's brain activity is distinct and consistent over time, it is challenging to steal a mental passphrase[1].

II. EASE OF USE

A.System of Authentication:

Prioritizing a certain set of qualities is necessary for a reliable and strong authentication system. The mechanism needs to always ensure a sufficiently high accuracy level to prevent repeated failed login attempts for all authorized users. In a similar vein, the system has to reduce the likelihood that an unauthorized user will authenticate into it. There is more danger involved in allowing an unauthorized user to access the system than in preventing an authorized user from doing so [2]. Using Biometrics to Verify Identity. The user is spared from having to remember their login credentials when they utilize a biometric authentication method. The biometric method depends for authentication on an individual's innate biological traits. Some of the most widely used techniques in the market today include retina scanning, iris recognition, facial recognition, and fingerprint analysis. The novelty of certain biological traits is what makes using biometrics for authentication appealing. Due to these characteristics shared by all people and the difficulty of falsifying such data, it is possible to use it in an authentication system. Because of this, biometric authentication is the best way to safeguard sensitive data, particularly in sectors like national defense, finance, and healthcare where strict security standards are necessary. [2]

B. EEG-Based Biometric Authentication System:

We suggest developing a new authentication system as a way to address these two pressing problems. To address both problems, we propose to use the user's EEG reactions as an authenticator while they listen to certain musical selections. By including music into the authentication process, the first problem—that biometric authentication cannot be updated—is resolved. Since the user is listening to a selected song while the EEG data is being gathered, we may easily alter the song the user is listening to because the EEG signal response depends on the song the user is listening to. The first limitation is solved by updating the machine learning model by training it on updated data to reflect the user's changing musical preferences.[2]

III. RELEVENT WORKS

Researchers used music in an experiment to objectively evaluate the efficacy and validity of the suggested EEG-based method. They discovered really encouraging findings that back up their theory. The current work is built upon the inspiring findings from prior research.
Researchers used an EEG-based authentication method to classify individuals in an experiment they did in [9], recording 2620 individuals with a highest accuracy of 96.97%. Researchers developed an EEG-based person authentication system with music tailored for cloud environments in [10]. The gathered EEG data from the headset is first sent over Bluetooth to a mobile device, which subsequently uses a RESTful web service to send the data to a cloud server for storage.

A.EEG Considerations

Researchers used music in an experiment to objectively evaluate the efficacy and validity of the suggested EEG-based method. They discovered really encouraging findings that back up their theory. The current work is built upon the inspiring findings from prior research.
Researchers used an EEG-based authentication method to classify individuals in an experiment they did in [9], recording 2620 individuals with a highest accuracy of 96.97%. Researchers developed an EEG-based person authentication system with music tailored for cloud environments in [10]. The gathered EEG data from the headset is first sent over Bluetooth to a mobile device, which subsequently uses a RESTful web service to send the data to a cloud server for storage.

B.Machine Learning

Since each participant in this study has a unique model that is represented, trained, and optimized using an authentication method, the idea of machine learning is prominently incorporated into this study. We advise playing around with a variety of well-liked classification techniques for supervised machine learning.
The K-Nearest Neighbors (KNN), Artificial Neural Network (ANN), and Support Vector Machine (SVM) are three of the most often used techniques.
When it comes to categorizing individuals using EEG data, the KNN algorithm exhibits promise. Based on how close each new data point is to an existing data point in a recognized class, it classifies new data points. One of the algorithm's best features is how quickly the model is trained, even with a little data set. ANN are frequently utilized in classification jobs and are best suited for situations when a substantial quantity of data is provided. To train the model and assess its performance, the data is divided into three sets: training data, validation information, and testing data. Researchers showed in [20] that employing ANN as a person classification algorithm holds potential for creating a safe authentication system. Studies like this one show that employing neural networks to create an EEG-based authentication system is undoubtedly possible. An SVM algorithm works incredibly well for the classification tasks in guided machine learning, much like KNN and ANN do.
A patient-specific approach was used in research at Massachusetts Institute of Technology (MIT) to classify seizures.An SVM algorithm works incredibly well for tasks such as classification in supervised machine learning, much like KNN and ANN do.
A 96% identification rate was achieved in a Massachusetts Institute of Technology (MIT) study on seizure categorization utilizing an SVM algorithm and a patient-specific model [21]. The method deserves praise for its exceptional accuracy, since it may be effectively utilized for categorization in an authentication system that uses electroencephalography. In comparison to a multi-patient method, the patient-specific model produced fewer false-positives and faster detection times for seizure-related research at MIT. According to this research, a user-specific model for EEG categorization will produce an efficient system with high rates of authentication accuracy while also having fewer false positives.

IV. EXPERIMENTAL DETAILS

The process of gathering and evaluating data is essential to the research. One of the main objectives of an EEG-based biometric authentication system is to demonstrate that it is possible to identify a person with high confidence using only their EEG measurements while they are listening to a song they have picked for themselves.
In order to instruct the model and complete the assignment, information from both authorized and unauthorized users is gathered. Because each participant listens to their own music selection as well as the music of other participants, a significant amount of EEG data is gathered from each participant during the EEG data collecting process. Multiple sensors capture distinct values for various frequencies, including beta, gamma, and alpha, inside each EEG reading.

A. Proposed Approach Guidelines

In the experiment, there are two primary stages involved in developing an authentication system. According to Figure 1, there are two phases: user registration in the first phase and user authentication in the second.
The user's choice of music is restricted to two things: it can't be the same as that of any other study participant, and users and music cannot have any emotional connections. Additionally, no duplicates of the overall musical selection comprised of the tastes of all participants are allowed.
The guidelines for data collection are as follows: participants should wear loose, comfortable clothing, sit in a chair with their feet flat on the floor and rest their arms on their thighs.
All participants receive instructions on what to do and what not to do during data collection, in addition to the recommended actions.
These include covering one's scalp with a handkerchief or speaking or stuttering during the EEG comprehension, shifting or becoming distracted, and ingesting any substance—coffee, tea, alcohol, large doses of medication, opioids, etc.—that can influence neurological activity on the day of data collection.
One factor that would need more consideration by different study teams is the prohibition against the use of any substance. For example, in scientists asserted that there is no significant statistically effect of coffee on EEG activity based on an experiment. Consequently, allowing the consumption of tea and coffee may be appropriate.

ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁂ Peer-reviewed & Refereed journal ⁂ Vol. 12, Issue 5, May 2024

DOI: 10.17148/IJIREEICE.2024.12530

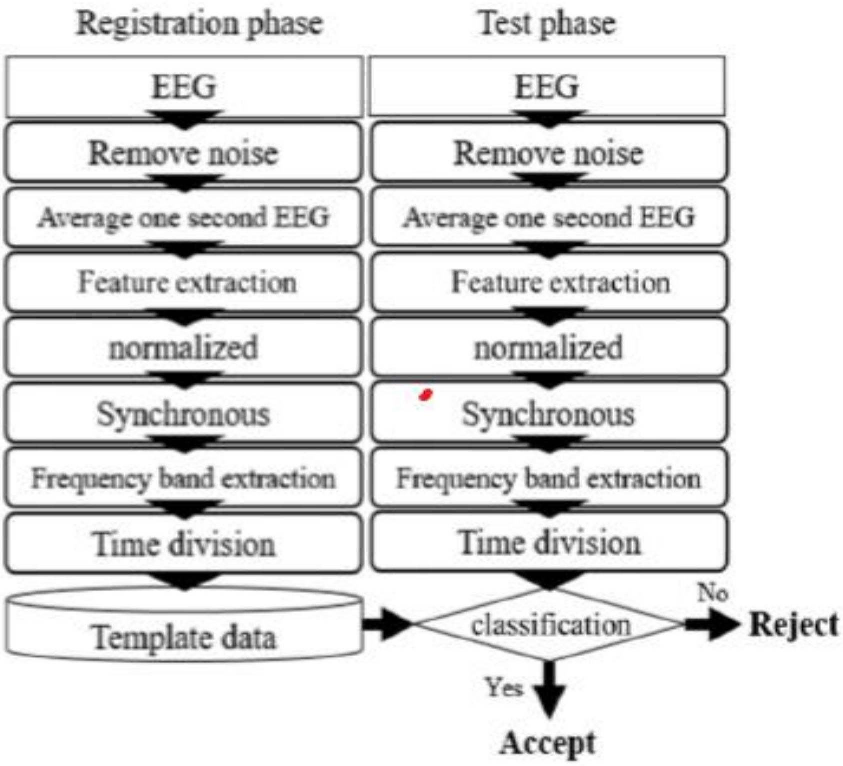


Fig.2. Flow of the verification procedure

B. **Selection Criterion**

A criterion for aqualification needs to be developed in order to choose study participants. Such a user qualification measure is required due to factors pertaining to EEG and advised procedures of beginning with a small group and gradually expanding to a broader community. Suggested criteria for selection as study participants at a university lab include being in overall good health, not having a family history of neurological disease, not being addicted to drugs, not covering one's head, being right-handed, being older than eighteen (18) years old, and being enrolled in university courses.

C. **Data Collection Protocol**

For the purpose of gathering experiment data, each participant will have their EEG readings taken independently twenty-four times. There are four trials for each participant. Every trial comprises six readings, with a thirty-second interval between each reading. The time from [0-] to [3-] seconds is trimmed, [3-] to [28] seconds is recorded, and (28–30] seconds is clipped for every reading. Consequently, 25 seconds are saved from a single EEG readout. In contrast, a negative reading 2622 suggests that the individual is listening to music that has been submitted by another participant. Every participant's negative readings are chosen at random from the whole catalogue of music selections. Every bad reading song selection made by a single participant must be distinct from self-selected music for that trial.It is allowed to select the same song twice in a row for negative readings from separate trials. When a participant is given a control music reading, they are subjected to a selection of music made specifically for the study and not from the individual's whole repertoire.

All participants hear the same, unfamiliar music that serves as the control. Lastly, a quiet reading is just an EEG reading that takes place without the subject listening to any kind of music. It is intended to serve as a reference, resting reading. In general, the ratio of negative to positive values is 80% to 20%. Each participant has a total for 16 negative readings, four positive readings, two silent readings, and two controlled song readings gathered. The duration of each reading is 25 seconds. Each participant is given the chance to ask questions of the researcher at the start of each experiment, instructed to prepare for the trial, and given a reminder of the guidelines. When the saline sensors have been cleaned and resaturated, the headset's battery level has reached 50%, and the researcher observes that the EEG amplitudes have clearly stabilised, the recording for each reading starts. The researcher and the participant are not aware of which person the music belongs to for each negative reading. Whenever possible, the idea of a double-blind trial is included. Every reading from each of the four trials' data is gathered in a single sitting.

D. Environmental Considerations

Environment specifications are developed and ought to be adhered to. The experiment's room is situated in a peaceful, noise-free area. Every object in the room is evaluated for requirement, retaining only those necessary for the experiment to be effective. The Wi-Fi access point, table, chair, CPU, monitor, keyboard, mouse, headphones, and any required cable cables are all in the room. Everything else has been temporarily moved. The participant is positioned six feet from the computer during the experiment, while the investigator is three to five feet in behind of the person. Reducing electromagnetic and auditory noise means minimizing devices and enacting stringent regulations. There are just two people in the room, and the environment is comfortably set at seventy degrees Fahrenheit.

There are just two people in the room, and the ambient temperature is comfortably set at seventy degrees Fahrenheit. Every data collection process is carried out between 8:00
In order to reduce the impact of any variable elements, the same day at AM and PM. Researchers go into great depth and offer a framework for creating an EEG laboratory in [24], which may be used as a guide for designing the experiment. The paper discusses how to build the necessary infrastructure, offers equipment considerations, and offers personnel and training requirements that are relevant for carrying out a successful experiment using the suggested methodology.

E. Instrument Details and Channel Selection

It's important to pick a device and certain sensors to use for the data collection. Using the Emotive EPOC X- 14 Channels Cordless EEG Headset is one recommendation. With all required sensors included, the device is easy to operate and produces great accuracy. The electrodes that serve as sensors on the apparatus consist of felt pads bathed in saline, devoid of any adhesive gels. The configuration for the electroencephalogram (EEG) signals should be 256 SPS sampling rate and 16 bits resolution at 1 LSB = 0.1275 µV. For data storage, the device is connected to a computer via Bluetooth in the 2.4GHz frequency.

The matching sensor location on the head for the 10-20 system instrument is shown in the lower half .

V. EEG SIGNAL PROCESSING

An EEG is a measurement of electrical activity in the brain. In order to record the voltage variations in µV, a device is applied to the scalp for this study.

A. Preprocessing and Feature Extraction

To undertake an analysis utilizing a Morlet transform, the collected EEG data needs to be transformed from a time series into a timed frequency series. You can use the MNE Python3 package to accomplish this. version [26] of 0.14.0. Each sensor generates a time series with an Alpha band and a Beta band. The frequencies between 8 and 13 hertz are known as the Alpha band, while the frequencies from 13 to 30 hertz are known as the Beta band. The process of creating feature vectors involves deducting baseline (quiet) measurements for every sensor from reaction (musical) readings. We excluded 12 dimensions due to their lack of need and the large response size across all participants. Each of the eight sensors produces two dimensions of Alpha and Beta band values, resulting in a sixteen-dimensional feature vector. Feature vectors are labeled as 0 or 1. The score is 0 if participants listened to music chosen by others, and 1 if they chose their own music. The Label 0 vector contains attacker samples as it simulates non-matching sound and a user attempting to access the system. Label 1 includes user samples, indicating an authorized user attempting to access the system with their own music selection.

Xdifference = |Xmusic response Xsilent response |

Feature extraction is extremely important and beneficial. Uniform Manifold Approximation and Projection (UMAP) is a new method for dimension reduction [4]. The algorithm can reduce vectors of features of any number of dimensions, preserving and representing the most important data from excluded dimensions. Deep learning classification uses automatic feature extraction during training.

B. Classification

Create a user-specific machine learning model after selecting an algorithm. Scikit-learn Python3 module version 0.21.3 allows for quick implementation [28].

Classification involves creating a unique algorithm system for each user. The training set for authorized users includes

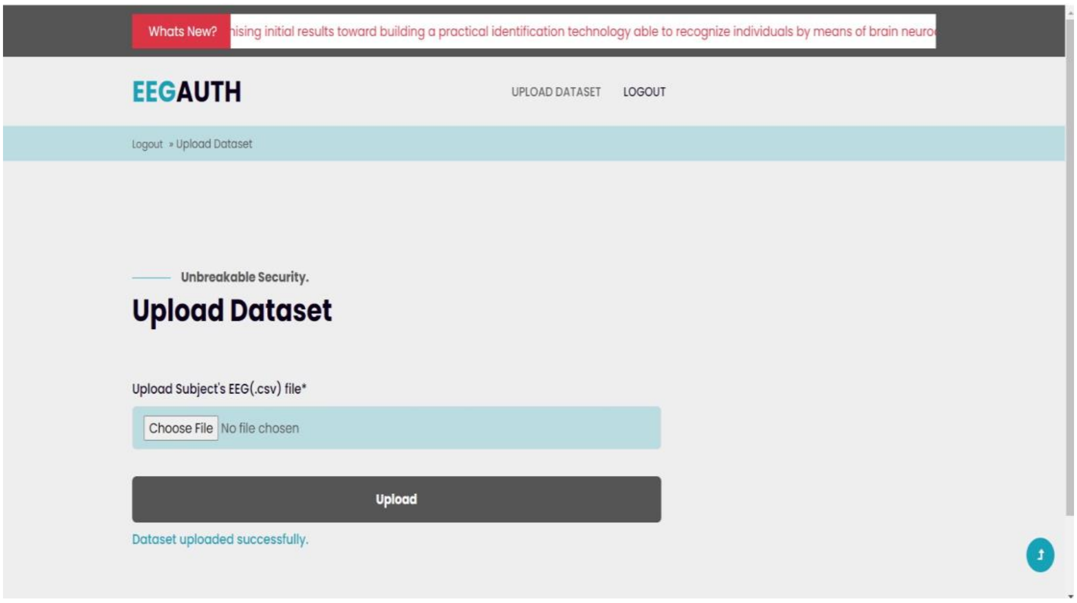
DOI: 10.17148/IJIREEICE.2024.12530

80% of the total samples, while the remaining 20% is reserved for testing. An equal number of attacker samples are chosen at random from the larger set. The percentage of training data varies by algorithm.

VI. RESULT ANALISYS

There are N machine learning models with N accuracies, one for each participant. The classification precision is accessible for each participant.

Model in percentages ranging from 0 to 100. Higher accuracy leads to better classification performance. If model's accuracy is considered not high enough, alternatives categorization algorithms can be used and tested. Using a different directed machine learning algorithm could enhance model classification accuracy. To better understand complex data, it's recommended to visualize it across multiple dimensions. We recommend using UMAP or a similar algorithm to visualize data graphs**.**


Whats New? ising initial results toward building a practical identification technology able to recognize individuals by means of brain neuro

Unbreakable Security.

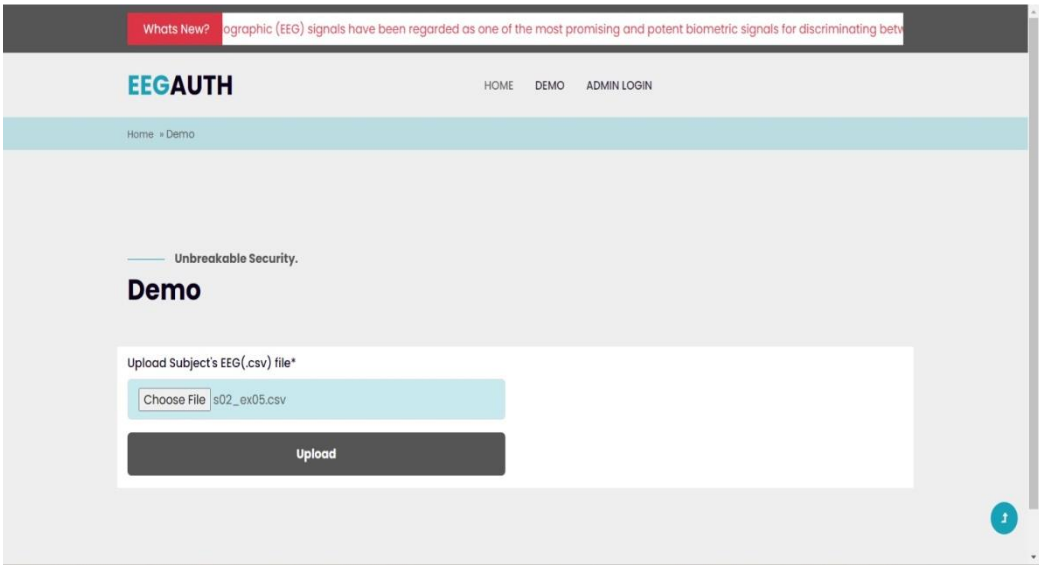
Upload Dataset

Upload Subject's EEG(.csv) file*

Choose File No file chosen

Dataset uploaded successfully.

Fig 3. In the demo page the random subjects will try to login/authenticate the system.


Whats New? ographic (EEG) signals have been regarded as one of the most promising and potent biometric signals for discriminating betw

Unbreakable Security.

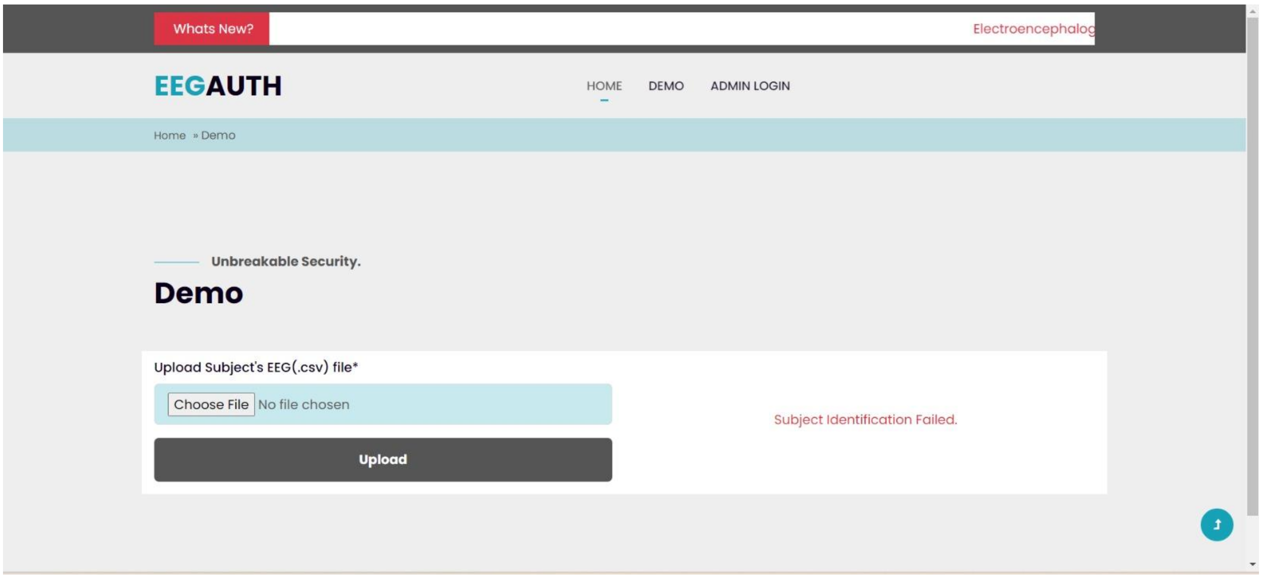
Demo

Upload Subject's EEG(.csv) file*

Choose File s02_ex05.csv

Fig 4.The system will compare the testers data with the subjects data enrolled in the system. If the data is matched with the verified enrolled subject then it gives access with a message "welcome $<subject>$", as shown in the above figure.

DOI: 10.17148/IJIREEICE.2024.12530



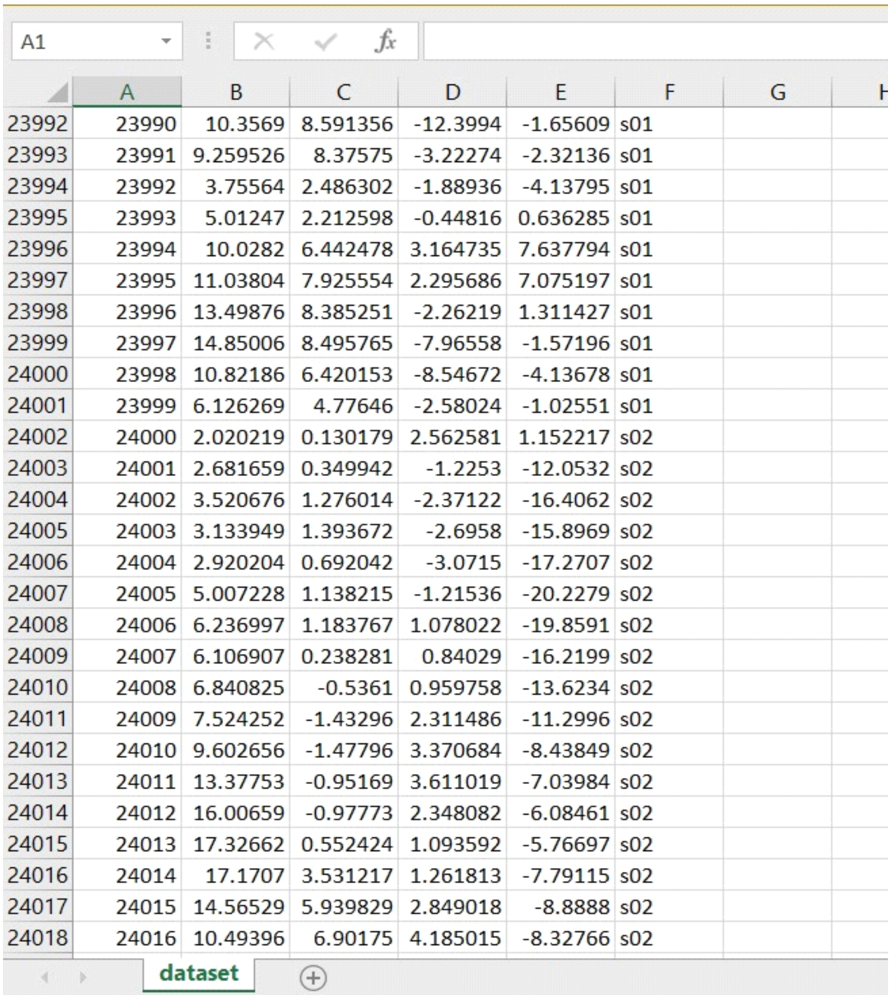
Unbreakable Security.

Demo

Upload Subject's EEG(.csv) file*

Subject Identification Failed.

Fig 6.If the testers data is not matched with the enrolled data the system will not give access to the tester and will show a message " User Identification failed".



	A	B	C	D	E	F	G	H
23992	23990	10.3569	8.591356	-12.3994	-1.65609	s01		
23993	23991	9.259526	8.37575	-3.22274	-2.32136	s01		
23994	23992	3.75564	2.486302	-1.88936	-4.13795	s01		
23995	23993	5.01247	2.212598	-0.44816	0.636285	s01		
23996	23994	10.0282	6.442478	3.164735	7.637794	s01		
23997	23995	11.03804	7.925554	2.295686	7.075197	s01		
23998	23996	13.49876	8.385251	-2.26219	1.311427	s01		
23999	23997	14.85006	8.495765	-7.96558	-1.57196	s01		
24000	23998	10.82186	6.420153	-8.54672	-4.13678	s01		
24001	23999	6.126269	4.77646	-2.58024	-1.02551	s01		
24002	24000	2.020219	0.130179	2.562581	1.152217	s02		
24003	24001	2.681659	0.349942	-1.2253	-12.0532	s02		
24004	24002	3.520676	1.276014	-2.37122	-16.4062	s02		
24005	24003	3.133949	1.393672	-2.6958	-15.8969	s02		
24006	24004	2.920204	0.692042	-3.0715	-17.2707	s02		
24007	24005	5.007228	1.138215	-1.21536	-20.2279	s02		
24008	24006	6.236997	1.183767	1.078022	-19.8591	s02		
24009	24007	6.106907	0.238281	0.84029	-16.2199	s02		
24010	24008	6.840825	-0.5361	0.959758	-13.6234	s02		
24011	24009	7.524252	-1.43296	2.311486	-11.2996	s02		
24012	24010	9.602656	-1.47796	3.370684	-8.43849	s02		
24013	24011	13.37753	-0.95169	3.611019	-7.03984	s02		
24014	24012	16.00659	-0.97773	2.348082	-6.08461	s02		
24015	24013	17.32662	0.552424	1.093592	-5.76697	s02		
24016	24014	17.1707	3.531217	1.261813	-7.79115	s02		
24017	24015	14.56529	5.939829	2.849018	-8.8888	s02		
24018	24016	10.49396	6.90175	4.185015	-8.32766	s02		

Fig 7.We created datasets for datasets of 25 subjects.

VII. CONCLUSION

Our foundation lays the groundwork for a new authentication system that addresses the shortcomings of current biometric approaches. The current authentication system can Additionally, a traditional authentication mechanism can be used as a second factor. The new approach offers numerous applications and usage possibilities, with the only drawback being the initial set up and cost. A detailed recommendations is provided for creating and carrying out an experiment to validate an EEG-based authentication system. Experiment design, participant selection, gathering data protocol, sensor selection, model examination, data visualization, and other relevant information are presented to ensure a successful outcome.
Deep learning model for person recognition using SSVEP signal analysis and a convolutional neural network, comprising two scenarios that are person verification and identification. To illustrate the benefit of deep learning, we also looked into two other criteria: (1) utilizing traditional classifiers on obtained power spectral features; and (2) applying a CCA-based spatial filter to SSVEP signals prior to feature extraction. We assessed the approaches' performance using accuracy, FAR, and TAR (for verification only). The results demonstrated that, in terms of robustness and recognition performance, the suggested deep learning model using convolutional neural network technology significantly outperformed the traditional techniques, suggesting that it was capable of automatically learning discriminative illustrations from raw SSVEP signals

VIII. REFERENCES

[1] S. Bak and J. Jeong, "User Biometric Identification Methodology via EEG-Based Motor Imagery Signals," in IEEE Access, vol. 11, pp. 41303-41314, 2023, doi: 10.1109/ACCESS.2023.3268551.
keywords: {Feature extraction;Electroencephalography;Support vector machines;Biometrics (access control);Task analysis;Reliability;Electrodes;Biometric;electroencephalography (EEG);motor imagery (MI);support vector machine (SVM);user identification methodology;Gaussian Naïve Bayes (GNB)},

[2] A. Rahman et al., "Multimodal EEG and Keystroke Dynamics Based Biometric System Using Machine Learning Algorithms," in IEEE Access, vol. 9, pp. 94625-94643, 2021, doi: 10.1109/ACCESS.2021.3092840.
keywords: {Electroencephalography;Authentication;Biometrics (access control);Feature extraction;Machine learning;Headphones;Brain modeling;Biometric system;electroencephalography (EEG);keystroke dynamics;identification;authentication;multimodal system;machine learning},

[3] K. P. Thomas and A. P. Vinod, "Toward EEG-Based Biometric Systems: The Great Potential of Brain-Wave-Based Biometrics," in IEEE Systems, Man, and Cybernetics Magazine, vol. 3, no. 4, pp. 6-15, Oct. 2017, doi: 10.1109/MSMC.2017.2703651.
keywords: {Electroencephalography;Feature extraction;Authentication;Behavioral sciences;Fingerprint recognition;Brain modeling;Biometrics (access control)},

[4] K. Elissa, “Title of paper if known,” unpublished.

[5] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.