International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(20s) 2026 pp. 103-126
https://doi.org/10.70917/ijcisim-2026-5158
Article

NEUROAUTH-GNN: EEG-BASED EYE-BLINK CAPTCHA AUTHENTICATION USING ATTENTION-GUIDED GRAPH NEURAL NETWORKS AND ADAPTIVE NEURO-SVM

S. Nooriya begam[1], * R. M. Vidhyavathi[2]

[1]Research Scholar, Department of Computer Science, Alagappa University, Karaikudi, Tamil Nadu, India
Co – Author Mail ID: nooriyabegam25@gmail.com
[*2]Assistant Professor, Department of Bioinformatics, Alagappa University, Karaikudi, Tamil Nadu, India.
[1*]Corresponding Author email: vidhyavathirm@alagappauniversity.ac.in

Abstract: Brain-Computer Interface (BCI) based authentication techniques have become a promising option for various secure healthcare devices, smart assistive technologies, cognitive security, human-machine interaction, etc. Because of their adaptive and user-specific authentication capabilities. Among them, EEG-based eye-blink authentication achieves hands-free and effortless user verification. For physically disabled persons, EEG-based eye-blink authentication is more helpful. Conventional EEG authentication algorithms mostly rely on removing noise and artifact, weak spatial-temporal features extraction and poor classification accuracy when there are nonlinear EEG signal distributions. Traditional machine learning classifiers are difficult to differentiate overlapping blink patterns due to highly dynamic and complex EEG signals. In this paper, we develop an EEG-based eye-blink CAPTCHA authentication scheme, namely NeuroAuth-GNN, using Attention-Guided Graph Neural Networks (GNN) and Adaptive Neuro-SVM (AN-SVM). This scheme acquires EEG signals during directional eye blinks (e.g., left, right, up, down) by a non-invasive BCI headset. After bandpass filtering and normalization on the collected EEG signals, a discriminative spatial-temporal EEG representation is extracted using an attention-guided GNN, which models the relationship between electrode connectivity and neural activity. Extracted features are classified by AN-SVM with adaptive margin and weights. Experimental results achieved better performance with higher authentication accuracy, robustness and attack resilience in contrast to prior methods and are suitable for next-generation cognitive authentication applications.
Keywords: EEG signal processing, Eye-blink CAPTCHA, Graph Neural Networks, Cognitive authentication, Human-computer interaction

1. INTRODUCTION

A rapidly evolving field, BCI has been a significant research area in intelligent health, cybersecurity, assistance and human-computer interface systems owing to its ability to directly communicate between the human brain and devices [1][2]. Out of various BCI methods, the EEG-based systems have been popular among users as they collect brainwave signals from the body without any invasive processes and at relatively less cost [3]. Since the EEG signals produced during eye-blink activity are unique and used for CAPTCHA authentication and user identification [4][5]. Hence, an EEG-based eye-blink authentication system are useful for people with disabilities [6].

Recent research in EEG-based authentication has considered various classification techniques, such as Machine Learning (ML) and Deep Learning (DL) models [7][8]. Mostly, the proposed systems were about detecting blinks from the EEG signal, classification of the signals and using handcrafted or shallow feature extraction to achieve authentication [9][10]. Recently, the emergence of GNN has been of great interest to model the spatial and temporal relationship of electrodes, and the previously introduced EEG-based authentication has shown very promising performance for eye-blink recognition and enhancement of human-computer interaction for disabled people [11][12].

However, traditional EEG-based authentication systems have several problems, such as sensitivity to noise and artefacts, limited spatiotemporal feature extraction, and poor classification performance when the EEG signal distribution is nonlinear [13]. It is also difficult for conventional classifiers to distinguish overlapping blink patterns due to fluctuations in brainwaves [14][15]. To overcome this, the research proposes NeuroAuth-GNN, which models relationships among electrodes. The method efficiently extracts discriminative EEG features, making authentication much more robust, accurate, and secure, and it will be part of future cognitive authentication. The contributions of the research are given below:

- The research proposes an EEG-based eye-blink CAPTCHA authentication system called the NeuroAuth-GNN by combining Attention-Guided GNN and Adaptive Neuro-SVM.
- Attention-Guided GNN effectively captures spatial-temporal EEG relations to enhance EEG blink-pattern feature extraction and representation learning.
- The proposed Adaptive Neuro-SVM effectively boosts the non-linear EEG classification accuracy with adaptive optimization and weighted learning.

The research is organized as follows: Section 2 provides the literature review, Section 3 describes the proposed methodology, Section 4 contains the results and discussion and Section 5 concludes the research.

2. LITERATURE REVIEW

In 2023, Gorur et al [16] suggested a Fourier Synchrosqueezing Transform (FSST)-Independent Component Analysis (ICA)-Empirical Mode Decomposition (EMD) scheme for EOG-based biometric authentication using forced voluntary blink. This approach integrates advanced signal processing techniques to increase feature extraction accuracy, mixed biosignal separation and clean EOG component separation, to be classified via a deep RNN. The main advantages are the increased robustness, reliability and continuous authentication for security purposes. The disadvantages were the increased computational complexity, and validation on a small number of subjects limited the generalizability.

In 2024, Alyan et al. [17] presented the pcEEG+ framework, a synchronization-based fusion method for EEG principal components and eye blink signal (syncBlink) for decoding locomotion. The framework emphasizes on strict synchronization of neuronal activity with ocular behavior for better feature fusion and classification accuracy. The major benefit is more accurate and robust decoding over a variety of movements, which was demonstrated on different datasets. But a major limitation is that precise synchronization between the EEG and eye blink signal is not easy, and thus, this is a potential issue for real-time applications.

In 2025, Criscuolo et al. [18] suggested an approach for semi-automated detection and elimination of eye blink artifacts in EEG signals using a CVAE model. The CVAE learn representations of the EEG in a latent space, where distinctive blink components are located and manipulated to remove the artifacts while retaining the neuronal signals. Its advantage lies in its ability to perform automatic blink removal without manual supervision to improve the EEG signal. Its limitation is mainly in offline applications, which would be hindered due to the potential latency of a real-time application.

In 2025, Chae et al. [19] suggested a new framework based on multi-modality EEG for authentication within an XR setup by integrating eye-blink signals and SSVEP responses. Their goal was to create an authentication system that provides highly accurate as well as user-friendly biometric verification within the XR space. A new grow-shrink visual stimulus was implemented to enhance usability by lowering the ocular fatigue without decreasing signal quality, followed by SHAP-based feature selection and machine learning algorithms. Their proposed framework benefits from highly accurate and interpretable authentication in real-time XR authentication with minimal user effort. On the downside, the system requires multi-channel EEG and precise control over the stimulus settings, hence its applicability for unrestricted real-world settings might be limited.

In 2024, Khalil et al. [20] proposed an EEG-based user authentication system that utilize MLP FFNN based on P300 potentials. Feature extraction from EEG was done based on mutual information and power spectral density in different frequency bands, and then a two- stage procedure of user identification and authentication was carried out. The primary benefit of this method was performing classification and verification with both efficiency and ease of supporting new users enrolling without re-training, but this method relies on the control P300 stimulus paradigms, and it may fail in scalability and spontaneous usage circumstances.

In 2023, Alyan et al. [21] presented a new method for decoding eye blinks and associated EEG responses in real work environments using multivariate pattern analysis. This study looked at blink-related EEG responses recorded while participants were performing simulated driving and machinery operation tasks in order to distinguish between mental workload and neural dynamics particular to the task being performed. The advantage of this study is that it attempts to decode mental workload in naturalistic environments by pairing blink information and EEG signals in order to further predict workload and optimize the human-machine interface. The performance of the decoder was not uniform across conditions and suggests issues with predicting brain states with consistent accuracy across alertness levels and environmental complexity.

In 2025, Rehman et al. [22] presents a deep learning-based multi-modal data fusion framework for EEG-based biometrics. The solution uses different EEG frequencies of brain activity tasks and a fusion of such to enhance the robustness and adaptability of biometrics systems. Evaluation for cross-task generalization of learning on one task and testing on different tasks leads to a more effective solution to handle heterogeneous EEG data. The main contribution is a significant improvement in the identification rate and a more adaptable solution by applying intelligent data fusion and deep learning methods. However, its performance may be strongly determined by the variety of tasks, massive EEG datasets and computationally expensive deep learning models.

In 2024, Dragu et al. [23] proposed an EEG-based cryptographic authentication technique that identifies the use of the brain-wave characteristics as biometric features, for the authentication of users, ensuring security. The proposed architecture employs statistical signal processing techniques for the extraction of required EEG features for cryptographic use. The prime benefit of this system is the usage of the unique characteristics of brain waves, enabling higher security, non-duplicability and reusability for the Brain-Computer Interface systems. Still, it is at the research stage and may require a solution for variations in the EEG signal, the sensitivity to the noise and usage in the authentication system.

In 2023, Alsumari et al. [24] introduced an EEG-based person authentication and identification framework that employs a shallow CNN. The system uses EEG signals with only two channels and a short temporal window for secured biometric recognition with fewer calculation overhead and avoiding the deep CNN learning process overfitting. The greatest advantage of the system is the design is highly efficient and practical for a biometric real system with few constraints on EEG acquisition. Despite its efficiency and practicality, the variance and influence of recording conditions affect its authentication stability.

In 2022, Stergiadis et al. [25] developed an individualized ML based EEG user authentication system based on features derived from power spectral EEG values over 3 channels. It involves finding an optimal classification algorithm for individual users to enhance the robustness and flexibility of the system. Its core advantages include adaptive, speedy and individualized training mechanisms, making it useful for continuous, real-time authentication purposes. The major drawback of this system includes individualized model adaptation and restriction of only 3-channel EEG features, limiting the system's ability to work efficiently in a variety of real-world scenarios.

2.1 Problem Statement

Traditional authentication schemes are prone to security threats, and it is not easy for physically handicapped users to use it. Though EEG-based eye-blink authentication provides a prospective security system, current methods are characterized by noisy EEG signals, lack of effective extraction of spatio-temporal features, and poor classification performance in distinguishing complex and overlapping blink features. Thus, there is a demand for a secure and reliable EEG-based authentication framework that is able to accurately model neuronal interactions and efficiently discriminate directed eye-blink features in CAPTCHA-based user authentication.

3. PROPOSED METHODOLOGY

The NeuroAuth-GNN framework proposed aims to be an end-to-end authentication system based on an EEG eye-blink CAPTCHA, by correctly modeling the intricacies of neural information arising from blink directions. Instead of using handcrafted features or traditional machine learning techniques to construct a traditional authentication framework, the proposed system makes use of graph based deep learning and adaptive classification techniques in order to efficiently model spatial-temporal dependencies of the EEG signals among the different channels. Firstly, raw EEG signals collected from a non-invasive BCI headset pre-processed to get rid of artifacts, noise while keeping the blink neural data. The pre-processed EEG signals then represented as graphs, with the channels being represented as nodes connected based on their connectivity. Then, a Multi-Scale Attention-Guided Graph Neural Network would be employed to extract the features associated with blinking-related events from local and global EEG spatial-temporal patterns. Finally, an AN-SVM classifier is adopted to classify the EEG features. The Adaptive Neuro-SVM classifier is an improvement over standard SVM due to its adaptive margin update and active sample weighing mechanism. Blink sequences classified based on EEG signals is used for the CAPTCHA-based authentication and thus make it the first hands-free, intuitive and secure access control method to be used for next-generation cognitive authentication. Figure 1 shows the overall architecture of the proposed model.

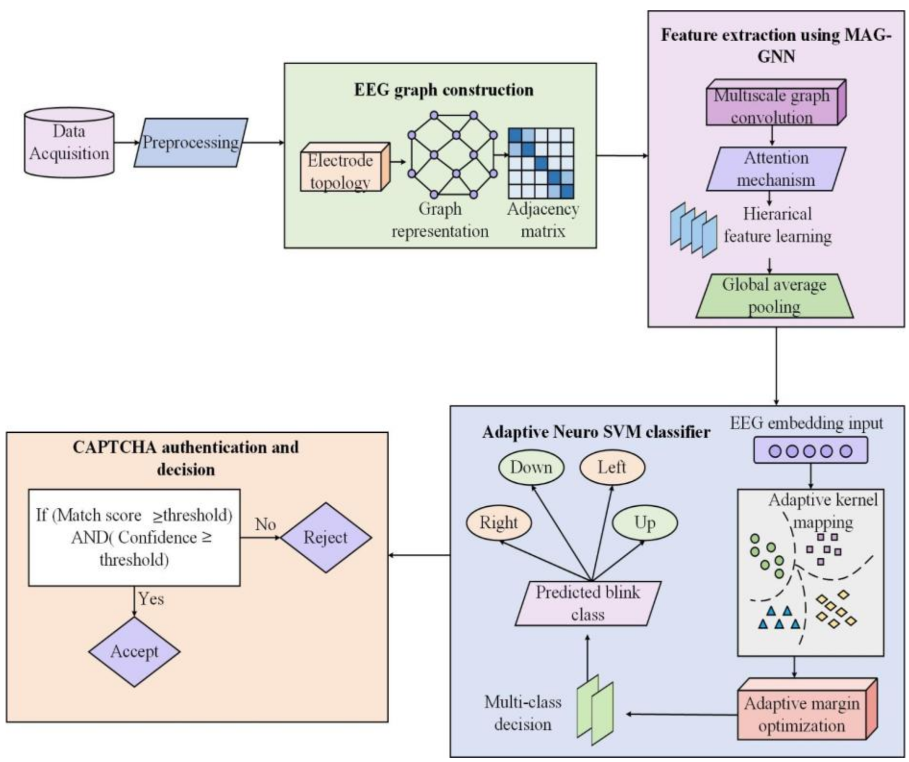


Figure 1: Overall architecture of the proposed methodology

Figure 2 depicts the general flowchart of this methodology, which gives a clear picture of the step-by-step process and the computational framework.

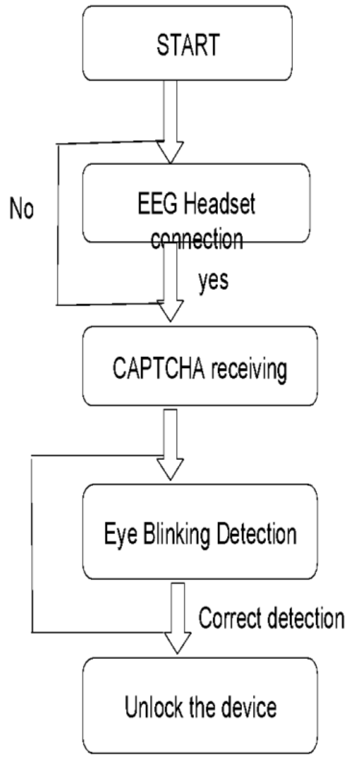
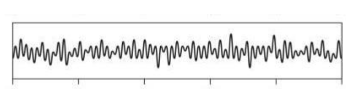
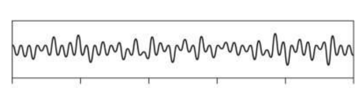


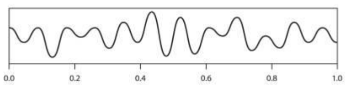
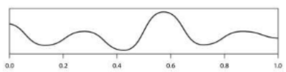
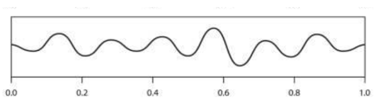
Figure 2: flow chart of the Eye Blinking Detection method.

3.1 Data Acquisition

The first phase of the proposed EEG-based authentication system is the data acquisition. A non-invasive BCI headset, which is a set of electrodes on the head of the individual making the eye-blinking gestures, records the electrical activity of the brain. EEG is a recording of the brain activity using electrodes on the scalp, which records electrical signals created by the brain. EEG is an important instrument in the investigation of the processes within the brain because it possesses high temporal resolution, measures the neural activity directly, is cheap, portable, and has the capability of recording the cognitive processes without the participant responding to the questions. The brainwaves are of five different frequencies: Gamma, Beta, Alpha, Theta and Delta, which are the different states of brain activity and consciousness expressed in cycles per second (Hz). It is mentioned in Table 1.

Table 1: Brainwave, Frequency and Mental State

Brainwave	**Frequency**	**Mental state**
Gamma: Above 40 Hz		Critical thinking, Thought patterns
Beta: 13 – 40 Hz		Concentration, Focus, Problem-solving

Alpha: 8 – 12 Hz		Calmness, Closed eyes, Decreased cortical activity, Increased creativity
Theta: 4 – 7 Hz		Deep relaxation, Meditation, Increased creativity, Intuition, Dream-like states Enhanced memory recall
Delta: 0.1 – 4 Hz		Deep sleep, Restoration, Healing, Trance-like states.

An EEG headset is used to identify eye movement and to make the recording of the movement of eye blink. It is processed as the main feature of EEG Signal detection with a collection of information that provides clear info about signal movement. Human Brain signal movement collected with the spectra. Figure 3 illustrates the device of the EEG Headset and lobe expansion in the EEG Electrode.

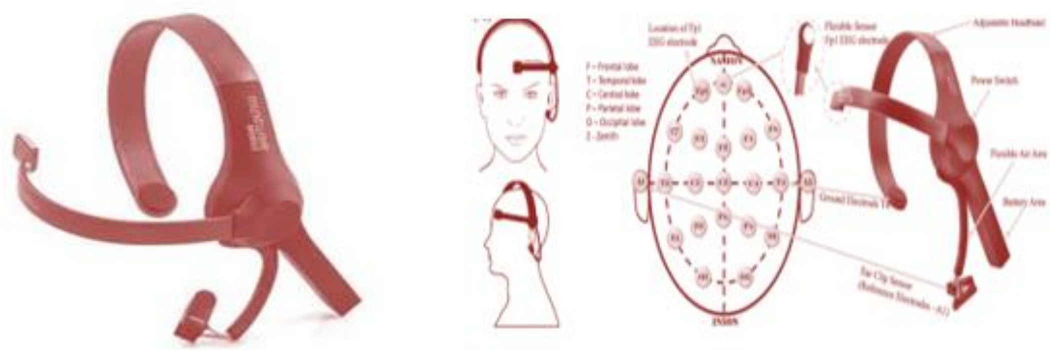


Figure 3: The device of the EEG Headset and lobe expansion in the EEG Electrode.

EEG Signal used to detect eye-blink artifacts. It is used for the movement of devices, robotics and unlocking the apps or devices. Here, in this paper, eye blinking detection is for the security purpose to unlock the device using a CAPTCHA image. Figure 4 shows the CAPTCHA number image used to unlock the device, and how to enter the CAPTCHA number with the help of eye movement is illustrated in Figure 5.

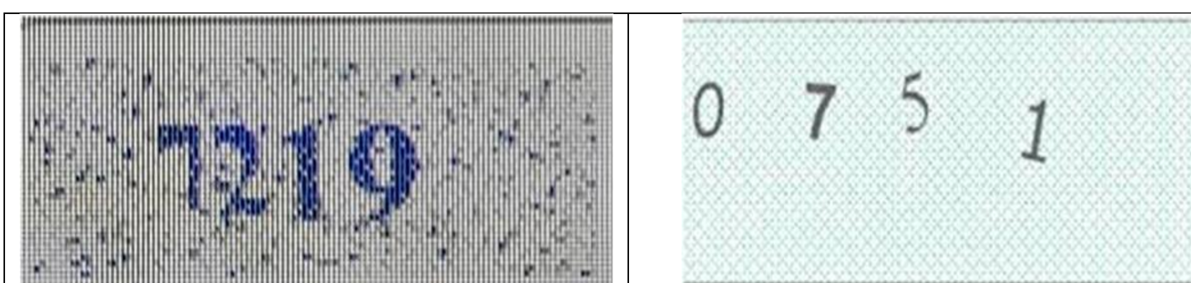


Figure 4: The image represents the CAPTCHA number image used to unlock the device

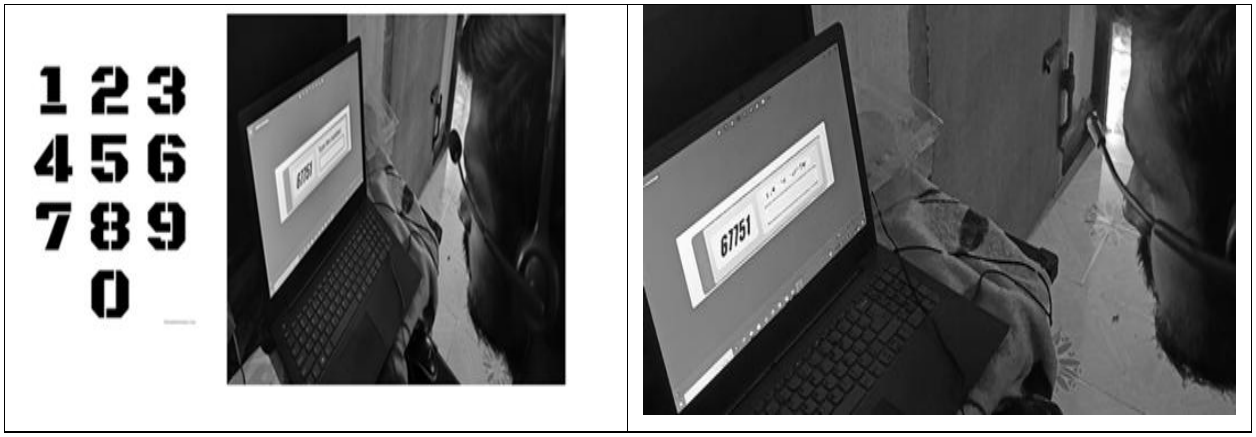


Figure 5: This Figure illustrates how to enter the captcha number with the help of eye movement

3.2 Preprocessing

EEG signals are often contaminated by noise and artefacts resulting from muscle movements (EMG), eye movements, or environmental disturbances. Thus, the purpose of this step is to clean and stabilise the data to ensure that only the brain activity connected with a blink remains for analysis.

3.2.1Bandpass Filtering

The bandpass filter is used to isolate significant EEG frequency bands and the band is chosen to be 0.5-40 Hz to retain the signal in the range of major cognitive and ocular activity bands (delta, theta, alpha, and beta). Mathematically, the filtered signal is written as using Eq. (1)

$$x_f(t) = x(t) * h(t) \tag{1}$$

Where $x(t)$ is the raw EEG signal, $h(t)$ denotes the impulse response. In the frequency domain, this is represented as in Eq. (2): where, $x(\omega)$ shows the Fourier transform of the EEG signal, $H(\omega)$ keeps the response from the frequency.

$$x_h(\omega) = x(\omega) \cdot H(\omega) \tag{2}$$

3.2.2 Normalization

Normalization follows filtering and provides all EEG channels with a uniform scale, which enhances the convergence and stability of the learning algorithms that follow. Min–max scaling is used to obtain the normalized signal of each channel. This is expressed in Eq. (3)

$$x_n(t) = \frac{x_f(t) - min(x_f)}{max(x_f) - min(x_f)} \tag{3}$$

Where $x_f(t)$ denotes the filtered EEG signal, $min(x_f)$ provides the minimum amplitude and $max(x_f)$ provides the maximum amplitude.

3.2.3 Artifact Removal

ICA eliminates artifacts that are not related to cognitive or blink activity. The EEG signal X that is observed is modeled as a linear sum of statistically independent source signals S. This is formulated using Eq. (4). The goal of ICA is to estimate the unmixing matrix Wsuch that it is expressed in Eq. (5)

$$X = AS \tag{4}$$

$$S = WX \tag{5}$$

These combined preprocessing operations enable the acquisition of clean and stable EEG signals, which give an ideal basis for the feature extraction using the proposed architecture.

3.3 EEG Graph Construction

The preprocessed EEG signals are converted into a graph-structured representation so as to efficiently capture the spatial and functional connections among the EEG electrodes during the eye blinks. Neural interactions inherently exist between multiple regions in scalp EEG signals, and the traditional feature extraction techniques are not capable of effectively encoding these dependencies, as they treat each channel in the EEG independently. Thus, NeuroAuth-GNN takes EEG channels as graph nodes, while their connections are viewed as graph edges in the framework to properly formulate the spatial-temporal neural dynamics in the direction-wise eye blinks.

The EEG graph is given by $G = (V, E)$ where V represents the set of EEG electrodes and E represents the connections between electrodes. An EEG electrode channel is associated with a vertex as given in Eq. (6), where $n$denotes the total number of EEG channels.

$$V = \{v_1, v_2, v_3, \ldots, v_n\} \qquad (6)$$

Both spatial electrode distance and the correlation of functional EEGs were utilized to retain both local and global interaction patterns. The edge set is given in Eq. (7).

$$E = \{(v_i, v_j) \mid v_i, v_j \in V\} \qquad (7)$$

The connectivity relations of the EEG electrodes are shown by a weighted adjacency matrix A. This is shown in Eq. (8), where w_{ij}denotes the connectivity weight between electrodes $i$and j.

$$A_{ij} = \{w_{ij}, if\ electrodes\ i\ and\ j\ are\ connected\ 0, otherwise \qquad (8)$$

The edge weights are computed using correlation-based EEG similarity as given in Eq. (9), where $Cov(X_i, X_j)$ represents covariance between EEG channels $X_i$and X_j, while $\sigma_{X_i}$and σ_{X_j}denote their standard deviations.

$$w_{ij} = \frac{Cov(X_i, X_j)}{\sigma_{X_i}\sigma_{X_j}} \qquad (9)$$

This weighted graph structure keeps the neural interaction strengths between different scalp regions and enhances the representation learning from EEG.

Every graph node stores the temporal EEG signal from its corresponding electrode channel. The representation of node features is denoted in Eq. (10), where $X_i$denotes the temporal EEG feature vector associated with electrode i, and Trepresents the temporal sampling duration.

$$X_i = [x_i^1, x_i^2, x_i^3, \ldots, x_i^T] \qquad (10)$$

where $X_i$denotes the temporal EEG feature vector associated with electrode i, and Trepresents the temporal sampling duration. For stable learning of graphs and feature consistency, the node features are normalized as shown in Eq. (11), where $\mu_i$and $\sigma_i$represent the mean and standard deviation of the EEG channel.

$$X_i^{norm} = \frac{X_i - \mu_i}{\sigma_i} \qquad (11)$$

The degree matrix Dcorresponding to the EEG graph is computed using Eq. (12). The normalized graph Laplacian used for graph propagation is represented using Eq. (13), where Idenotes the identity matrix.

$$D_{ii} = \sum_j \quad A_{ij} \qquad (12)$$

$$L = I - D^{-\frac{1}{2}} A D^{-\frac{1}{2}} \quad (13)$$

The constructed EEG graph keeps both local electrode connections and global neural connections, and is capable of spatial-temporal learning in the upcoming Attention-Guided GNN feature extraction step. The proposed graph-based EEG representation helps to improve the capacity of the framework for sensing small differences in neural activity during eye blinks with different directions (up, down, left, right) for blink authentication.

3.4 Feature Extraction Using Multi-Scale Attention-Guided Graph Neural Network

The proposed NeuroAuth-GNN, after constructing the graph representation of the EEG graph use a Multi-Scale Attention-Guided GNN (MAG-GNN) to learn discriminative spatio-temporal EEG embeddings for directional eye-blink authentication. The non-linear correlations and channel dependencies inherent in EEG signals are non-trivial, and simple methods that analyze individual channels can't fully extract the connectivity information in the brain. Multi-Scale Attention-Guided GNN takes advantage of multi-scale graph convolution combined with adaptive attention to model local electrode interactions and long-range brain-wide interdependencies together. Unlike traditional static GNNs, it dynamically focuses on blink-associated regions of the EEG signal, while also effectively capturing both local and long-range dependencies at different time scales and retaining fine-grained variations of the EEG signal even in the presence of noise.

Firstly, normalize EEG graph node representations, then push them through graph convolution layers to accumulate neighbor information. The graph convolution operation is defined using Eq. (14), where $H^{(l)}$denotes node embeddings at layer l, Arepresents the weighted adjacency matrix, Ddenotes the degree matrix, and $W^{(l)}$indicates trainable graph weights.

$$H^{(1)} = \sigma\left(D^{-\frac{1}{2}} A D^{-\frac{1}{2}} H^{(l)} W^{(l)}\right) \quad (14)$$

The initial EEG node representation is defined in Eq. (15), where Xdenotes the normalized EEG feature matrix. The nonlinear activation operation used during graph propagation is expressed in Eq. (16)

$$H^{(0)} = X \quad (15)$$

$$\sigma(x) = max(0, x) \quad (16)$$

In order to enhance the feature discrimination power of this framework, a dynamic self-attention is employed. This adaptive self-attention method selectively attends to more informative EEG electrodes involved in blink-induced neural responses than standard fixed attention methods that assign a certain level of importance to electrodes. Electrode significance weights could be adaptively learned by considering the neighborhood neural activity responses, blink pattern changing and so on. The attention score between neighbor EEG nodes are expressed in Eq. (17).

$$e_{ij} = LeakyReLU\left(a^T [WX_i \parallel WX_j]\right) \quad (17)$$

where $a$denotes the trainable attention vector and $\parallel$represents feature concatenation. The attention coefficients are normalized with the softmax operation as shown in Eq. (18).

$$\alpha_{ij} = \frac{exp(e_{ij})}{\sum_{k \in N_i} \quad exp(e_{ik})} \quad (18)$$

The adaptive attention-guided feature aggregation process is represented using Eq. (19).

$$H_i' = \sigma\left(\sum_{j \in N_i} \quad \alpha_{ij} W X_j\right) \quad (19)$$

In order to learn spatial-temporal EEG representations more effectively, the designed framework leverages multiple receptive fields in multi-scale graph propagation to learn the local neural activations and remote EEG correlations among different regions at the same time. Multi-scale graph aggregation is formulated using Eq. (20), where K denotes the number of graph propagation scales, A^k represents the k^{th}-order adjacency relationship, and β_k denotes adaptive scale importance weights.

$$H_{multi} = \sum_{k=1}^{K} \beta_k A^k X W_k \tag{20}$$

This multi-scale learning ability greatly enhances the capacity of this framework in detecting fine blink-induced neural differences between different regions of the scalp.

An additional residual feature enhancement mechanism is implemented to retain low-level EEG information after deep graph propagation. The residual learning is formulated using Eq. (21), where $MLP(.)$ denotes nonlinear multilayer feature transformation. This residual propagation stabilizes the gradients and preserves the discriminative information associated with blinks when performing a hierarchical graph learning on the EEG signal.

$$Z^{(1)} = H^{(l)} + MLP(H^{(l)}) \tag{21}$$

Finally, the global attention pooling is used to produce a compact high-level EEG embedding for classification as shown in Eq. (22), where γ_i denotes adaptive pooling weights assigned to EEG nodes and N represents the total number of EEG electrodes.

$$Z = \sum_{i=1}^{N} \gamma_i H_i' \tag{22}$$

The generated embeddings maintain significant spatially-temporal discriminating blink-associated neural information and increase the separability between the directions of blink pattern (i.e., up, down, left and right directions). The obtained high-level EEG representations are then passed through the proposed AN-SVM classifier for secure EEG-based CAPTCHA authentication.

3.5 Classification Using AN-SVM

Once spatio-temporal EEG embeddings are obtained via Multi-Scale Attention-Guided GNN, the features are fed into AN-SVM to perform final authentication. Given that EEG eye-blink features are nonlinear, noisy, and person-specific, overlapped feature spaces pose difficulties for ordinary classifiers. To this end, AN-SVM uses adaptive margin tuning, dynamic sample weight updating, and nonlinear kernel learning to improve its classification and authentication accuracy on complex EEG distributions. The extracted EEG embedding vector is represented in Eq. (23), where Z denotes the discriminative EEG feature representation generated from the proposed MAG-GNN framework.

$$Z = [z_1, z_2, z_3, \dots, z_n] \tag{23}$$

An optimum separating decision hyperplane is built by an AN-SVM classifier that maximally separates the directional eye-blink patterns from each other's classes. The classification function is given in Eq. (24), where w denotes the hyperplane weight vector, b represents the bias term, and $\phi(x)$ denotes nonlinear feature transformation.

$$f(x) = w^T \phi(x) + b \tag{24}$$

The non-linear distribution of EEG embeddings being complex, the suggested approach uses an RBF kernel to map the EEG features into the higher-dimensional feature space. This is represented using Eq. (25), where x_i and x_j denote EEG feature samples and γ controls the kernel influence region.

$$K(x_i, x_j) = exp(-\gamma \parallel x_i - x_j \parallel^2) \tag{25}$$

The nonlinear kernel mapping contributes to increased discrimination among intermingled blink pattern classes and more stable classification in noisy EEG.

Unlike the traditional fixed-margin SVM classifiers, the presented AN-SVM adopts the mechanism of adaptive margin learning to flexibly adjust the classification boundary in the feature space depending on the complexity of the

EEG feature space. The learning objective is shown in Eq. (26), where C represents the regularization parameter, $\xi_i$denotes slack variables, and $\alpha_i$indicates adaptive sample weights assigned to EEG samples.

$$min \frac{1}{2} \| w \|^2 + C \sum_{i=1}^{N} \quad \alpha_i \xi_i \tag{26}$$

EEG instances near the intersection of two decision regions get a higher adaptive weight for better margin enhancement and classifier stability. The classification constraint is formulated using Eq. (27), where $y_i$denotes the class label associated with the EEG sample x_i.

$$y_i(w^T \phi(x_i) + b) \geq 1 - \xi_i \tag{27}$$

The adaptive sample weighting mechanism is adjusted by classification error feedback. This is shown in Eq. (28), where ηdenotes the adaptive learning rate and $e_i$represents classification error.

$$\alpha_i^{t+1} = \alpha_i^t + \eta \cdot e_i \tag{28}$$

The feature adaptation mechanism allows the classifier to evolve the decision boundary depending on the complexity of the EEG feature distribution.

In addition, in order to enhance authentication performance, the presented system provides a confidence-based classification score of blink-pattern matching. The confidence score is calculated by:

$$S_c = \frac{f(x)}{||w||} \tag{29}$$

where $S_c$represents the classification confidence score. The higher the value of the confidence factor in the EEG samples, the better the authentication reliability and separation of the blink patterns.

In multi-class blink authentication, the AN-SVM used a one-against-one approach to discriminate between up, down, left and right eye-blink patterns, and the resultant authentication class is identified using Eq. (30), where $\hat{y}$denotes the predicted blink class and $f_c(x)$represents the classification score corresponding to the class c.

$$\hat{y} = arg\, max_c\, f_c(x) \tag{30}$$

The adaptive margin optimization, nonlinear kernel mapping, confidence-driven decision learning, and dynamic sample weighting mechanisms adopted by the proposed AN-SVM allow it to provide highly robust EEG classification against the noise and overlapping neural signals. The generated classification outputs are then employed for reliable EEG-based CAPTCHA authentication and user verification.

The proposed AN-SVM implements an RBF kernel to learn the non-linear distribution of EEG embeddings. A one-versus-one multi-class classifier is used for separating the four different direction blink classes (up, down, left, and right). While training the network, the weights of samples are adaptively adjusted based on the misclassification; misclassified samples close to boundaries are given a higher weight. The classifier parameters are selected by using a cross-validation process to better adapt classifier performance to unseen data. The final classification of theblinkclass is decided by selecting the AN-SVM classification that has the largest confidence value.

3.6 EEG-Based CAPTCHA Authentication and Decision Mechanism

The predicted blink patterns obtained after classification by the Adaptive Neuro-SVM (AN-SVM) are then applied in the EEG-based CAPTCHA authentication by comparing if the detected eye blink direction sequence matches the predetermined login challenge or not. This authentication is different from traditional text/image-based CAPTCHA, since it utilizes a cognitive EEG based on eye blinks and hence is more secure, convenient and difficult for automatic attacks to be launched. Initially, the CAPTCHA challenge sequence is represented using Eq. (31), where Cdenotes the predefined CAPTCHA blink sequence and $m$represents the total number of blink actions required for authentication.

$$C = [c_1, c_2, c_3, \dots, c_m] \quad (31)$$

Each element of the CAPTCHA represents a directional eye blink command: up, down, left or right blink. The predicted EEG blink sequence using the AN-SVM classifier is given in Eq. (32), where $\hat{Y}$denotes the classified blink sequence generated from EEG neural responses.

$$\hat{Y} = [\hat{y}_1, \hat{y}_2, \hat{y}_3, \dots, \hat{y}_m] \quad (32)$$

The sequence matching operation, for authentication validation, compares the predicted sequence with the corresponding CAPTCHA template. This is represented using Eq. (33), where $\delta(c_i, \hat{y}_i)$represents the matching function.

$$M = \sum_{i=1}^{m} \delta(c_i, \hat{y}_i) \quad (33)$$

The authentication accuracy score is computed using Eq. (34), where A_{score}denotes the CAPTCHA matching accuracy percentage.

$$A_{score} = \frac{M}{m} \times 100 \quad (34)$$

Higher authentication consistency between the challenge and the user's blink EEG response is measured by a higher authentication consistency score.

To make the authentication result more robust, a confidence-aware verification is employed in the authentication process. The confidence score output from the AN-SVM classifier is shown in Eq. (35), where $S_i$denotes the classification confidence score.

$$Conf = \frac{1}{m} \sum_{i=1}^{m} S_i \quad (35)$$

The authentication result is accepted only if the sequence matching accuracy as well as the confidence score are greater than the given thresholds. The final authentication decision is given in Eq. (36), where $\tau_a$and $\tau_c$denote the authentication accuracy threshold and confidence threshold, respectively.

$$Auth(x) = \{Accept, A_{score} \geq \tau_a \ and \ Conf \geq \tau_c \ Reject, otherwise \quad (36)$$

By employing neural signals triggered from human cognitive blink activity for real-time verification, the suggested EEG-based CAPTCHA authentication system provides a high level of security against automated bots and unauthorized intruders. Also, the architecture offers an easy and human-friendly authentication mechanism for handicapped people by means of a hands-free CAPTCHA verification using a brainwave-operated directed eye blink interface.

The label is the direction of the eye-blink that is detected and is used as the input of the EEG-based CAPTCHA system. Basically, the AN-SVM transforms the continuous and high-dimensional EEG embeddings into a discrete and actionable decision for the authentication mechanism. Figure 6 shows the eye movement

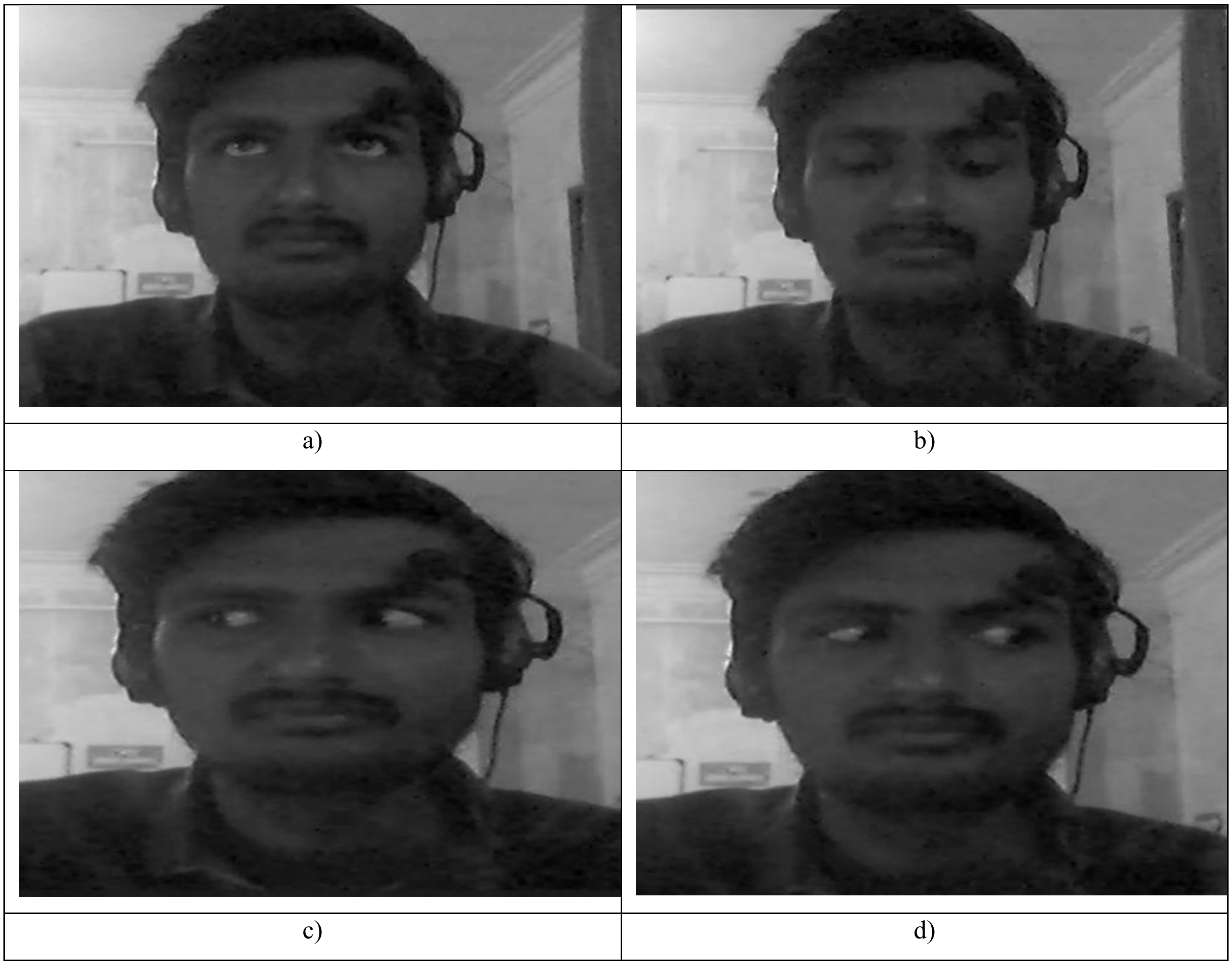


Figure 6: a) Up, b) Down, c) Left, d) Right directions of the eye movement

4. RESULT AND DISCUSSION

The proposed NeuroAuth-GNN model was tested on eye-blink recorded EEG data of 20 individuals on four directional blinks: up, down, left and right. Each of the participants provided 200 data samples for each of the four blink types that sum up to 16,000 samples. Each of the EEG signals obtained was filtered through certain preprocessing methods for removing unwanted noise and artifacts. Later, it was converted to a graph form for classification and feature extraction. The training set was considered to be 70% of the total data, and the testing set being 30%. The implemented NeuroAuth-GNN-AN model was compared with the following few machine learning and deep learning methods. Some important experimental conditions for EEG acquisition are illustrated in Table 2.

Table 2: EEG Data Acquisition and Experimental Configuration

Parameter	**Value**
EEG Device	Non-invasive EEG Headset
Electrode Placement	10–20 International System
Number of Electrodes	14 Channels
Sampling Frequency	128 Hz
Frequency Range	0.5–40 Hz

Signal Type	EEG Eye-Blink Signals
Number of Subjects	20 Participants
Age Group	20–35 Years
Gender Distribution	12 Male, 8 Female
Blink Classes	Up, Down, Left, Right
Number of Classes	4
Samples per Class	200
Total EEG Samples	16,000

4.1 Performance Metrics

The value of the correlation coefficient is used to determine the occurrence of eye blinks. The results of the classification are classified as True Positive (TP) or True Negative (TN) when the classification is correct, whereas the misclassifications are denoted by the False Positive (FP) and False Negative (FN) cases. The positive signals are detected by the eye blinking status, and the negative signals are detected by the non-eye blinking status. This is shown in Table 3.

Table 3: This table provides the Status of eye blinking Prediction state with TP, FP, TN, and FN.

	Status of Eye blinking		
		Eye blink	No Eye blink
Eye blinking prediction state	Eye - blinking detection	TP	FP (Type I Error)
	No Eye - blinking detection	FN (Type II Error)	TN

Table 4 gives the most important formulas and definitions applied to measure the effectiveness of the predictions of the model. It provides a definite method of measuring the effectiveness of the model on various kinds of results.

Table 4: Performance Evaluation Metrics for Classification Models

Metrices	**Formula**	**Definition**
Accuracy	$Accuracy = \frac{TP + TN}{TP + FP + FN + TN}$	Proportions of total correct predictions.
Recall	$Recall = \frac{TP}{TP + FN}$	It is the measure of the accuracy of the model in identifying the actual positive cases.
Specificity	$Specificity = \frac{TN}{FP + TN}$	It demonstrates the degree to which the model identifies the actual negative cases.
Precision	$Precision = \frac{TP}{TP + FP}$	It shows the proportion of the number of predicted positive cases that are truly positive.

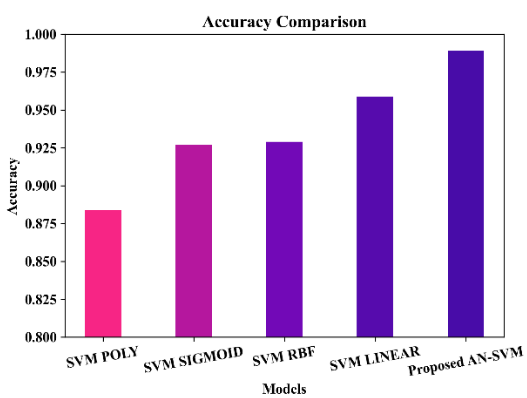
F1_Score	$$F1\_Score = 2\,\frac{Precision * Recall}{(Precision + Recall)}$$	It is the tradeoff between accuracy and recall, providing one value of general accuracy.

4.2 Comparative analysis

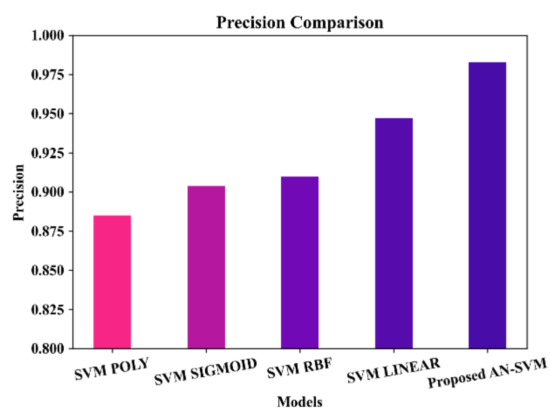
A performance of different SVM models is compared in the table, and AN-SVM showed better efficiency. Table 5 and Figure 7 display the results of the performance comparison between the various conventional SVM models and the proposed AN-SVM in the domain of EEG-based eye-blink CAPTCHA authentication. In the context of the traditional models, the SVM Linear classifier achieved the best results among the selected SVMs with 95.9% accuracy. Compared with the above, SVM Poly, Sigmoid, and RBF delivered a somewhat lower performance. Nevertheless, the proposed AN-SVM delivered results superior to all other base classifiers, achieving a high accuracy of 98.9%, precision 98.3%, recall 98.2%, and F1-score 98.8%. The aforementioned performance enhancement indicates the superior capability of the adaptive learning mechanism in distinguishing sophisticated and intersecting EEG eye-blink patterns with robust performance.

Table 5: Performance Comparison of SVM Variants and Proposed AN-SVM

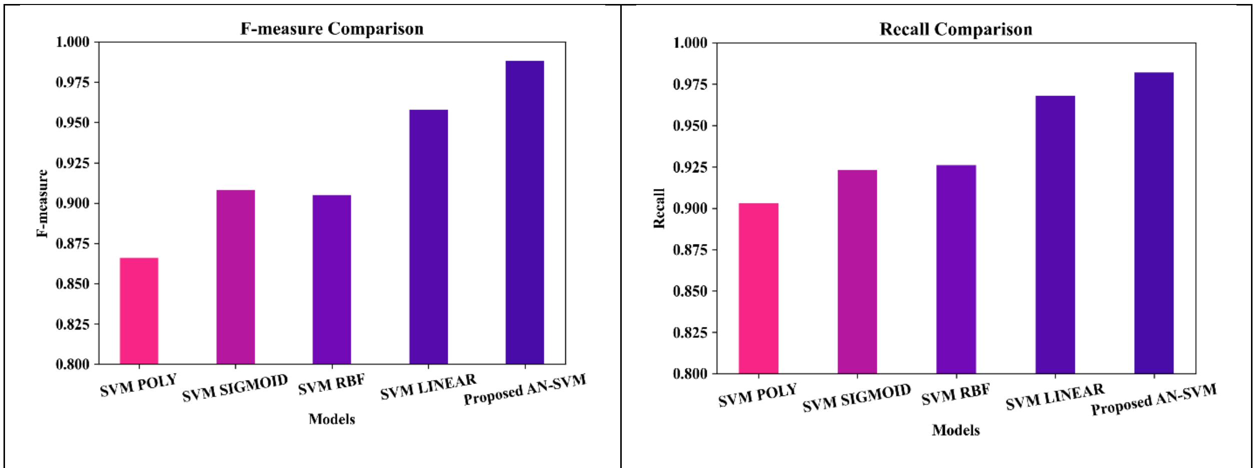
Models	Precision	Recall	F1-Score	Accuracy
SVM POLY	0.885	0.903	0.866	0.884
SVM SIGMOID	0.904	0.923	0.908	0.927
SVM RBF	0.910	0.926	0.905	0.929
SVM LINEAR	0.947	0.968	0.958	0.959
Proposed AN-SVM	0.983	0.982	0.988	0.989



a)



b)



c)	d)

Figure 7: a) SVM poly, b) SVM sigmoid, c) SVM RBF, d) SVM linear, e) Proposed iSVM

For better validation, performance of the developed framework is compared with state-of-the-art SVM-based methods namely least squares SVM (LS-SVM), fuzzy SVM (FSVM) and GA-SVM as shown in Table 6. LS-SVM provides computational advantage through the least square formulation, FSVM offers robustness using fuzzy membership for each sample, and GA-SVM employs evolution theory to optimize SVM parameters. The presented NeuroAuth-GNN framework outperforms all of the state-of-the-art SVM methods in eye-blink verification.

Table 6: Performance Comparison with Advanced SVM Models

Method	Accuracy (%)	Precision (%)	F1-Score (%)
LS-SVM	95.8	95.3	95.1
FSVM	96.4	96.0	95.8
GA-SVM	97.1	96.8	96.6
Proposed NeuroAuth-GNN-AN	98.9	98.3	98.8

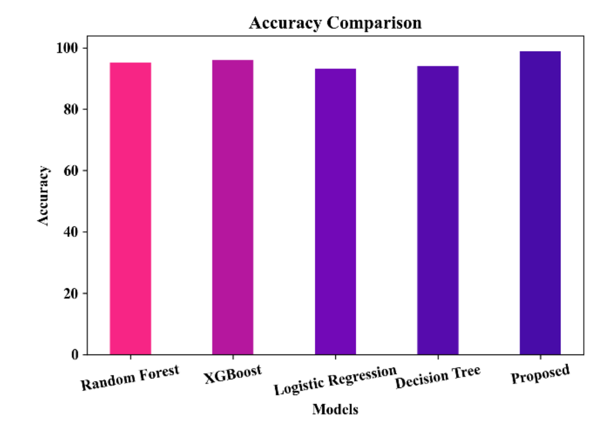
Table 7 summarizes the proposed model along with some machine learning classifiers in EEG-based eye-blink CAPTCHA authentication. Almost all the evaluation metrics recorded optimal values in the proposed model as compared to other classifiers, which are 98.9% of Accuracy, 98.3% of Precision, 98.2% of Sensitivity, 98.8% of Specificity and 98.8% of F-Measure. The overall MCC 98.6%, NPV 98.5% and GMean 98.5% show stable classification with efficient balanced prediction in the proposed model. FPR of the proposed model was 1.2% which is the lowest as compared to others, and the misclassification rate is drastically reduced as compared to the base models. Although its computation time is a little more than that of logistic regression, it is still considered an efficient model and could be used for efficient EEG-based authentication.

Table 7: Performance Comparison of ML Classifiers and Proposed iSVM

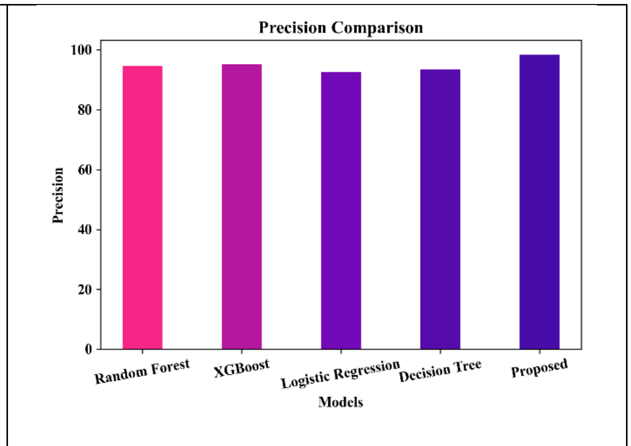
Model	Random Forest	XGBoost	Logistic Regression	Decision Tree	Proposed
Accuracy	95.1	95.9	93.2	94	98.9
Precision	94.6	95.3	92.7	93.6	98.3
Sensitivity	94.1	94.9	91.8	92.8	98.2
Specificity	95.4	96	93.6	94.4	98.8

F_measure	94.3	95.1	92.1	93.2	98.8
MCC	93.9	94.7	91.7	93	98.6
NPV	95.2	95.9	93.1	93.9	98.5
FPR	4.6	4	6.4	5.6	1.2
FNR	5.9	5.1	8.2	7.2	9
GMean	94.8	95.4	92.7	93.6	98.5
Computational Time (s)	2.84	3.12	1.45	2.1	1.89

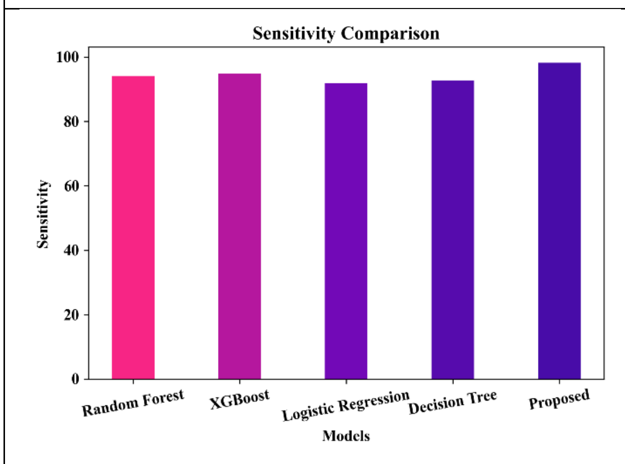
The performance of machine learning classifiers, compared to proposed method is shown in Figure 8 below. The proposed classifier achieves high classification accuracy and low error rates among all the prominent evaluation factors which shows it is superior over conventional classifiers. From this, we conclude that the adaptive learning makes it robust enough to discriminate eye-blink pattern and more reliable.



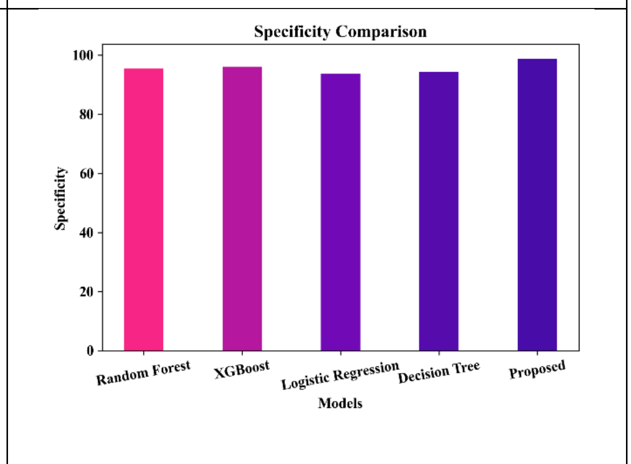
a)



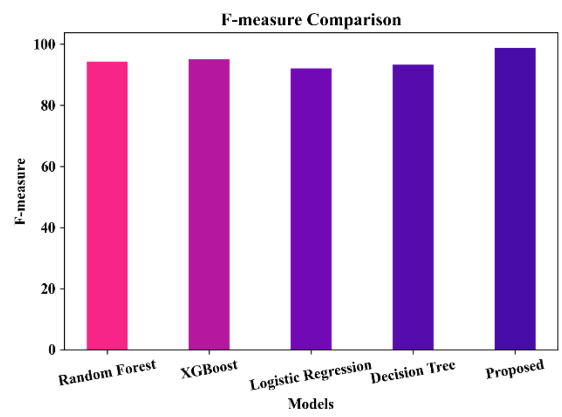
b)



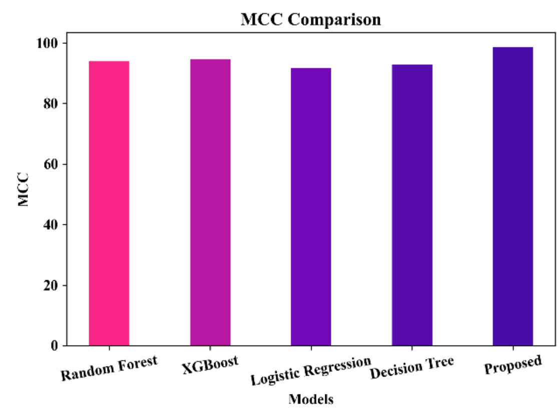
c)



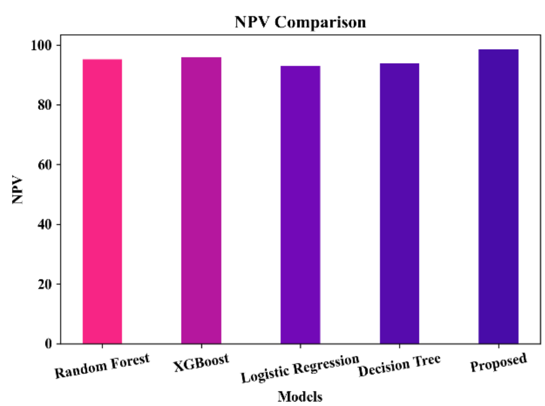
d)


F-measure Comparison
F-measure
Random Forest
XGBoost
Logistic Regression
Decision Tree
Proposed
Models

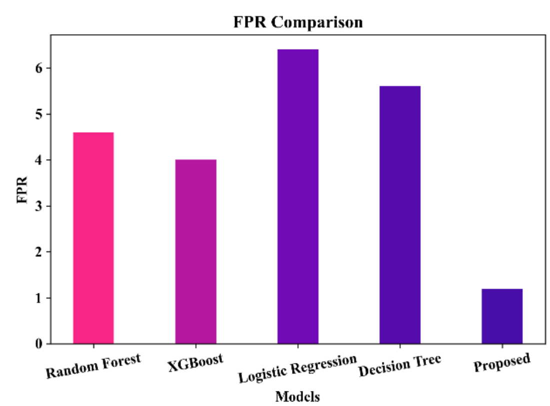
e)


MCC Comparison
MCC
Random Forest
XGBoost
Logistic Regression
Decision Tree
Proposed
Models

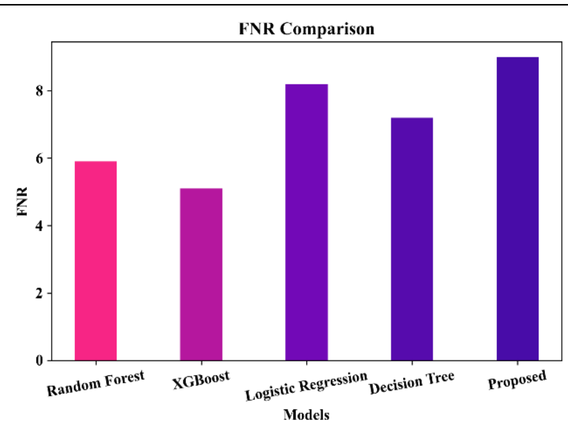
f)


NPV Comparison
NPV
Random Forest
XGBoost
Logistic Regression
Decision Tree
Proposed
Models

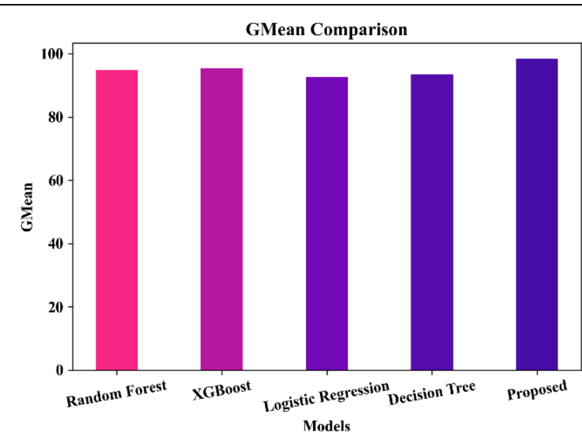
g)


FPR Comparison
FPR
Random Forest
XGBoost
Logistic Regression
Decision Tree
Proposed
Models

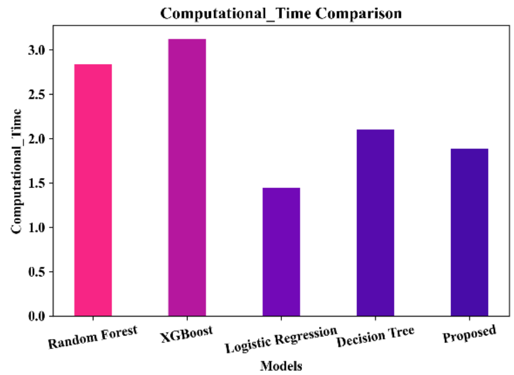
h)


FNR Comparison
FNR
Random Forest
XGBoost
Logistic Regression
Decision Tree
Proposed
Models

i)


GMean Comparison
GMean
Random Forest
XGBoost
Logistic Regression
Decision Tree
Proposed
Models

j)



k)

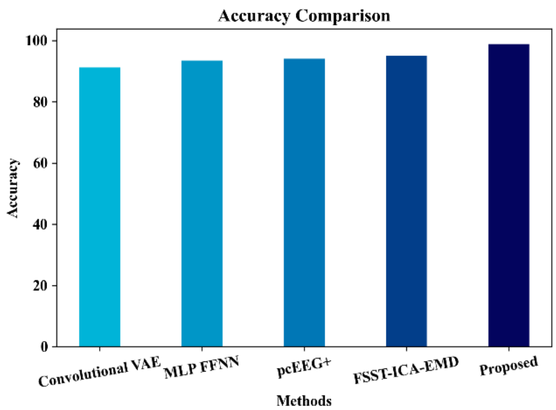
Figure 8: a) Accuracy, b) Precision, c) Sensitivity, d) Specificity, e) F-Measure, f) MCC, g) NPV, h) FPR, i) FNR, j) G-mean, k) computational time

The proposed model, compared to other DL techniques like Convolutional VAE, MLP-FFNN, pcEEG+, and FSST-ICA-EMD for EEG-based authentication in Table 8. It is observed that the traditional DL models achieve an acceptable performance level between 91.2%-95% accuracy and relatively higher execution time. On the other hand, the proposed model has outstanding classification results in all performance measures like accuracy (98.9%), precision (98.3%), sensitivity (98.2%), specificity (98.8%) and F1-score (98.8%), and greatly improved MCC along with significantly lower error rate (FPR=1.2%). The low computational time of the proposed model (1.89 s) also proved its efficiency. In all it claimed that the proposed method possesses excellent classification performance, generalization ability and low computational time over traditional DL approaches.

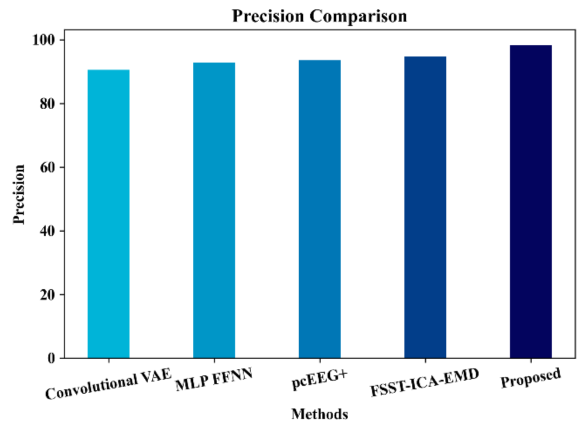
Table 8: Performance comparison of the proposed model with the existing DL models

Method	Convolutional VAE	MLP FFNN	pcEEG+	FSST-ICA-EMD	Proposed
Accuracy	91.2	93.5	94.1	95	98.9
Precision	90.5	92.8	93.6	94.7	98.3
Sensitivity	89.8	91.9	93.1	94.2	98.2
Specificity	92.1	94	95	95.6	98.8
F_measure	90.1	92.3	93.3	94.4	98.8
MCC	82	86	88	90	98.6
NPV	91	93	94.2	95.1	98.5
FPR	8	6	5	4	1.2
FNR	12	11	10	9.5	9
GMean	90.8	92.9	94	94.9	98.5
Computational Time (s)	4.85	4.12	3.76	2.95	1.89

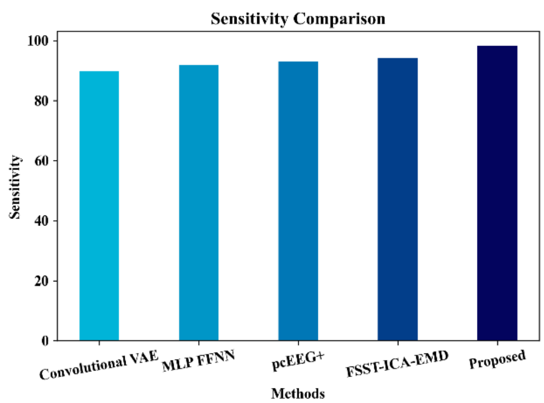
Figure 9 shows the performance comparisons between the proposed approach and traditional deep learning models on the EEG-based authentication. As the result demonstrates, traditional models such as Convolutional VAE, MLP-FFNN, pcEEG+, and FSST-ICA-EMD could achieve fairly decent authentication, while the proposed model surpasses all the base models on all measurement metrics. The classification with the proposed method achieves the best classification accuracy, and F1-score and its false rates are much lower than any other baselines. The classification also achieved best performance in terms of computation time, and that proves it's useful for a real-time EEG eye-blink CAPTCHA authentication system.



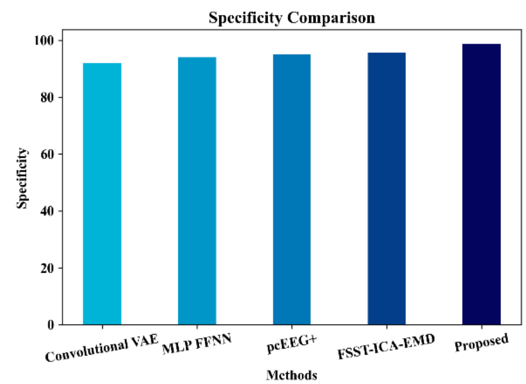
a)



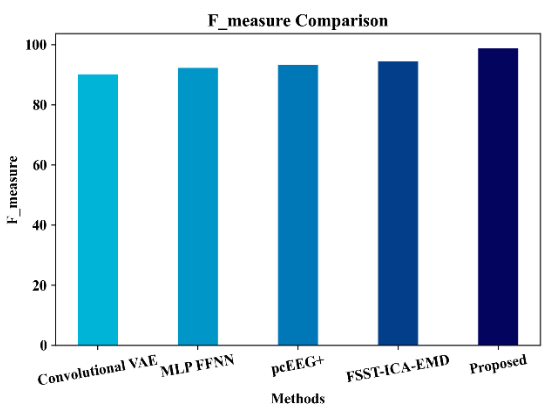
b)



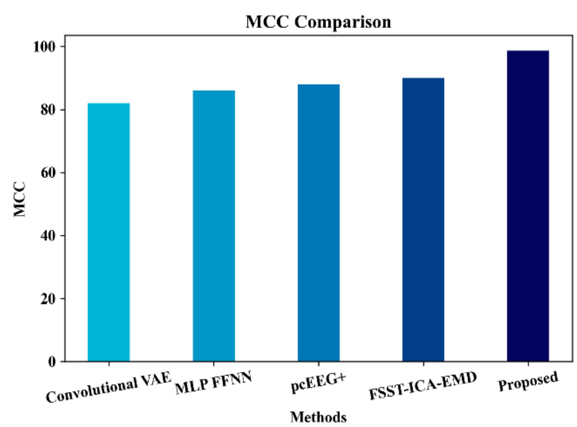
c)



d)



e)



f)

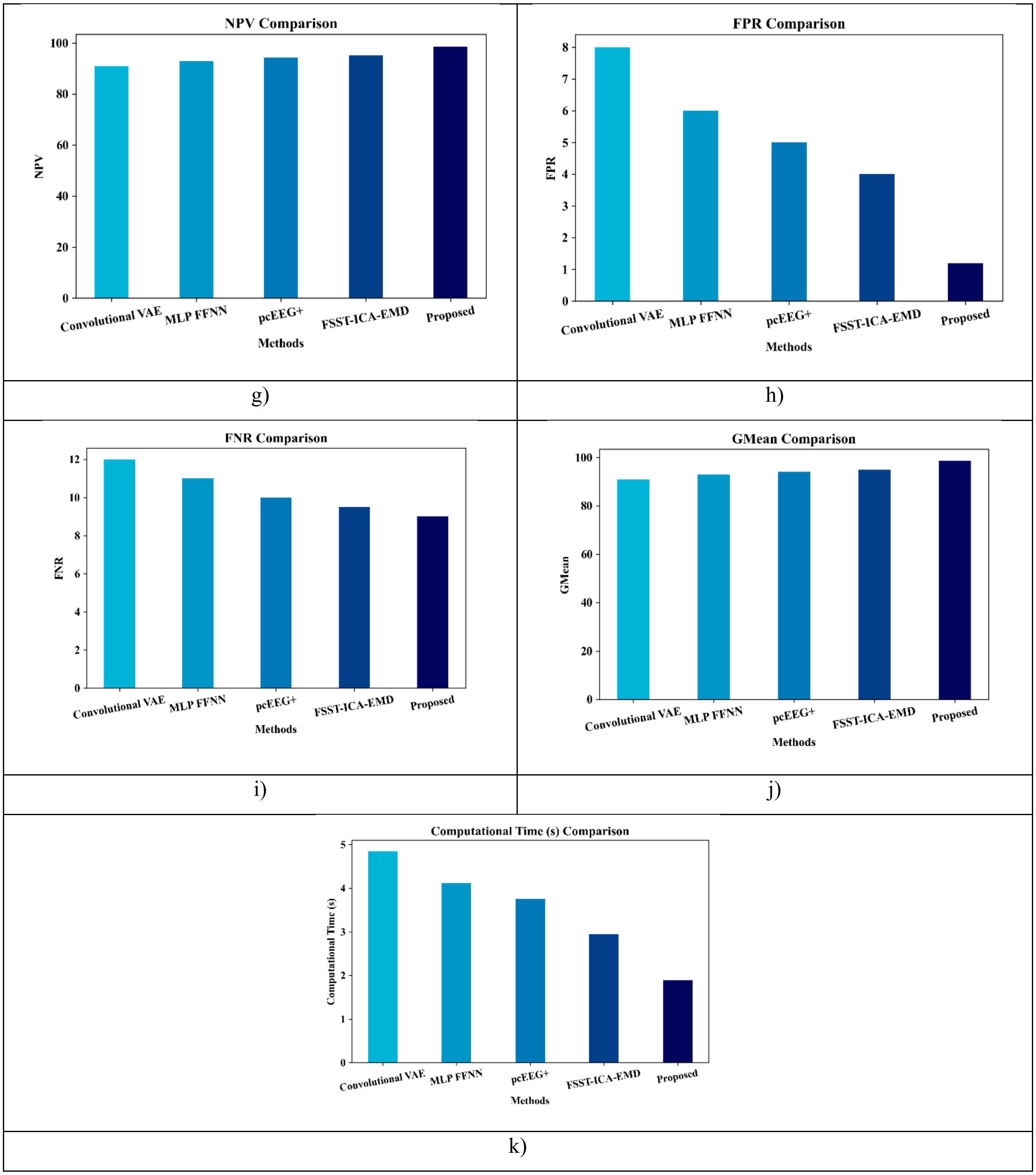


Figure 9: a) Accuracy, b) Precision, c) Sensitivity, d) Specificity, e) F-Measure, f) MCC, g) NPV, h) FPR, i) FNR, j) G-mean, k) computational time

These results in Table 9 illustrate how the NeuroAuth-GNN system performs under practical authentication situations by classifying user and imposter eye-blink CAPTCHA patterns based on EEG data. The user is allowed access only if the perceived blink sequence matches that in the enrolment template. Otherwise, the user is rejected. The achieved FAR of 1.2% and FRR of 1.5% indicates the robustness of the system in terms of security and reliability, and prove that the model works not only for classification measures but also well under real authentication conditions.

Table 9: Authentication results of the proposed model with the existing models

Method	FAR (%)	FRR (%)	EER (%)
Convolutional VAE	5.2	6.5	4.9
MLP-FFNN	6.8	5.9	5.2
pcEEG+	3.5	3.4	4.9
FSST-ICA-EMD	4.2	3.1	2.6
Proposed NeuroAuth-GNN	1.2	1.5	1.35

The ablation results in Table 10 shows the individual effectiveness of each component in the proposed NeuroAuth-GNN framework. After deleting the preprocessing process, the accuracy drops to 93.7%, which shows the crucial importance of improving the signal before learning features. Then, add the GNN module into the system, and the accuracy of the classification rises to 95.6%, which is the result of effectively learning spatial features using graph information. Adding the Graph-SVM hybrid model to the system, the accuracy rises to 96.9%, which is a better classification ability for eye-blink CAPTCHA. The NeuroAuth-GNN framework gets the best accuracy 98.9%, precision 98.3% and F1-score 98.8%. The proposed framework, with all its components, was applied to the robustness of EEG-based eye-blink CAPTCHA authentication.

Table 10: Ablation study of the proposed model

Model Variant	Accuracy (%)	Precision (%)	F1-Score (%)
Without Pre-processed Variant	93.7	92.1	91.4
Only GNN-Based Model	95.6	95.2	95.0
Only Graph-SVM Hybrid Model	96.9	96.5	96.3
Proposed NeuroAuth-GNNModel	98.9	98.3	98.8

4.3 Discussion

The experiments also validated that the NeuroAuth-GNN method is feasible to improve the EEG-based eye-blink CAPTCHA authentication system effectively in overcoming drawbacks in traditional methods regarding feature extraction and classification. The accuracy of authentication is up to 98.9%, which suggests it could well discriminate the direction of eye-blinks on the EEG. Multi-Scale Attention-Guided GNN contributed greatly to this increase by extracting both spatial locality and global interactions between electrodes on the EEG signal, while at the same time prioritizing more informative regions associated with eye-blinks. As such, more discriminative and noise-resistant features were extracted, resulting in higher classification accuracy than that achieved by machine learning and deep learning-based methods. The effectiveness of the proposed framework was further corroborated by the security and reliability analysis conducted. The system produced low FAR (1.2%) and FRR (1.5%), indicating the ability to block unauthorized authentication with a high percentage of correct authentication for authentic users. The ablation study conducted showed that the proposed NeuroAuth-GNN-AN always showed superior performance than its alternatives, such as without preprocessing, stand-alone GNN, and Graph-SVM hybrid methods, thus validating the importance of each component in the whole system. These results may indicate that EEG signal preprocessing combined with attention-guided graph learning and an adaptive classifier would achieve reliable cognitive authentication for the sake of security systems, assistive technologies, and other future human-computer interfaces.

The NeuroAuth-GNN-AN has a satisfactory classification accuracy. There were a few samples misclassified due to weak blink response of the EEGs, as well as due to existing artifact and similar blink direction overlap of the neural patterns of two different directions. Compared with other methods, the proposed framework performs quite well on complex multi-channel EEG samples, which are generally misclassified by other methods, because it extract the spatial-temporal association among electrodes using graph learning with an attention mechanism. Thus, the proposed framework is very powerful for EEG with complex neuronal networks and minute blink-pattern differences.

5. CONCLUSION

The research introduced a security framework based on EEG-based eye-blink CAPTCHA authentication, NeuroAuth-GNN integrated the multi-scale attention guided graph neural networks and AN-SVM to achieve robust user verification. Through the implementation of graph-based neural representation learning and adaptive decision boundary, the system successfully overcame the difficulties caused by noisy EEG signals, low spatial-temporal feature extraction and complex nonlinear classification of blink patterns. The verification experiment shows an outstanding performance with an accuracy of 98.9% and low FAR and FRR values, which proves that the framework is robust and secure. Moreover, the proposed system provides an ideal hands-free and easy-to-use authentication mode and may apply for the physically disabled and cognitive security fields. The framework provides a promising biometric authentication for the next generation, with the future work of field application, extensive validation and fused multi-modal biometric signal for enhanced security.

DECLARATIONS:

FUNDING

On Behalf of all authors the corresponding author states that they did not receive any funds for this project.

CONFLICTS OF INTEREST

The authors declare that we have no conflict of interest.

COMPETING INTERESTS

The authors declare that we have no competing interest.

DATA AVAILABILITY STATEMENT

The EEG dataset used in this study was collected under controlled experimental conditions. The data supporting the findings of this work are available from the corresponding author upon reasonable request.

ETHICS APPROVAL

No ethics approval is required.

CONSENT TO PARTICIPATE

Not Applicable

CONSENT FOR PUBLICATION

Not Applicable

DECLARATION OF INTERESTS

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

AUTHOR'S CONTRIBUTIONS MODEL

Author 1: **S. Nooriya begam**

He participated in the methodology, Conceptualization, Data collection and writing the study

Author 2**: R. M. Vidhyavathi**

He participated in the methodology and overall concept

Author 3: **J. Joseph Sahayarayan**

He analysis the paper and supervisor of this paper.

REFERENCES

1. Rabbani, M., Sabith, N. U. S., Parida, A., Iqbal, I., Mamun, S. M., Khan, R. A., ... & Ahamed, S. I. (2025). EEG based real time classification of consecutive two eye blinks for brain computer interface applications. Scientific Reports, 15(1), 21007.
2. Page, C., Liu, C. C., Meltzer, J., & Ghosh Hajra, S. (2024). Blink-related oscillations provide naturalistic assessments of brain function and cognitive workload within complex real-world multitasking environments. Sensors, 24(4), 1082.
3. Suri, A., Wani, M. A., Jabin, S., Khan, M., Sherwani, K. I. K., Sardar, M., ... & Alomran, A. (2026). BMT_EEG: A Novel EEG Dataset for evaluating the effects of new protocols on biometric authentication systems. IEEE Access, 14, 49535-49549.
4. Shahbakhti, M., Beiramvand, M., Nasiri, E., Far, S. M., Chen, W., Solé-Casals, J., ... & Marozas, V. (2023). Fusion of EEG and eye blink analysis for detection of driver fatigue. IEEE Transactions on Neural Systems and Rehabilitation Engineering, 31, 2037-2046.
5. Biondi, F. N., Graf, F., Pillai, P., & Balasingam, B. (2023). On validating a generic camera-based blink detection system for cognitive load assessment. Cognitive Computation and Systems, 5(4), 255-264.
6. Guttmann-Flury, E., Sheng, X., & Zhu, X. (2025). Dataset combining EEG, eye-tracking, and high-speed video for ocular activity analysis across BCI paradigms. Scientific Data, 12(1), 587.
7. Makkar, K., & Bisen, A. (2023). EEG signal processing and feature extraction. International Journal for Modern Trends in Science and Technology, 9(08), 45-50.
8. Wang, Q., Smythe, D., Cao, J., Hu, Z., Proctor, K. J., Owens, A. P., & Zhao, Y. (2023). Characterisation of cognitive load using machine learning classifiers of electroencephalogram data. Sensors, 23(20), 8528.
9. Egambaram, A., Badruddin, N., & Yahya, N. (2025). Re-purposing EEG Artifacts: Eye Blink Artifact Features as Predictors of Drowsiness Using Deep Learning. Applied Artificial Intelligence, 39(1), 2587985.
10. Wang, Y., Duan, W., Dong, D., Ding, L., & Lei, X. (2022). A test-retest resting, and cognitive state EEG dataset during multiple subject-driven states. Scientific Data, 9(1), 566.
11. Wibirama, S., Alfarozi, S. A. I., Suhari, A. R., Fristiana, A. H., Nurlatifa, H., & Santosa, P. I. (2025). Classification of cognitive load using deep learning based on eye movement indices. IEEE Access.
12. Kaushik, P., Moye, A., Vugt, M. V., & Roy, P. P. (2022). Decoding the cognitive states of attention and distraction in a real-life setting using EEG. Scientific Reports, 12(1), 20649.
13. Bidgoly, A. J., Bidgoly, H. J., & Arezoumand, Z. (2022). Towards a universal and privacy preserving EEG-based authentication system. Scientific Reports, 12(1), 2531.
14. Meng, L., Jiang, X., Huang, J., Li, W., Luo, H., & Wu, D. (2023). User identity protection in eeg-based brain–computer interfaces. IEEE transactions on neural systems and rehabilitation engineering, 31, 3576-3586.
15. Baraku, T., Stergiadis, C., Veloudis, S., & Klados, M. A. (2024). Personalized user authentication system using wireless eeg headset and machine learning. Brain Organoid and Systems Neuroscience Journal, 2, 17-22.
16. Gorur, K. (2023). Fourier synchrosqueezing transform-ICA-EMD framework based EOG-biometric sustainable and continuous authentication via voluntary eye blinking activities. Biomimetics, 8(4), 378.
17. Alyan, E., Arnau, S., Reiser, J. E., & Wascher, E. (2024). Synchronization-based fusion of EEG and eye blink signals for enhanced decoding accuracy. Scientific Reports, 14(1), 26918.
18. Criscuolo, S., Apicella, A., Prevete, R., & Longo, L. (2025). Interpreting the latent space of a Convolutional Variational Autoencoder for semi-automated eye blink artefact detection in EEG signals. Computer Standards & Interfaces, 92, 103897.
19. Chae, M. S., Rehman, A., Kim, Y., Kim, J., Han, Y., Park, S., & Mun, S. (2025). Voluntary Eye Blink and SSVEP-Based Selective Attention Interface for XR User Authentication: An Explainable Neural Decoding and Machine Learning Approach to Reducing Visual Fatigue. IEEE Access.
20. Khalil, A. E. K., Perez-Diaz, J. A., Cantoral-Ceballos, J. A., & Antelis, J. M. (2024). Unlocking security for comprehensive Electroencephalogram-based user authentication systems. Sensors, 24(24), 7919.
21. Alyan, E., Arnau, S., Reiser, J. E., Getzmann, S., Karthaus, M., & Wascher, E. (2023). Decoding eye blink and related EEG activity in realistic working environments. IEEE Journal of Biomedical and Health Informatics, 27(12), 5745-5754.
22. Rehman, T. U., Alruwaili, M., Siddiqi, M. H., Alhwaiti, Y., Anwar, S., Halim, Z., & Alam, M. (2025). Advancing EEG-based biometric identification through multi-modal data fusion and deep learning techniques. Complex & Intelligent Systems, 11(9), 398.
23. Dragu, M. A., Nicolae, I. E., & Frunzete, M. C. (2024). Cryptographic Algorithm Designed by Extracting Brainwave Patterns. Mathematics, 12(13), 1971.
24. Alsumari, W., Hussain, M., Alshehri, L., & Aboalsamh, H. A. (2023). Eeg-based person identification and authentication using deep convolutional neural network. Axioms, 12(1), 74.
25. Stergiadis, C., Kostaridou, V. D., Veloudis, S., Kazis, D., & Klados, M. A. (2022). A personalized user authentication system based on EEG signals. Sensors, 22(18), 6929.