EEG-based Biometric Authentication Using Machine Learning: A Comprehensive Survey

Tarik Bin Shams[1], **Md. Sakir Hossain**[1†], **Md. Firoz Mahmud**[1], **Md. Shahariar Tehjib**[1], **Zahid Hossain**[1], and **Md. Ileas Pramanik**[2], Non-members

ABSTRACT

An electroencephalogram (EEG) is a measurement that reflects the overall electrical activity in the brain. EEG signals are effective for biometric authentication and robust against malware attacks and any kind of fraud activities due to the uniqueness of the signals. Significant progress in research on EEG-based authentication has been achieved in the last few years, with machine learning being extensively used for classifying EEG signals. However, to the best of our knowledge, there has been no investigation into the overall progress made in such research. In this paper, the literature on the various factors involved in state-of-the-art biometric authentication systems is reviewed. We provide a thorough comparison of different machine learning biometric authentication techniques. The comparison criteria include the research objectives, machine learning algorithms, computational complexity, source of brainwaves, feature extraction methods, number of channels, and so on. Alongside the discussion of existing works, directions for future research are suggested to improve authentication accuracy. This paper provides an in-depth discussion of different advanced biometric authentication techniques, and a vivid picture of state-of-the-art machine learning-based biometric authentication techniques using EEG.

Keywords: Electroencephalogram, EEG, Machine Learning, Signal Processing, Biometric, Authentication

1. INTRODUCTION

In the case of computer science and security mechanisms for cryptography, authentication can be interpreted as a process for ensuring the subject's assumed identity. Authentication is a crucial technique for controlling access to digital or physical infrastructure such as rooms or appliances. The use of unique human biological features is one of the most important approaches for user authentication. In the growth of new interdisciplinary research, the biometric field, recent development of computing power, and machine learning have been decisive. The purpose of biometrics is to detect physical and behavioral features and discriminate between individuals.

The authentication method acknowledges the identity of a recipient. Authentication technology offers systems access protection by verifying whether the credentials of a user correlate with those stored in an approved user database. In order to detect the identity of a person, various systems need different types of credentials. The password is a secret string, known only to the user and machine. The password is a very popular way of authentication. An authentication process can be represented in two separate phases: identification and actual authentication. It offers the user an identity and a password to the authentication framework [1]. There are also other authentication forms such as biometric authentication.

Biometric authentication is a type of protection for testing and matching the user's biometrics to ensure that they are allowed to access a computer or any other systems. Biometric features are physical and molecular unique traits that can be readily compared to the licensed features contained in a database. The classification of the biometric authentication process is shown in Fig. 1. Biometric characteristics can be grouped into two classes: physiological and behavioral. Physiological authentication recognizes an individual based on the forms of various parts of the human body including fingerprints, eye iris, face, and hand geometry. A hand geometry device uses a reader to record, process, and create a digital biometric prototype to define and validate human hand geometry. Hand geometry readers are also used by attending staff and apps for physical entry. The behavioral biometrics, on the other hand, are based on behavioral characteristics such as voice, gestures, keystrokes on the keyboard, signature, etc. The authentication process often allows the use of a primary biometric or secondary password unit to authenticate in two stages (two-factor authentication; 2FA), or more than two stages (multiple-factors authentication; MFA) with a combination of several biometric patterns. Some popular authentication forms are fingerprint scanners, face recognition, eye scanners, and so on. The biometric process poses some challenges to its general acceptance by consumers. Some biometric technologies are very

Manuscript received on March 19, 2021; revised on September 10, 2021; accepted on December 12, 2021. This paper was recommended by Associate Editor Pornchai Phukpattaranont.

[1] The authors are with the Department of Computer Science, American International University-Bangladesh (AIUB), Bangladesh.

[2] The author is with the Begum Rokey University Rangpur, Bangladesh.

[†] Corresponding author: sakir.hossain@aiub.edu

Digital Object Identifier: 10.37936/ecti-eec.2022202.246906

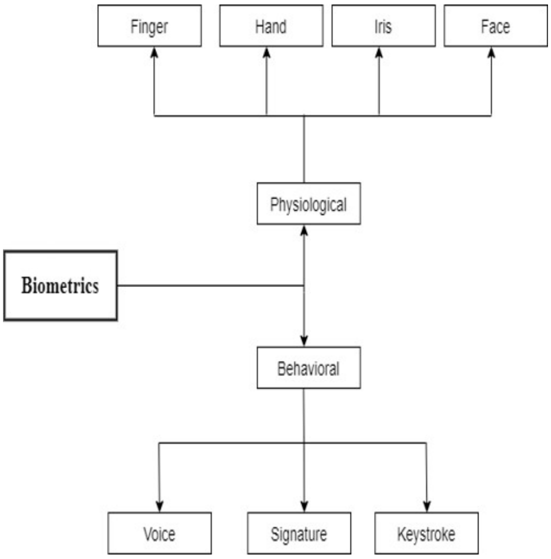

***Fig. 1**: Classification of biometric authentication.*

difficult to configure, install, and use, and may require consumers to be trained to make sure the devices are properly used [2]. Security updates are necessary to ensure the continuous availability of biometric data and functions. Error rates continue to be a concern with biometric-based authentication, and the high error rate could limit the chance of consumers bringing biometrics into their habits of daily life.

Among biometric measurement systems, the electroencephalogram (EEG) is becoming widely used. The EEG biometric system has special benefits that make it more popular than other biometric systems. Some biometric systems can be forged or imitated such as those involving fingerprint or iris recognition. For example, some experiments suggest that a suspect could have an image of themselves and create a fake finger print. However, the EEG is not exposed to the potential attacker, making it uncapturable and therefore hard to forge, unlike other biometric devices. In comparison, a deceased (and warm) body may be used to allow entry to the device in other biometrics, but the dead brain does not generate EEG signals in the EEG biometric [3].

The EEG is a signal for monitoring and analyzing the electrical function of the brain. The brain nerve cells produce electrical impulses that fluctuate rhythmically in distinct patterns. A device detects and tracks these brain wave variations. The recording made by such an instrument is called an electroencephalogram, usually abbreviated to EEG. The EEG detects and monitors brain wave patterns. Thin metal discs with electrodes are mounted on the subject's scalp and the signals then transmitted to the computer to record the data [4]. Natural electrical activity in the brain is a familiar sequence and found to be more effective as a medical aid in the case of severe head trauma, brain cancers, cerebral illnesses, sleep disturbances, seizures, and other degenerative diseases of the nervous system [5]. Furthermore, it is helpful for detecting whether patients are brain dead, which is particularly relevant if organs need to be preserved for transplantation as soon as brain death has been verified. However, an EEG cannot provide clear reasons for different brain-related dysfunctions. Rather, the sensitivity of the EEG signal toward different episodes helps physicians to observe the physiological and behavioral states of individuals caused by various medical events such as unconsciousness, seizures, lesions, sleep disorders, and so on [6]. The EEG waveform is identified as irregular when the properties of a frequency band are higher or lower than the normal range. Based on the frequency and its position, as the EEG records are collected, the regular EEG waveforms may be graded. These characteristics are compared in Table 1 [6–8].

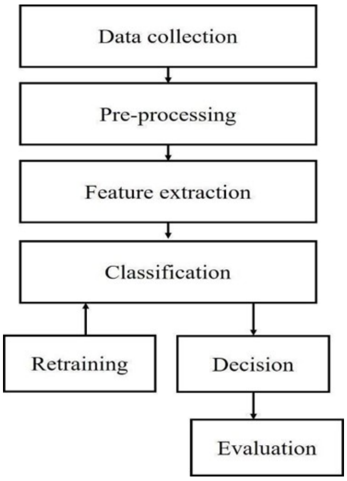

***Fig. 2**: Biometric authentication steps [9].*

Compared to other authentication factors, the EEG biometric factors have more attractive features. For example, it cannot be robbed like the factors of possession nor expected to be memorized like the factors of information. Consequently, biometric factors provide users with the most convenient authentication method. Signals registered against visual-evoked potentials (VEPs) in response to light stimuli or resting status are tested using EEG signals to validate authentication mechanisms.

The design of an EEG authentication device involves several steps, usually straightforward, and under a certain protocol, the user can do a predefined job. These activities are specified such that the brain can be activated without moving other parts of the body. Instances of these activities include chanting a tune, providing the image of a sport, thinking about a certain keyword, or just resting. The EEG authentication mechanism architecture is presented in Fig. 2 [9]. A compact and commercially available EEG headset can capture the necessary signals. Initially, these signals are pre-processed to increase their efficiency, and the useful features then extracted prior to classification. The improved signals will be set to extract the features after pre-processing, with the resulting features then used

Table 1*: Classification of brain waves.*

Waveform	Range of Frequencies and Characteristics	State of Occurrence	State of Abnormality	Location
Delta	0.5–4 Hz Highest amplitude [7]	Wakefulness, serious brain disorder, deep sleep [7]	Lesion, tumor, severe damage from stroke	Posteriorly in children and frontal in adults
Theta	4–8 Hz Large amplitude	Deep meditation, emotional stress (disappointment or frustration), drowsiness	Brain lesion and head injuries	Frontal region
Alpha	8–13 Hz 30–50 μV [7]	Wakeful and resting state, dominant when eyes closed [8]	Head injuries, attention problems, and depression	Posterior and central regions
Beta	13–30 Hz Low in amplitude	Alertness, drug-taking, strongly engaged in problem-solving, focused on the outside world	Sleep disorder and lack of attention in problem-solving	Mostly frontal
Gamma	>30 Hz Small in amplitude	Cognitive and motor functions, long-term memory	Epilepsy, Alzheimer's disease, schizophrenia, hallucinations	Somatosensory cortex

Table 2*: Existing papers relating to biometric authentication.*

Reference	Purpose	Signal Processing	Machine Learning	Description	Reviewed up to
[10]	Discussing the different organs used for data collection	✓	✗	Elaboration	2010
[11–15]	Use of keystroke	✓	Partial	Brief	Before 2011
[16]	Discussing different organs of the human body and privacy issues concerning biometric data	✓	✓	Brief	2018
[17]	Biometric pattern recognition	✗	✓	Brief	2018
This work	Machine learning-based authentication	✓	✓	Elaboration	2021

to train a classifier. After analyzing and classifying the registered signal with the help of a model, the user is identified through recognition or validated by authentication, depending on the form of the classifier. However, the classifier may need to be retrained several times if the precision does not reach a certain threshold. Retraining may also be required in the case of any change in the dataset. Historically, classifiers such as the support vector machine (SVM) and the K-nearest neighbors (KNN) were used for this purpose, but in recent years these have often been replaced by deep learning methods. A judgment is made on the basis of classifier output. Finally, estimation is used to evaluate the performance of the authentication mechanism.

Recent research has identified biological signals, including brain waves, as a feasible means of reliable authentication. Since the brain stimulus is proven to be specific to the individual, the EEG may be used to discriminate. The EEG authentication approach of visual stimulation shows high precision verification and can be used with brain communication methods for further development.

Research into biometric authentication has made significant progress during the last few decades, with several papers published on the topic (see Table 2). In [10], the author reviewed the different features commonly used in biometric authentication, including face, gait, iris, voice, signature, lips, fingerprints, veins, DNA, and so on. Although various organs for capturing data have been clearly surveyed, the engineering and analysis techniques used to capture and analyze data from organs have not. A behavioral-based approach to authentication is considered in [11]. The benefit of this approach is that the data for user authentication can be collected anonymously without the subject noticing. For example, biometric authentication using keystrokes [11–15].

Rather than reviewing only biometric authentication based on a single feature, a comprehensive review of authentication based on several kinds of biometric data is presented in [16]. The features include iris, hand geometry, face, fingerprints, and so on. However, the difference between [10] and [16] is that instead of describing the organs used to extract biometric data, the main emphasis in [16] is on the processing of extracted data and the security and privacy of the data. Various machine learning algorithms have been exploited in evaluating the data extracted from various organs to authenticate an individual. A survey on EEG-based user authentication is presented in [16], in which a handful of papers are reviewed. However, the application of various machine learning algorithms is not explicitly discussed.

All the papers reviewed briefly describe each aspect of biometric authentication. However, the objective of this paper is to cover all works that use machine learning algorithms in classifying EEG data to authenticate a user. Furthermore, rather than merely touching on each paper, here we provide an elaborate review of each work to enable the reader to get a clear picture.

A comparative analysis of the different state-of-the-art EEG-based authentication techniques is also presented.

2. MACHINE LEARNING CLASSIFICATION ALGORITHMS

This section presents a review of the various machine learning algorithms widely applied in user authentication. However, only the supervised classification algorithms are considered here. A classification algorithm can be defined as supervised if it learns from a dataset in which each instance is accompanied by its class label. Once trained, the algorithm can predict the class of an instance in the dataset where the class label is unknown. The supervised learning algorithms appearing frequently in this paper are briefly described in the following subsections.

2.1 *K*-Nearest Neighbor

In this technique, an instance without any class label is compared with all instances of the dataset, and the K closest instances selected. Finally, a majority voting technique is applied to the labels of the K closest instances to identify the label of the candidate instance [18].

2.2 Decision Tree

This is a tree like structure where the root represents a condition and the branches represent the outcomes of the tree while the leaf represents the class of the instance. The path from the root to the leaf is known as the set of decision rules [19].

2.3 Random Forest

This is an ensemble of multiple classifiers for classifying an instance, with majority voting then applied to decide the class of the instance. Many decision trees are constructed in random forest, each from randomly selected attributes [20].

2.4 Artificial Neural Network

This is a supervised machine learning algorithm. It consists of an input layer, one output layer, and one or more hidden layers between the two. A labeled dataset is fed into the network as an input which changes its weight. The network becomes trained after an iterative process and can then be used to classify an instance without any label. In a convolutional neural network (CNN), the processing of the inputs to a neuron is performed differently. Rather than multiplying the inputs by weight, a filter is used. The repeated overlapping use of a filter on the input to a neuron allows the network to identify patterns in the data more accurately. For this reason, the CNN is usually used in image classification. However, it can also be used for one-dimensional and three-dimensional data [21]. The artificial neural network can work with high accuracy on a large dataset. However, it requires a long training time [21].

Table 3: *Works based on task type.*

Activities During EEG Recording	References
Real	[23], [32], [24], [43], [33], [25], [26], [34], [35], [37], [38], [40], [41], [44], [28], [45], [29], [42], [30]
Motor imagery	[50], [51], [46], [52], [47], [48]
Real and motor imagery	[60], [56], [57], [58]
Rest state	[61]

2.5 Support Vector Machine

In this machine learning algorithm, the data points are divided by hyperplanes. Data points in different sides of a hyperplane belong to different classes. If there are two input features in the dataset, the hyperplane will be a line. However, the hyperplane will be two-dimensional if there are three features. Things become more complex with a higher number of input features. A dataset point close to the hyperplane is called a support vector, which influences the orientation and position of the hyperplane [22]. The benefits of the support vector machine include low computational overhead and generalization error. However, one of the challenging tasks of this algorithm is to tune the hyperparameters. It is usually used for binary classification [18].

3. BIOMETRIC AUTHENTICATION USING MACHINE LEARNING

This section describes the different works using machine learning to classify EEG data for authentication. The different parameters used in the works are also compared. The EEG-based authentication techniques are divided into four broad categories, depending on the type of activities performed by the subjects during the EEG recording. The categories consist of: (i) Real activity; (ii) Imagery activity; (iii) Combined real and imagery activity; and (iv) No activity or resting state. The papers presented in Table 3 are based on these categories.

3.1 Authentication Using Real Activity

This section presents the authentication techniques used to collect the EEG data when real activities are performed. The authentication techniques are divided into three categories: (i) Traditional machine learning algorithms (this refers to any machine learning algorithm except the artificial neural network); (ii) Artificial neural network; and (iii) Multiple machine learning algorithms from categories (i) and (ii). Works based on classifier type are presented in Table 4.

3.1.1 Traditional machine learning algorithm with real activity

An authentication technique was proposed in [23] to investigate the impact of a large pool of people on the accuracy of the process. Emulating the various authentication situations involved four different steps: EEG signal collection, pre- processing, feature extraction, and authentication. The raw EEG signal was gathered by placing "EASYCAP" devices containing six midline electrodes on 32 participants (11 females, aged 18–25; average age 19.12). The signals were sampled at 500 Hz. Since the raw EEG signals have outliers, the noise needs first to be minimized by ensemble averaging. After pre-processing, various techniques were used to extract the features of the EEG signal. These can be categorized in three ways: time-frequency-domain extraction, time-domain extraction, and frequency-domain feature extraction. The time domain consists of mean, median, and variance. Fourier transform was used to analyze the frequency spectrum of EEG signals through the frequency-domain properties. The wavelet transforms the time and frequency domain. For EEG pattern classification, feedforward, backpropagation, multi-layer perception neural networks were used. The accuracy of the hidden layer in 25 neurons varied from 5.75 to 10.68%. Accuracy varied between 28.71 and 36.27% in the 32 submodels and the maximum accuracy of 40 neurons was 36.27%. The highest average accuracy of the hidden layer in 45 neurons was 94.04%. The side-by-side approach, which involves a large dataset being divided into a number of smaller datasets and submodels, built using the small datasets, increased the efficiency of authentication in all subjects. The highest average accuracy of the hidden layer in 45 neurons was 94.04%. However, when 45 neurons are used in the hidden layer, the complexity of the system increases and the training phase becomes more time-consuming.

In [24], person authentication with EEG was investigated using cost-effective portable devices. A technique was proposed for person authentication utilizing EEG signals acquired from ease gadgets. The EEG signal was first pre-processed to eliminate artifacts and noise with a bandpass finite impulse response (FIR) filter. The noise-minimized EEG signals were then split randomly into five parts. For EEG feature extraction, two multi-scale strategies were used: a multi-scale shape descriptor (MSD) and multi-scale wavelet packet statistics (MWPS). The first approach involved breaking down EEG fragments into four layers by decomposing a wavelet packet. For statistical characteristic extraction, sub-bands of brain impulses corresponding to delta, theta, alpha, beta, and gamma frequency bands were used. In the second procedure, at each sampling point of the EEG signal, a set of binary patterns were extracted. Based on restricted data, three segments of each EEG signal were used to train error-correcting output code (ECOC) multi-class model SVM classifiers, with the remaining two segments used to test the learned model. Using these functions, a supervised ECOC was eventually trained using an SVM classifier to classify individuals with EEG testing signals. The real positive rating of 94.44% for the suggested procedure indicated a tentative trial of nine EEG records from nine participants. This was a comprehensive study on cost-effective portable devices with minimal electrodes.

***Table 4**: Number of works per classifier.*

Machine Learning Algorithms	References
SVM	[50], [24], [56], [26], [46], [58], [44], [47], [28], [45], [29], [30]
Random forest	[23], [58], [29]
Bayesian network	[56]
Naive Bayes	[61], [25], [58]
KNN	[57], [43], [58], [29]
LDA	[57], [29]
ENN	[43]
CART	[29]
XGBoost	[29]
FRNN	[42]
MLP	[50], [32], [60], [43], [33], [44], [45]
CNN	[51], [34], [35], [52], [37], [38], [48]
LSTM	[51], [38], [40], [41]
RNN	[38]

In [25], the authors first estimate the separate components from five EEG brain regions, by obtaining a dominant independent component (DIC) for each region. independent component analysis (ICA) is a popular technique for blind source separation. A multivariate signal can be divided into additive sub-components, assuming the non-Gaussian source signals have relative statistical equality. The EEG data consists of electrical potential recordings on the scalp in a number of different places, and it is commonly accepted that these scalp recordings are simply linear mixtures of unknown underlying neural source activity. The auto-regressive (AR) scalar coefficients are then calculated as a feature collection with each DIC. A model of the DIC is provided using nonparametric auto-regression. The actual value of a time series can be estimated from the previous measurements of the same time series by a univariate AR model. In the EEG-based person authentication method, Naive Bayes models for decision-making are implemented due to their flexibility and efficiency in real-world applications. Since the order of the AR model influences the feature extraction process and hence the overall efficiency of the authentication method, error rates are found at multiple orders. These error rates are obtained at optimum thresholds.

The brain signals generated during various imaginary tasks are used for authentication in [26]. It was observed that, while capturing EEG signals, the subjects performed four mental imaging tasks consisting of baseline measurement, referential limb movement, counting, and rotation. Each electrode extracted three sets of characteristics: sixth-order AR coefficients, spectral density, and total power in five frequency bands. Six AR coefficients were used as proposed for EEG classification in [27]. Specifically, biologically significant bands and spectral powers were used to obtain brain activity. The extracted features include AR coefficient, power spectral density (PSD), spectral power, interhemispheric power difference, and interhemispheric channel linear complexity. These feature sets were integrated into a vector which is then used for classification by a linear SVM with cross-validation. Four separate mental tasks were performed by each subject, with the images captured at 128 Hz. To obtain six AR coefficients, the sixth-order AR model was used on the filtered data. Feature vector classification was carried out using a one-vs-all linear SVM, with the aim of reducing false accept rates (FARs) and false reject rates (FRRs). For each block, the FAR and FRR values were computed and then summed over the 15 folds. Finally, to achieve the half total error rate (HTER), the average of FAR and FRR values were computed.

In [28], the impact of various feature extractors on authentication accuracy is investigated. Four different entropies: fuzzy, approximate, sample, and spectral were con sidered. A total of 16 subjects were seated on armless chairs in front of display systems. The subjects were shown a random sequence of self-images and non-self-images and asked to identify their own images. The EEG data were collected using a 32-electrodes EEG headset. After applying feature extractors and feature selection based on Fisher distance, the number of features selected varied from 21 to 22 depending on the entropies used. The EEG of the forehead area was more orderly when the self-images were shown to the subjects. All entropies were higher for the self-image compared to non-self-image. The SVM classifier with linear, polynomial, sigmoid, and radial-based kernels was used to identify a subject. The fuzzy entropy was found to provide the highest classification accuracy of 90.7%.

To avoid the impact of variability on the EEG over time and the cognitive state of a person, a multimodal authentication system is proposed combining EEG and keystroke statistics in [29]. The EEG and keystroke statistics were collected when the subject typed a specific password, namely “qu-ELEC371”. A total of 45 features were extracted from the keystrokes. In contrast, the EEG contained 206 features, consisting of 27 frequency domains, 11 statistical, and three time-domain features in each channel. From a total of 251 features, 88 were selected based on correlation coefficients and random forest classifiers. A variety of classifiers were used such as random forest, linear discriminant analysis (LDA), linear SVM (LSVM), quadrature-enhanced SVM (QSVM), KNN, classification and regression tree (CART), and XG-Boost. Although feature selection improved the computational overhead, it reduced the authentication accuracy rather than increasing it. Up to 99.8% authentication accuracy was found when multimodal authentication was used, while 99.5 and 95.8% accuracy were achieved when keystrokes and EEG were considered individually, respectively. The highest accuracy was observed with the XGBoost classifier. In practice, each user has a different password, thereby increasing the dissimilarity in keystroke statistics. This may adversely affect the authentication accuracy.

An investigation was carried out in [30] to find EEG channels for use in person authentication. The 26 subjects in the study were asked to look at a letter on the screen and find it in the group of letters shown by the P300-speller system. If a subject can find the letter, he provides positive feedback. Otherwise, negative feedback is given. To capture the EEG generated by the activity, a 56-electrode EEG headset was used. For each channel, the first two intrinsic mode functions (IMFs) were separated using empirical mode decomposition (EMD). Thereafter, four features, namely instantaneous and Teager energy distribution, and Higuchi and Petrosian fractal dimension, were extracted from each IMF, resulting in 448 features. A subset of the best features was selected using the forward-addition or backward-elimination method [31] and SVM classifier. The positive feedback-related response was 4% more accurate compared to that of the negative feedback. The accuracy in the case of male-only was 1% higher than the female-only case. The number of channels varied for male-only and female-only cases, with nine and eight channels required, respectively. However, the set of channels differed significantly between male and female. The reduction in the number of channels had little impact on the accuracy of subject authentication.

3.1.2 Artificial neural networks with real activity

Eye activity was used in [32] for an individual biometric framework. Two separate datasets were used to construct an entity biometric system: eyes open (EO) and eyes closed (EC). The EEG signals were demonstrated utilizing two distinct classifiers: SVM and random forest. A feature selection process was then used to minimize the number of features and generate the necessary results to discover the ideal element measurement. Information on the signal processing technique used in the preparation of the raw signals and features extracted prior to classification were provided for signal processing and classification. SVM training was performed on the EEG data in EO and EC scenarios independently. In the first scenario, the subjects had their eyes open and closed or resting in the second scenario. In this case, only the variation of the statistical features from the EEG signals with a combination of the gamma band was considered. The feature vector consisted of three features: mean (M), mean square (RMS), and standard deviation (SD) of the signals. The EO scenario achieved maximum accuracy with the random forest classifier.

In [33], the authors propose a technique for utilizing VEP signals when an image is shown to the subjects during the recording of the EEG. Exploiting the spectral power ratio of the VEP gamma band, the backpropagation neural network was used to authenticate a person. The VEP signals were collected from subjects when shown a single image. Each channel of the VEP signals was separated utilizing a zero-stage Butterworth bandpass digital filter. A multi-layer perceptron neural network with a single hidden layer trained by the backpropagation calculation was used to classify the VEP spectral power ratio. The trained network provided average accuracy of 99.06%, indicating that the VEP signals conveyed hereditary explicit data and were appropriate for designing biometric systems. The normal layout execution of 99.06% implies that VEP designs can be ordered into their related classifications accurately. However, the preparation of VEPs can take longer than other biometrics such as fingerprints.

Systematic research is carried out in [34] to investigate the possibility of merging ConvNet and steady-state visual-evoked potentials (SSVEP) with a user authentication system. The low-frequency elements of the SSVEP were used as biometric patterns. The discriminating capacities were tested through various parameter settings to refine the CNN model. The effect of the EEG data duration on authentication efficiency was also studied. The authors then integrated the low-frequency element of the SSVEPs with 40 target stimuli for further study. As a result, each subject had 240 SSVEP epochs (trials) with 600 epochs between the first and second sessions. The proposed system achieved 97% accuracy on a cross-day basis for user authentication among eight persons, demonstrating EEG-based biometric CNN-based brain decoding. This paper proposes and develops an EEG-based user authentication framework, using SSVEP brain responses and CNN- based decoding.

As can be observed from the foregoing, CNN is widely used in user authentication. In [35], the authors propose a CNN method for EEG-based person authentication. They review CNN's performance on datasets involving one driving fatigue experiment with 100 subjects. The input of raw EEG data was used in CNN, thus decreasing the need for feature engineering. A wide selection of EEG datasets was tested for CNN, involving 100 subjects from one particular BCI driving fatigue task. The EEG data produced by conducting a BCI experiment, referred to as the BCIT experiment Baseline Driving (XB Driving) [36], was used in this paper. For target prediction, deep learning (DL) models, specifically CNN approaches, were studied in RSVP tasks. The CNN architecture comprised dense convolutional layers accompanied by fully connected layers. Each convolutional layer was connected by many kernals to input data (vectorized EEG). These filters were designed to collect a range of local spatial characteristics. is the authors suggest that fewer cases exist on use of biometric identification based on EEG. The CNN model was found to be very fast and capable of providing 97% accuracy in the case of 100 subjects. The accuracy of the authentication was demonstrated to be much higher than that of randomly selected epochs (90%).

In [37], the authors investigate the performance of CNN for EEG-based person authentication with a larger number of subjects. CNN has recently been used as a new tool for biometric automatic feature extraction and classification. A total of 33 healthy subjects participated in the experiment in this paper, with P300 speller being introduced [37]. The results show that the CNN-based biometric achieves 99.9% accuracy for eight classes, 99.3% for 10 classes, and 99.3% for 13 classes. The authors fine-tuned the network structure of the 10-class and 13-class classifications. The convergence speed of the network was also improved, while the time to achieve the best classification model was reduced by changing the CNN structure. It also ensured that the accuracy and loss functions do not change significantly.

Rather than considering the brain signals produced by the different imaginary and non-imaginary movement of different organs, emotions are used for individual identification using EEG in [38]. Human emotions were extracted as the primary nature of feelings from facial expressions. EEG can be used to illustrate feelings since human reactions are related to cortical functions. Emotion-related signals include contextual temporal dependencies. Research on person authentication allows one to achieve a better knowledge of the output between various affective states of personal identity. This research mainly focused on the DEAP EEG dataset [39], an emotion processing dataset of EEG, video, and physiological signals for emotion analysis. A deep neural network is proposed in this study using a combination of CNNs and recur rent neural networks (RNNs). There are two kinds of RNN: the CNN long short-term memory (LSTM) and the CNN-gated recurrent unit (CNN-GRU). Both CNN-LSTM and CNN-GRU have been found to achieve person authentication accuracy of 99.9–100%. However, the CNN-GRU can achieve faster convergence.

For more productive differentiation between people, the authors in [40] merge the SSVEP and event-related potential (ERP) features and apply LSTM networks to analyze the data extracted from the EEG signal. To differentiate between individuals and apply the LSTM network for study, the SSVEP and ERP functions were incorporated. The proposed technique was subdivided into three steps. The raw EEG data were obtained from 20 people with a 7.5 Hz square SSVEP stimulant in the image set proposed by Snodgrass and Vanderwart as targeted and non-targeted ERP stimulation. The raw data were then filtered using a passband notch filter, and the eye blinking artifacts eliminated. Deep learning was used to construct the latest form of individual EEG authentication. Through the use of LSTM SSVEP and ERP functionality, this system was able to achieve a decent 91.44% verification accuracy. A broader selection of users with ordinary eyes and brains can use the method. The successful results obtained in this paper would not only encourage the automatic authentication technique to become more robust and impersonation-tolerant but provide a building block to expand related studies.

An EEG-based user authentication technique applying multiple machine learning algorithms is proposed in [41]. A total of 105 subjects were seated before a display screen with instruction given to either tighten or relax the fists of both hands. They were also asked to imagine these activities. There were three sessions, each consisting of seven trials. The 21 trials were then converted into 105 trials using the sliding window technique. Three different sets of electrodes were used: 8, 16, and 64. To reduce complexity, the EMD was exploited to select the first four EMFs, since these contain the most information. Two-stage feature selection was then performed. Firstly, 18 features were extracted using the following entropies: log, approximate, sample, and Shannon. Subsequently, three different machine learning techniques neural network, visual geometry group (VGG), and principal component analysis (PCA), were independently used to select two features for each channel. The resulting features are input into the SVM classifiers. The highest accuracy (95.64%) is achieved by the SVM classifier with PCA feature selection and 64 electrodes. The VGG neural network gives the worst performance. The computation complexity is comparatively high in this method because it involves several processing steps such as feature extraction, a PCA, neural network, VGG neural network, and SVM.

The authentication systems discussed here require retraining when new data are added to the dataset, which is quite common in practical application. Furthermore, significant memory space is required to store the datasets. To overcome this limitation, an incremental fuzzy-rough nearest neighbor (IncFRNN) base classifier is proposed in [42] combining the concept of the fuzzy set theory and rough set theory. The objective of this paper is to properly handle the uncertainty involved in EEG. Data were collected from 37 subjects by asking them to identify their own password in the display system. A total of 405 features were extracted using wavelet packet decomposition, mean of amplitude, cross-correlation, coherence, and Hjorth parameter. The IncFRNN technique outperformed the incremental KNN in terms of area under the receiver operating characteristic (ROC) curve in both unlimited and predefined instances in the dataset. However, the IncFRNN was found to be less accurate than the incremental KNN.

3.1.3 Mixed machine learning algorithm with real activity

In [43], a new framework for establishing VEP-based biometrics is proposed. A total of 3560 VEP signals were obtained from 102 subjects. There were at least 10 VEP signals from each subject with a maximum of 50 eye squints free. Three unique examinations were carried out on features created by the selection metrics, and the enhanced features of the proposed technique. Two classifiers were utilized: Elaman neural network (ENN) and KNN. For correlation, KNN was selected since it does not require any training. Training was conducted utilizing nine feature vectors, and testing carried out utilizing the remainder of the set. ENN order exhibitions tend to be somewhat better than KNN and demonstrate validity for all distinctive utilized component extraction techniques. In terms of computational overhead, ENN appears to be much more algorithmically difficult than KNN and needs long-term analysis during training, due to the process taking much longer. Conversely, KNN requires no unequivocal training. However, a significant drawback of KNN is its high computational complexity in the testing phase, since characterizing a test VEP feature vector requires the distance of all VEP features used for training to be determined. The examination in this study [43] revealed the capability of prevailing recurrence powers in gamma band VEPs as biometrics.

A quite interesting investigation is carried out in [44] concerning the impact of time variance on the authentication accuracy. The contribution can be divided into two parts. In the first part, the impact of different feature selection techniques were investigated such as discrete Fourier transform (DFT), zero-crossing rate (ZCR), and Hjorth. It was found that DFT provided the highest classification accuracy, possibly because a total of 180 features were extracted from DFT, with only four and 12 from ZCR and Hjorth, respectively. The impact of the number of electrodes on subject classification accuracy was also investigated. Higher accuracy was observed with more electrodes. In addition, as a classifier the DNN outperforms SVM. The tasks considered included relaxation and listening to music. Relaxation provided the highest accuracy. In the second part, 10 subjects were considered. EEG data were collected on two occasions from each subject for three different tasks with a time gap of 1–2 weeks. An astounding result was revealed. The authentication accuracy dropped dramatically. The highest accuracy of 52.72% was obtained by SVM, while the DNN provided 47.64%. The EEG data were found to be inconsistent over time.

Most of the papers described so far use EEG, produced either by actual movement or the motor movement imagery of body parts. In addition, a significant number of papers consider visual stimuli [28]. A different approach is considered in [45] where the EEG produced by displaying a shape is used to authenticate subjects. Twenty subjects participated in the experiment. They were told to identify the existence of a black circle above a red plus sign. A varying degree of contrast was used in the circle: 0% (indicating the absence of a circle), 5%, 10%, and 100%. All subjects failed to perceive the presence of a circle when 5% contrast was used. Four features were extracted based on the power spectra of the α, low β, high β, and γ bands. A headset containing four electrodes was used to capture the EEG. The electrodes were positioned at O1, O2, P7, P8, covering the occipital region generating the responses to visual stimulation. Among the SVM and neural network, the equal error rate (EER) for SVM was 11.2%, obtained from the O2 electrode, while the neural network ensemble consisting of six neural networks provided an EER of 8.1% for the EEG obtained from E1. The EER from a single neural network was comparatively higher. The higher EER could have been due to its ability to overcome the impact of random weights in the first iteration of the individual neural network. The training complexity of the ensemble neural network would be very high since this system involves multiple neural networks. Pertinently, the EEG generated from this type of approach may not always be feasible in practice.

3.2 Authentication Using Motor Imagery Activity

This section presents the authentication techniques used when the EEG data are collected from motor imagery movement. In similarity to Section 3.1, this section is divided into three groups: (i) Authentication using traditional machine learning techniques; (ii) Artificial neural network; and (iii) Authentication using multiple machine learning techniques from groups (i) and (ii).

3.2.1 Traditional machine learning algorithm with imagery activity

In [46], the authors suggest that EEG can be used for authentication in multi-level security systems where users are asked to provide EEG authentication signals by executing motor imagery tasks. These activities can be single or mixed, based on the level of security required. The EEG-based authentication method has two phases: enrollment and verification. During the enrollment process, a person is asked to perform certain tasks, such as imagining moving their hand, foot, finger, or tongue, and recording the EEG signals. For authentication purposes, the imaging activities themselves are often part of the credentials and should not be accessed by any third party. After data selection, the EEG signals of each activity belonging to the user are pre-processed, the features extracted, and subsequently used to train the model for that individual, which is stored securely in the database. Security networks can have different levels, based on the regions and services of EEG-based authentication, and then adjusted according to the number of tasks assigned. AR models may be used with an EEG single-channel signal. The signal PSD is a positive number function of frequency factor analysis with a stationary stochastic operation. The linear AR parameters and PSD elements of these signals are derived as features. SVM uses the C-support vector classification (C-SVC) algorithm to find the optimum hyperplane. The SVM system is used to build individual EEG models. Experiments are carried out using five-fold cross-validation training. EEG-based authentication has been shown to provide all the benefits of password-based authentication.

Multimodal authentication using SVM is proposed in [47]. The EEG and eye tracking data were used from [48] and [49], respectively. The datasets were combined by considering the similarity of data to produce a fused dataset of hypothetical subjects. On the one hand, the EEG data for the fists of the left and right hands were collected from the motor movement imagery task. On the other hand, the eye tracking data were collected for the jumping dot stimulus task. Multimodal classification was found to provide much better performance compared to each mode (either EEG or eye tracking). The FAR of the multimodal authentication was less than half the FAR obtained from baseline EEG authentication. This improvement might be due to the increased features. The fused dataset has greater data diversity which may result in better FAR. The computational overhead is slightly lower since the SVM requires less computational overhead compared to neural network or KNN-based solutions.

3.2.2 Artificial neural networks with imagery activity

Many similar tasks are concurrently used for machine learning, all using a single-task classifier design and subsequent recognition. The benefit of this mechanism is that it incorporates data from extra activities. A complex problem is split into smaller problems by the traditional single-task learning (STL) mechanism in pattern recognition and machine learning. Each of the smaller tasks are trained separately before combining them together. Alternatively, multi-task learning (MTL) trains a variety of different tasks in sequence and may use latent domain-specific knowledge in additional tasks. Inspired by this, MTL is employed in [50] for user authentication purposes. In general, additional MTL tasks function as an inductive bias, leading a learner to choose the hypotheses that better describe the main task and the additional tasks simultaneously. EEG-based biometrics apply extra yet similar tasks to the existing neural network. The main task and extra tasks of common hidden layer representation incorporate the inductive bias of additional tasks, potentially benefiting the learning of the main task. Since a neural network with two layers of appropriate units can approximate every bounded continuous function, a neural network with one hidden layer was used for the experiments in [50]. EEG signals for imagining left and right index finger gestures were used independently for STL, with two precision tests obtained. In MTL, for training and enabling comparison, both signals were used. The output of the learning network was tested using each type of signal. Multiple related tasks were performed in parallel, with the generated outputs representing the results of the main and extra tasks, performed by one feedforward neural network. This paper compared the accuracy between STL and MTL in a small dataset of nine subjects. However, the real accuracy may be different when the number of subjects increases.

In [51], a new approach is introduced for the classification of EEG signals using a combination of CNN and LSTM. To improve the performance, one dimensional (1D) convolutional LSTM neural networks were used for CNN and LTSM. All the EEG biometrics of users were processed in a neural network of 1D-convolution LSTM, trained in the enrollment phase. The recorded EEG signal was pre-processed for normalization, either in the enrollment phase or during authentication, and segmented into 1-second normalized signal recordings before being sent to the 1D convolutional LSTM. This proposed network consisted of 10 layers with multiple convolutional layers, LSTM layers, and fully connected layers. For each training iteration, EEG segments were organized, shuffled, and randomly selected in batches. Each batch consisted of 80 sets of EEG samples, based on the number of channels. The network training was built to avoid over 1000 epochs or minimize the lack of training or validation. Since the performance of the proposed LSTM authentication system with 1D convolution depends heavily on parameter type, a trade-off is made to balance and improve the system's performance, cost, and effectiveness.

In order to address the reliability problem of the ongoing EEG biometrics, an investigation is carried out in [52] to provide more accurate and easier to use EEG biometric systems. A computational approach based on functional connectivity (FC) and CNN is suggested to ingest identity-bearing information from ongoing EEGs to help secure biometric EEGs against human states. The proposed approach combines a functional connectivity prediction module with a CNN-based deep learning module that learns discriminatory patterns from the FC maps predicted by the first module. The workflow of signal processing starts with bandpass filtering (0.5–42 Hz) and denoizing, followed by feature extraction and the classification of the two major modules. The authors compare their proposed approach with the common features and methods of EEG biometrics (those using EEG signals ongoing). Three features were chosen: AR model coefficients, spectral power density functions, and fuzzy entropy, each offered details of individual distinctiveness and incorporated these features to further improve performance. All three features were determined on the basis of the EEG from each single channel, also known as univariate features, due to their combined "united features." CNN was used as the classifier. CNN provides a higher correct recognition rate (CRR) than traditional classifiers such as shallow neural networks and SVMs within a fair com putation time. The suggested approach was evaluated on two datasets, namely the PhysioNet [53] and self-collected database. The latter included the EEG signals obtained from 109 subjects during motor imagery tasks.

The EEG varied significantly, depending on the mood of the subject. Furthermore, there was a temporal variation in the signal for the same mood. For this reason, the impact of temporal signal variation in person authentication based on the EEG signal is investigated in [48]. EEG data were collected from 50 subjects in response to their imagery movements of hands and legs. The data were collected using the Galileo BE Light amplifier system in two sessions with a one-week gap. Despite 19 electrodes being employed to capture the signals, two channels were excluded since the imagery EEG signals were generated in the parietal and central regions of the brain. Only the α band was considered due to it being the most widely used in motor imagery [55]. No feature selection and extraction algorithms were included since CNN itself can extract features from the different layers of row data. Importantly, in this paper, the CNN model was created using EEG signals captured in session 1, while the testing of the model was conducted using the signal captured in session 2. Consequently, this paper emphasizes on the effectiveness of EEG-based person authentication in a real-world situation. Up to 93.5% accuracy in identifying persons was found to be achievable when employing CNN.

3.3 Authentication Using Combined Real and Motor Imagery Activities

In this section, the authentication methods using both real and imagery activities during EEG recording are presented. In similarity to Sections 3.1 and 3.2, the authentication methods are divided according to the machine learning algorithms.

3.3.1 Traditional machine learning algorithm with combined activities

A single-channel-based authentication technique is proposed in [56], consisting of three steps: pre-processing, feature extraction, and classification. Features were extracted using DFT, discrete wavelet transform (DWT), AR modeling, and entropy. In this research, a dataset of five behavioral tasks was used to analyze seven participants (325 examples). The neural network, Bayesian classifier, and SVM were ordered for these features. Channel enhancement can produce better performance by decreasing the quantity of EEG channels and characterizing the ideal cathode arrangement for various mental exercises. Choosing a fitting channel with high precision for various errands is a significant part of authentication systems. Various classifiers such as SVM, Naive Bayes, and neural networks are used in [56] to achieve the optimal classifier. In this study, the highest accuracy was obtained for the single channel case by the neural network. The classification accuracy varied from 97 to 98% for the neural network classifier using a single channel validation framework.

The feasibility of implementing imaginary and non-imaginary tasks for user authentication is investigated in [57]. The participants were expected to execute non-imaginary tasks (left or right hand movements) and imaginary tasks (either left or right hand movements had to be imagined). The time allowed for each task was one minute, with one minute of rest between tasks. The bandpass filter was used to remove α and β waves during pre-processing. The signal was segmented and the power spectral density calculated by the Welch and Burg methods. The statistical characteristics derived from the PSD were used as classifier inputs (mean, medium, mode and variance, standard deviation, and minimum and maximum). For classification, KNN and LDA were applied. The Welch procedure provided the highest accuracy of 98% for β waves from channel C4 with the KNN classifier. The imaginary tasks provided 98.03% accuracy, which was higher when compared to 94.95% for the non-imaginary tasks. Thus, the imaginary function was found to be more suitable for authentication.

Instead of performing user authentication based on a single imagery activity as in [41], a combination of both actual and imagery actions are used in [58] to classify subjects. The experimental setup was similar to [41]. The subjects were seated on chairs with arm rests in front of a display system with visual instruction given to the subject in the performance of a particular task. Two tasks, namely hand lift and fist tightening, were performed with each hand in both actual action mode and imaginary action mode. The data were collected from 10 subjects using 32 channels on an EEG headset. However, only data from four channels were used for further processing due to the specific region of the brain being of interest. Prior to classification, the desired range of frequencies (0.1 Hz to 70 Hz) were extracted since this frequency range contained useful information. Wavlet transform was then used for noise removal. Only one feature, namely PSD, was extracted for each channel using Burg's method [59]. Finally, the data on actual and imagery actions were fed into a classifier (e.g., random forest, KNN, SVM, and Naive Bayes) separately for each subject. The highest accuracy was found by the random forest with imagery tasks. All eight tasks (two tasks for each hand in the case of actual action and imagery movement) were combined for multimodal analysis. In this case, the average accuracy was 98.28%. The computational burden in the case of random forest was comparatively less than that for the solutions using neural networks for classification.

3.3.2 Artificial neural networks with combined activities

Here, the EEG-based authentication techniques using neural networks for combined real and imagery activities are described. In [60], the impact of eyes-open and eyes-closed scenarios on the person authentication based on EEG signals is investigated. The signals for the subjects with eyes-closed and eyes-open states were recorded. The features were extracted utilizing the WPD and classified with neural networks. The EEG signals were gathered from 10 male participants while resting with their eyes open and eyes closed in five different meetings lasting about 14 days. Two channels recorded the EEG signals as the subjects sat for a moment with their eyes closed. The WDM was chosen since it can provide information both in time and frequency domains. The EEG segments were arbitrarily partitioned into training and testing sets with 90% and 10% of the data used for training and testing, respectively. The extracted features were then fed into the input layer of the neural network. Two hidden layers were utilized with 100 nodes in every layer. The eyes open and eyes closed features had no significant impact on the rate of correct personal identification. In this paper, only 10% of the dataset was used for testing the network. However, just 10% of the dataset may not represent the characteristics of the whole dataset. For this reason, the effectiveness of the technique proposed in [60] needs further investigation.

3.4 Traditional Machine Learning with no Activity

While most EEG-based authentication systems focus on increasing the level of accuracy, the usability and timeliness of the systems in practical scenarios are largely overlooked. Furthermore, all the above-mentioned authentication techniques use EEG recording during certain activities. Thus, a new system of authentication is proposed in [61] which is easy to implement in practical scenarios with low computational complexity. In this technique, the EEG signals are collected from users in a state of relaxation and sent to the respective user's smartphone. Considering the low processing power of smartphones and limited battery power, the authentication task is offloaded to a fog computing server located nearby. The Naive Bayes classifier was used in the fog server. Fast Fourier transform (FFT) was used for feature extraction only from the α band (which provides the best performance) of the EEG signal. The authentication accuracies were 81 and 95% when the EEG was operated for five seconds and 10 seconds, respectively.

From the above discussion, it is evident that considerable diversity exists in pre-processing EEG data prior to classification. Thus, Table 5 provides a comparison of the authentication techniques based on the type of pre-processing carried out. A detailed comparison of different machine learning algorithms for biometric authentication is presented in Table 6.

4. FUTURE RESEARCH DIRECTIONS

It is important to note that this is the first thorough investigation into the progress of machine learning assisted biometric authentication using brain waves. In contrast to other biometric methods, a relatively small number of experiments on the topic have been reported. Therefore, the scope for future research is considerable. Potential future research directions include:

- In [50], a multi-tasking-based biometric authentication technique is proposed involving a neural network with one hidden layer for classification. However, with the advancement of research on neural networks, we have entered the new domain of deep learning, leaving behind the notion of a shallow neural network. Deep learning appears to outperform the shallow neural network in all perspectives. Therefore, it would be interesting to perform multi-tasking-based biometric authentication using deep learning rather than the shallow neural network. There is also the potential to achieve better accuracy.

***Table 5**: Comparison of different papers based on pre-processing steps.*

Ref.	No. of Subjects	No. of EEG Channels	No. of Extracted Features	Feature Extraction Methods	EEG Bands	Type of Tasks
[50]	5	59	8	Common feature patterns [63]	α, β	Reading an unconnected list of words
[23]	32	6	15	Mean, standard deviation and entropy Wavelet packet decomposition (WPD) coefficient	All	Eyes open and closed
[32]	109	64	192	Mean, standard deviation, root mean square error	γ	Left hand movement and eyes open
[60]	10	8	168	Mean, standard deviation and entropy Wavelet packet decomposition (WPD) coefficient	All	Eyes
[24]	5	9	168	Multi-scale shape descriptor (MSD), multi-scale wavelet packet statistics (MWPS), multi-scale wavelet packet energy statistics (MWPES)	All (MSD, MWPS) α, β (MWPES)	Eyes close
[56]	7	6	85	DWT, log energy entropy, sample entropy, auto-regressive coefficients	All	Rest, math, visual counting, geometric figure rotation
[61]	10	1		FFT	α	Resting state
[57]	20	19	7	Statistical features of PSD	All	Eyes
[51]	109	4, 16, 32, 64	10240		γ	Motor movement for opening and closing fists and moving feet
[43]	10	61	61	Multiple signal classification (MUSIC)	γ	Image visualization
[33]	20	61	61	Spectral power ratio	All	Images of different objects
[25]	7	17	5	ICA	γ	Motion related activity in virtual environment
[26]	5	14	1358	AR, FFT, interhemispheric power difference, interhemispheric channel linear complexity	All	Different activities such as resting with eyes closed, limb movement, geometric figure rotation
[46]	9	5	99	FFT, AR	All	Motor imagery single and combined left and right hands
[34]	8	9			θ	Low frequency SSVEP from retina
[35]	100	256	1408	AR, FFT	All	In virtual reality environment, keeping in lane when driving of a car
[52]	109, 59	64, 46		AR, fuzzy entropy, PSD	α, β	Motor imagery due to fists or feet movement
[37]	33	20			All	Visualization of different English characters
[38]	32	5, 32	32, 496	PSD (Welch method), spectral coherence	$\alpha, \beta, \gamma, \theta$	To score subjective rating by watching a music video
[40]	20	7	2637		δ, θ	Image visualization, and facing flash light
[41]	105	8, 16, 64	16, 32, 128	EMD	All	Fist tightening or relaxation
[58]	10	4	4	PSD (Burg method)	α, β, γ	Actual movement and imagery movement (each hand lift, fist tightening)
[44]	20, 10	4	196	DFT, ZCR, Hjorth	All	Relax mode, listening to music, and counting numbers such as 2, 4, 8, ...
[47]	37	64	64	DFT, ZCR, Hjorth	All	Left and right hand motor movement imagery
[28]	16	32	30	Fisher distance	All	Viewing self and non-self images
[45]	20	4	4	Wavelet transform	α, β, γ	Viewing circles with varying (0 to 100%) contrasts
[29]	10	5	251	Statistical, time domain, frequency domain	All	Typing specific password
[42]	37	8	414	Mutual information, cross-correlation, coherence, and Hjorth parameter	α, β	Viewing own and others' passwords
[30]	26	56	448	EMD	All	Viewing a letter followed by finding that letter in a group of letters
[48]	40	17			α	Motor imagery movement of hands and legs

***Table 6**: Comparison of machine learning-based biometric authentication techniques.*

Ref.	Objective	Machine Learning Techniques	Accuracy	Computational Complexity	Dataset
[50]	EEG-based user identification and authentication	Feedforward backpropagation, multi-layer neural network	94.04%	Low complexity, high training time	[64]
[23]	Biometric user identification on from eye activity	SVM, Random Forest	SVM: EO-97.64%, EC-96.02% RF: EO-98.16%, EC-97.30%	Moderate	Experimental
[32]	Multiple related tasks are performed simultaneously	Two-layer neural network	Left-95.60%, Right-94.81%	Low complexity prediction, high training time	PhysioNet [53]
[60]	Human identification by EEG signal with four channels or less	Neural network	Eyes open 78%, Eyes closed 81%	Low complexity, high training time	Experimental
[24]	Human recognizable proof utilizing EEG signals	SVM	94.44%	Moderate	Experimental
[56]	Effect of electrode placement on authentication accuracy in the case of different mental states	Bayesian network, SVM	95%	Low	[65]
[61]	Mobile phone assisted EEG authentication	Naive Bayes	95%	Low	Experimental
[57]	Authentication using imagery and non-imagery tasks	KNN, LDA	94.95%	High complexity prediction, no training	Experimental
[51]	Authentication based on 1D convolutional LTSM	CNN, LSTM	99.58%	Low complexity, high training time	PhysioNet [53]
[43]	VEP-based biometric	KNN, ENN	KNN-96.13%, ENN-98.12%	High computational overhead in prediction	Experimental
[33]	Evoked brain signals to identify individuals	Back-propagation neural network	99.06%	Low complexity, high training time	Experimental
[25]	Independent component analysis-based authentication	Naive Bayes		Low	Experimental
[26]	EEG-based authentication with low cost	Linear SVM	100%	Low	Experimental
[46]	EEG authentication with multi-level security	SVM	Equal error rate: 0.002 to 0.007	Moderate	[66]
[34]	Extraction of low frequency SSVEP for user authentication	CNN	97%	Low complexity, high training time	[67]
[35]	EEG-based identification from driving fatigue experiment	CNN	97%	Low complexity, high training time	[36]
[52]	Stability of EEG biometrics across diverse human states	CNN	99.94%	Low complexity, high training time	PhysioNet [53]
[37]	Investigating the effects on subjects in experiments to assess CNN's identification performance	CNN	99.9%	Low complexity, high training time	Experimental
[38]	Person identification on affective EEG (e.g. the subject is in different states during the experiment)	CNN, RNN, CNN-LSTM	up to 97.97%	Complex	[39]
[40]	To combine SSVEP and ERP	LSTM	up to 91.44%	Long training time	Experimental
[41]	Finding appropriate feature extraction and selection algorithms for improving authentication using the SVM classifier	LSTM	91.44%	High complex in training	Experimental
[58]	Classifying subjects using different classifiers with multimodal input to the classifier	Random forest, KNN, SVM, Naive Bayes	98.28%	Comparatively less complex during the training phase, but more complex in the testing phase	Experimental

[44]	To investigate the effect of time variance on authentication accuracy	SVM, DNN	Time invariant test;
			SVM: 93.12%, DNN: 97.0%
			Time variant test;
			SVM: 51.72%, DNN: 47.64%
				For DNN, training complexity is very high, while testing complexity is extremely low	Experimental

[47]	To combine eye tracking and EEG for user authentication	SVM	98.28%	FAR: 23.6% (base-line EEG: 42.1%)	[48, 49]
[28]	To analyze the impact of different entropies as feature extractors for classifying subjects	SVM with linear, polynomial, radial basis and sigmoid kernels	90.7% with linear SVM and Fuzzy entropy	Moderate	Experimental
[45]	To investigate the im pact of the invisible visual stimuli on user authentication	SVM with linear, polynomial and radial basis kernels, neural networks	EER-SVM: 11.2% EER-NN: 8.1%	Low for SVM, very long training time for multiple NNs	Experimental
[29]	To authenticate a subject based on EEG and keystroke statistics	LSVM, QSVM, KNN, CART, XGBoost, Random forest, LDA	XGBoost: 99.8%	High	Experimental
[42]	To investigate the use of IncFRNN to adapt to changes in dataset size	FRNN	95.1%	Very high	Experimental
[30]	To develop a low-density EEG headset for person authentication	SVM	89% with five channels (mixed gender), 95% with nine channels (male only)	Moderate	Experimental
[48]	To assess the impact of the EEG recording session on the authentication accuracy	CNN	99.3%	Moderate	Experimental

- Similarly, deep learning can be applied in all authentication techniques which use shallow neural networks. The conventional CNN can be replaced by the deep CNN to investigate the corresponding classification accuracy.
- From a review of existing literature, only one machine learning technique seems to be used for classification in a particular paper. The algorithm can be any one of CNN, SVM, KNN, and so on. However, no classifier can provide the best solution to all problems [62]. Thus, a possible research direction could involve the identification of the best classification algorithm for a given biometric authentication scenario.
- The effect of a drug can change the electrical activities of the brain. This can also change the response of the brain with respect to different real and imagery activities. For this reason, an investigation is required into each brainwave-based authentication technique to assess the impact of drugs on the accuracy of machine learning-based authentication.
- Electrical activities in the brain change according to age. Thus, what is the impact of age on the accuracy of biometric authentication? Does an authentication algorithm achieve the same level of accuracy in older people as for children? All works discussed in this paper consider subjects within a very short age range. However, the age range is likely to be broad in practical applications. For this reason, a thorough investigation is required to assess the authentication accuracy in such a scenario.
- The combination of multiple types of activity is found to improve authentication accuracy. In addition, the use of other statistics, such as keystrokes as well as EEG, improves accuracy. However, the amount of effort made in this direction remains very limited. Thus, a more holistic approach could be considered involving the exploitation of facial expression, EEG, keystrokes, and other information in the authentication process.

5. CONCLUSION

EEG is a person-dependent signal, and the authentications methods presented in this paper indicate that the identification accuracy of a person using EEG signals is very promising. This paper gives an outline of machine learning assisted EEG-based biometric authentication methods. The investigation process and outcomes found in each paper have been thoroughly discussed. In addition, various papers have been compared using different criteria such as objectives, classifiers, feature extraction methods, number of channels, computational overheads, type of tasks, and so on. The findings of this investigation reveal that the following machine learning classification algorithms are widely used in brainwave-based biometric authentication: CNN, MLP, SVM, KNN, RNN, LSTM, FRNN, BLSTM. Of these, CNN and SVM are the most commonly used algorithms and provide comparatively high classification accuracy. Furthermore, there are a limited number of publicly available datasets for this type of research, and hence, researchers prefer to generate their own data experimentally. This paper offers in-depth knowledge of state-of-the-art biometric authentication techniques and opens a path for future research.

ACKNOWLEDGMENTS

This work is supported by Research Grants from Begum Rokeya University, Rangpur, Bangladesh (Reference: BRUR/Reg./2020–21/669(11)).

REFERENCES

[1] "Authentication Definition," TechTerms.com. https://techterms.com/definition/authentication (accessed Jan. 4, 2021).

[2] "What is 'Authentication'," The Economic Times. https://economictimes.indiatimes.com/definition/authentication (accessed Jan. 4, 2021).

[3] L. Norton *et al.*, "Electroencephalographic recordings during withdrawal of life-sustaining therapy until 30 minutes after declaration of death," *Canadian Journal of Neurological Sciences / Journal Canadien des Sciences Neurologiques*, vol. 44, no. 2, pp. 139–145, Oct. 2016.

[4] "EEG (Electroencephalogram)," KidsHealth. https://kidshealth.org/en/parents/eeg.html (accessed Jan. 7, 2021).

[5] Britannica, The Editors of Encyclopaedia. "electroencephalography," Encyclopedia Britannica, Oct. 31, 2017. https://www.britannica.com/science/electroencephalography (accessed Jan. 4, 2021).

[6] J. W. C. Medithe and U. R. Nelakuditi, "Study of normal and abnormal EEG," in *2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2016.

[7] S. Siuly, Y. Li, and Y. Zhang, *EEG Signal Analysis and Classification: Techniques and Applications*. Cham, Switzerland: Springer, 2016, ch. 1, pp. 11–14.

[8] A. S. Malik and H. U. Amin, *Designing EEG Experiments for Studying the Brain: Design Code and Example Datasets*. London, UK: Academic Press, 2017, ch. 1, p. 4.

[9] M. L. Ali, J. V. Monaco, C. C. Tappert, and M. Qiu, "Keystroke biometric systems for user authentication," *Journal of Signal Processing Systems*, vol. 86, pp. 175–190, Mar. 2016.

[10] O. S. Adeoye, "A survey of emerging biometric technologies," *International Journal of Computer Applications*, vol. 9, no. 10, pp. 1–5, Nov. 2010.

[11] S. P. Banerjee and D. Woodard, "Biometric authentication and identification using keystroke dynamics: A survey," *Journal of Pattern Recognition Research*, vol. 7, no. 1, pp. 116–139, 2012.

[12] H. Crawford, "Keystroke dynamics: Characteristics and opportunities," in *2010 Eighth International Conference on Privacy, Security and Trust*, 2010, pp. 205–212.

[13] M. Karnan, M. Akila, and N. Krishnaraj, "Biometric personal authentication using keystroke dynamics: A review," *Applied Soft Computing*, vol. 11, no. 2, pp. 1565–1573, Mar. 2011.

[14] R. Napier, W. Laverty, D. Mahar, R. Henderson, M. Hiron, and M. Wagner, "Keyboard user verification: toward an accurate, efficient, and ecologically valid algorithm," *International Journal of Human-Computer Studies*, vol. 43, no. 2, pp. 213–222, Aug. 1995.

[15] D. Shanmugapriya and G. Padmavathi, "A survey of biometric keystroke dynamics: Approaches, security and challenges," *International Journal of Computer Science and Information Security*, vol. 5, no. 1, pp. 115–119, Sep. 2009.

[16] Z. Rui and Z. Yan, "A survey on biometric authentication: Toward secure and privacy-preserving identification," *IEEE Access*, vol. 7, pp. 5994–6009, 2019.

[17] N. Ortiz, R. D. Hernandez, R. Jimenez, M. Mauledeoux, and O. Aviles, "Survey of biometric pattern recognition via machine learning techniques," *Contemporary Engineering Sciences*, vol. 11, no. 34, pp. 1677–1694, 2018.

[18] P. Harington, *Machine Learning in Action.* New York, USA: Manning Publication, 2012.

[19] S. Shalev-Shwartz and S. Ben-David, *Understanding Machine Learning: From Theory to Applications.* New York, USA: Cambridge University Press, 2014, pp. 124–126.

[20] T. M. Oshiro, P. S. Perez, and J. A. Baranauskas, "How Many Trees in a Random Forest?," in *Machine Learning and Data Mining in Pattern Recognition*, P. Perner, Ed. Berlin, Germany: Springer, 2012, pp. 154–168.

[21] J. Brownlee, *Deep Learning for Computer Vision: Image Classification, Object Detection, and Face Recognition in Python.* Machine Learning Mastery, 2019.

[22] M. Mohri, A. Rostamizadeh, and A. Talwalkar, *Foundations of Machine Learning*, 2nd ed. Cambridge, UK: The MIT Press, 2018, pp. 79–83.

[23] Q. Gui, Z. Jin, and W. Xu, "Exploring EEG-based biometrics for user identification and authentication," in *2014 IEEE Signal Processing in Medicine and Biology Symposium (SPMB)*, 2014.

[24] M. K. Bashar, I. Chiaki, and H. Yoshida, "Human identification from brain EEG signals using advanced machine learning method EEG-based biometrics," in *2016 IEEE EMBS Conference on Biomedical Engineering and Sciences (IECBES)*, 2016, pp. 475–479.

[25] C. He and J. Wang, "An independent component analysis (ICA) based approach for EEG person authentication," in *2009 3rd International Conference on Bioinformatics and Biomedical Engineering*, 2009.

[26] C. Ashby, A. Bhatia, F. Tenore, and J. Vogelstein, "Low-cost electroencephalogram (EEG) based authentication," in *2011 5th International IEEE/EMBS Conference on Neural Engineering*, 2011, pp. 442–445.

[27] A. Lecko and Y. J. Sim, "Coefficient problems in the subclasses of close-to-star functions," *Results in Mathematics*, vol. 74, May 2019, Art. no. 104.

[28] Z. Mu, J. Hu, J. Min, and J. Yin, "Comparison of different entropies as features for person authentication based on EEG signals," *IET Biometrics*, vol. 6, no. 6, pp. 409–417, Apr. 2017.

[29] A. Rahman *et al.*, "Multimodal EEG and keystroke dynamics based biometric system using machine learning algorithms," *IEEE Access*, vol. 9, pp. 94 625–94 643, 2021.

[30] L. A. Moctezuma and M. Molinas, "Event-related potential from EEG for a two-step identity authentication system," in *2019 IEEE 17th International Conference on Industrial Informatics (INDIN)*, 2019.

[31] L. Moctezuma and M. Molinas, "Subject identification from low-density EEG-recordings of resting-states: A study of feature extraction and classification," in *Advances in Information and Communication*, K. Arai and R. Bhatia, Eds. Cham, Switzerland: Springer, 2020, pp. 830–846.

[32] B. Kaur and D. Singh, "Neuro signals: A future biomertic approach towards user identification," in *7th International Conference on Cloud Computing, Data Science & Engineering – Confluence*, 2017, pp. 112–117.

[33] R. Palaniappan, "Method of identifying individuals using VEP signals and neural network," *IEE Proceedings - Science, Measurement and Technology*, vol. 151, no. 1, pp. 16–20, Jan. 2004.

[34] T. Yu, C.-S. Wei, K.-J. Chiang, M. Nakanishi, and T.-P. Jung, "EEG-based user authentication using a convolutional neural network," in *2019 9th International IEEE/EMBS Conference on Neural Engineering (NER)*, 2019, pp. 1011–1014.

[35] Z. Mao, W. X. Yao, and Y. Huang, "EEG-based biometric identification with deep learning," in *8th International IEEE/EMBS Conference on Neural Engineering (NER)*, 2017, pp. 609–612.

[36] J. Touryan, G. Apker, B. J. Lance, S. E. Kerick, A. J. Ries, and K. McDowell, "Estimating endogenous changes in task performance from EEG," *Frontiers in Neuroscience*, vol. 8, Jun. 2014, Art. no. 155.

[37] Y. Di, X. An, S. Liu, F. He, and D. Ming, "Using convolutional neural networks for identification based on EEG signals," in *10th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC)*, 2018, pp. 119–122.

[38] T. Wilaiprasitporn, A. Ditthapron, K. Matchaparn, T. Tongbuasirilai, N. Banluesombatkul, and E. Chuangsuwanich, "Affective EEG-based person identification using the deep learning approach," *IEEE Transactions on Cognitive and Developmental Systems*, vol. 12, no. 3, pp. 486–496, Sep. 2020.

[39] S. Koelstra, C. Muhl, M. Soleymani, J.-S. Lee,

A. Yazdani, T. Ebrahimi, T. Pun, A. Nijholt, and I. Patras, “DEAP: A database for emotion analysis using physiological signals,” *IEEE Transactions on Affective Computing*, vol. 3, no. 1, pp. 18–31, Jan. 2012.

[40] S. Puengdang, S. Tuarob, T. Sattabongkot, and B. Sakboonyarat, “EEG-based person authentication method using deep learning with visual stimulation,” in *11th International Conference on Knowledge and Smart Technology (KST)*, 2019, pp. 6–10.

[41] U. Barayeu, N. Horlava, A. Libert, and M. V. Hulle, “Robust single-trial EEG-based authentication achieved with a 2-stage classifier,” *Biosensors*, vol. 10, no. 9, Sep. 2020, Art. no. 124.

[42] S.-H. Liew, Y.-H. Choo, Y. F. Low, and Z. I. M. Yusoh, “EEG-based biometric authentication modelling using incremental fuzzy-rough nearest neighbour technique,” *IET Biometrics*, vol. 7, no. 2, pp. 145–152, Mar. 2018.

[43] R. Palaniappan and D. P. Mandic, “Biometrics from brain electrical activity: A machine learning approach,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 738–742, Apr. 2007.

[44] F. P. Sjamsudin, “EEG-based authentication with machine learning,” M.S. thesis, Department of Computer Science and Communications Engineering, Waseda University, Tokyo, Japan, 2017.

[45] T. Miyake, N. Kinjo, and I. Nakanishi, “Wavelet transform and machine learning-based biometric authentication using EEG evoked by invisible visual stimuli,” in *IEEE Region 10 Conference (TENCON)*, 2020.

[46] T. Pham, W. Ma, D. Tran, P. Nguyen, and D. Phung, “EEG-based user authentication in multilevel security systems,” in *Advanced Data Mining and Applications*, H. Motoda, Z. Wu, L. Cao, O. Zaiane, M. Yao, and W. Wang, Eds. Berlin, Germany: Springer, 2013, pp. 513–523.

[47] V. Krishna, Y. Ding, A. Xu, and T. Höllerer, “Multimodal biometric authentication for VR/AR using EEG and eye tracking,” in *2019 International Conference on Multimodal Interaction*, 2019.

[48] R. Das, E. Maiorana, and P. Campisi, “Motor imagery for EEG biometrics using convolutional neural network,” in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2018, pp. 2062–2066.

[49] P. Kasprowski, O. V. Komogortsev, and A. Karpov, “First eye movement verification and identification competition at BTAS 2012,” in *2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, 2012.

[50] S. Sun, “Multitask learning for EEG-based biometrics,” in *2008 19th International Conference on Pattern Recognition*, 2008.

[51] Y. Sun, F. P.-W. Lo, and B. Lo, “EEG-based user identification system using 1d-convolutional long short-term memory neural networks,” *Expert Systems with Applications*, vol. 125, pp. 259–267, Jul. 2019.

[52] M. Wang, J. Hu, and H. Abbass, “Stable EEG biometrics using convolutional neural networks and functional connectivity,” *Australian Journal of Intelligent Information Processing Systems*, vol. 15, no. 3, pp. 19–26, 2019.

[53] G. Schalk, D. McFarland, T. Hinterberger, N. Birbaumer, and J. Wolpaw, “BCI2000: A general-purpose brain-computer interface (BCI) system,” *IEEE Transactions on Biomedical Engineering*, vol. 51, no. 6, pp. 1034–1043, Jun. 2004.

[54] B. J. Edelman, B. Baxter, and B. He, “EEG source imaging enhances the decoding of complex right-hand motor imagery tasks,” *IEEE Transactions on Biomedical Engineering*, vol. 63, no. 1, pp. 4–14, Jan. 2016.

[55] M. Zeynali and H. Seyedarabi, “EEG-based single-channel authentication systems with optimum electrode placement for different mental activities,” *Biomedical Journal*, vol. 42, no. 4, pp. 261–267, Aug. 2019.

[56] T. Z. Chin, A. Saidatul, and Z. Ibrahim, “Exploring EEG based authentication for imaginary and non-imaginary tasks using power spectral density method,” *IOP Conference Series: Materials Science and Engineering*, vol. 557, 2019, Art. no. 012031.

[57] A. Valsaraj, I. Madala, N. Garg, M. Patil, and V. Baths, “Motor imagery based multimodal biometric user authentication system using EEG,” in *2020 International Conference on Cyberworlds (CW)*, 2020.

[58] T. Thorvaldsen, “A comparison of the least squares method and the Burg method for autoregressive spectral analysis,” *IEEE Transactions on Antennas and Propagation*, vol. 29, no. 4, pp. 675–679, Jul. 1981.

[59] M. K. Abdullah, K. S. Subari, J. L. C. Loong, and N. N. Ahmad, “Analysis of the EEG signal for a practical biometric system,” International Journal of Biomedical and Biological Engineering, vol. 4, no. 8, pp. 364–368, 2010.

[60] J. Sohankar, K. Sadeghi, A. Banerjee, and S. K. Gupta, “E-Bias: A pervasive EEG-based identification and authentication system,” in *Proceedings of the 11th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, 2015, pp. 165–172.

[61] D. H. Wolpert, “The lack of a priori distinctions between learning algorithms,” *Neural Computation*, vol. 8, no. 7, pp. 1341–1390, Oct. 1996.

[62] J. Müller-Gerking, G. Pfurtscheller, and H. Flyvbjerg, “Designing optimal spatial filters for single-trial EEG classification in a movement task,” *Clinical Neurophysiology*, vol. 110, no. 5, pp. 787–798, May 1999.

[63] P. Sajda, A. Gerson, K.-R. Muller, B. Blankertz, and L. Parra, “A data analysis competition to evaluate machine learning algorithms for use in brain-computer interfaces,” *IEEE Transactions on Neural*

Systems and Rehabilitation Engineering, vol. 11, no. 2, pp. 184–185, Jun. 2003.

[64] X. Bao, J. Wang, and J. Hu, "Method of individual identification based on electroencephalogram analysis," in *2009 International Conference on New Trends in Information and Service Science*, 2009, pp. 390–393.

[65] J.-F. Hu, "Biometric system based on EEG signals by feature combination," in *2010 International Conference on Measuring Technology and Mechatronics Automation*, 2010, pp. 752–755.

[66] X. Chen, Y. Wang, M. Nakanishi, X. Gao, T.-P. Jung, and S. Gao, "High-speed spelling with a noninvasive brain–computer interface," *Proceedings of the National Academy of Sciences*, vol. 112, no. 44, pp. E6058–E6067, Oct. 2015.

Tarik Bin Shams received his B.Sc. degrees in computer science and software engineering from American International University-Bangladesh (AIUB). Currently, he is studying M.Sc. in Computer Science and Engineering at Brac University, Bangladesh. From 2021, he works as a Software Developer in Deepchain Labs Ltd, Bangladesh. As a Software Developer, he contributes to developing many local and global projects. In addition to his current duties, he did research on machine learning techniques and integrated them into several projects.

Md. Sakir Hossain received the B.Sc. and M.Sc. degrees in information and communication engineering from University of Rajshahi, Bangladesh, and the Ph.D. degree in information and computer science from Saitama University, Saitama, Japan. In 2019, he worked as a Postdoctoral Researcher with Czech Technical University in Prague, Prague, Czech Republic. As a postdoctoral researcher, he did research in interference management for the unmanned aerial vehicle (UAV) assisted wireless networks. He currently works as an Assistant Professor with the Department of Computer Science, American International University-Bangladesh (AIUB), Bangladesh. He works on the development of solutions for wireless networks with a special focus on UAV-assisted wireless networks, intelligent reflecting surfaces, machine learning-assisted wireless networks, malware analysis, and intrusion detection systems.

Md. Firoz Mahmud received his B.Sc. in Computer Science and Engineering from American International University-Bangladesh (AIUB). Between Aug. 2021 and Feb. 2022, he worked as a web developer at Prajukti 71, Bangladesh. Furthermore, Mr. Mahmud worked as a Teaching Intern at AIUB from Feb. 2020 to July 2020. His research interest include Machine learning and Bio-Signal Processing.

Md. Shahariar Tehjib received a B.Sc. degree in computer science and engineering from American International University-Bangladesh (AIUB), Dhaka, Bangladesh. He completed his secondary school certificate from Fulbari G.M pilot high school, Fulbari, Dinajpur, Bangladesh, and the higher secondary certificate from Fulbari Govt. College, Fulbari, Dinajpur, Bangladesh. Currently, he is working as a web developer. In addition, he works in Artificial intelligence, machine learning, and cyber security system.

Zahid Hossain received a B.Sc. in Computer science and Software Engineering from American International University-Bangladesh (AIUB), Bangladesh. In 2021, he worked as an online medicine shop business analyst. He also completed the Digital Marketing course.

Md. Ileas Pramanik received a Ph.D. in Information Systems from City University of Hong Kong in 2018. He is currently an Associate Professor of the Computer Science and Engineering Department, Begum Rokeya University, Rangpur, Bangladesh. His research interest includes data privacy, security, Big data analytics, Network complexity, and privacy.