IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 10 February 2023, accepted 23 February 2023, date of publication 6 March 2023, date of current version 10 March 2023.

*Digital Object Identifier 10.1109/ACCESS.2023.3253026*

SURVEY

# A Review of EEG-Based User Authentication: Trends and Future Research Directions

**CHRISTOS A. FIDAS[1] AND DIMITRIOS LYRAS[2], (Senior Member, IEEE)**
[1]Department of Electrical and Computer Engineering, University of Patras, 26504 Patras, Greece
[2]Athens 13121, Greece

Corresponding author: Christos A. Fidas (fidas@upatras.gr)

This work was supported in part by the Hellenic Foundation for Research and Innovation (HFRI) under the 2nd Call for Proposals for HFRI Research Projects to Support Faculty Members and Researchers under the Project Entitled Electroencephalography and Eye Gaze Driven Framework for Intelligent and Real-Time Human Cognitive Modeling (CogniX) under Grant 3849, and in part by Erasmus + CREAMS Project under the Call KA220-HED-Cooperation Partnerships in Higher Education [Greek State Scholarship's Foundation (IKY)] under Project KA220-HED-E06518FA.

**ABSTRACT** Recently, the use of Electroencephalography (EEG) in scientific research on User Authentication (UA) has led to cutting-edge experiments that seek to identify and authenticate individuals based on their brain activity in particular usage scenarios. Utilizing EEG signals, derived from brain activity, might provide innovative solutions to contemporary security issues in traditional knowledge-based user authentication, including the threat of shoulder surfing. In this review paper, we analyze 108 different EEG-based user authentication experiments based on the following perspectives: a) the user experimental setup, with an emphasis on the applied EEG- protocols; b) the artificial intelligence techniques employed and finally c) the security and privacy preservation aspects. The reviewed papers cover a broad time frame from 1998 to 2022 and include various experimental protocols and algorithms used for classifying EEG signals. Additionally, the majority of the referenced works report findings from multiple experiments that incorporate distinct approaches and configurations. This leads to a discussion on best practices for EEG-based User Authentication and conclusions suggesting future research directions that consists, among others, of considering homomorphically encrypted biometric templates for information leakage prevention through federated learning approaches in decentralized architectures. We anticipate that the present literature review will provide a roadmap for future research by considering efficiently and effective EEG-based User Authentication methods while at the same time preserving privacy.

**INDEX TERMS** User authentication, electroencephalography, artificial intelligence, security and privacy, usability in security and privacy, human-centered computing, interaction techniques.

## I. INTRODUCTION

Information systems design places significant emphasis on security as a fundamental aspect, with the goal of ensuring confidentiality, privacy, authorization, authentication, non-repudiation, and integrity. These elements serve as key pillars in establishing a robust and secure system [3]. However, these principles have been compromised nowadays resulting to nearly $1 trillion losses caused by cybercrime [59]. One of the important aspects in the security of information systems relates to User Authentication (UA).

In the current era of cloud-based computing and globalized services, user authentication has become increasingly crucial from both a user-centric and service provider perspective. Millions of users with diverse cultural backgrounds, cognitive abilities, and usage contexts perform these authentication tasks daily. In fact, every computing device or information system requires the user to complete an authentication task before it allows access to specific applications and services. The term ''User Authentication'' refers to the process of

The associate editor coordinating the review of this manuscript and approving it for publication was Zheng Yan.

verifying that an individual who interacts with a service is indeed the person claimed to be. Traditional UA methods confirm the authenticity of a user based on what a user knows (e.g., password secrets), what the user has (e.g., credit cards etc.) or what the user is (e.g., biometric traits).

A variety of knowledge-based user authentication methods have been proposed, like textual passwords (consists of a combination of numbers, special characters, and letters), graphical ones (consists of a combination of a specific gestures on an image, specific pattern drawing, or sequential selection of small images on a grid) and pin-based passwords (consists of a combination of N-digit numbers).

Currently, knowledge-based authentication schemes are widely used due to their ease of implementation and low cost. Moreover, they do not entail the privacy flaws associated with other authentication methods such as tokens (which can be lost or stolen, like credit cards) and biometrics (which may leek sensitive physiological data) [122].

However, recent research has shown that existing knowledge-based authentication schemes do not provide an acceptable balance between security and usability. Each scheme has its strengths and weaknesses, which can lead to user frustration and hence to the adoption of insecure authentication practices such as reusing passwords across multiple online services or writing passwords on sticky notes and leaving them in plain sight on an office desk.

Textual passwords fail to meet the usability requirements due to the complex authentication policies enforced by online service providers, which nowadays require a combination of at least ten characters/symbols in the password to be considered secure. Similarly, pictorial schemes have been proven to be less secure due to their inherent limited key space and the respective security entropies, whereas PIN-based schemes are being deployed solely in combination with other factors (e.g., device login), also due to their limited key space [122].

Aiming to improve on the security within UA, recent research focuses on biometric traits [28], [47], which must adhere to several key principles [3]: *Universality* (Every person possesses the biometric trait in question), *Uniqueness* (the biometric trait is distinct and unique to everyone, *Permanency* (the biometric trait maintains its properties and remains relatively constant over time, *Collectability* (the biometric trait can be measured quantitatively through some type of collection process), *Performance* (the collection process must be practical, and the trait must be accurate and effective for authentication purposes), *Acceptability* (the use of the biometric trait is acceptable to users and does not create privacy concerns or other issues), *Robustness* (the biometric trait cannot be easily circumvented or replicated through fraudulent means).

Although traditional biometric attributes like fingerprints, iris scans, and 3D facial data have been used for user authentication, they have some shortcomings. These attributes have been reported to be susceptible to falsification using standard computational tools and camera devices [29], [38]. Additionally, they are not always user-friendly. For example, fingerprints may not be suitable for workplaces where gloves are mandatory (such as hospitals and industrial settings), while 3D facial data has become less user-friendly due to the requirement of wearing masks during the recent pandemic. As a result, they may not offer considerable advantages over the omnipotent text-based passwords.

The concept of using brain signals for user authentication was introduced in 2005 by Thorpe et al. [67]. They proposed that instead of typing in a password, a user could be authenticated by thinking of a pass-thought, which could be transformed into a password-key using AI to analyze EEG waves. This approach offers several security and usability benefits from the end-user and service provider perspective, including the ability to withstand dictionary attacks and the capability to resist shoulder surfing.

EEG conforms to biometric trait standards since every individual generates distinct EEG signals [1], [52], which can be easily acquired [30]. Moreover, EEG signals are suitable for pre-processing, feature extraction, and classification [8] and compared to other biometric traits (e.g., iris, fingerprints etc.) are more difficult to be fabricated [3]. Finally, EEG-based user authentication methods might outperform other biometric-based approaches because: i) EEG activity reflects an internal and personal process that cannot be observed by others, ii) brainiac signals that are triggered by similar external stimuli are not identical across different individuals, iii) it is challenging to fabricate EEG signals because brain activity is influenced by the individual's mental and emotional state, iv) unlike other biometric-based user credentials such as fingerprints, iris, or voice, EEG signals require a live recording from the individual, making it more secure against interception or fraud [54].

Despite the benefits of using EEG for user authentication, there are also drawbacks. The process involves training highly accurate AI models for each individual user, which can be challenging. Additionally, there may be issues with user acceptance and privacy preservation, and the method is vulnerable to security threats that involve the creation of fake brain wave signals. Moreover, EEG-UA, necessitate continuously training of AI models for each user enrolment and/or password reset. Moreover, GAN-type artificial intelligence models have been shown to be capable of producing artificial brain signals, highly resembling the ones of the original users, making thus such systems vulnerable to spoofing attacks [33]. Finally, there are concerns about privacy preservation, given that the UA process involves storage and processing of EEG signals, which can potentially lead to information leakage of sensitive personal data [8]. Hence, EEG-based User Authentication approaches embrace new challenges and opportunities [9].

The remaining of the article is organized as follows. In Section II, we refer to related works that attempted to provide a literature survey on how EEG can be applied in UA. Afterwards, in Section III, we provide the theoretical

background of this review with the goal to lay a common ground for important semantics within our research. Subsequently, Section IV provides a systematic analysis of existing user authentication research based on our research motivation. In Section V, we present the analysis of existing works. Then, in Section VI, we suggest specific research challenges for future research. Finally, in Section VII we finalize the paper by outlining our findings and limitations.

## II. RELATED WORK

Based on our research, there are currently two systematic literature surveys that aim to provide a comprehensive review in EEG-based User Authentication: a) Bidgoly et al. [8] provide a complete guide of EEG-based User Authentication methods while also discussing future challenges with respect to the EEG technology when used in User Identification (i.e. ability of a system to identify uniquely a user) and in User Authentication (the ability to prove that a user is genuinely who that person claims to be). On the other hand, the survey of Zhang et al. [77] is primarily provides comprehensive information on feasibility, accuracy and performance in relation to AI-methods applied to cope with the EEG-based User Authentication task.

Bidgoly et al. [8] provide a comprehensive literature survey that delves into EEG-based User Authentication tools in detail. Within their paper, they present a thorough compilation of the EEG equipment that is currently available on the market, the datasets that are accessible to researchers, the typical signal acquisition methods that are utilized, as well as a concise reference to artificial intelligence topics that are relevant to this field. Additionally, the paper thoroughly addresses all the prevailing concerns and challenges associated with EEG-based User Authentication at the time.

In addition, Zhang et al. [77] conducted a comprehensive literature review that specifically focuses on the scientific challenges that arise in the field of biometric cryptosystems. Notably, their study is the first to introduce EEG as a component of biometric cryptosystems within the scope of this type of review. The authors provide a detailed analysis of the technical characteristics of EEG, along with the primary protocols used for EEG acquisition. The review also delves into the theoretical background of signal processing and analysis and outlines various techniques for feature extraction. Furthermore, the study covers the shallow and deep learning approaches to signal classification and their effectiveness.

The two most recent systematic literature surveys have significantly improved the scientific advancement in the area of EEG-based User Authentication. However, we have identified a research gap in terms of a comprehensive discussion that encompasses the variety of User experimentation protocols and their association with the applied AI techniques. Moreover, we argue that this discussion should consider in more depth the aspects of security and privacy preservation and how they affect the accuracy and performance of EEG-based User Authentication tasks.

## III. BACKGROUND THEORY

### A. USER AUTHENTICATION PRINCIPLES

To ensure proper User Authentication, it is essential to maintain confidentiality, integrity, and availability of services and information. If any of these aspects are not adequately addressed, information systems security is degraded. *Confidentiality* involves preventing unauthorized access to data and maintaining the anonymity of authorized users. Breaches of confidentiality can occur due to poor encryption, man-in-the-middle attacks, or the disclosure of sensitive data [22]. *Integrity* protects data from unauthorized modification, ensuring that changes are made only in a specified and authorized manner. Threats to integrity may include hijacking a computational machine or embedding malware into web pages [19]. *Availability* ensures that authorized users can access the information when needed. Factors that can threaten availability include security incidents such as DDoS attacks, hardware failures, programming errors, and human error [22].

### B. EEG - USER AUTHENTICATION PROTOCOLS

The concept of Electroencephalogram (EEG) was first introduced in 1875 by Richard Caton, who reported in the British Medical Journal that animals with exposed cerebral hemispheres show electrical phenomena [10]. The first human EEG was recorded by Berger [31]. EEG operates on the principle of differential amplification, which involves recording voltage differences between distinct cerebral points using a pair of electrodes. One electrode acts as an active exploring site, while the other serves as a reference electrode, which can be located nearby or at a distance. These points typically belong to a standardized grid known as the 10-20 montage [81], which is widely used in the literature. Brain signal acquisition protocols used in User Authentication can be classified into four main categories, which are Rest state protocols, External Stimuli-based protocols, Mental activity protocols, and Hybrid protocols. The categorization criteria are related to contextual and user interaction settings during the EEG acquisition process, as described in Table 1.

**TABLE 1. EEG-based user authentication protocols.**

| EEG Protocol | Interaction Context | Contextual Settings |
|---|---|---|
| **Rest** | The subject remains calm and relaxed. | Requires calm environmental conditions. |
| **External Stimuli** | The subject comprehends one or more stimuli. | Stimuli triggers might be related to all human senses. |
| **Mental Task** | The subject thinks of an object or movement. | Requires users to be engaged in mental tasks. |
| **Hybrid** | The subject performs a multi-modal task. | Combinations of the above protocols. |

Accordingly, variations in brain wave frequencies are correlated to individual cognitive tasks, e.g., attention, perception and emotion [82]. Table 2 presents a list of properties of EEG waves that were analyzed based on their frequency band measured in Hz, along with the brain region associated with them and the various states that are linked to different human activities. The recorded waveforms reflect the cortical electrical activity, among them the Beta and Gamma brainwaves being the fastest ones (highlighting cognitive activities) whereas the Delta brainwaves are the slowest but with the highest signal intensity.

**TABLE 2. EEG-wave properties [83], [84].**

| Brain Wave Band | Frequency (Hz) | Brainiac Region | Cognitive State |
|---|---|---|---|
| **Delta** | 0-4 | Front Region | Dreamless Sleep |
| **Theta** | 4-8 | Free of tasks Regions | Idling, actively trying to repress, Response reaction, Dreaming, Imagining. |
| **Alpha** | 8-13 | Both hemispheres, Posterior Regions | Relaxation, Resting Eyes Closed. |
| **mu** | 8-13 | Sensorimotor Cortex | Alert, Anxiety, Concentration, Working, Idle hands and arms. |
| **Beta** | 13-30 | Both hemispheres Frontal Lobe | Thinking |
| **Gamma** | 30-100 | Somatosensory Cortex | Two senses combined, Object Recognition, Short memory matching |

#### 1) REST STATE PROTOCOLS

Rest state protocols are simple EEG acquisition protocols which involve recording brainiac activity when the user is relaxed, calm, and awake, without engaging in any specific cognitive or emotional activity. While Rest state is primarily used for user identification rather than authentication, it is widely applied as a baseline measure. Although Rest state approaches do not offer password reset or recovery services, they are well known because of their transparency with regards to required user tasks. Well known methods of rest state protocols include the Rest Eyes Open (REO) and Rest Eyes Closed (REC) protocols.

#### 2) EXTERNAL STIMULI-BASED PROTOCOLS

External stimuli-based protocols involve the collection, preprocessing and computation of brainiac activity that is triggered by a specific stimulus. These stimuli, which are referred to as events in the literature, are often used in Event-Related Potential (ERP) protocols. Resetting the user credentials may be achieved by altering the source of the stimuli, which requires a brain-computer interface with a stimulus trigger. Furthermore, this protocol may require frequent password resets due to alterations in brain activity over time, which can be accomplished through the replacement of stimulus triggers. Examples of paradigms used in External stimuli-based protocols include Visual Evoking Potentials, Rapid Serial Visual Presentation (RSVP), and sound-based protocols, among others.

#### 3) MENTAL ACTIVITY PROTOCOLS

Mental activity protocols require from end-users to engage in one or several tasks that embraces information processing, recalling or comprehension. As such, the user cognitive processes generate brain signals that reflect users' internal cognitive states related to memory, attention or content comprehension tasks. Resetting the user credentials may be achieved by altering the mental activity task. Paradigms of mental activity protocols include the Motor Imaginary, Number Imaginary, Speech Imaginary, Vowel Imaginary, and others.

#### 4) HYBRID PROTOCOLS

Hybrid Protocols involve often a combination of traditional user authentication methods i.e., textual or image-based passwords along with EEG ones. As such, they can be considered as multi-modal and multi-factor approaches that aim to increase systems security, personalization and adaptation in a variety of usage scenarios. In hybrid protocol contexts, the user credentials can be easily reset since they rely on traditional knowledge-based approaches. Usage scenarios of such protocols might include PIN and EEG User Authentication, Android pattern drawing and EEG, Picture based authentication and EEG or combinations of the EEG protocols etc.

## IV. MOTIVATION AND METHODOLOGY

### A. MOTIVATION

A plethora of user experiments have been reported that employ various EEG acquisition protocols and utilize EEG montages that range from mono-channel to multi-channel apparatus. These experiments also employ a diverse range of techniques, including both traditional machine learning and deep learning, resulting in noticeable levels of accuracy [36]. In this context, researchers must often make decisions about the specifics of signal acquisition, including the brain areas to be monitored and which of the acquisition channels can generate useful information for a given EEG-based user authentication protocol.

Furthermore, sampling and preprocessing of the acquired brain signals might be computationally demanding, making conventional computational methods inefficient for the task. However, selecting appropriate UA methods and EEG- protocols and parameterizing appropriate technicalities might provide a solution for improved pre-processing, feature extraction and classification tasks thus ensuring usable and secure implementation of EEG-based user authentication. Given that importance of security and privacy issues in UA activities, it is essential to prioritize implementations that

offer improved performance while also protect systems from unauthorized access by users.

Consequently, we argue that future research endeavors would benefit from a coherent analysis of existing literature, through a three-pillar perspective: a) the EEG-Authentication policy; b) the applied AI techniques in respect to the accuracy and performance reported; and c) the related Security and Preservation aspects (see Figure 1).

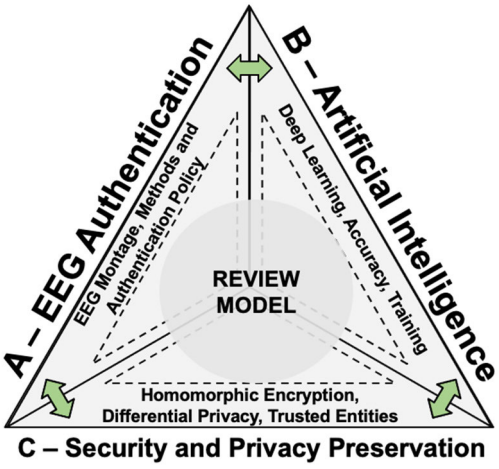


**FIGURE 1.** The adopted analysis framework consisting of a three-pillars perspective for a solid review of existing works within EEG - User Authentication research.

Therefore, our aim with this review is to support research in the wider field of Electroencephalography-based User Authentication by presenting existing research efforts from multiple perspectives and by providing a fruitful ground for discussion on emerging EEG-based user authentication challenges and research topics. We hope to enhance discussions on topics related to performance, accuracy, security, and privacy preservation in this research area.

### B. RESEARCH QUESTIONS

Based on our research motivation and the adopted analysis framework, we formulated three research questions that are analyzed in more details as follows:

*Research Question A (RQA):* Which is the mostly applied user experimental setups and how do they correlated with the AI-algorithms by considering several aspects like the number of subjects, the EEG-montage, the sampling rate and signal filtering, the number of sessions and number of trials per session and finally the accuracy. By investigating this research question, we will have a complete view on multiple perspectives in this field, how the interplay with each other and hence provide a solid springboard for further research.

*Research Question B (RQB)*: Whether and how security and privacy issues have been considered in existing works. By investigating this research question, we anticipate defining a holistic threat model for each EEG-based protocol, which will help us to understand the potential vulnerabilities and risks associated of EEG-based user-generated secrets.

*Research Question C (RQC):* Considering RQA and RQB how can we drive the evolution of next generation EEG-based User Authentication schemes by also considering privacy aspects?

### C. METHODOLOGY

We conducted a thorough investigation in the most popular scientific digital libraries, namely: a) Elsevier Scopus; b) IEEE Xplore, and c) the ACM Digital Library. More specifically, PRISMA method [85] was employed to extract valid experimental EEG studies from the scientific databases with keywords [*EEG*, *User*, *Authentication*, *Classification*, *Artificial*, *Intelligence*]. The main inclusion criteria were to include articles that reported results from at least one experiment. The initial search returned a total of 138 papers, 70 of which were duplicates and were thus filtered out, resulting in a total of 68 distinct works. From these 68 papers, we stemmed 108 different EEG-UA experiments, which were further grouped based on the EEG-protocol (Figure 2).

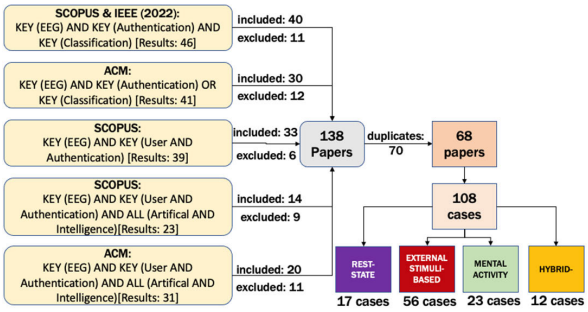


**FIGURE 2.** PRISMA flow diagram related to the selection process of reviewed EEG and User Authentication research papers.

We note that the first experiment was conducted in 1998 by Poulos et al. [57] and it took about 15 years to observe significant research development, starting to draw again the attention of the research community in the early-2013s, a period that coincides with major advances in the artificial intelligence field (Figure 3).

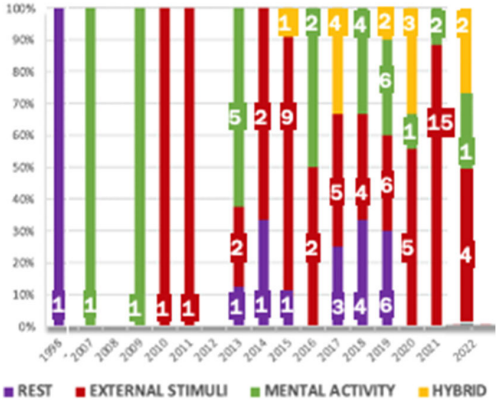


**FIGURE 3.** Literature timeline analysis consisted of 68 articles and 108 distinct experiments dating from 1998 to 2022.

## V. ANALYSIS OF RESULTS

In terms of applied EEG-UA research, the most employed protocol is the External stimuli-based one, while interest in the Rest protocol seems to have declined in the most recent years, possibly because they are rather applicable for user identification scenarios, and they do not support straightforward password reset or recovery. Although there are some variations in hybrid and mental-activity protocols, our analysis has shown that these protocols have been studied more extensively in recent research. This may be attributed to their ability to better accommodate user enrollment and password-reset or recovery activities.

### A. SETUP, FEATURES, CLASSIFICATION & ACCURACY

#### 1) REST STATE PROTOCOLS

According to these protocols, the user is instructed to remain calm and simultaneously no to engage in activities that would necessitate cognitive or body activity. They can either keep their eyes open (Rest Eyes Open - REO protocol) or closed (Rest Eyes Closed - REC protocol).

The primary disadvantages of the rest state protocol, for user authentication purposes, are its sensitivity to external environmental stimuli that can distract and modify their generated signals. Moreover, controlled, or uncontrolled movements like eye-blinking, can cause ''artifacts'' that can also affect significantly impact system accuracy.

*User Tasks, Sessions and Trials.* The user is required to follow the authentication protocol specified during the registration and verification stages. During the enrollment stage, an AI system typically gathers EEG data, which is then compared to the corresponding data collected during the verification stage to authenticate the user's claimed identity. The authentication solutions that are based on rest-state protocols usually require password reset after a predetermined time, as per system specifications and authentication policies, to adapt to biological conditions of the individuals caused by health-related or other factors.

Two distinct methodologies can be found in the literature for storing and categorizing brainiac signals across multiple recording sessions. A recording session is a distinct experimental procedure that differs from other sessions recording trials on different conditions (usually different days), and each session may comprise multiple trials.

In multi-session experiments, researchers record N sessions for the enrollment and one for the *'verification'* part. Notable multi-session approaches include: Chuang et al. [13] and Curran et al. [14] who performed two sessions on two different dates with five trials each. Nakamura et al. [53] and LaRocca et al. [60] who opted for two different day-sessions, also investigating longevity factors in their experiments.

Moreover, Maiorana et al. [49] managed 5-6 trials in two different sessions per subject across 3 years, further researching longevity factors related to the EEG-based User Authentication task. Kang et al. [34], Shons et al. [62], Kim et al. [37] opted for three different session recordings. Regarding single-session approaches: Poulos et al. [57] kept 100 EEG recordings from a pool of four subjects in one session, Haukipuro et al. [30] performed five trials on the same day session. Li et al. [43] and Di et al. [20] performed 3-4 trials on each subject on the same day session. Finally, Waili et al. [70] just performed a single-trial experiment.

*EEG-Montage.* Resting-state protocols typically utilize the Fp1 channel located in the frontal region to capture low frequencies. Additionally, the C3 and C4 channels are utilized, as they are associated with idle brain conditions. Furthermore, the use of P7, P3, P4, and P8 channels, which correspond to posterior regions of the brain and are related to alpha band activity, is commonly observed.

*Feature extraction, Classification and Accuracy.* With respect to the feature extraction task, the analyzed literature suggests the following: Waili et al. [70] employed Wavelet transformation, Haukipuro et al. [30], Di et al. [20] and Nakamura et al. [53] utilized PSD (Power Spectral Density), and Autoregressive (AR) models. La Rocca et al. [60] also used AR models. In addition, Li et al. [43] preferred SPS (Spectral Power Statistics) while Poulos et al. [57] opted for the application of Fast Fourier Transformations. Finally, Kang et al. [34] and Maiorana et al. [49] opted for multi-modal feature extracting approaches.

Concerning the AI algorithms employed for the classification task of the EEG data, Rocca et al. [60], Di et al. [20], Li et al. [43], Nakamura et al. [53] opted for Support Vector Machines (SVM), while Chuang et al. [13], Hwan Kang et al. [34] and Poulos et al. [57] chose Euclidean Distances. Maiorana et al. [49] selected Hidden Markov Models (HMM) and Curran et al. [14] classified their data using Boosting techniques (XGBoost). There are also cases employing neural network based and/or deep learning architectures, with notable mentions being the work of Waili et al. [70] and Haukipuro et al. [30] who used a Multilayer Perceptron classifier (MLP), Kim et al. [37] who used Functional Networks (FN) and finally, La Ma et al. [48] and Shons et at al. [63] who relied on the usage of Convolutional Neural Networks (CNNs) for the classification task.

We conclude that rest-state protocol experiments have reported satisfactory accuracy rates (>90% in almost all examined cases) using both traditional machine learning approaches such as SVM, HMM and Euclidean distances as well as deep learning-based ones, such as CNNs. Similarly, the works of [30] and [70] indicate that the usage of SPS and Wavelet transformation for feature extraction along with MLP as a classifier, may be less performant for the task of rest-state based user authentication. Last, due to the nature of the algorithms themselves, no specific algorithm can provide adequate guarantees in terms of security or privacy preservation of biometric data.

#### 2) EXTERNAL STIMULI-BASED PROTOCOLS

User authentication methods that rely on external stimuli-based protocols are leveraging the fact that human brains generate unique brain signals when they are exposed to external

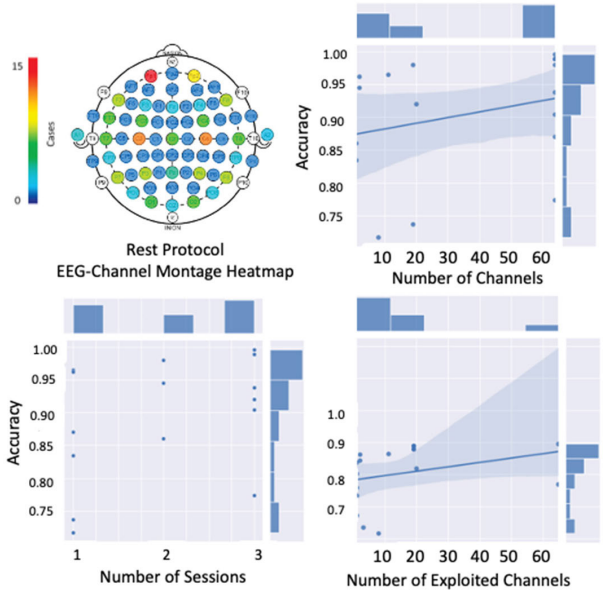


**FIGURE 4.** Rest - state channel montage heat map, number of sessions-channels- exploited channels & correlation to accuracy.

stimuli. These stimuli, which are also refereed as events in the literature, can be related to any human-sense and in general such UA-approaches are labeled as *Event-Related Potential (ERP)* protocols.

The Visual Evoked Potential (VEP) is the most used category of ERP, as shown in Figure 5. In this protocol, the user's brain produces waves in response to a visual stimulus. A specific type of VEP is the Steady-State Visual Evoked Potential (SSVEP) protocol, which generates more stable and stronger signals. SSVEPs are generated in the brain in response to visual stimuli that flicker at a specific frequency [39]. Those potentials can be evoked by different means, such as LEDs flashing on and off or an alternating pattern presented on a screen oscillating at a particular frequency [58]. SSVEPs are typically preferred in the research because of their excellent signal-to-noise ratio and relative immunity to artifacts [55].

Studies suggest that low-frequency SSVEPs demonstrate substantial inter-subject variability and relatively minimal intra-subject variability [75]. As a result, it is advisable to utilize the potential of low-frequency transient SSVEP responses, which are personalized and reliable, to create innovative EEG-based biometrics.

Nonetheless, these responses are uncomfortable to look at and can lead to visual fatigue [50]. A countermeasure to the flickering challenge relate to approaches called Steady-State-Motion-Visually-Evoked-Potentials (SSMVEP) [58], which hide such patterns within different kinds of motions.

Rapid serial visual presentation (RSVP) is a specialized technique designed to elicit targeted stimuli, such as number, letters and/or images, presented sequentially. This technique aids in the detection of the brain's response to the serial stimuli. RSVP involves sequentially displaying images at a high presentation rate, typically 2-20 Hz, in the same spatial position [8].

To optimize artifact capturing, the RSVP protocol is frequently coupled with eye-blinking activity. This is because the rate of change in visual stimuli can be synchronized with the rate of blinking. Compared to traditional ERP protocols, RSVP produces more reliable potential differences, resulting in cleaner and less artifact-contaminated data acquisition. This has been supported by various studies, including those cited as [32], [73], [76], [77], and [80]. Additionally, ERP protocols may rely on audio stimuli (Audio ERP), which is a popular and easy to implement. A plethora of research studies that utilized audio-based ERP protocols have been reported in the literature that have achieved satisfactory accuracy rates [13], [35], [65], [72].

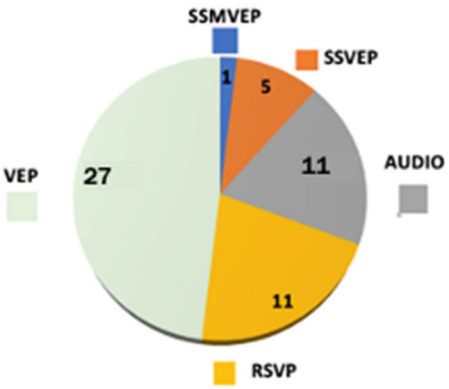


**FIGURE 5.** Literature analysis points towards the popularity of VEP-based EEG-UA research, followed by RSVP- and AUDIO-based research.

*User Tasks, Sessions and Trials.* Event-Related Potential protocols embrace user authentication policies that necessitates from end-users to be exposed to a selected stimulus (or a series of stimuli) which in turn triggers brain signal that are being continuously recorded and further analyzed.

During the user registration or enrollment task the user is asked within one or multiple sessions to follow a specific procedure which exposes her to the stimuli. The utter goal of the repeated measure process is to record representative EEG-recordings about a single individual, under diverse contextual settings, to train accurate AI-models.

Resetting the user credentials, in terms of repeating the enrolment process with a different stimulus, is often required given that the brain response, to a given stimuli, does change overtime. In such scenarios, password reset is easy as it may be performed by replacing the stimuli. External stimuli-based protocols necessitate repeated measurements related to brainiac activity in order to achieve high accuracy of classifiers. Chuang et al. [13], Gopal et al. [25], and Liew et al. [44] reported two distinct session recordings, Armstrong et al. [5], Lin et al. [46] implemented three different recording sessions.

*EEG-Montage.* External-stimuli protocols mainly use O1, O2 and Oz channels located in the back region, from which high frequencies related to the visual context comprehension are utilized. This observation might be also accredited to

the fact that the most applied research in External-stimuli protocols is related to Visual Evoking Potentials.

*Feature extraction, Classification and Accuracy.* The analyzed literature suggests the following methods: Gui et al. [26], Kaur et al. [35] and Chen et al. [12] employed Wavelet transformation, Debie et al. [18], whereas Vahid et al. [68] and Pham et al. [54] opted for PSD (Power Spectral Density). Lin et al. [46] and Pham et al. [54] used AR models in their work and Gopal et al. [25] preferred CFS (Correlation based Feature Selection). Finally, Ozdenici et al. [80] opted for multi-modal feature extracting approaches.

With respect to the algorithms used for the EEG classification task, the most common technique employed was the SVMs, as in the works of: Wiliaiprasitporn [72], Wang et al. [71], Sooriyaarachchi et al. [65], Lee et al. [42], Armstrong et al. [5], Arnau Gonzalez et al. [6], Debie et al. [18], Lin et al. [46], Chen et al. [12], Kaur et al. [35], Chen et al. [12], Vahid et al. [68], Alzahab et al. [112], Rahman et al. [114], Leon et al [116], and Gupta et al. [28].

Moreover, Convolutional Neural Networks (CNNs) were applied in Arnau et al. [6], Zhang et al. [76], Yu et al. [75], Wu et al. [73], Debie et al. [18] and Ozdenici et al. [80]. Multimodal classification techniques were applied in the following works: Chuang et al. [13], Gui et al. [27], Armstrong et al. [5], Piciucco et al. [56], Armstrong et al. [5], Wiliaiprasitporn [72], Zuquete et al. [79], Liew et al. [44], Wiliaiprasitporn [72], Ruiz-Blondet et al. [61], Chen et al. [12]. Last, Gaspar et al. [24] and Bingkun [111] employed Euclidean Distances as classifiers or selected Hidden Markov Models (HMMs), Multilayer Perceptron classifier (MLP) or Functional Networks (FN). For a detailed listing of the feature extraction and classification techniques per experiment please refer to the Appendix.

From the analyzed papers, we may conclude that the usage of AI algorithms can support high-accuracy rates against EEG-based User Authentication External-Stimuli Protocols (Figure 6). Depending on the applied ERP method, the lowest accuracy reported for Audio ERP experiments was ∼90% whereas for the VEP-based protocols it yields consistent accuracy rates higher than 90% in almost every case.

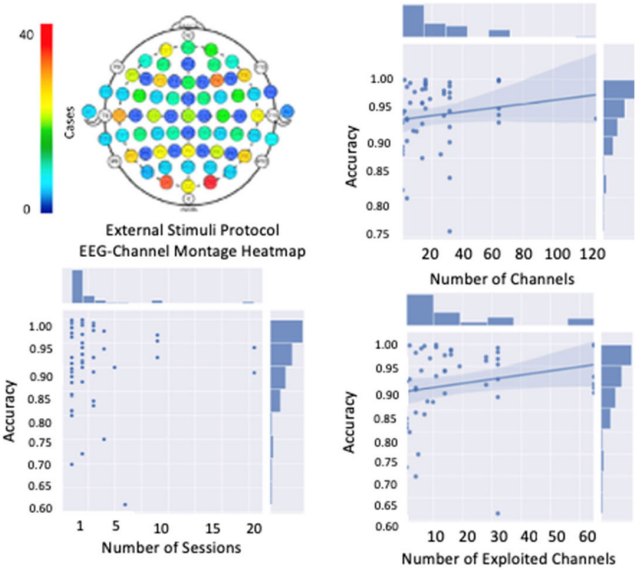


**FIGURE 6.** External - stimuli channel montage heat map, number of sessions, number of channels & number of exploited channels correlation to accuracy.

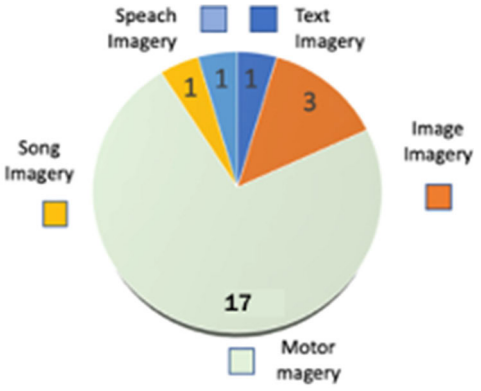


**FIGURE 7.** Literature analysis points towards the popularity of motor-imagery based EEG-UA research, followed by text-imagery, song- and speech-imagery research.

### 3) MENTAL ACTIVITY PROTOCOLS

Mental EEG-based protocols acquire brainiac activity that correspond to the user's thoughts about specific topics. One popular protocol is motor imagery (as shown in Figure 7), which involves the user imagining the movement of a body part without physically performing it. [13]. Extensive research has been conducted on this protocol, and it has been shown to achieve a high level of accuracy, as reported in the literature. [8], [66]. Other protocols based on cognitive activities include text, music, sound [13], numeric [41], image [30], and speech imagery [16].

Compared to resting protocols, mental activity protocols tend to produce signals with less noise, as reported in literature [77]. They are particularly well-suited for individuals with motor disabilities, as they can support user authentication tasks [13], [66].

Furthermore, mental protocols are shoulder surfing resistant - given the absence of an external trigger (stimuli) as it is the case in ERP protocols [47], [67] - and as such mental-based protocols are more secure compared to ERP protocols. On the downside, research works have reported that they can cause mental fatigue on users [13], which can affect the accuracy of user authentication process [47]. Finally, mental activity protocols often require Deep Learning approaches for effective classification analysis.

*User Tasks, Sessions and Trials*. Regarding user registration or enrollment, the end-user is required to complete a mental task that necessitates information processing e.g., thinking about a specific sequence of numbers. The number of times the user needs to perform this action is determined by the AI model during the training phase. From a procedural perspective, similarly to the Event-Related Potential (ERP)

protocols, Mental-activity protocols necessitate acquisition and processing of the EEG data, feature extraction and classification during the user registration and login process aiming to confirm the user's claimed identity. Resetting the user password is possible to be required after a specific predefined time, depending on the applied authentication policies. This approach is necessary because the user's brain activity can be affected by various factors such as repeated exposure, aging, and changes in cognitive state. As a result, combining different user authentication methods, including EEG-based techniques, can help to mitigate these changes. Additionally, resetting passwords can be achieved by modifying the requested mental activity, simplifying the process.

*EEG-Montage.* Mental-activity protocols utilize different EEG-channels based on the imaginary task they employ (e.g., text-, image-, speech- and/ or song-imagery). O1, O2 and Oz channels are utilized mainly for image-imagery mental activity tasks, T3, T4, T5 for information retrieval tasks, Fp1 and Fp2 for problem solving tasks and finally C3, C4 and Cz channels are utilized for motor-imagery tasks.

*Feature extraction, Classification and Accuracy.* Regarding the most used feature extraction schemes, the analyzed literature suggests the following: Alomari et al. [4] and Kumarisharma et al. [64] employed Wavelet transformations whereas Debie et al. [18] and Marcel et al. [52] opted for PSD (Power Spectral Density). Finally, Valsaraj et al. [69], Pham et al. [54] and Haukipuro et al. [30] opted for multimodal feature extracting approaches.

Concerning the algorithms selected for classification of the EEG data, the most applied technique was the Support Vector Machines (SVM) as appearing in following works: Alomari et al. [4], DaSalla et al. [16], Pham et al. [54]. Moreover, Convolutional Neural Networks (CNNs) were applied in Das et al. [15], Sun et al. [66] whereas Self/Cross Similarities was applied in Chuang et al. [13] and Genetic Algorithms in Lim et al. [45].

Haukipuro et al. [30] utilized Multilayer Perceptron classifier (MLP) whereas multimodal classification techniques were applied in Sun et al. [66]. For a detailed listing of the feature selection and classification techniques used per experimental setup, please refer to the table in Appendix A. From this analysis we may conclude that the employment of AI algorithms contributes significantly to the observed high-accuracy rates for the EEG-based User Authentication task when utilizing Mental-Activity Protocols (Figure 8). However, in some cases researchers have reported lower accuracy [11], [16] which nonetheless might also be accredited to the EEG-device setup characteristics.

#### 4) HYBRID PROTOCOLS

Hybrid EEG-based protocols for user authentication are comprised of a combination of conventional UA approaches with EEG-based methods, like: Resting - VEP [43], VEP - Image Imagery [74], VEP - number imagery [41], and RSVP - Motor Imagery [23].

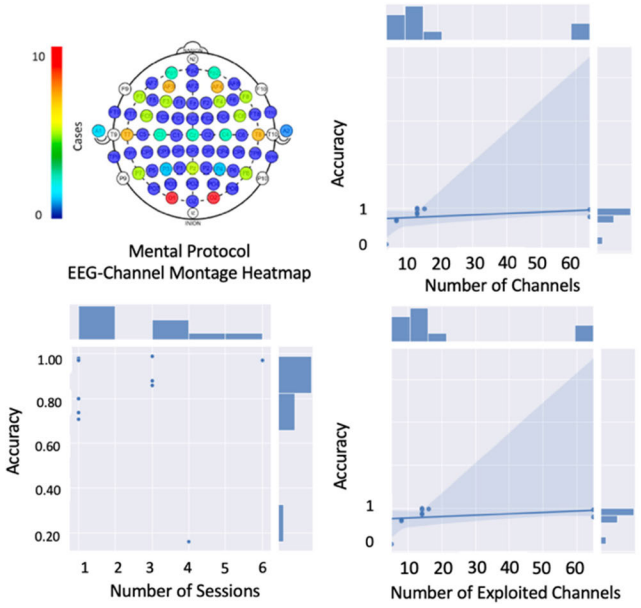


**FIGURE 8. Mental-activity protocol channel montage heat map, number of sessions - channels - exploited channels & correlation to accuracy.**

The integration of traditional user authentication methods with EEG-based techniques encompasses the utilization of pattern passwords on smartphones while simultaneously recording EEG signals [40], [103], [105], EEG signal recording while driving [51], and recording of EEG and Gait signals when the user walks [78]. Hybrid-protocols at one hand improve security through multi-factor authentication schemes but on the other lower usability since they embrace more complex User Authentication solutions. Regarding the parametrization of hybrid protocols, the User Authentication parameters are depended on the protocol policies of each single adjunct protocol employed.

*EEG-Montage.* The EEG-montage settings for Hybrid protocols vary based on the user activity that were deployed e.g. combining REST state with number- or image-imagery tasks as suggested by Li et al. [43], or similarly with number-imagery VEP tasks as suggested by Kumari et al. [41]. Hence, there is a distribution of utilized EEG-channels (T3, T4, T5, T6) concerning the cognitive information processing, employment of O1, O2 and Oz channels for image-imagery mental activity tasks, and /or channels C3, C4 and Cz for motor-imagery tasks.

*Feature extraction, Classification and Accuracy*. Regarding the feature extraction schemes and classifiers employed, the literature reports high accuracy (Figure 9) in almost all cases and albeit the most common applied technique was the Support Vector Machines (SVM), as in: Li et al. [43], Yousefi et al. [74] and Frank et al. [23], the analysed literature also suggests a combination of algorithms depending on the applied EEG-based UA policy.

### B. SECURITY AND PRIVACY CONSIDERATIONS

In general, there are several open research questions regarding how the EEG-based user authentication solutions

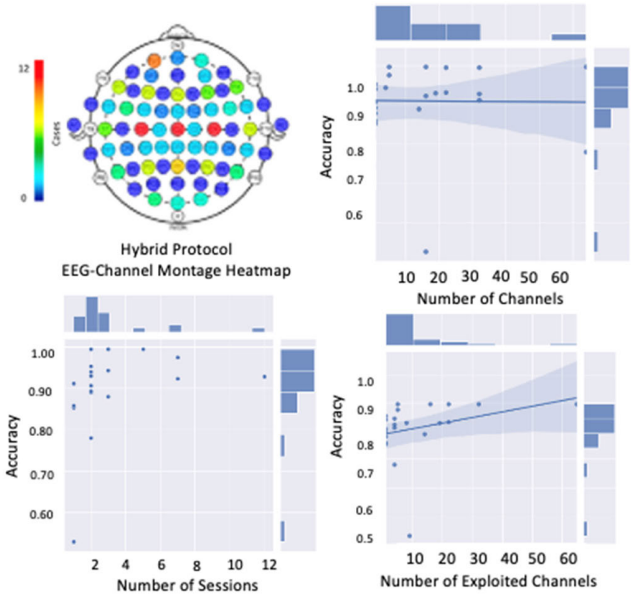


**FIGURE 9.** Hybrid-activity protocol channel montage heat map, number of sessions, number of channels & number of exploited channels correlation to accuracy.

consider security and privacy. Albeit all reviewed works aim to achieve high accuracy results and thus provide accurate user authentication solutions, critical security aspects like theoretical or practical entropy of user selected passwords, are often not examined. The same holds true regarding implementation details on how and where the EEG-acquired signals are stored alongside with architectural suggestions for secure storage, which nonetheless preserves privacy and at the same time provides satisfactory performance and user acceptance. Sporadically, some researchers mention that instead of the EEG-signals per se, they rather store the derived AI-models. However, across almost all the reviewed works, key questions regarding the security and privacy preservation of biometric data remain unanswered. Privacy preservation and security consideration remain up to date an open research agenda.

More specifically, the authors in Poulos et al. [57], albeit being the first to successfully employ in EEG in the User Authentication context, do not explicitly evaluate the security aspects from an EEG biometric perspective, neither do they consider any biometric preservation policies. Chuang et al. [13] and Curran et al. [14], focus on developing a verification method that relies on self/cross similarities across the user pool, and authenticates a user only if the selfSim rate is greater than crossSim; nonetheless this approach tends to neglect cases where someone unregistered to the system (outside the registrants' pool) may attempt to be authenticated in lieu of an authenticated user. They also did not explicitly study the performance of the system in case the user pool increases to a much larger scale and suggested that the biometric data of each user should be stored in a database, which concurrently is raises additional concerns in terms of biometric preservation.

Likewise, Rocca et al. [60], albeit conducting extensive research on EEG biometric permanency, they do not provide estimates on the entropy of the proposed authentication system, nor do they mention any biometric preservation policy. Ma et al. [48] and Schons et al. [62] introduced Deep Learning models for the User Authentication task, which partially solves some concerns related to privacy preservation (since their systems do not store the actual EEG-biometric signals but a trained Neural Network model instead). However, a comprehensive evaluation of the system's permanency was also not performed in this case neither. Maiorana et al. [49] and Nakamura et al. [53] both studied EEG longevity, and acknowledged for the absence of biometric preservation policy, while omitting analyses related to how the proposed system would react in the presence of malicious users attacking their system.

Kang et al. [34] introduced a personalized classifier threshold to their system, improving hence the methodology initially proposed in [13]. Li et al. [43] studied the case of adding an extra layer of rest state, consisting of the subject watching a VR and a non-VR 2min video, proving that non-VR contribute more to the system's security and performance compared to VR-videos, probably due to the VR-heavy information load that degenerates EEG-signals for rest protocol. Di et al. [20] made an interesting observation by proving that their system can compare signals driven from REC protocol with signals driven from REO protocol and still achieve high accuracy, but like in other research, they did not account for the biometric privacy aspect neither did they study the case of adding new users to the system. Finally, Kim et al. (2019), studied the case of impostor trials achieving high accuracy results. However, they also did not consider any privacy preservation aspects.

## VI. CHALLENGES & FUTURE RESEARCH DIRECTIONS

The research domain of EEG-based biometric identification and authentication is a rapidly growing area of research and practice [86], and it offers numerous advantages in terms of security and usability. Biometric data used for authentication can create high levels of entropy, minimize administrative costs, and provide a positive user experience when evaluated against text-based passwords and token-based solutions like Time-based One-Time Passcodes (TOTP) [87], [88]. Additionally, biometric-based authentication offers a sense of technological advancement to end-users.

Biometric-based authentication commonly uses the physiological and/or behavioral characteristics of end-users, such as fingerprints, iris scans, facial recognition, voice patterns, typing patterns, interaction patterns, and engagement patterns [89], [90]. These technologies have become crucial for enforcing stringent security policies in various domains, including education, healthcare, banking, government, and others [86], [87], [91]. However, the use of biometric technologies currently poses several challenges regarding privacy preservation (as shown in Figure 10), which need to be addressed:

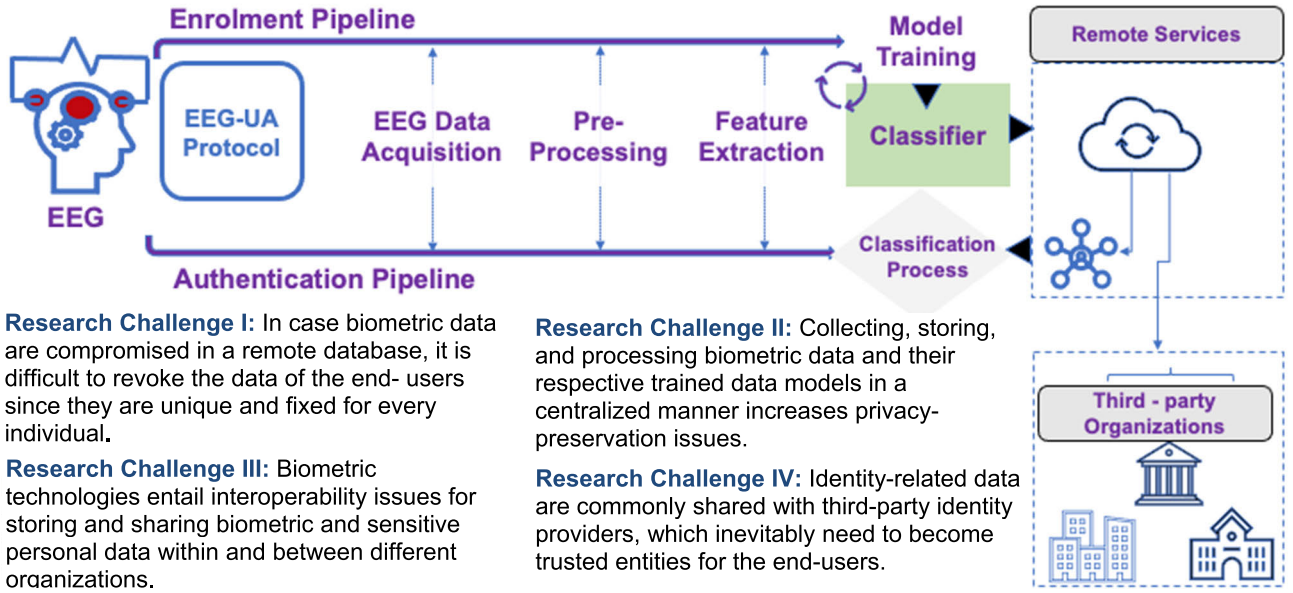


**FIGURE 10.** ECG-based user authentication pipeline and feature research challenges.

*Research Challenge I*: In use-case scenarios in which biometric data are compromised in a remote database, it is difficult to revoke the data of the end-users since they are unique and fixed for every individual. In order to tackle this problem, biometric technologies apply *biometric template protection methods based on homomorphic encryption*. However, such methods are typically computationally expensive and practically infeasible, and they require multiple user enrollments to improve the matching performance.

*Research Challenge II:* Biometric technologies are based on user verification models that are required to be trained within diverse sessions and heterogeneous data for improved accuracy and performance. However, collecting, storing, and processing biometric data and their respective trained data models in a centralized manner increases privacy-preservation issues. Hence, there is a need for methodologies that train biometric data without having full and direct access to the raw data and the trained models.

*Research Challenge III:* Biometric technologies entail *interoperability issues* for storing and sharing biometric and sensitive personal data within and between different organizations and institutions given the heterogeneity of such biometric data and their respective data models.

*Research Challenge IV:* Identity-related data are commonly *shared with third-party identity providers*, which inevitably need to become trusted entities for the end-users. However, such identity providers become single points of attacks as they store large amounts of sensitive personal data of users, and face liability risks given the responsibility of securely managing sensitive personal data.

*Research Challenge V*: Biometric technologies currently follow *a one-size-fits-all approach* when it comes to providing control over the users' data, neglecting the fact that users have preferred ways of perceiving and interacting with data privacy policies. It is therefore important to enable end-users to fully control, manage and share biometric data through personalized data privacy wallets based on the self-sovereign identity concepts.

Despite, the importance of privacy preservation of biometrical data within numerous application domains, there is an absence of a unified, sustainable, and scalable data privacy framework that incorporates recent advancements of privacy-preserving biometric technologies, and limited knowledge with regards to real-world use-case validation of such technologies in real-life contexts. We further elaborate on the suggested research agenda in the following sections.

### A. PRIVACY-PRESERVING BIOMETRIC TEMPLATES OF EEG-BASED USER AUTHENTICATION

In order to address concerns regarding the privacy preservation of biometric templates, several methods and approaches are presented in the literature. One such approach is the use of biometric cryptosystems, which bind a key to a biometric template [92], [93]. Another method is homomorphic encryption, which could serve as the basis for biometric template protection [94], [95]. These schemes use error-correcting codes to accommodate intra-class variations in biometric data, though performance may suffer when dealing with large intra-class variations. Another approach involves transforming the biometric template into a new domain by integrating biometric data with externally generated randomness in a non-invertible manner. This process protects privacy of biometric data as it is the case in cryptographic cipher [96]. Multiple cancellable identifiers can be constructed from a biometric template using various non-invertible transform methods [97].

Furthermore, the biometric cryptosystem approach can be combined with neural networks-based transform approaches [86], [98], [99], [100]. However, the neural networks used for transforming biometric templates are stored in an unprotected form and thus are vulnerable to attacks. Homomorphic encryption is another approach to protect biometric templates in centralized architectures which usually keep in a databased the biometric templates and verify through computational methods the similarity score between the encrypted biometric template and the encrypted query template [87], [91]. Despite these developments, the feature extraction methods and template protection methods have been developed independently of each other and thus a trade-off between matching performance, privacy, and computational cost arises.

### B. EEG-BASED BIOMETRIC ENCRYPTION TECHNIQUES AND DECENTRALIZED MANAGEMENT AND STORAGE

#### a: BIOMETRIC ENCRYPTION TECHNIQUES

Moving beyond the centralized Machine Learning space, in which all the biometric data needs to be stored on a cloud-based solution, some new initiatives have been proposed.

Certain open-source community initiatives are proposing frameworks that enable users to compute machine learning (ML) models in a decentralized, secure, and privacy-preserving (PP) manner. The use of privacy-preserving machine learning (PP-ML) techniques have been suggested based on the *TensorFlow Federated* framework or *PySyft* and *PyGrid* libraries to employ techniques such as multiparty computation, homomorphic encryption, differential privacy (DP), and federated learning (FL) [90]. Other noteworthy efforts are being undertaken by *Datafleets* and *Sherpa.ai*, which offers an open-source platform that unifies FL and DP for AI. It provides full support for DP mechanisms and even includes a federated attack simulator [101], [102], [103], [104].

Finally, *LEAF* [105] is a benchmark framework for federated learning within various deployment scenarios and use cases, such as client-side data source (local-DP [106]), central server-side [107], or intermediate stages like edge computing nodes using hybrid and hierarchical methods [108], [109].

#### b: DECENTRALIZED DATA MANAGEMENT AND STORAGE OF BIOMETRIC DATA

Decentralized data management empowers individuals to manage their own identity credentials as independent entities. Historically, data management has been dependent on the organizational management of identity data within centralized datastores. Such approaches led to the collation of large datasets containing personal information and resulted in several high-profile data breaches that has compromised individual data. Decentralized data management offers a solution whereby data is managed by individuals at the periphery of the network. Such a decentralized approach has the potential to improve privacy, security and control; simultaneously increasing the attack surface and reducing the potential returns for malicious actors. Often dependent on decentralized Public Key Infrastructure (PKI), current approaches state that no personal identifiable information (PII) should ever be stored on any form of decentralized PKI and that personal data should always be held external to the network. Storing biometric data may require utilizing a user's personal device, such as a smartphone, or cloud-based storage. It is important to consider the role of an identity custodian - an entity that is entrusted to securely manage an individual's data. It is essential to distinguish between the storage of biometric data in a personal data wallet and the storage and management of entity keys, which enable individuals to maintain control and access to their personal data store.

### C. SECURITY THREAD MODELS

Designing secure and privacy-preserving biometric technologies presents several challenges and potential threats. Some of the key challenges and threats as discussed in [88], [89], [90], and [110], and more specifically in [117] relate to:

*i*) *Data breaches, Hacking and Identity Theft*. Storing biometric data in centralized databases or on end-user devices can lead to data breaches and hacking attacks, potentially resulting in compromised biometric data. In addition, biometric data can be used to impersonate individuals, making it critical to protect the confidentiality and integrity of biometric templates [90]; *ii) Privacy Risks & Spoofing*. Biometric data can reveal sensitive information about an individual, leading to privacy concerns [88]. Moreover, adversaries can potentially create fake biometric data to gain unauthorized access, making it essential to implement anti-spoofing measures; and *iii) Performance, User Acceptance & Costs*. Biometric systems need to balance security and usability, providing seamless and user-friendly experiences without compromising security or privacy. However, pitfalls related to revocability of biometric data lower end-user acceptance of biometric-based solutions [90]. In addition, biometric data can have significant intra-class variations, leading to authentication errors, and hindering performance. Finally, implementing biometric technologies can be costly, requiring investments in hardware, software, and infrastructure.

State-of-the-art approaches that are at the forefront of efforts to improve security and maintain privacy of biometric data are discussed in recent literature [88], [89], [90], [110]. These methods include the use of biometric templates, which capture certain characteristics of biometric samples while avoiding the storage of raw data to mitigate privacy risks in case of a breach. Biometric encryption is another approach that has been employed to address privacy concerns, although conventional cryptographic hashing may not be adequate for the highly variable nature of biometric data. Instead, other cryptographic techniques, such as homomorphic encryption, have been explored (see [88], [110] for further analysis of these methods). Additionally, protocol-based approaches have been developed to safeguard biometric data, such as secure multiparty computation protocol and zero-knowledge proof protocol [110].

**TABLE 3.** List of reviewed papers.

| Work | Year | Channel Numbers | Exploited Channels | Protocol | Sessions | Participants | Featuring | Classification | Accuracy |
|---|---|---|---|---|---|---|---|---|---|
| Poulos et al. | 1998 | 2 | 2 | REST | 1 | 4 | FFT | Euclidean Distances | 0.9620 |
| Chuang et al. | 2013 | 1 | 1 | REST | 2 | 15 | NM | Self/Cross Similarities | 0.8600 |
| La Rocca et al. | 2014 | 64 | 19 | REST | 2 | 9 | AR | SVM | 0.9800 |
| Lan Ma et al. | 2015 | 64 | 65 | REST | 1 | 10 | NM | CNN | 0.8700 |
| Curran et al. | 2017 | 11 | 11 | REST | 1 | 7 | NM | XGBoost | 0.9650 |
| Maiorana et al. | 2017 | 19 | 19 | REST | 2 | 45 | AR, MFCC,Bump | HMM | 0.9800 |
| Nakamura et al. | 2017 | 2 | 2 | REST | 2 | 15 | AR, PSD | SVM | 0.9450 |
| Haukipuro et al. | 2018 | 1 | 1 | REST | 1 | 27 | PSD, MFCC | MLP | 0.8340 |
| Hwan Kang et al. | 2018 | 64 | 19 | REST | 3 | 109 | BPF, HT, NF | Euclidean Distances | 0.9893 |
| Hwan Kang et al. | 2018 | 64 | 19 | REST | 3 | 109 | BPF, HT, NF | Euclidean Distances | 0.9893 |
| Schons et al. | 2018 | 64 | 65 | REST | 3 | 109 | NM | CNN | 0.9962 |
| Li et al. | 2019 | 8 | 8 | REST | 1 | 32 | SPS | SVM | 0.7166 |
| Di et al. | 2019 | 20 | 20 | REST | 3 | 17 | PSD | SVM | 0.9200 |
| Waili et al. | 2019 | 19 | 3 | REST | 1 | 6 | Wavelets | MLP | 0.7365 |
| Kim et al. | 2019 | 64 | 16 | REST | 3 | 109 | NM | FN | 0.9040 |
| Kim et al. | 2019 | 64 | 16 | REST | 3 | 109 | NM | FN | 0.9378 |
| Kim et al. | 2019 | 64 | 16 | REST | 3 | 109 | NM | FN | 0.7733 |
| **EEG-BASED UA RESEARCH UTILIZING EXTERNAL STIMULI PROTOCOLS** | | | | | | | | | |
| Zuquete et al. | 2010 | 64 | 7 | VEP | 1 | 70 | NM | KNN, SVDD | 0.99620 |
| Gaspar et al. | 2011 | 128 | 65 | VEP | 5 | 5 | ERP | CC, ICC | 0.90000 |
| Chuang et al. | 2013 | 1 | 1 | Audio | 2 | 15 | NM | Self/Cross Similarities | 0.91300 |
| Chuang et al. | 2013 | 1 | 1 | VEP | 2 | 15 | NM | Self/Cross Similarities | 0.72000 |
| Lee et al. | 2014 | 32 | 32 | RSVP | 6 | 14 | DCT | SVM | 0.61450 |
| Gui et al. | 2014 | 6 | 6 | VEP | 2 | 32 | Wavelets | ANN | 0.94040 |
| Pham et al. | 2015 | 32 | 7 | ERP | 1 | 32 | PSD, AR | SVDD | 0.84000 |
| Armstrong et al. | 2015 | 1 | 1 | VEP | 3 | 45 | ERP | Cross-correl. + NDL | 0.92000 |
| Armstrong et al. | 2015 | 1 | 1 | VEP | 3 | 45 | ERP | SVM | 0.83000 |
| Armstrong et al. | 2015 | 1 | 1 | VEP | 3 | 45 | ERP | NDL | 0.82000 |
| Armstrong et al. | 2015 | 1 | 1 | VEP | 3 | 45 | ERP | DIVA | 0.89000 |
| Armstrong et al. | 2015 | 1 | 1 | VEP | 3 | 45 | ERP | Cross-correlation | 0.92000 |
| Abo-Zahhad | 2015 | 2 | 2 | VEP | 1 | 6 | AR | LDA | 0.99800 |
| Gui et al. | 2015 | 4 | 4 | VEP | 2 | 37 | ERP | RBF, Euclidean Dist. | 0.90000 |
| Phothisonothai | 2015 | 14 | 2 | SSVEP | 1 | 5 | STFT | KNN | 0.80000 |
| Ruiz-Blond et al. | 2016 | 26 | 1 | VEP | 1 | 50 | ERP | SVM, ANN | 0.81000 |
| Vahid et al. | 2016 | 32 | 5 | VEP | 4 | 32 | PSD, Wavelet | SVM | 0.75000 |
| Kaur et al. | 2017 | 14 | 14 | Audio | 4 | 60 | Wavelets | SVM | 0.93830 |
| Piciucco et al. | 2017 | 19 | 19 | SSVEP | 2 | 25 | MFCC, AR | Manhattan Distance | 0.95000 |
| Lin et al. | 2018 | 6 | 6 | VEP | 3 | 179 | PSD, AR | SVM | 0.99050 |
| Wu et al. | 2018 | 16 | 16 | RSVP | 3 | 15 | ERP | CNN | 0.97600 |
| Zhang et al. | 2018 | 64 | 65 | RSVP | 1 | 15 | NM | CNN | 0.89000 |
| Liew et al. | 2018 | 8 | 8 | VEP | 2 | 37 | WPD | KNN, FRNN | 0.87000 |
| Yu et al. | 2019 | 9 | 9 | SSVEP | 2 | 8 | NM | CNN | 0.96780 |
| Ozdenici et al. | 2019 | 16 | 16 | RSVP | 3 | 10 | SPD, QDA, PCA | CNN | 0.98600 |
| Chen et al. | 2019 | 28 | 28 | RSVP | 1 | 157 | NM | GSLT-CNN | 0.97060 |
| Chen et al. | 2019 | 28 | 28 | RSVP | 1 | 157 | PSD, SFFS | SVM | 0.96300 |
| Chen et al. | 2019 | 28 | 28 | RSVP | 1 | 157 | AR, SFFS | SVM | 0.90800 |
| Bhateja et al. | 2019 | 1 | 1 | Blinking | 1 | 15 | Wavelets, ICA | ANN | 0.80942 |
| Gupta et al. | 2020 | 2 | 2 | Blinking | 1 | 20 | Nat. Features | SVM | 0.92000 |
| Jalilifard et al. | 2020 | 16 | 16 | RSVP | 2 | 46 | BLINKER | GRU | 0.98700 |
| Wiliaiprasitporn | 2020 | 32 | 32 | Audio | 1 | 32 | NM | CNN, LSTM, GRU | 0.99170 |
| Wiliaiprasitporn | 2020 | 32 | 32 | Audio | 1 | 32 | NM | CNN, LSTM | 0.98230 |
| Wiliaiprasitporn | 2020 | 32 | 32 | Audio | 1 | 32 | NM | SVM | 0.88000 |
| Debie et al. | 2021 | 64 | 65 | SSVEP | 2 | 54 | PSD | SVM | 0.90940 |
| Debie et al. | 2021 | 64 | 65 | SSVEP | 2 | 54 | PSD | CNN | 0.99805 |
| Debie et al. | 2021 | 64 | 65 | ERP | 2 | 54 | PSD | SVM | 0.92605 |
| Debie et al. | 2021 | 64 | 65 | ERP | 2 | 54 | PSD | CNN | 0.99810 |
| Rekrut et al. | 2021 | 10 | 10 | SSMVEP | 1 | 18 | NM | CCA | 0.86800 |
| Wang et al. | 2021 | 32 | 32 | VEP | 9 | 20 | NM | KNN | 0.92000 |
| Wang et al. | 2021 | 32 | 32 | VEP | 9 | 20 | NM | RF | 0.95400 |
| Wang et al. | 2021 | 32 | 32 | VEP | 9 | 20 | NM | SVM | 0.96600 |
| Sooriyaarachchi | 2021 | 4 | 4 | Audio | 1 | 20 | NM | SVM | 0.69890 |
| Sooriyaarachchi | 2021 | 4 | 4 | Audio | 1 | 20 | NM | DT | 0.84400 |
| Sooriyaarachchi | 2021 | 4 | 4 | Audio | 1 | 20 | NM | LR | 0.89700 |
| Sooriyaarachchi | 2021 | 4 | 4 | Audio | 1 | 20 | NM | RF | 0.98110 |
| Gopal et al. | 2021 | 16 | 11 | VEP | 2 | 26 | CFS | ANN | 0.92700 |
| Gopal et al. | 2021 | 16 | 11 | VEP | 2 | 26 | CFS | ANN | 0.99290 |

**TABLE 3.** *(Continued.)* **List of reviewed papers.**

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Gopal et al. | 2021 | 16 | 11 | VEP | 2 | 26 | CFS | ANN | 0.99850 |
| N. Alzahab et al. | 2022 | 4 | 4 | Audio | 2 | N/M | CFS | MLP, SVM, XGBoost | 0.69000 |
| Rahman et al. | 2022 | 16 | 16 | VEP | 2 | 8 | CFS | SVM | 0.88000 |
| Leon et al. | 2022 | 16 | 16 | VEP | 2 | 12 | CFS | SVM | 0.72400 |
| **EEG-BASED UA RESEARCH UTILIZING MENTAL ACTIVITY PROTOCOLS** | | | | | | | | | |
| Marcel et al. | 2007 | 32 | 8 | Image | 12 | 10 | PSD | GMM | 0.92900 |
| DaSalla et al. | 2009 | 64 | 4 | Speech | 2 | 3 | CSP | SVM | 0.78000 |
| Chuang et al. | 2013 | 1 | 1 | Motor | 2 | 15 | NM | Self/Cross Similarities | 0.90700 |
| Chuang et al. | 2013 | 1 | 1 | Motor | 2 | 15 | NM | Self/Cross Similarities | 0.89300 |
| Chuang et al. | 2013 | 1 | 1 | Song | 2 | 15 | NM | Self/Cross Similarities | 0.95300 |
| Chuang et al. | 2013 | 1 | 1 | Image | 2 | 15 | NM | Self/Cross Similarities | 0.94000 |
| Pham et al. | 2013 | 5 | 5 | Motor | 5 | 9 | PSD | SVM | 0.99600 |
| Chellaiah et al. | 2016 | 16 | 9 | Image | 1 | 4 | FFT | AdaBoost | 0.52770 |
| Kumarish. et al. | 2016 | 1 | 1 | Motor | 3 | 5 | Wavelets | ANN | 0.88000 |
| Haukipuro et al. | 2018 | 1 | 1 | Image | 1 | 27 | PSD, MFCC | MLP | 0.85300 |
| Haukipuro et al. | 2018 | 1 | 1 | Motor | 1 | 27 | PSD, MFCC | MLP | 0.85900 |
| Lim et al. | 2018 | 16 | 4 | Motor | 7 | 16 | FCM | Genetic Algorithm | 0.92300 |
| Das et al. | 2018 | 19 | 19 | Motor | 2 | 40 | Not Mention | CNN | 0.93000 |
| Alomari et al. | 2019 | 14 | 14 | Text | 2 | 19 | Wavelets | SVM | 0.89000 |
| Pham et al. | 2019 | 5 | 5 | Motor | 7 | 9 | PSD, AR | SVM | 0.97600 |
| Sun et al. | 2019 | 4 | 4 | Motor | 3 | 109 | NM | CNN, LSTM | 0.94405 |
| Sun et al. | 2019 | 16 | 16 | Motor | 3 | 109 | NM | CNN, LSTM | 0.99590 |
| Sun et al. | 2019 | 32 | 32 | Motor | 3 | 109 | NM | CNN, LSTM | 0.99505 |
| Sun et al. | 2019 | 64 | 64 | Motor | 3 | 109 | NM | CNN, LSTM | 0.99585 |
| Valsaraj et al. | 2020 | 32 | 4 | Motor | 1 | 10 | PSD, AR | RF | 0.91250 |
| Debie et al. | 2021 | 22 | 22 | Motor | 2 | 9 | PSD | SVM | 0.93180 |
| Debie et al. | 2021 | 22 | 22 | Motor | 2 | 9 | PSD | CNN | 0.99490 |
| Bingkun et al. | 2022 | 16 | 16 | Motor | 2 | 9 | PSD | CNN | 0.93456 |
| **EEG-BASED UA RESEARCH UTILIZING HYBRID PROTOCOLS** | | | | | | | | | |
| Kumari et al. | 2015 | 14 | 14 | Hybrid | 6 | 6 | Wavelets | LVQ NN | 0.9700 |
| Kumar et al. | 2017 | 16 | 16 | Hybrid | 1 | 50 | DFT | SVM - HMM | 0.9799 |
| Mao et al. | 2017 | 64 | 65 | Hybrid | 1 | 100 | NM | CNN | 0.9700 |
| Mao et al. | 2017 | 64 | 65 | Hybrid | 1 | 100 | AR | SVM | 0.8000 |
| Frank et al. | 2017 | 5 | 5 | Hybrid | 4 | 4 | ERP | SVM, ANN | 0.1600 |
| Li et al. | 2019 | 8 | 8 | Hybrid | 1 | 32 | AR, SPS | SVM | 0.7368 |
| Li et al. | 2019 | 8 | 8 | Hybrid | 1 | 32 | PSD, SPS | SVM | 0.7092 |
| Yousefi et al. | 2020 | 14 | 14 | Hybrid | 3 | 20 | PSD | LDA | 0.8600 |
| Yousefi et al. | 2020 | 14 | 14 | Hybrid | 3 | 20 | PSD | SVM | 0.8800 |
| Zhang et al. | 2020 | 14 | 14 | Hybrid | 3 | 7 | NM | LSTM | 0.9900 |
| K. Białas et al. | 2022 | 32 | 32 | Hybrid | 2 | N/A | AR | Fast Forest | 0.8333 |
| Z. Alkhyeli et al. | 2022 | 16 | 16 | Hybrid | 1 | N/A | N/A | Fast Forest | 0.31 |

## VII. CONCLUSION & LIMITATIONS

The present literature review aims to provide a state-of-the-art analysis of user authentication practices that are utilized with EEG apparatus. The utter goal is to summarize existing research trends and suggest accordingly future research directions in the context of privacy preservation and security within EEG-based user authentication research. Hence, we anticipate that this paper will be useful for researchers, that aspire to deploy EEG-based user authentication schemes and experiments, to take informed decisions in terms of experimental setup procedures, apparatus, artificial intelligence techniques and privacy preservation methods.

We performed a detailed investigation over the last twenty-four years and organized the derived papers based on the applied EEG-UA protocol. Hence, from 1998 to 2022, we analyzed 108 different experimental use cases and organized them based on the EEG-protocols: *Rest state*, *External stimuli-based*, *Mental* & Hybrid. For each of them, we adopted an analysis framework (Figure 1) that consisted of three-pillars: a) the EEG-Authentication policy b) the applied AI techniques in respect to accuracy and performance and c) the security and privacy preservation.

By doing so, we aimed to analyze in detail the main research challenges that we do consider important when designing EEG-based User authentication schemes. As such, research decisions concerning EEG-montage characteristics, user trials, sessions, number participants, featuring and classification techniques and privacy preservation aspects were in detail inspected (*Appendix*).

A first conclusion that is derived from this paper is that EEG-based authentication has shifted, during the last five years, its focus from rest-state protocols to external-stimuli, mental and hybrid protocols. This can be accredited to the fact that rest-state protocols necessitate silent contextual settings which differ significantly from ecological valid user authentication scenarios. Moreover, rest state protocols are rather used to identify a person than to authenticate her. As such, these protocols have been surpassed by more complex ones e.g., mental, hybrid or external stimuli.

Another conclusion that is derived from this literature survey is that EEG-based UA research has reached high accuracy within carefully designed laboratory-based experimental settings. However, there is an absence of research performed within ecological valid settings. Moreover, most of the existing research focus rather on the AI-aspect and does not address sufficiently the aspects of security and privacy preservation. From this perspective this paper suggests also specific future research suggestions aiming to develop secure and privacy friendly EEG-based user authentication systems.

Hence, we pointed towards the following on-going research endeavors: a) to apply template protection methods to address the security threat of brain-based biometric leaks from centralized architectures; b) to increase privacy preservation of trained models without having full and direct access at raw data by deploying federated architectures; c) to involve the end-user in the decision making process of who, when and where her biometric data are being accessed, stored or processed; d) to drive innovation and research on hybrid EEG-based protocols aiming to combine state-of-the-art knowledge-based UA schemes with EEG-based ones.

In conclusion, there is a need for sustainable and decentralized technologies for data storage and sharing based on distributed ledger technologies aiming to increase scalability of biometric data [111], [112]. In addition, there is a need for standardized data models that describe in a holistic manner static and dynamic contextual data and personal biometric-driven data that will coherently reflect end-users based on semantic-based meta-data descriptions. Furthermore, there is a need for technologies that enable end-users to control, manage and share their biometric data from their device, by applying a sustainable self-sovereign identity management approach. In addition, end-users should be able to share their identity attributes (e.g., biometric data, sensitive personal data) securely over a decentralized system. Hence, it is important to further explore self-sovereign identity (SSI) management architectures as a potential solution for end-users to maintain control over different access levels to their biometric data. In such a scenario, combining the above-mentioned solutions - biometric template protection and SSI - with blockchain technology (which provides a ledger solution for tracking the usage of user anti-phishing models) would also contribute to non-repudiation solutions.

**Limitations and Challenges.** Although we performed a systematic literature investigation over the last twenty-four years, one limitation of this survey relates to the existing possibility that there might be research papers that have not been identified. Whatsoever, we triangulated our search results following state of the art literature survey methods [85]. In addition, we would like to also refer to limitations of EEG-based user authentication approaches. These limitations are related to the fact that EEG-based user authentication nowadays necessitates for end-users to wear headsets (for performing such experiments) which are rather inconvenient for end-users. Furthermore, EEG-based user authentication requires the processing and/or storage of sensitive users' data, such as, brainiac activity-related data. As such, a system implementing EEG-based authentication should be compliant with state-of-the art privacy protection regulations (e.g., General Data Protection Regulation - GDPR) and preserve the privacy of users' data [117], [118], [119].

## APPENDIX

See Table 3.

## ACKNOWLEDGMENT

The authors would like to thank Verouchis George for assisting this research and the anonymous reviewers for their insightful and constructive feedback.

## REFERENCES

[1] M. K. Abdullah, K. S. Subari, J. L. C. Loong, and N. N. Ahmad, "Analysis of effective channel placement for an EEG-based biometric system," in *Proc. IEEE EMBS Conf. Biomed. Eng. Sci. (IECBES)*, Nov. 2010, pp. 303–306, doi: 10.1109/IECBES.2010.5742249.

[2] M. Abo-Zahhad, S. M. Ahmed, and S. N. Abbas, "A new EEG acquisition protocol for biometric identification using eye blinking signals," *Int. J. Intell. Syst. Appl.*, vol. 7, no. 6, pp. 48–54, May 2015, doi: 10.5815/IJISA.2015.06.05.

[3] A. Almehmadi and K. El-Khatib, "The state of the art in electroencephalogram and access control," in *Proc. 3rd Int. Conf. Commun. Inf. Technol. (ICCIT)*, Jun. 2013, pp. 49–54, doi: 10.1109/iccitechnology.2013.6579521.

[4] R. Alomari, M. V. Martin, S. MacDonald, and C. Bellman, "Using EEG to predict and analyze password memorability," in *Proc. IEEE Int. Conf. Cognit. Comput. (ICCC)*, Jul. 2019, pp. 42–49, doi: 10.1109/ICCC.2019.00019.

[5] B. C. Armstrong, M. V. Ruiz-Blondet, N. Khalifian, K. J. Kurtz, Z. Jin, and S. Laszlo, "Brainprint: Assessing the uniqueness, collectability, and permanence of a novel method for ERP biometrics," *Neurocomputing*, vol. 166, pp. 59–67, Oct. 2015, doi: 10.1016/j.neucom.2015.04.025.

[6] P. Arnau-Gonzalez, S. Katsigiannis, N. Ramzan, D. Tolson, and M. Arevalillo-Herrez, "ES1D: A deep network for EEG-based subject identification," in *Proc. IEEE 17th Int. Conf. Bioinf. Bioeng. (BIBE)*, Oct. 2017, pp. 81–85, doi: 10.1109/BIBE.2017.00-74.

[7] V. Bhateja, A. Gupta, A. Mishra, and A. Mishra, "Artificial neural networks based fusion and classification of EEG/EOG signals," in *Advances in Intelligent Systems and Computing*. Singapore: Springer, 2019, pp. 141–148, doi: 10.1007/978-981-13-3338-5_14.

[8] A. J. Bidgoly, H. J. Bidgoly, and Z. Arezoumand, "A survey on methods and challenges in EEG based authentication," *Comput. Secur.*, vol. 93, Jun. 2020, Art. no. 101788, doi: 10.1016/j.cose.2020.101788.

[9] A. J. Bidgoly, H. J. Bidgoly, and Z. Arezoumand, "Towards a universal and privacy preserving EEG-based authentication system," *Sci. Rep.*, vol. 12, no. 1, pp. 1–12, Feb. 2022, doi: 10.1038/s41598-022-06527-7.

[10] R. Caton, "Electrical currents of the brain," *J. Nervous Mental Disease*, vol. 2, no. 4, p. 610, 1875. [Online]. Available: https://journals.lww.com/jonmd/Fulltext/1875/10000/Electrical_Currents_of_the_Brain.13.aspx

[11] P. Chellaiah, S. Bodda, R. Lal, C. Madhu, V. Zamare, B. Nair, S. Diwakar, P. Chellaiah, and K. Achuthan, "EEG-based assessment of image sequence-based user authentication in computer network security," in *Proc. Int. Conf. Electr., Electron., Optim. Techn. (ICEEOT)*, Mar. 2016, pp. 3674–3677, doi: 10.1109/ICEEOT.2016.7755395.

[12] J. X. Chen, Z. J. Mao, W. X. Yao, and Y. F. Huang, "EEG-based biometric identification with convolutional neural network," *Multimedia Tools Appl.*, vol. 79, pp. 15–16, Feb. 2019, doi: 10.1007/s11042-019-7258-4.

[13] J. Chuang, H. Nguyen, C. Wang, and B. Johnson, "I think, therefore I am: Usability and security of authentication using brainwaves," in *Financial Cryptography and Data Security*. Berlin, Germany: Springer, 2013, pp. 1–16, doi: 10.1007/978-3-642-41320-9_1.

[14] M. T. Curran, N. Merrill, J. Chuang, and S. Gandhi, "One-step, three-factor authentication in a single earpiece," in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput. Proc. ACM Int. Symp. Wearable Comput.*, New York, NY, USA, Sep. 2017, pp. 21–24, doi: 10.1145/3123024.3123087.

[15] R. Das, E. Maiorana, and P. Campisi, "Motor imagery for eeg biometrics using convolutional neural network," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Apr. 2018, pp. 2062–2066, doi: 10.1109/ICASSP.2018.8461909.

[16] C. S. DaSalla, H. Kambara, Y. Koike, and M. Sato, "Spatial filtering and single-trial classification of EEG during vowel speech imagery," in *Proc. 3rd Int. Conv. Rehabil. Eng. Assistive Technol.*, 2009, pp. 1–4, doi: 10.1145/1592700.1592731.

[17] D. Dasgupta, A. Roy, and A. Nag, *Advances in User Authentication*. Cham, Switzerland: Springer, 2017.

[18] E. Debie, N. Moustafa, and A. Vasilakos, "Session invariant EEG signatures using elicitation protocol fusion and convolutional neural network," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 4, pp. 2488–2500, Jul. 2022, doi: 10.1109/TDSC.2021.3060775.

[19] S. Deepika and P. Pandiaraja, "Ensuring CIA triad for user data using collaborative filtering mechanism," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Feb. 2013, pp. 925–928.

[20] Y. Di, X. An, F. He, S. Liu, Y. Ke, and D. Ming, "Robustness analysis of identification using resting-state EEG signals," *IEEE Access*, vol. 7, pp. 42113–42122, 2019, doi: 10.1109/ACCESS.2019.2907644.

[21] W. T. Edgar and O. D. Manz, "Science and cyber security," in *Research Methods for Cyber Security*. Amsterdam, The Netherlands: Elsevier, 2017, pp. 33–62, doi: 10.1016/b978-0-12-805349-2.00002-9.

[22] K. Fenrich, "Securing your control system: The 'CIA triad' is a widely used benchmark for evaluating information system security effectiveness," *Power Eng.*, vol. 112, no. 2, pp. 44–49, 2008.

[23] D. Frank, J. Mabrey, and K. Yoshigoe, "Personalizable neurological user authentication framework," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Jan. 2017, pp. 932–936, doi: 10.1109/ICCNC.2017.7876258.

[24] C. M. Gaspar, G. A. Rousselet, and C. R. Pernet, "Reliability of ERP and single-trial analyses," *NeuroImage*, vol. 58, no. 2, pp. 620–629, Sep. 2011, doi: 10.1016/j.neuroimage.2011.06.052.

[25] S. R. K. Gopal and D. Shukla, "Concealable biometric-based continuous user authentication system an EEG induced deep learning model," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Aug. 2021, pp. 1–8, doi: 10.1109/IJCB52358.2021.9484345.

[26] Q. Gui, Z. Jin, and W. Xu, "Exploring EEG-based biometrics for user identification and authentication," in *Proc. IEEE Signal Process. Med. Biol. Symp. (SPMB)*, Dec. 2014, pp. 1–6, doi: 10.1109/SPMB.2014.7002950.

[27] Q. Gui, Z. Jin, W. Xu, M. V. Ruiz-Blondet, and S. Laszlo, "Multichannel EEG-based biometric using improved RBF neural networks," in *Proc. IEEE Signal Process. Med. Biol. Symp. (SPMB)*, Dec. 2015, pp. 1–6, doi: 10.1109/SPMB.2015.7405418.

[28] E. Gupta, M. Agarwal, and R. Sivakumar, "Blink to get in: Biometric authentication for mobile devices using EEG signals," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6, doi: 10.1109/ICC40277.2020.9148741.

[29] P. Gupta, S. Behera, M. Vatsa, and R. Singh, "On iris spoofing using print attack," in *Proc. 22nd Int. Conf. Pattern Recognit.*, Aug. 2014, pp. 1681–1686, doi: 10.1109/ICPR.2014.296.

[30] E.-S. Haukipuro, V. Kolehmainen, J. Mylläri nen, S. Remander, J. Salo, T. Takko, L. N. Nguyen, S. Sigg, and R. D. Findling, "Mobile brainwaves: On the interchangeability of simple authentication tasks with low-cost, single-electrode EEG devices," *IEICE Trans. Commun.*, vol. 102, no. 4, pp. 760–767, Apr. 2019, doi: 10.1587/transcom.2018sep0016.

[31] R. Ince, S. S. Adanır, and F. Sevmez, "The inventor of electroencephalography (EEG): Hans Berger (1873–1941)," *Child's Nervous Syst.*, vol. 37, no. 9, pp. 2723–2724, Sep. 2021, doi: 10.1007/s00381-020-04564-z.

[32] A. Jalilifard, D. Chen, A. K. Mutasim, M. R. Bashar, R. S. Tipu, A.-U.-K. Shawon, N. Sakib, M. A. Amin, and M. K. Islam, "Use of spontaneous blinking for application in human authentication," *Eng. Sci. Technol., Int. J.*, vol. 23, no. 4, pp. 903–910, Aug. 2020, doi: 10.1016/j.jestch.2020.05.007.

[33] B. Johnson, T. Maillart, and J. Chuang, "My thoughts are not your thoughts," in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput., Adjunct Publication*, Sep. 2014, pp. 1329–1338, doi: 10.1145/2638728.2641710.

[34] J.-H. Kang, Y. C. Jo, and S.-P. Kim, "Electroencephalographic feature evaluation for improving personal authentication performance," *Neurocomputing*, vol. 287, pp. 93–101, Apr. 2018, doi: 10.1016/j.neucom.2018.01.074.

[35] B. Kaur, D. Singh, and P. P. Roy, "A novel framework of EEG-based user identification by analyzing music-listening behavior," *Multimedia Tools Appl.*, vol. 76, no. 24, pp. 25581–25602, Dec. 2017, doi: 10.1007/s11042-016-4232-2.

[36] W. Khalifa, A. Salem, M. Roushdy, and K. Revett, "A survey of EEG based user authentication schemes," in *Proc. 8th Int. Conf. Inform. Syst. (INFOS)*, 2012, pp. 55–60.

[37] D. Kim and K. Kim, "Resting state EEG-based biometric system using concatenation of quadrantal functional networks," *IEEE Access*, vol. 7, pp. 65745–65756, 2019, doi: 10.1109/ACCESS.2019.2917918.

[38] Z. Kleinman. (2014). *Politician's Fingerprint 'Cloned From Photos' by Hacker*. [Online]. Available: https://www.bbc.com/news/technology-30623611

[39] P. Kumar, R. Saini, B. Kaur, P. P. Roy, and E. Scheme, "Fusion of neuro-signals and dynamic signatures for person authentication," *Sensors*, vol. 19, no. 21, p. 4641, Oct. 2019, doi: 10.3390/s19214641.

[40] P. Kumar, R. Saini, P. Pratim Roy, and D. Prosad Dogra, "A bio-signal based framework to secure mobile devices," *J. Netw. Comput. Appl.*, vol. 89, pp. 62–71, Jul. 2017, doi: 10.1016/j.jnca.2017.02.011.

[41] P. Kumari and A. Vaish, "Brainwave based user identification system: A pilot study in robotics environment," *Robot. Auto. Syst.*, vol. 65, pp. 15–23, Mar. 2015, doi: 10.1016/j.robot.2014.11.015.

[42] S.-Y. Lee and E.-S. Jung, "User authentication systems based on brain finger-prints," *Proc. SPIE*, vol. 9118, pp. 113–118, May 2014, doi: 10.1117/12.2053494.

[43] S. Li, S. Savaliya, L. Marino, A. M. Leider, and C. C. Tappert, "Brain signal authentication for human–computer interaction in virtual reality," in *Proc. IEEE Int. Conf. Comput. Sci. Eng. (CSE) IEEE Int. Conf. Embedded Ubiquitous Comput. (EUC)*, Aug. 2019, pp. 115–120, doi: 10.1109/CSE/EUC.2019.00031.

[44] S. Liew, Y. 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, doi: 10.1049/iet-bmt.2017.0044.

[45] C. G. Lim, C. Y. Lee, and Y. M. Kim, "A performance analysis of user's intention classification from EEG signal by a computational intelligence in BCI," in *Proc. 2nd Int. Conf. Mach. Learn. Soft Comput.*, Feb. 2018, pp. 174–179, doi: 10.1145/3184066.3184092.

[46] F. Lin, K. W. Cho, C. Song, W. Xu, and Z. Jin, "Brain password," in *Proc. 16th Annu. Int. Conf. Mobile Syst., Appl., Services*, Jun. 2018, pp. 296–309, doi: 10.1145/3210240.3210344.

[47] M. A. Lopez-Gordo, R. Ron-Angevin, and F. Pelayo, "Authentication of brain–computer interface users in network applications," in *Advances in Computational Intelligence*. Cham, Switzerland: Springer, 2015, pp. 124–132, doi: 10.1007/978-3-319-19258-1_11.

[48] L. Ma, J. W. Minett, T. Blu, and W. S.-Y. Wang, "Resting state EEG-based biometrics for individual identification using convolutional neural networks," in *Proc. 37th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Aug. 2015, pp. 2848–2851, doi: 10.1109/EMBC.2015.7318985.

[49] E. Maiorana and P. Campisi, "Longitudinal evaluation of EEG-based biometric recognition," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 5, pp. 1123–1138, May 2018, doi: 10.1109/TIFS.2017.2778010.

[50] D. Makri, C. Farmaki, and V. Sakkalis, "Visual fatigue effects on steady state visual evoked potential-based brain computer interfaces," in *Proc. 7th Int. IEEE/EMBS Conf. Neural Eng. (NER)*, Apr. 2015, pp. 70–73, doi: 10.1109/NER.2015.7146562.

[51] Z. Mao, W. X. Yao, and Y. Huang, "EEG-based biometric identification with deep learning," in *Proc. 8th Int. IEEE/EMBS Conf. Neural Eng. (NER)*, May 2017, pp. 609–612, doi: 10.1109/NER.2017.8008425.

[52] S. Marcel and J. D. R. Millan, "Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 743–752, Apr. 2007, doi: 10.1109/TPAMI.2007.1012.

[53] T. Nakamura, V. Goverdovsky, and D. P. Mandic, "In-ear EEG biometrics for feasible and readily collectable real-world person authentication," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 3, pp. 648–661, Mar. 2018, doi: 10.1109/TIFS.2017.2763124.

[54] 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*. Berlin, Germany: Springer, 2013, pp. 513–523, doi: 10.1007/978-3-642-53917-6_46.

[55] M. Phothisonothai, "An investigation of using SSVEP for EEG-based user authentication system," in *Proc. Asia–Pacific Signal Inf. Process. Assoc. Annu. Summit Conf. (APSIPA)*, Dec. 2015, pp. 923–926, doi: 10.1109/apsipa.2015.7415406.

[56] E. Piciucco, E. Maiorana, O. Falzon, K. P. Camilleri, and P. Campisi, "Steady-state visual evoked potentials for EEG-based biometric identification," in *Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG)*, Sep. 2017, pp. 1–5, doi: 10.23919/biosig.2017.8053521.

[57] M. Poulos, M. Rangoussi, N. Alexandris, and A. Evangelou, "Person identification from the EEG using nonlinear signal classification," *Methods Inf. Med.*, vol. 41, no. 1, pp. 64–75, 2002.

[58] M. Rekrut, T. Jungbluth, J. Alexandersson, and A. Krüger, "Spinning icons: Introducing a novel SSVEP-BCI paradigm based on rotation," in *Proc. 26th Int. Conf. Intell. User Interfaces*, Apr. 2021, pp. 234–243, doi: 10.1145/3397481.3450646.

[59] T. Riley. (2020). *Analysis | The Cybersecurity 202: Global Losses From Cybercrime Skyrocketed to Nearly $1 Trillion in 2020, New Report Finds*. [Online]. Available: https://www.washingtonpost.com/politics/2020/12/07/cybersecurity-202-global-losses-cybercrime-skyrocketed-nearly-1-trillion-2020/

[60] D. La Rocca, P. Campisi, and G. Scara, "Stable EEG features for biometric recognition in resting state conditions," in *Biomedical Engineering Systems and Technologies*. Berlin, Germany: Springer, 2014, pp. 313–330, doi: 10.1007/978-3-662-44485-6_22.

[61] M. V. Ruiz-Blondet, Z. Jin, and S. Laszlo, "CEREBRE: A novel method for very high accuracy event-related potential biometric identification," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 7, pp. 1618–1629, Jul. 2016, doi: 10.1109/TIFS.2016.2543524.

[62] T. Schons, J. P. G. Moreira, H. L. P. Silva, N. V. Coelho, and J. S. E. Luz, "Convolutional network for EEG-based biometric," in *Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications*. Cham, Switzerland: Springer, 2018, pp. 601–608, doi: 10.1007/978-3-319-75193-1_72.

[63] S. W. Shah and S. S. Kanhere, "Recent trends in user authentication—A survey," *IEEE Access*, vol. 7, pp. 112505–112519, 2019, doi: 10.1109/ACCESS.2019.2932400.

[64] P. K. Sharma and A. Vaish, "Individual identification based on neurosignal using motor movement and imaginary cognitive process," *Optik*, vol. 127, no. 4, pp. 2143–2148, Feb. 2016, doi: 10.1016/j.ijleo.2015.09.020.

[65] J. Sooriyaarachchi, S. Seneviratne, K. Thilakarathna, and A. Y. Zomaya, "MusicID: A brainwave-based user authentication system for Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 8304–8313, May 2021, doi: 10.1109/JIOT.2020.3044726.

[66] Y. Sun, F. P.-W. Lo, and B. Lo, "EEG-based user identification system using 1D-convolutional long short-term memory neural networks," *Expert Syst. Appl.*, vol. 125, pp. 259–267, Jul. 2019, doi: 10.1016/j.eswa.2019.01.080.

[67] J. Thorpe, P. C. van Oorschot, and A. Somayaji, "Pass-thoughts: Authenticating with our minds," in *Proc. Workshop New Secur. Paradigms*, 2005, pp. 45–56, doi: 10.1145/1146269.1146282.

[68] A. Vahid and E. Arbabi, "Human identification with EEG signals in different emotional states," in *Proc. 23rd Iranian Conf. Biomed. Eng. 1st Int. Iranian Conf. Biomed. Eng. (ICBME)*, 2016, pp. 242–246, doi: 10.1109/ICBME.2016.7890964.

[69] A. Valsaraj, I. Madala, N. Garg, M. Patil, and V. Baths, "Motor imagery based multimodal biometric user authentication system using EEG," in *Proc. Int. Conf. Cyberworlds (CW)*, Sep. 2020, pp. 272–279, doi: 10.1109/cw49994.2020.00050.

[70] T. Waili, M. G. M. Johar, K. A. Sidek, N. S. H. M. Nor, H. Yaacob, and M. Othman, "EEG based biometric identification using correlation and MLPNN models," *Int. J. Online Biomed. Eng.*, vol. 15, no. 10, p. 77, Jun. 2019, doi: 10.3991/ijoe.v15i10.10880.

[71] Y. Wang, S. Wang, and M. Xu, "The function of color and structure based on EEG features in landscape recognition," *Int. J. Environ. Res. Public Health*, vol. 18, no. 9, p. 4866, May 2021, doi: 10.3390/ijerph18094866.

[72] T. Wilaiprasitporn, A. Ditthapron, K. Matchaparn, T. Tongbuasirilai, N. Banluesombatkul, and E. Chuangsuwanich, "Affective EEG-based person identification using the deep learning approach," *IEEE Trans. Cognit. Develop. Syst.*, vol. 12, no. 3, pp. 486–496, Sep. 2020, doi: 10.1109/TCDS.2019.2924648.

[73] Q. Wu, Y. Zeng, C. Zhang, L. Tong, and B. Yan, "An EEG-based person authentication system with open-set capability combining eye blinking signals," *Sensors*, vol. 18, no. 2, p. 335, Jan. 2018, doi: 10.3390/s18020335.

[74] F. Yousefi, H. Kolivand, and T. Baker, "SaS-BCI: A new strategy to predict image memorability and use mental imagery as a brain-based biometric authentication," *Neural Comput. Appl.*, vol. 33, no. 9, pp. 4283–4297, Aug. 2020.

[75] T. Yu, C.-S. Wei, K.-J. Chiang, M. Nakanishi, and T.-P. Jung, "EEG-based user authentication using a convolutional neural network," in *Proc. 9th Int. IEEE/EMBS Conf. Neural Eng. (NER)*, Mar. 2019, pp. 1011–1014, doi: 10.1109/NER.2019.8716965.

[76] F. Zhang, Z. Mao, Y. F. Huang, L. Xu, and G. Y. Ding, "Deep learning models for EEG-based rapid serial visual presentation event classification," *J. Inf. Hiding Multimedia Signal Process.* vol. 9, pp. 177–187, Jan. 2018.

[77] S. Zhang, L. Sun, X. Mao, C. Hu, and P. Liu, "Review on EEG-based authentication technology," *Comput. Intell. Neurosci.*, vol. 2021, pp. 1–20, Dec. 2021, doi: 10.1155/2021/5229576.

[78] X. Zhang, L. Yao, C. Huang, T. Gu, Z. Yang, and Y. Liu, "DeepKey," *ACM Trans. Intell. Syst. Technol.*, vol. 11, no. 4, pp. 1–24, Aug. 2020, doi: 10.1145/3393619.

[79] A. Zúquete, B. Quintela, and J. P. S. Cunha, "Biometric authentication using brain responses to visual stimuli," in *Proc. 3rd Int. Conf. Bio-Inspired Syst. Signal Process.*, 2010, pp. 103–112, doi: 10.5220/0002750101030112.

[80] O. Özdenizci, Y. Wang, T. Koike-Akino, and D. Erdoğmuş, "Adversarial deep learning in EEG biometrics," *IEEE Signal Process. Lett.*, vol. 26, no. 5, pp. 710–714, Mar. 2019, doi: 10.1109/LSP.2019.2906826.

[81] The Ten Twenty Electrode System, "International federation of societies for electroencephalography and clinical neurophysiology," *Amer. J. EEG Technol.*, vol. 1, no. 1, pp. 13–19, 1961, doi: 10.1080/00029238.1961.11080571.

[82] L. Hu and Z. Zhang, "Evolving EEG signal processing techniques in the age of artificial intelligence," *Brain Sci. Adv.*, vol. 6, no. 3, pp. 159–161, Sep. 2020.

[83] X. Wan, K. Zhang, S. Ramkumar, J. Deny, G. Emayavaramban, M. S. Ramkumar, and A. F. Hussein, "A review on electroencephalogram based brain computer interface for elderly disabled," *IEEE Access*, vol. 7, pp. 36380–36387, 2019.

[84] B. Zhang, C. Chai, Z. Yin, and Y. Shi, "Design and implementation of an EEG-based learning-style recognition mechanism," *Brain Sci.*, vol. 11, no. 5, p. 613, May 2021.

[85] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *Int. J. Surg.*, vol. 8, no. 5, pp. 336–341, 2010, doi: 10.1016/j.ijsu.2010.02.007.

[86] A. K. Jindal, S. R. Chalamala, and S. K. Jami, "Securing face templates using deep convolutional neural network and random projection," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2019, pp. 1–6.

[87] A. K. Jindal, I. Shaik, V. Vasudha, S. R. Chalamala, R. Ma, and S. Lodha, "Secure and privacy preserving method for biometric template protection using fully homomorphic encryption," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Dec. 2020, pp. 1127–1134.

[88] A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognit. Lett.*, vol. 79, pp. 80–105, Aug. 2016.

[89] A. Bhalla, "The latest evolution of biometrics," *Biometric Technol. Today*, vol. 2020, no. 8, pp. 5–8, Sep. 2020.

[90] *Information Technology—Vocabulary—Part 37: Biometrics*, International Organization for Standardization, Geneva, Switzerland, 2012.

[91] V. N. Boddeti, "Secure face matching using fully homomorphic encryption," in *Proc. IEEE 9th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, Oct. 2018, pp. 1–10.

[92] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," *Proc. IEEE*, vol. 92, no. 6, pp. 948–960, Jun. 2004.

[93] A. Cavoukian and A. Stoianov, "Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacy," Information and Privacy Commissioner, Ontario, Toronto, ON, Canada, Tech. Rep., 2007.

[94] M. Ao and S. Z. Li, "Near infrared face based biometric key binding," in *Advances in Biometrics*. Berlin, Germany: Springer, 2009, pp. 376–385.
[95] H. Lu, K. Martin, F. Bui, K. N. Plataniotis, and D. Hatzinakos, "Face recognition with biometric encryption for privacy-enhancing self-exclusion," in *Proc. 16th Int. Conf. Digit. Signal Process.*, Jul. 2009, pp. 1–8.
[96] A. B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 28, no. 12, pp. 1892–1901, Dec. 2006.
[97] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.
[98] S. K. Jami, S. R. Chalamala, and A. K. Jindal, "Biometric template protection through adversarial learning," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2019, pp. 1–6.
[99] A. K. Jindal, S. Chalamala, and S. K. Jami, "Face template protection using deep convolutional neural network," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2018, pp. 462–470.
[100] R. K. Pandey, Y. Zhou, B. U. Kota, and V. Govindaraju, "Deep secure encoding for face template protection," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2016, pp. 77–83.
[101] N. Rodríguez-Barroso, G. Stipcich, D. Jiménez-López, J. A. Ruiz-Millán, E. Martínez-Cámara, G. González-Seco, M. V. Luzón, M. A. Veganzones, and F. Herrera, "Federated learning and differential privacy: Software tools analysis, the Sherpa.ai FL framework and methodological guidelines for preserving data privacy," *Inf. Fusion*, vol. 64, pp. 270–292, Dec. 2020.
[102] DataFleets. (2020). *DataFleets: The Federated Intelligence Platform*. [Online]. Available: https://www.datafleets.com
[103] FATE. (2020). *Federated AI Technology Enabler*. [Online]. Available: https://github.com/FederatedAI/FATE
[104] TensorFlow. (2020). *TensorFlow Federated: Machine Learning on Decentralized Data*. [Online]. Available: https://www.tensorflow.org/federated
[105] S. Caldas, S. M. K. Duddu, P. Wu, T. Li, J. Konecny, H. B. McMahan, V. Smith, and A. Talwalkar. (2019). *Leaf: A Benchmark for Federated Settings*. [Online]. Available: https://leaf.cmu.edu
[106] K. Wei, J. Li, M. Ding, C. Ma, H. H. Yang, F. Farokhi, S. Jin, T. Q. S. Quek, and H. V. Poor, "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3454–3469, 2020.
[107] R. C. Geyer, T. Klein, and M. Nabi, "Differentially private federated learning: A client level perspective," in *Proc. NIPS Workshop, Mach. Learn. Phone Consum. Devices*, 2017, pp. 1–7.
[108] J. Zhang, J. Wang, Y. Zhao, and B. Chen, "An efficient federated learning scheme with differential privacy in mobile edge computing," in *Proc. Int. Conf. Mach. Learn. Intell. Commun.* Cham, Switzerland: Springer, 2019, pp. 538–550.
[109] S. Truex, N. Baracaldo, A. Anwar, T. Steinke, H. Ludwig, R. Zhang, and Y. Zhou, "A hybrid approach to privacy-preserving federated learning," in *Proc. 12th ACM Workshop Artif. Intell. Secur.*, Nov. 2019, pp. 1–11.
[110] Z. Rui and Z. Yan, "A survey on biometric authentication: Toward secure and privacy-preserving identification," *IEEE Access*, vol. 7, pp. 5994–6009, 2018.
[111] B. Wu, W. Meng, and W.-Y. Chiu, "Towards enhanced EEG-based authentication with motor imagery brain-computer interface," in *Proc. 38th Annu. Comput. Secur. Appl. Conf.*, New York, NY, USA, 2022, pp. 799–812, doi: 10.1145/3564625.3564656.
[112] N. A. Alzahab, A. D. Iorio, M. Baldi, and L. Scalise, "Effect of auditory stimuli on electroencephalography-based authentication," in *Proc. IEEE Int. Conf. Metrol. Extended Reality, Artif. Intell. Neural Eng. (MetroXRAINE)*, Oct. 2022, pp. 388–392, doi: 10.1109/METROXRAINE54828.2022.9967652.
[113] K. Bialas, M. Kedziora, R. Chalupnik, and H. H. Song, "Multifactor authentication system using simplified EEG brain–computer interface," *IEEE Trans. Hum.-Mach. Syst.*, vol. 52, no. 5, pp. 867–876, Oct. 2022, doi: 10.1109/THMS.2022.3196142.
[114] M. A. Rahman and I. Nakanishi, "Person authentication using brain waves evoked by individual-related and imperceptible visual stimuli," in *Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG)*, Darmstadt, Germany, Sep. 2022, pp. 1–5, doi: 10.1109/BIOSIG55365.2022.9897041.
[115] Z. Alkhyeli, A. Alshehhi, M. Alhemeiri, S. Aldhanhani, K. AlBalushi, F. A. AlNuaimi, and A. N. Belkacem, "Secure password using EEG-based BrainPrint system: Unlock smartphone password using brain–computer interface technology," in *Proc. IEEE Int. Conf. Bioinf. Biomed. (BIBM)*, Las Vegas, NV, USA, Dec. 2022, pp. 1982–1987, doi: 10.1109/BIBM55620.2022.9995304.
[116] M. S. I. Leon, J. Akter, N. Sakib, and M. K. Islam, "Analysis of EEG signal classification for application in SSVEP-based BCI using convolutional neural network," in *Proc. Int. Conf. Big Data, IoT, Mach. Learn.*, in Lecture Notes on Data Engineering and Communications Technologies, vol. 95, 2022, pp. 593–606, doi: 10.1007/978-981-16-6636-0_45.
[117] C. Fidas, M. Belk, D. Portugal, and A. Pitsillides, "Privacy-preserving biometric-driven data for student identity management: Challenges and approaches," in *Proc. Adjunct Proc. 29th ACM Conf. User Modeling, Adaptation Personalization*, New York, NY, USA, Jun. 2021, pp. 368–370, doi: 10.1145/3450614.3464470.
[118] M. Gomez-Barrero, P. Drozdowski, C. Rathgeb, J. Patino, M. Todisco, A. Nautsch, N. Damer, J. Priesnitz, N. Evans, and C. Busch, "Biometrics in the era of COVID-19: Challenges and opportunities," *IEEE Trans. Technol. Soc.*, vol. 3, no. 4, pp. 307–322, Dec. 2022.
[119] M. Hernandez-de-Menendez, R. Morales-Menendez, C. Escobar, and J. Arinez, "Biometric applications in education," *Int. J. Interact. Des. Manuf.*, vol. 15, pp. 1–16, Jul. 2021.
[120] P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security Privacy*, vol. 16, no. 4, pp. 20–29, Jul./Aug. 2018.
[121] N. D. Sarier, "Privacy preserving biometric identification on the bitcoin blockchain," in *Proc. Int. Symp. Cyberspace Saf. Secur.* Cham, Switzerland: Springer, 2018, pp. 254–269.
[122] A. Constantinides, M. Belk, C. Fidas, R. Beumers, D. Vidal, W. Huang, J. Bowles, T. Webber, A. Silvina, and A. Pitsillides, "Security and usability of a personalized user authentication paradigm: Insights from a longitudinal study with three healthcare organizations," *ACM Trans. Comput. Healthcare*, vol. 4, no. 1, pp. 1–40, Jan. 2023, doi: 10.1145/3564610.

**CHRISTOS A. FIDAS** received the Diploma degree in electrical and computer engineering and the Ph.D. degree in information systems from the University of Patras, Greece. He is a currently a Faculty Member with the Department of Electrical and Computer Engineering, University of Patras. His research interests include information systems, with an emphasis on human–computer interaction, usable-security, and cultural heritage. He has an extensive publication record in reputable scientific journals and conferences, has been granted a patent, and has received several scientific awards and research grants for his contributions to the field. For more information visit the link (http://cfidas.info).

**DIMITRIOS LYRAS** (Senior Member, IEEE) received the Diploma degree in electrical and computer engineering and the Ph.D. degree in artificial intelligence from the University of Patras, Greece.

He continued with his postdoctoral studies with the Ludwig Maximilian University of Munich, Germany. He has significant experience and leading research on machine learning, natural language processing, and stochastic and statistical computational modeling, which combined with his technical fluency in the most popular programming languages and software stacks, enabled him to design and implement efficient data-driven solutions and expert systems for business-critical operations. He is currently a principal data scientist for multinational software companies and in parallel pursuing his independent research with focus on the application of cutting-edge artificial intelligence solutions to address challenges of the human–computer interaction domain.

Dr. Lyras has led the IEEEXtreme Programming Competition from the Chairperson position and was awarded the IEEE MGA Achievement Award, in 2009.