Short Review of EEG-Based Authentication Systems: Motivations, Challenges, and Recommendations

Aseel Yasir Younis[1], Moceheb Lazam Shuwandy[*1]

[1]Computer Sciences Department, College of Computer and Mathematical Sciences Tikrit University Tikrit, Iraq

aseel.y.younis22ms@st.tu.edu.iq, *moceheb@tu.edu.iq

Abstract:
Recent years have detected a spike in fascination with mobile authentication methods, especially EEG-based ones. These strategies are gaining favor for their potential to boost security efforts. Various authentication methods are available across different platforms, some more effective in smartphone security. A study analyzes articles on EEG technology for smartphone authentication across platforms, aiming to provide best practices and address academic challenges and motivations. The methodological approach used in previous research is discussed to guide future researchers. A deep probe was executed on major databases from 2013 to 2023, identifying articles based on specific criteria. EEG-based smartphone authentication is a significant topic requiring attention, with this research exploring current perspectives and possibilities for further investigation in the field.

Keywords:(EEG-Based Authentication, Smartphone Security, Cognitive Biometrics, Signal Processing, Machine Learning, Cybersecurity).

1. Introduction

Recent years have shown a remarkably widespread interest in mobile authentication methods, especially those using electroencephalography (EEG) [1]. The integration of these methods into everyday life globally is primarily driven by their potential to enhance smartphone security. As smartphones become increasingly essential to personal and professional activities, ensuring their security has become crucial. The expansion and desirability of EEG-based authentication methods are increasing because of their capability to deliver heightened security levels in contrast to standard approaches [2]. These techniques rely on the distinct brainwave patterns produced during different cognitive tasks to authenticate user identity [3]. The demand for secure authentication mechanisms has sparked interest in EEG-based approaches, further supported by their high accuracy, resistance to replication, and non-intrusiveness, positioning them as a viable solution for mobile security [4].

EEG-based techniques are becoming more and more popular because of their advantages, such as improved security, ease of use, and the ability to use biometric data for dependable authentication [5]. They have a wide range of applications, spanning from user authentication on personal devices to safeguarding confidential information in professional environments [6]. These techniques operate on various mobile gadgets and systems, like Android and iOS [7]. Nevertheless, challenges persist, encompassing the acquisition and interpretation of EEG signals, the usability of authentication systems, and the assurance of data security [9]. Some techniques may lack the requisite robustness and accuracy, particularly in high-security scenarios [11]. Therefore, a thorough evaluation and analysis of EEG-based authentication methods are imperative for their practical implementation [13][14].

This study reviews and analyzes EEG-based smartphone authentication articles across platforms. Classifying written works, identifying driving forces and obstacles, and offering suggestions aim to deepen understanding of this developing area. The evaluation explored IEEE Xplore, Scopus, and ScienceDirect from 2013 to 2023, identifying 18 articles based on inclusion and exclusion criteria. EEG-based smartphone authentication significantly enhances mobile security [17], highlighting current research opportunities and encouraging further efforts [18]. This study aims to advance efficient, user-centric authentication systems to meet evolving mobile security needs [19].

The paper makes significant contributions to the field of EEG-based smartphone authentication:

A thorough literature review systematically categorizes and examines existing research, giving an overview of cutting-edge methods and technologies. Identifying motivations and challenges sheds light on the key factors driving or hindering the adoption of EEG-based authentication. Ideas for Future Research: Puts forward practical recommendations for increasing efficiency and usability. Methodological insights delve into the strategies utilized in previous studies, offering valuable perspectives and recommendations for future research directions. Authentication methods are evaluated, and various approaches are analyzed and highlighted, as well as their strengths and limitations. The promotion of multidisciplinary collaboration is emphasized, advocating for contributions from diverse fields such as neuroscience, machine learning, and cybersecurity. These contributions significantly contribute to the advancement of knowledge and enhancements in EEG-based smartphone authentication and mobile security.

2. Method of Systematic Review

EEG-based authentication in smartphones is a relatively recent academic field. This study's important term is "smartphone authentication" because it eliminates any devices that do not

use smartphones for authentication. This searches for and displays all results relating to authentication, including phones that use passwords and other types of EEG.

2.1. Source of Information

This particular research inquiry utilized three numeric repositories: IEEE Xplore, Scopus, and ScienceDirect. The scholarly articles covered a timeframe of the previous decade, from 2013 to 2023. Validation procedures were applied to remove redundancies and materials not pertinent to the scope of this study.

2.2. Selection of the Study and Search Scenario

Initially, a comprehensive literature search was undertaken, followed by two distinct phases of screening and filtering. During the initial phase, duplicates and irrelevant articles were eliminated by examining the titles and abstracts. The literature underwent a comprehensive examination during the second stage by thoroughly reading the articles filtered during the initial stage. On 8/2023, the search was carried out utilizing the search boxes of the three digital databases: IEEE Xplore, Scopus, and ScienceDirect, using the following keywords in combination: "EEG," "phone," "smartphone," "mobile health," "hand phone," "authentication." Books, reports, and survey findings were not included in the database selections. Only the most recent international journal and conference papers were used, covering the years 2013 to 2023.

2.3. Process of Data Collection

Following the search in the three digital databases, all articles from various sources were used to improve the search and yield better results. After reading them, the most important findings were summarized, organized, and presented. The necessary information was recorded in the form of Word and Excel lists and charts, including a complete list of articles, their respective source databases, motivations, challenges, recommendations, and other pertinent data.

3. Research Literature Taxonomy

The research spans seven years, from 2015 to 2021. The query search showed (n=351) articles published in 2015–2021: Science Direct (n=281/351), IEEE Xplore (n=52/351), and Scopus (n=18/351). In the four libraries, (n=3/351) were duplicates. After filtering titles and abstracts, (n=348/351) were excluded, leaving (n=323/348) articles. Reading the entire text resulted in the exclusion of (n=7/25), leaving (n=18/25) articles. Most selected articles (n=18) were from the US, with others from nine countries. The three main research categories were defense, attack, and others. The defense focused on protecting

smartphones, attacks utilized sensors to compromise phones, and others discussed defense development without precise sensor details, Figure 1.

3.1. Articles of Defense

These articles aim to identify and develop methods for securing smartphones through EEG authentication, leveraging the numerous sensors in these devices, such as accelerometers and gyroscopes. The defense group within the reviewed literature comprises various categories focusing on different biometric and traditional authentication methods to enhance smartphone security.

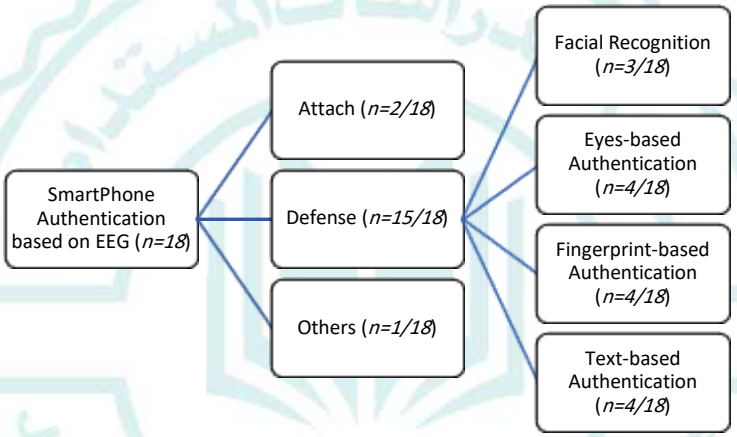

Figure 1 Research Literature Taxonomy

One key component highlighted in the articles is the integration of facial recognition technology. Specifically, 3 out of the 18 articles focus on extracting facial characteristics from digital images or video frames for authentication purposes [1][3][7]. These research endeavors investigate sophisticated algorithms for examining facial characteristics and improving precision in recognition systems. For example, some mobile devices, like Face ID on iPhones, have adopted this method to improve user authentication [7].

In the category of physiological biometrics related to the eyes, 4 out of the 18 articles discuss iris-based authentication methods [6][8][9][10]. These studies indicate that iris recognition can efficiently authenticate users by examining the distinctive patterns in the iris. Fingerprint-based authentication is another significant focus, with 4 out of the 18

articles dedicated to this method [1][3][11][12]. These studies capture distinctive features from the friction ridges on a user's fingertip to verify identity.

Text-based authentication schemes, including PINs and passwords, remain widely discussed despite more advanced methods. Despite the advancement of biometric substitutes, text-based authentication remains prevalent due to its ease of use and familiarity. [2][5][13][14]

3.2. Articles of Attack

These articles clarify attacks on smartphones using EEG and exploiting device vulnerabilities. Two articles discuss gait-based user authentication. Attackers aim to access private information or control devices by bypassing authentication mechanisms, either by leveraging identity details or circumventing procedures (e.g., database breaches or data interception). Surfing is also attacked [12][13].

3.3. Other Research Related to EEG

These are 1 out of 18 articles because they are not in the area of attack or defense but rather questionnaires to determine which EEGs are ideal for smartphone defense and which EEGs are the most practical and extensively utilized. Consequently, these specific publications were omitted from the analysis. These publications have nothing to do with the research's goal, which is to address EEG-based authentication in smartphones [14].

4 Motivations

Researchers are currently highlighting smartphone authentication by leveraging device sensors. The rationales behind this focus encompass advantages associated with usability, security, biometric authentication, and application functionalities. The primary objective of this study is to improve mobile security using EEG signals, mitigating vulnerabilities present in conventional methods such as PINs and passwords, establishing a pertinent architecture for cloud settings, and guaranteeing data authentication and security.

4.1 Benefits Related to Security Impact on Smartphones

Currently, protecting and securing information stored on smartphones is crucial. Authentication systems must be robust to guard against attacks and hackers due to prevalent hardware and security vulnerabilities. Leveraging unique EEG signals for user authentication offers significant advantages. This method protects against common attacks, such as shoulder surfing, and presents a highly secure biometric solution that is difficult to counterfeit by analyzing unique EEG signal patterns [2].

Moreover, the framework is designed to meet the demands of the security cloud environment, which is vulnerable to various attacks. This framework can significantly enhance security measures within the cloud [5]. It employs the Hidden Markov Model (HMM) to accurately capture and represent EEG signals for authentication purposes, ensuring only authorized individuals access the smartphone [15]. The strategy is further strengthened by using the SVM algorithm [16]. Traditional authentication methods have weaknesses that can be exploited by malicious individuals [17].

Additionally, this technique can integrate with portable gadgets, ensuring security for users on the move. Users frequently retain substantial quantities of personal and official information on mobile gadgets, utilizing passwords, PINs, biometric data, or patterns to ensure security. These methods are vulnerable to various attacks, such as shoulder surfing. EEG signals can mitigate these limitations and be transmitted wirelessly for processing [2]. The need for greater security for personal and business data on mobile devices is growing, and innovative biometric techniques offer a potential solution [8].

Traditional methods, like locking and keypad locking, need to be updated. PINs and patterns are vulnerable to guessing attacks, as users choose easily memorable secrets. Authentication tokens are also vulnerable to hacking. Research shows that smudges on screens can mimic unlock patterns [2]. Embedded sensors like accelerometers and microphones can guess PINs or patterns through side-channel attacks. BCI developments in smartphone security use new technologies to understand thoughts and intentions, capturing EEG waves non-intrusively. Electrodes on the user's cranium visualize geometric shapes and unlock phones based on user intentions and thoughts [14]. EEG signals offer a new biometric for user authentication, combining the benefits of traditional methods and overcoming their limitations. This study leverages EEG signal information, such as age and gender, for multi-level security systems [3].

4.2 Benefits Related to Authentication Usability

Biometric authentication through distinctive physiological characteristics has gained traction alongside the emergence of methods such as fingerprint identification, iris scanning, facial detection, voice verification, and analysis of walking patterns. Researchers explore EEG-based tasks—resting, thinking about a picture, and moving a finger—for authentication [3]. They detail data processing steps, feature extraction from the frequency spectrum and MFCC, and training a multilayer perceptron classifier [3]. While physiological features like facial attributes, iris patterns, and fingerprints are effective, they face impersonation attacks [1]. Researchers present an EEG-based person authentication framework for cloud environments, capturing signals through portable gadgets and transmitting them via REST for authentication [10].

4.3 Benefits Related to Application Activities

Emerging smartphone commerce apps and services require secure access to sensitive data. The EEG Workbench, a prototyping framework for building EEG data analytics on Android, addresses this need [10]. EEG signals vary significantly among individuals, making them suitable for authentication [2]. Consumer-grade EEG devices have increased the accessibility of EEG research for smartphones. However, specific implementations for Android are needed. The EEG Workbench aims to provide developers with tools to build EEG data analytics frameworks for Android [10].

A new framework secures mobile devices using EEG signals alongside pattern-based authentication methods. Researchers collected EEG signals from 50 users drawing patterns on their screens, revealing a promising method for robust authentication protocols [2]. EEG recording is considered the fastest, with characteristics dependent on cerebral cortex activity, representing a unique neural network for each person. EEG signals combine waveforms classified by frequency, amplitude, morphology, spatial distribution, and reactivity [8].

EEG signals offer unobtrusive input, especially with wearable devices like AR/VR. The main challenge is adaptability across users. Researchers used publicly available EEG motor imagery and eye-tracking data, demonstrating strong feasibility for authentication [7].

5 Challenges

Smartphones relying on EEG authentication lack robust data security. Key concerns include data accessibility, usability of authentication methods, and overall security. Researchers have identified pivotal issues in using EEG signals for authentication, emphasizing the need for secure and user-friendly data access. The feasibility of integrating EEG-based techniques is scrutinized, particularly regarding usability and security measures.

5.1 Concerns on Data Access

Data access is the primary challenge in authentication and smartphone security. Implementing transfer and file applicability systems for handheld devices, like smartphones, against various known attack types is difficult [2]. The study suggests using single and multimodal methods with a bidirectional short-term memory neural network (BLSTM-NN) for smartphone protection [1]. BCI algorithms using brain EEG data could be more generalizable across users. Researchers investigate using this technology for user authentication, akin to smartphone facial recognition [17]. They are developing biometric

authentication systems and combinations thereof. The current study uses publicly available EEG motor images and eye-tracking data, demonstrating the feasibility of using EEG and eye-tracking for authentication in VR/AR [7]. A unique approach leverages the connection between hand movements and brainwave signals to produce counterfeit EEG signals, exposing a significant threat to EEG-based authentication. An adversary with access to hand movement patterns and knowledge of their correlation with brainwave signals poses a severe security threat [13]. The final challenge with mobile big data is meeting growing performance demands while minimizing resource consumption. This research proposes a scalable architecture with three new algorithms for mobile data processing and analytics: mobile resources optimization, mobile analytics customization, and mobile offloading [19]. In EEG-based authentication for smartphones, data access is pivotal. They were acquiring, storing, and retrieving EEG data, which presented difficulties in safeguarding sensitive biometric data. Balancing security with user convenience is critical for EEG-based authentication solutions [19].

5.2 Concerns on Usability of EEG-Based Authentication

The intricate process of acquiring and interpreting EEG signals is a crucial element that directly affects the user acceptance and the practical implementation of such systems. While EEG signals provide a unique method for ensuring secure authentication, this process can impact the overall user-friendliness of the system. The requirement for users to perform specific cognitive tasks to generate authenticable EEG patterns may create obstacles regarding the time and effort needed for successful authentication.

Moreover, it is imperative to consider the replicability and dependability of EEG signals in different scenarios and user conditions to ensure a smooth and continuous authentication encounter. Addressing these usability concerns is essential to ensure that EEG-based authentication is protective, practical, and accessible to all users. The general idea is to build authentication on something "built" for the person, such as a text file, password, fingerprint, or smart card. Notarized [8] presents a multimodal framework for capturing dynamic and EEG signatures at different time points, indicating the development of a mobile user authentication system [1]. Validation methods of EEG as an alternative to alphanumeric or pattern-based mobile authentication are explored [3]. They systematically analyzed features from EEG signals and corresponding hand movements. The brainwave patterns were recorded using a Neuro Sky headset and an Emotive Epoc+ headset, whereas the hand movement patterns were captured using a Sony smartwatch. Data was collected from 59 users while they watched a video for 300 seconds and then typed on the keyboard about the video's content for another 300 seconds. Feature analysis and the study of any interrelation among users' hand movements and brainwave signals show a strong correlation between the two biometric modalities [13].

5.3 Concern on Data Protection in EEG-Based Authentication

The fusion of EEG signals with non-existent pattern-based matching is selected to authenticate users on portable devices. Including validation based on the EEG signal helps to avoid security attacks such as shoulder surfing and crackling matching [2]. A novel system has been devised using the Hidden Markov Model (HMM) to authenticate the current proposition. To showcase its resilience, the system has yet to be contrasted with the Support Vector Machine (SVM), and the identification and verification processes have been executed employing two established classifiers, specifically HMM and SVM [2]. A classifier combination approach has been adopted to improve the identification and verification performance [2][5]. They do not offer a person authentication framework that applies to the cloud environment using EEG signals recorded on a mobile phone while users listen to music [5]. A minor effort was made to study, design, and implement an appropriate combination of different algorithms in the preprocessing module [10]. This module was responsible for preparing EEG signals for further processing. They implemented algorithms that resample, smooth signals, and remove artifacts from signals [2].

The integration of EEG signal analysis with a non-existent pattern-based matching technique has been chosen to authenticate users' mobile devices. This approach is instrumental in mitigating security breaches, such as shoulder surfing and pattern cracking. A cutting-edge system has been engineered, employing the Hidden Markov Model (HMM) to substantiate the current innovative concept. While this system's resilience has yet to be compared to the Support Vector Machine (SVM), utilizing both HMM and SVM classifiers has been instrumental in conducting tasks related to identification and verification. A combination of classifiers has been implemented to enhance the identification and verification performance. It was important to note that our framework does not extend to any person's authentication in cloud environments using EEG data captured from mobile devices. At the exact moment, users in these research endeavors were actively involved in listening to music. Efforts have been concentrated on the development, design, and execution of a suitable amalgamation of algorithms within the preprocessing module [2]. The domain of EEG-based Recognition Systems (EEGRS) continues to present challenges. Specifically, developing an EEGRS as a mobile application could be more efficient due to the necessity of crafting implementations for each module within the system. Selecting the appropriate spectral analysis transformation, such as Fourier Transform (FT) versus Wavelet Transform (WT), or choosing the optimal mother wavelet for WT in the preprocessing module, is an experiment. This selection process can significantly extend the development timeline for an individual developer or escalate costs by necessitating additional developers.

Moreover, the scarcity of readily available code for mobile computing platforms often requires the creation of custom code or translating EEG solutions, developed initially as MATLAB modules, into the native coding language of the mobile application platform, such as Java for Android. The journey of a software developer towards implementing an EEGRS is complex and non-linear. Additionally, the challenge of differentiating between subjects and tasks using mobile phones is compounded by the high costs of single-channel EEG devices [3].

6 Recommendations

Previous studies provide crucial recommendations to mitigate issues researchers, developers, and users face when misusing smartphones. Scholars propose strategies to address obstacles and visually portray key measures to reduce the negative consequences of misuse. Putting these recommendations into practice can pave the way to a secure and optimized setting for everyone participating.

6.1 Recommendations to Developers

The deployment and evaluation of optimization algorithms on iOS-based mobile devices are part of the scope, along with a comparative analysis of various studies. The objective is to create a comprehensive application that addresses a specific health issue and utilizes Big Data to thoroughly evaluate the framework and algorithms under more extensive experimental conditions [19]. The envisioned EEG Workbench tool aims to facilitate the development of a broader range of wavelets that can be customized for individual users. It is expected that an EEG Recognition System (EEGRS) will require a tool like EEG Workbench to provide a user-friendly configuration interface. Additionally, software developers can enhance the Feature Extraction component by incorporating characteristics that have yet to be extensively explored, such as auto-regressive modeling, source localization, information theory, and chaos theory, which must be thoroughly verified for reliability. Unlike traditional Knowledge-Based Identification (KBI) methods, EEG authentication is dynamic and requires users to adapt their EEG data during the authentication process, including guidance during enrollment. EEG Workbench is designed to simplify the development of configuration tools [19].

Furthermore, the plan is to utilize MATLAB's parallel computing toolbox to reimplement the core algorithm in a distributed and synchronized manner, enhancing response times for user inquiries and improving the efficiency and scalability of the expert and intelligent system [6]. The research also involves the development of an advanced fusion methodology to strengthen the current EEG-based authentication mechanisms against forgery attacks and explore the impact of human emotional states on the attack model [13]. Thus, the EEG Workbench can be utilized to develop more wavelets and even explore the

possibility of creating wavelets per individual. Ultimately, an EEGRS will need a tool like EEG Workbench to provide a configuration interface for regular users. Similarly, software developers can extend the Feature Extraction module with additional features yet to be fully explored, such as auto-regressive modeling, source localization, information theory, and chaos theory, which must be thoroughly verified for reliability [10].

Given that, in the third direction, we will use the parallel computing toolbox provided by MATLAB to reimplement the main developed algorithm in a distributed and synchronized manner. This will provide prospective users with answers to their inquiries quickly and reasonably. Finally, all these directions will increase the efficiency and scalability of the developed expert and intelligent system [6]. This consists of building a sophisticated fusion methodology that improves the present EEG-based authentication mechanism and is less vulnerable to forgery attacks. They also plan to examine how the diverse emotional states of a human affect the attack model [12].

6.2 Recommendations to Researchers

In future research, more system versions should be included, utilizing unique features that complement each other and cover all five EEG characteristics: frequencies, amplitudes, wave morphology, spatial distribution, and reactivity. This ensures that both behavioral and physiological data are used for authentication. Emotional states (extractable from the Emotive research package) should be considered to adjust features accordingly, with facial expressions detected from brain waves and smartphone cameras as additional context triggers [11]. Such features can distinguish seizure states effectively, with all p-values less than 0.004. RQA parameters from recurrence plots, displaying "all the times at which a state of the dynamical system recurs," should be employed [14]. Other biometric traits can enhance system robustness [5]. Multi-classifier combination methods and other neural network topologies can improve identification and verification accuracies. Future work should explore signal stability during stressful and dynamic situations and their effects on robustness [1]. Various EEG tasks should be investigated to ensure distinguishability with larger sample sizes [14].

Authentication errors observed with new test subjects indicate potential overlap in the chosen feature space. Therefore, the password space for EEG-based authentication should be investigated with more test subjects [3]. Experiments with proposed EEG-based methods on larger datasets and additional information extracted from EEG signals are necessary for enhanced system evaluation [9]. Large-scale datasets for deep learning should be used, offering solutions for various devices beyond mobile phones, including intelligent bands, watches, and goggles. Similar systems could be applied to laptops, desktops, and home/office login security systems. Remote user authentication using brain signals over secure internet protocols should be explored [2]. A framework for easy setup

with generic interfaces should be created using data from mobile device sensors and APIs to control connected devices. A location engine could triangulate and measure Bluetooth signal strength to locate connected devices, implementing a drag-and-drop interface for movable devices [9][18].

7. Conclusion

EEG-based smartphone authentication offers a secure alternative to traditional methods but faces obstacles like privacy vulnerabilities and a lack of security awareness. Research in this area has grown due to widespread smartphone use and issues with data accessibility and usability. A review of published works highlights findings and contributions, establishing a classification system covering defense, attack, and methodological approaches. Critical elements like sample size, demographics, devices, evaluation techniques, and experimental configurations have been meticulously examined. This research is pioneering in its thorough examination of sensor-based smartphone authentication. Recommendations address EEG-based authentication challenges and bridge gaps in biometric solutions. By organizing and analyzing current research, this study aims to inspire innovation in enhancing the security and usability of EEG-based authentication systems. Future work should address challenges and explore new applications of EEG technology in mobile security.

12. References:

[1] P. Kumar, R. Saini, B. Kaur, P. P. Roy, and E. Scheme, “Fusion of neuro-signals and dynamic signatures for person authentication,” *Sensors (Switzerland)*, vol. 19, no. 21, Nov. 2019, doi: 10.3390/s19214641.

[2] P. Kumar, R. Saini, P. Pratim Roy, and D. Prosad Dogra, “A bio-signal based framework to secure mobile devices,” *Journal of Network and Computer Applications*, vol. 89, pp. 62–71, Jul. 2017, doi: 10.1016/j.jnca.2017.02.011.

[3] E.-S. Haukipuro *et al.*, “Mobile Brainwaves: On the Interchangeability of Simple Authentication Tasks with Low-Cost, Single-Electrode EEG Devices.” [Online]. Available: https://www.emotiv.com/

[4] M. L. Shuwandy *et al.*, “mHealth Authentication Approach Based 3D Touchscreen and Microphone Sensors for Real-Time Remote Healthcare Monitoring System:

Comprehensive Review, Open Issues and Methodological Aspects," *Computer Science Review*, vol. 38, p. 100300, Nov. 2020, doi: https://doi.org/10.1016/j.cosrev.2020.100300.

[5] P. Kumar, A. Singhal, R. Saini, P. P. Roy, and D. P. Dogra, "A pervasive electroencephalography-based person authentication system for cloud environment," *Displays*, vol. 55, pp. 64–70, Dec. 2018, doi: 10.1016/j.displa.2018.09.006.

[6] M. El Menshawy, A. Benharref, and M. Serhani, "An automatic mobile-health based approach for EEG epileptic seizures detection," *Expert Syst Appl*, vol. 42, no. 20, pp. 7157–7174, Jun. 2015, doi: 10.1016/j.eswa.2015.04.068.

[7] V. Krishna, Y. Ding, A. Xu, and T. Höllerer, "Multimodal Biometric Authentication for VR/AR using EEG and Eye Tracking," in *Adjunct of the 2019 International Conference on Multimodal Interaction, ICMI 2019*, Association for Computing Machinery, Inc, Oct. 2019. doi: 10.1145/3351529.3360655.

[8] J. Klonovs, C. Petersen, H. Olesen, and A. Hammershoj, "ID proof on the go: Development of a mobile EEG-based biometric authentication system," *IEEE Vehicular Technology Magazine*, vol. 8, no. 1, pp. 81–89, 2013, doi: 10.1109/MVT.2012.2234056.

[9] Institute of Electrical and Electronics Engineers. Bangalore Section, Institute of Electrical and Electronics Engineers. India Council, and Institute of Electrical and Electronics Engineers, *2016 IEEE Annual India Conference (INDICON) : 16-18 Dec. 2016.*

[10] L. Gutierrez and M. Husain, "Design and Development of a Mobile EEG Data Analytics Framework," *2019 IEEE Fifth International Conference on Big Data Computing Service and Applications (BigDataService)*, Newark, CA, USA, 2019, pp. 333-339, doi: 10.1109/BigDataService.2019.00059.

[11] C. Wang, Y. Wang, Y. Chen, H. Liu, and J. Liu, "User authentication on mobile devices: Approaches, threats and trends," *Computer Networks*, vol. 170, Apr. 2020, doi: 10.1016/j.comnet.2020.107118.

[12] A. N. Navaz, M. A. Serhani, N. Al-Qirim, and M. Gergely, “Towards an efficient and Energy-Aware mobile big health data architecture,” *Comput Methods Programs Biomed*, vol. 166, pp. 137–154, Nov. 2018, doi: 10.1016/j.cmpb.2018.10.008.

[13] D. Shukla, P. P. Kundu, R. Malapati, S. Poudel, Z. Jin, and V. V. Phoha, “Thinking Unveiled: An Inference and Correlation Model to Attack EEG Biometrics,” *Digital Threats: Research and Practice*, vol. 1, no. 2, Jul. 2020, doi: 10.1145/3374137.

[14] I. Mustafa, H. Farooq and T. K. Khatri, "Notice of Violation of IEEE Publication Principles: EEG based user authentication using visual stimuli of geometric shapes," *2019 2nd International Conference on Communication, Computing and Digital systems (C-CODE)*, Islamabad, Pakistan, 2019, pp. 247-251, doi: 10.1109/C-CODE.2019.8680987.

[15] P. Kumar, R. Saini, P. Pratim Roy, and D. Prosad Dogra, “A bio-signal based framework to secure mobile devices,” *Journal of Network and Computer Applications*, vol. 89, pp. 62–71, Jul. 2017, doi: 10.1016/j.jnca.2017.02.011.

[16] Institute of Electrical and Electronics Engineers, "2016 IEEE Annual India Conference (INDICON)," in *Proceedings of the 2016 IEEE Annual India Conference (INDICON)*, Bangalore, India, Dec. 16-18, 2016.

[17] IEEE Computational Intelligence Society and Institute of Electrical and Electronics Engineers, *Proceedings of the 2014 International Joint Conference on Neural Networks: July 6-11, 2014, Beijing, China.*

[18] SCAD Institute of Technology and Institute of Electrical and Electronics Engineers, *Proceedings of the 3rd International Conference on loT in Social, Mobile, Analytics and Cloud (ISMAC 2019) : 12-14 December, 2019*.

[19] A. N. Navaz, M. A. Serhani, N. Al-Qirim, and M. Gergely, “Towards an efficient and Energy-Aware mobile big health data architecture,” *Comput Methods Programs Biomed*, vol. 166, pp. 137–154, Nov. 2018, doi: 10.1016/j.cmpb.2018.10.008.