Poster: Towards Practical Brainwave-based User Authentication

Matin Fallahi
Karlsruhe Institute of Technology
Karlsruhe, Germany
matin.fallahi@kit.edu

Patricia Arias-Cabarcos
Paderborn University
Paderborn, Germany
pac@mail.upb.de

Thorsten Strufe
Karlsruhe Institute of Technology
Karlsruhe, Germany
strufe@kit.edu

ABSTRACT

Brainwave measuring devices have transitioned from specialized medical tools to user-friendly and economically accessible consumer products. This shift has opened new avenues for pervasive services, with applications spanning brain-computer interfaces (BCIs), disease detection, criminal trials, and, notably, authentication in computer security. Electroencephalography (EEG) signals, being difficult to steal and revocable, present an attractive biometric option. However, the practical deployment of these signals is hindered by security threats, usability issues, and privacy concerns. To this end, we expect to improve the overall performance of authentication systems using consumer-grade devices, gain a better understanding of user attitudes toward this type of authentication, and protect the user's privacy against unauthorized use of samples collected during enrollment and verification.

CCS CONCEPTS

• **Security and privacy → Biometrics**.

KEYWORDS

Authentication, EEG, Biometric, Recognition

1 INTRODUCTION

Traditional authentication mechanisms that rely on something that users know or a physical asset, such as passwords and USB tokens, are vulnerable to theft, loss, and need to be remembered or carried. Alternatively, current research explores novel forms of biometrics as more advantageous options, including face, voice, eye-gaze, and EEG (Electroencephalography) signals. The latter, which represents brainwave patterns, exhibits significant benefits: it is revocable, works only on living users, is hand-free, and offers near-impossibility of the covert recording [3, 6]. Additionally, brainwaves can provide implicit authentication, where users are identified seamlessly and non-intrusively while wearing an EEG device. As a result, EEG is appealing for authentication purposes.

While extensive research has been conducted in the realm of EEG-based authentication, no market-ready product has yet been developed. This has been largely due to reliance on medical-grade devices, which, while precise, are cumbersome and impractical for everyday use. Now, the landscape is shifting. The increasing availability of inexpensive, user-friendly consumer-grade EEG devices opens the door to realistic, real-world deployment of EEG-based authentication systems. However, the algorithms that worked effectively with medical-grade quality sensing must now be adapted to achieve comparable performance with user-grade devices, which often record data at a lower quality [1]. Thus, the current focus in the field needs to be on refining and optimizing these algorithms to harness the full potential of consumer-grade EEG devices, allowing for a more widespread and practical application of this innovative authentication method. Additionally, understanding user attitudes and preferences toward this new brainwave-based authentication method is crucial. This includes assessing overall usability and acceptance to ensure a successful deployment.

Through the consideration of these two key areas—namely, the challenge of adapting algorithms for user-grade devices to enhance **security** and understanding user attitudes and preferences towards brainwave-based authentication concerning **usability**—we lay the groundwork for advancements in EEG-based authentication. We intend to contribute in the following ways:

- **Security:** Utilizing Siamese networks and integrating eye-tracking with brainwaves to enhance the overall robustness of brainwave-based authentication.
- **Usability:** Conducting a mock-up user study to understand user attitudes toward brainwave authentication.

2 RELATED WORK

The challenges in biometric authentication systems, especially those using brainwaves, can be broadly categorized into three main areas: security, usability, and privacy.

Security: Attacks on brainwave-based systems aim to impersonate the victim's brain activity. This can be achieved by the attacker presenting their own sample and trying to authenticate as another user (e.g., by entering the victim's username) in a *zero effort attack*. Alternatively, *brute force attacks* rely on randomly guessing features or creating fake signals. Another sophisticated approach involves *hill-climbing attacks*, where the attacker iteratively modifies the input to find a solution that closely matches the victim's brainwave signature.

With the transition from medical-grade to consumer-grade devices, zero-effort attacks have escalated due to lower data quality and, therefore, lower accuracy. To tackle *zero effort attack*, we need to improve the overall performance of brainwave-based authentication, minimizing the Equal Error Rate (EER). This reduction in EER leads to a decrease in both the False Acceptance Rate (FAR)

and False Rejection Rate (FRR), making imposture verification less likely when FAR is low. For context, Arias et al. [2] achieved an EER of 14.5% using a consumer-grade device, in contrast to the state-of-the-art 0.14% EER observed with medical-grade devices [5]. Achieving this goal may require the application of advanced machine learning techniques, sophisticated authentication strategies, and multimodal solutions, which together can provide robust mechanisms to enhance the security of brainwave-based authentication systems.

Usability: Since the result of this research is an authentication system for the general public, the perspective of users who encounter such an EEG-based authentication system is critical. Different types of user studies can be conducted to understand their mindset and satisfaction level, but related work in this area is scarce, only covering heuristic evaluations and questionnaires about authentication task preferences [2, 4]. However, no study so far provided users with hands-on experience with a real (or close to real) EEG-based authentication system. To fill this gap, we developed a mock-up authentication system that simulates state-of-the-art authentication performance [1], providing the closest possible user experience to that expected with current technology.

Privacy: Brainwaves contain sensitive personal information. Kaur et al. [7] demonstrated that users' age and gender could be inferred from their brainwaves, and other private information like illness, stress level, and focus can also be extracted. Additionally, Martinovic et al. [8] show that EEG signals can reveal or reduce the entropy of user information, such as bank cards, PINs, and areas of residence. The collection of EEG data during enrollment and verification raises serious privacy concerns. One promising solution lies in homomorphic encryption, a technique that allows computations on encrypted data, thereby maintaining privacy. However, the practical application of this method faces significant hurdles due to the computational overhead involved.

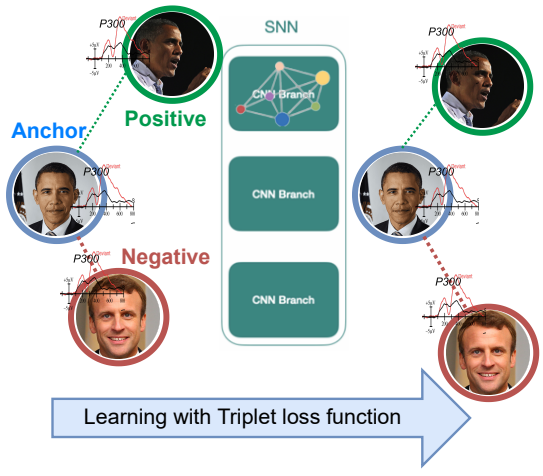

Figure 1: When training a Siamese Neural Network for brainwave-based authentication, the triplet loss function minimizes the distance between an anchor and a positive sample, both belonging to the same user, and maximizes the distance between an anchor and a negative sample belonging to different users.

3 IMPROVING SECURITY

Initially, we extended our previous [2] paper by implementing an enhanced shallow machine learning pipeline, including data normalization and unbalanced learning. We achieved EER of 8.5% for consumer-grade devices and 1.9% for a public medical dataset. Furthermore, we conducted an evaluation based on the unseen attackers' scenario, typically neglected in papers on EEG authentication. The unseen attacker scenario refers to a situation in which no attacker samples are included in the training set [1]. Afterward, we introduced BrainNet [5] to eliminate the need for retraining when enrolling a new subject in the system and further enhance EER. To this end, we used a Siamese Neural Network (SNN) (Figure 1) with a triplet loss function and trained a general similarity function capable of working with unseen subjects. Additionally, we improved EER from 1.9% to 1.37% on an identical medical-grad dataset compared with shallow classifies.

For further performance improvement in brainwave-based authentication, we explored the integration of eye gaze with EEG signals. This led to the development of multimodal authentication algorithms that can be implicitly sensed using cameras embedded in laptops or AR/VR headsets in conjunction with EEG sensors:

Experiment Design and Implementation: We designed an experiment to analyze the performance of eye gaze and brainwave data in user authentication while reacting to different visual stimuli. The experiment involved a dot-following task inspired by Sluganovic et al.'s paper [10]. Each subject participated in 36 rounds, with 25 dot positions in each round and a 15-second rest period between rounds. Eye movements and brainwaves were recorded using Pupil Core and Emotiv Epoc X devices, with data synchronization achieved through the Lab Stream Layer (LSL). The experiment was approved by KIT's IRB and conducted with a population of 30 subjects aged 18 or older.

Data Preprocessing and Model Training: In the development of our multimodal authentication system, data acquired during the experiment was preprocessed. This included pairing eye and brain samples with corresponding timestamps and trimming them to a duration of 0.4. Following this preparation, the BrainNet SNN was trained with 25 participants and evaluated using a distinct set of 5 users (group cross-validation with 25 for training and 5 for testing). This training and evaluation process was implemented for eye-tracking data, brainwave data, and feature fusion of both modalities. Additionally, score fusion methods were employed, which were computed based on the similarity scores derived from eye and brain models.

Initial Results and Future Directions: The initial results suggest 3.8% EER for eye movement, 4.8% EER for brainwaves, 1.2% for feature fusion, and 0.7% for the score fusion approach. Notably, multimodal systems reduce EER by about 85 percent compared to brain single-modal systems. The brainwave EER also outperformed our previous method by 8.5% EER for consumer-grade devices with shorter samples (1 second vs. 0.4 seconds). Continuing work will involve exploring different distance functions, implementing different evaluation scenarios, and focusing more on behavioral characteristics by excluding certain physiological features like pupil diameter in eye-tracking data before a paper based on this experiment can be published.

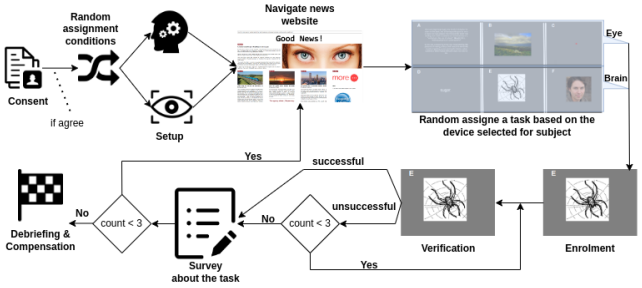

Figure 2: The overview of the mock-up user study

Overall, Through a series of studies, we have significantly enhanced the security of brainwave-based authentication systems, bringing the EER down from 14.5% [2] to 0.7% percent. As a result, zero-effort attacks have become more difficult.

4 UNDERSTANDING USER ATTITUDES

In the pursuit of making brainwave authentication more user-friendly and widely accepted, understanding users' attitudes toward this novel technology is paramount. Since no real brainwave authentication system is currently available, we designed an experiment simulating such a system to gauge user perceptions and preferences.

User Study Design: We conducted a user study with 32 participants to test three brainwave-based (Slideshow, Face, Reading) and three eye-tracking-based (Slideshow, Dot, Reading) authentication tasks, using the Emotiv Epoc X brainwave device and the Tobii Pro Fusion eye-tracker. After informing participants of the study's goal and obtaining signed consent, they were randomly assigned to either the brainwave or eye-tracking authentication condition. Participants interacted with a news website, registering and authenticating. The interactive usage phase and post-usage survey were repeated thrice for each participant, encompassing all three tasks. Survey questions covered usability using the System Usability Scale (SUS), participants' perceptions and preferences questions, insights into benefits, problems, trade-offs, and demographic data. Participants were then debriefed about the simulated nature of the experiment and compensated in cash (Figure 2).

Initial Findings: SUS scores were calculated for both brainwave-based and eye-tracking-based authentication mechanisms across three tasks. For brainwave-based authentication, the mean scores were 77.5 (± 17.6) for the slideshow task, 84.5 (± 10.4) for the face task, and 76.8 (± 13.8) for the reading task, resulting in an overall mean of 79.6 (± 14.3). In contrast, the eye-tracking-based authentication achieved mean scores of 83.8 (± 11.5) for the slideshow task, 78.8 (± 10.9) for the dot task, and 73.2 (± 15.4) for the reading task, with an overall mean of 78.6 (± 13.3). It is noteworthy the reading task had lower scores in both mechanisms, but all the scores were within the "good" (A^-) category, according to the qualitative grading Sauro *et al.*[9]. In addition, there was no significant difference between the brainwave and the eye-tracking mechanisms (79.6 vs. 78.6). Also, we asked participants whether they were concerned about disclosing their brainwave/eye-tracking data. The study indicates that a higher percentage of participants had privacy concerns about brainwaves than eye-tracking authentication mechanisms (35% vs 26%). In addition, brainwaves showed a higher percentage of undecided subjects regarding privacy concerns (33% vs 20%).

5 CONCLUSION AND FUTURE WORK

In this paper, we've presented an exploration of EEG-based authentication, a promising yet challenging field. Our focused approach outlines paths to improve security through Siamese networks and multimodal authentication. Though at an early stage, these directions lay essential groundwork for the development of more robust, user-friendly, and private brainwave-based authentication systems. We believe these paths contribute to the pursuit of practical brainwave-based user authentication.

Based on the privacy concerns expressed by subjects in the user study, our future work is aimed at enhancing privacy protection. We introduced BrainNet [5], a system that utilizes Siamese networks to transform high-density EEG data into a more manageable form, represented by just 32 distinct values. These values correspond to a latent vector space and encapsulate the similarities between subjects. This transformation, in conjunction with homomorphic encryption, may be able to mitigate concerns regarding the privacy of brainwave samples necessary for authentication with reasonable computational overhead.

ACKNOWLEDGMENTS

This work was funded by the Helmholtz Association (HGF) within topic "46.23 Engineering Secure Systems" (KASTEL Security Research Labs) and Germany's Excellence Strategy (EXC 2050/1 'CeTI'; ID 390696704).

REFERENCES

[1] Patricia Arias-Cabarcos, Matin Fallahi, Thilo Habrich, Karen Schulze, Christian Becker, and Thorsten Strufe. 2023. Performance and Usability Evaluation of Brainwave Authentication Techniques with Consumer Devices. *ACM Transactions on Privacy and Security* 26, 3 (2023), 1–36.

[2] Patricia Arias-Cabarcos, Thilo Habrich, Karen Becker, Christian Becker, and Thorsten Strufe. 2021. Inexpensive Brainwave Authentication: New Techniques and Insights on User Acceptance. In *30th {USENIX} Security Symposium*.

[3] Amir Jalaly Bidgoly, Hamed Jalaly Bidgoly, and Zeynab Arezoumand. 2020. A survey on methods and challenges in EEG based authentication. *Computers & Security* 93 (2020), 101788.

[4] John Chuang, Hamilton Nguyen, Charles Wang, and Benjamin Johnson. 2013. I think, therefore I am: Usability and security of authentication using brainwaves. In *Financial Cryptography and Data Security: FC 2013 Workshops, USEC and WAHC 2013, Okinawa, Japan*. Springer, 1–16.

[5] Matin Fallahi, Thorsten Strufe, and Patricia Arias-Cabarcos. 2023. BrainNet: Improving Brainwave-based Biometric Recognition with Siamese Networks. In *2023 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. IEEE, 53–60.

[6] Qiong Gui, Maria V Ruiz-Blondet, Sarah Laszlo, and Zhanpeng Jin. 2019. A survey on brain biometrics. *Comput. Surveys* 51, 6 (2019), 1–38.

[7] Barjinder Kaur, Dinesh Singh, and Partha Pratim Roy. 2019. Age and gender classification using brain–computer interface. *Neural Computing and Applications* 31, 10 (2019), 5887–5900.

[8] Ivan Martinovic, Doug Davies, Mario Frank, Daniele Perito, Tomas Ros, and Dawn Song. 2012. On the feasibility of side-channel attacks with brain-computer interfaces. In *21st {USENIX} Security Symposium*. 143–158.

[9] Jeff Sauro. 2011. Are both positive and negative items necessary in questionnaires. *Retrieved June* 20 (2011), 2013.

[10] Ivo Sluganovic, Marc Roeschlin, Kasper B Rasmussen, and Ivan Martinovic. 2018. Analysis of reflexive eye movements for fast replay-resistant biometric authentication. *ACM Transactions on Privacy and Security (TOPS)* 22, 1 (2018), 1–30.