On the Usability of Next-Generation Authentication: A Study on Eye Movement and Brainwave-based Mechanisms

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

Patricia Arias-Cabarcos
Chair of IT Security, Department of Computer Science
Paderborn University
Paderborn, Germany
pac@mail.upb.de

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

Abstract

Passwords remain a widely-used authentication mechanism, despite their well-known security and usability limitations. To improve on this situation, next-generation authentication mechanisms, based on behavioral biometric factors such as eye movement and brainwaves have emerged. However, their usability remains relatively under-explored. To fill this gap, we conducted an empirical user study (n=32 participants) to evaluate three brain-based and three eye-based authentication mechanisms, using both qualitative and quantitative methods. Our findings show good overall usability according to the System Usability Scale for both categories of mechanisms, with average SUS scores in the range of 78.6-79.6 and the best mechanisms rated with an "excellent" score. Participants identified brainwave authentication as particularly more secure yet more privacy-invasive and effort-intensive compared to eye movement authentication.

Keywords

User study, Usability, Authentication, EEG, Biometric, eye movement

1 Introduction

Authentication is a cornerstone of security, ensuring that only authorized individuals gain access to sensitive systems or data. However, traditional methods relying on single knowledge factors such as passwords and PINs have shown significant drawbacks. Recent studies, including the 2020 Data Breach Investigations Report by Verizon [45], emphasize that approximately 80% of hacking-related breaches involve weak or stolen credentials, with passwords being a prime target. Furthermore, the Ponemon Institute revealed that 51% of respondents admitted to using the same password for multiple accounts, consequently increasing the risks of credential theft and identity fraud [18]. These statistics shed light on the vulnerabilities inherent in password-based authentication systems, calling for more robust, usable, and secure alternatives.

One promising solution to address the limitations of traditional authentication methods is biometric authentication [36]. This approach harnesses the unique physiological or behavioral characteristics of individuals to verify their identities. While physiological biometrics like face and fingerprint recognition are popular, they face critical challenges, including the inability to revoke biometric data once compromised and heightened vulnerability to spoofing attacks [3, 23]. On the other hand, behavioral biometrics measure unique features of activities users perform either consciously or unconsciously [4]. Behavioral biometrics have gained significant attention as they offer the potential to enhance security while minimizing user burden [43].

Among the behavioral biometric authentication approaches, brainwave-based [38, 41] and eye movement-based [28] mechanisms[1] have emerged as promising alternatives in desktop and Extended Reality (XR) environments, due to their distinct advantages. These mechanisms allow for implicit authentication, without requiring explicit user actions, such as typing a password or pressing a button, ensuring a seamless and effortless authentication experience. Furthermore, brainwaves are non-observable from the exterior and therefore difficult to compromise, and brain biometrics can be implemented in a adaptable fashion by altering stimuli even if the original brainwave sample is compromised [22, 26, 46]. Eye-based mechanisms do not require a wearable and can work with common camera hardware integrated into laptops/smartphones [27, 48]. Lastly, both types of mechanisms have demonstrated promising authentication accuracy in previous research [13, 39], which supports their potential for practical realization in the near future.

Despite the potential of brainwave and eye movement-based authentication mechanisms, their actual usability remains underexplored, and this is a crucial factor driving user acceptance and influencing security in practice. The limited number of prior studies investigating these mechanisms lacked a standardized approach for

[1] Brainwaves and eye movement patterns are generally categorized as behavioral biometrics [16], though they are also influenced by physiological aspects like the thickness of the skull or the dimensions of the eyeball. We conform to their categorization as behaviorals, which is dominant in the literature.

assessing perceived usability, such as the System Usability Scale (SUS) [6], and failed to provide usage conditions for an ecologically valid evaluation [1, 7, 9]. The main barrier in this regard is the absence of real authentication prototypes integrating brain and eye-based authentication mechanisms, which has hindered comprehensive evaluations of their practicality. To bridge this gap, we aim at answering the following research questions:

- **RQ1 [Usability]** How usable are brainwave-based and eye movement-based authentication mechanisms as perceived by users?
- **RQ2 [Perceptions &Usage]** How do users perceive brainwave-based and eye movement-based authentication mechanisms in terms of security, reliability, and effort? How would they use these mechanisms?
- **RQ3 [Benefits, Problems, & Tradeoffs]** What are the advantages, disadvantages, and tradeoffs of brainwave-based and eye movement-based authentication mechanisms from the users' perspective?

To answer the above questions, we conducted a lab study with 32 participants (Section 2). We tested three brainwave-based and three eye movement-based authentication methods in a controlled experiment. To facilitate early usability evaluation, protect user privacy, and ensure ethical research practices, our approach involved using interactive mock-ups that did not collect any actual biometric data as suggested by similar research [21, 34, 44, 49]. Our mock-ups were designed to realistically simulate the authentication mechanisms in a real-world use-case scenario: authenticating to a news website. We collected quantitative and qualitative data from participants after interacting with our prototypes, including SUS scores and responses to open-ended questions on envisioned benefits, problems, and other acceptability-related dimensions, i.e., privacy, confidence, and security. Our results show strong usability for eye and brain-based authentication and high intention to use them by the study participants.

2 Experiment Overview

We designed a lab study with an **interactive usage phase**, in which participants get to use the authentication prototypes, followed by a **post-usage survey**, to measure their perceptions. Our study employs a between-subjects design for the two mechanism categories (brainwave and eye-tracking), and a within-subjects design for the three conditions under each mechanism. The experiment flow (Figure 1) comprises these steps:

Step 1 - Initialization. The experiment begins by informing the participants about its goal: "*testing new authentication systems*". Each participant is then provided with a comprehensive consent form approved by our university's Institutional Review Board (IRB). They are asked to read this form carefully, and if they agree with its terms, sign it to proceed with the experiment. Subsequently, participants are randomly assigned to either the brainwave or the eye-tracking authentication condition[2]. The device associated with the assigned condition is then set up and calibrated.

Step 2 - Interactive Usage Phase. Participants are guided on how to navigate a news website displayed on a PC screen. Then, they are directed to a registration button to create an account and authenticate themselves, which allows them to access more comprehensive information about the news articles. Upon selecting registration, we initiate a task randomly based on the device assigned to the participant. This involves executing the enrolment and verification steps. The success rate for these verification attempts has been predetermined based on existing state-of-the-art literature(as detailed in appendix B). If a login attempt fails, participants are allowed three attempts before we record it as a definitive login failure[3].

Step 3 - Post-Usage Survey. Participants fill out a digital survey designed to answer our research questions as follows:

- **Usability (RQ1):** We assess the usability of the authentication systems using the established System Usability Scale (SUS) [6]. It comprises 10 questions, each rated on a 5-point Likert scale. The scores for each question are transformed and aggregated to calculate an overall usability score ranging from 0 to 100. It is important to note that questions 4 and 10 measure a separate dimension related to Learnability, complementary to the overall usability concept.
- **Perception and Usage (RQ2):** Participants are asked to provide their opinions and preferences regarding the presented authentication scheme. They have to rate their agreement with statements about the scheme's perceived security, ease of use, effort, and the balance between effort and benefits, following the approach of *Zimmerman et al.'s* study [49]. Participants are also asked to indicate whether they would want to use the authentication mechanism if possible and for which types of applications and devices. In case they do not express interest in using the system, we ask for the reasons.Finally, they are requested to rank various authentication schemes based on their preferences.
- **Benefits, Problems, and Trade-offs (RQ3):** To get further insights, participants are asked open questions about the benefits and problems they see in using brainwave or eye movement authentication. Considering that time to authenticate and privacy are usually factors where users make trade-offs, we ask them to specify their acceptable authentication time, and to rate their level of agreement with a statement regarding their concerns about disclosing brainwave/eye movement data for authentication purposes [49].
- **Demographic Data and Background:** We collect basic information about the participants and their backgrounds. This section includes questions related to participants' prior experience with brain-computer interfaces, age group, gender, the highest level of education completed, and whether they have an educational/job background on IT. These questions provide valuable context for analyzing the survey results.

The interactive usage phase and post-usage survey, steps second and third, were repeated thrice for each participant to ensure comprehensive data collection across all three tasks associated with

[2]Determined by a binary random process embedded in the main page of the experiment's local website.

[3]This is a common practice implemented to restrict attacker success. After three failed attempts or one successful attempt, participants are directed to the post-usage survey.

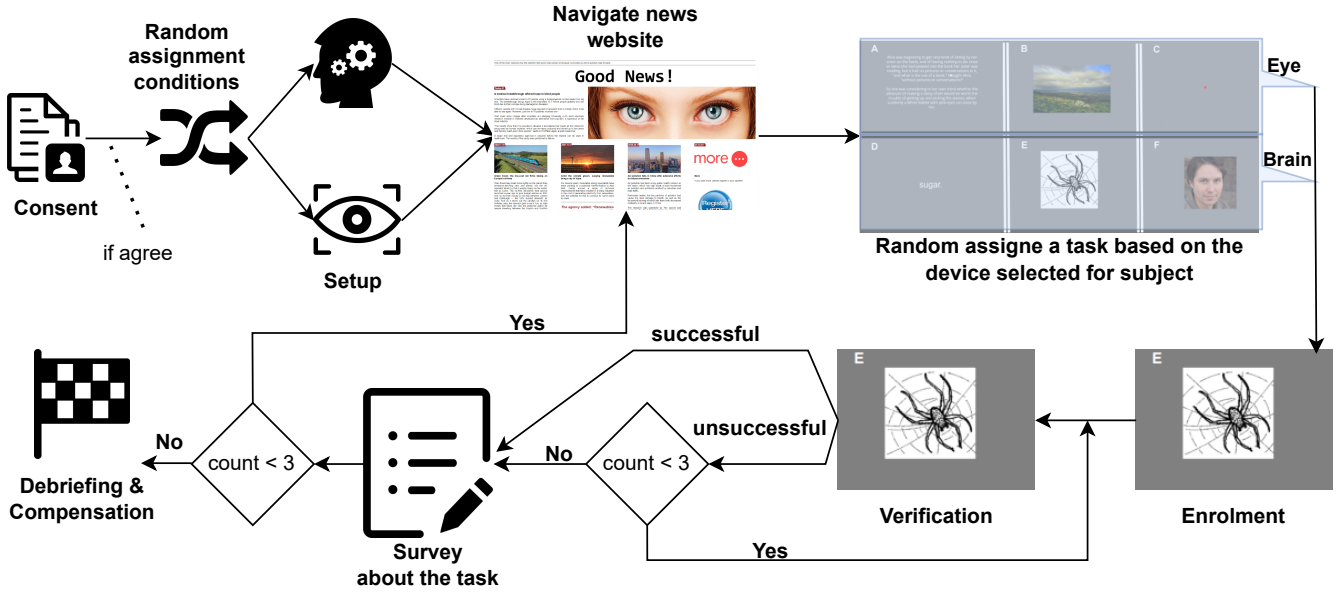


Figure 1: Detailed Experiment Process Flowchart. This figure illustrates the sequence of steps each participant follows in the study. Initially, participants sign a consent form, followed by a random assignment to one of the two authentication modalities: brainwave or eye movement. Subsequently, they undergo three separate enrollment and verification processes, each corresponding to one of the three authentication tasks within their assigned modality. After each task, participants are required to complete a short survey, making a total of three survey completions. The process concludes with a debriefing session and provision of compensation.

each device (Figure 1). It should be noted that demographic and background questions were only asked at the end of the first survey.

Step 4 - Debriefing & Compensation. In order to ensure transparency, at the end of the experiment, participants are shown a page explaining that the prototype they interacted with was a simulation based on state of the art performance metrics. Participants are then asked if they had already realized that the experiment was not real and why. This question is useful to understand the validity of the experiment and to filter out participants who were aware of the artifact. Finally, participants were given compensation in cash as agreed in the consent form.

3 Results

The study was conducted over a three-month period, from December 2022 to February 2023. A total of 35 participants took part in the study, of which 3 were filtered out because they realized about the simulation. From the final sample, 14 people used the brainwave-based authentication approach, and 18 used the eye-tracking-based authentication approach.

3.1 RQ1: Usability

Usability results according to the System Usability Scale are presented in Table 1. Brainwave authentication mechanisms got an average SUS of 79.6, slightly higher but very similar to the 78.6 obtained for the eye-tracking-based mechanisms. These scores are considered to be "good" (A^-), according to the qualitative grading from *Bangor et al.* [5] and *Sauro et al.* [37]. To gain deeper insight into the comparative usability of brainwave and eye-tracking mechanisms, we formulated three sub-questions:

RQ1-1: Are eye-tracking-based authentication mechanisms more usable than brainwave-based mechanisms? To investigate potential differences, we conducted independent samples t-tests on the average SUS scores (Table 1), which indicated no significant difference exists.

RQ1-2: Which eye-tracking or brainwave-based authentication tasks are more usable? The ranking of brainwave-based mechanisms from more to less usable was Face, with a SUS of 84.5, followed by Slideshow with 77.5, and Reading with 76.8. For the eye-tracking-based mechanisms, participants preferred the Slideshow 83.8 over the Dot interface 78.8, and the Reading task 73.2.

In assessing usability differences across interfaces, the Friedman tests indicated statistically significant disparities in usability scores, both in the brainwaves category ($\chi^2(2)$ 9.2692, p .00971) and eyetracking category ($\chi^2(2)$ 8.4, p 0.015). The Friedman test, a non-parametric alternative to the ANOVA, is particularly suited for analyzing ordinal data across multiple groups. This prompted further investigation through Conover's post-hoc test, employing a single-step p-value adjustment method to pinpoint specific task contrasts. Significant distinctions emerged, particularly between the Face and Reading tasks within the brainwave mechanism (p .0065), and between the Slideshow and Reading tasks in the eye-tracking mechanism (p .01).

To elucidate these findings, SUS scores were converted into user-specific ranks. For example, SUS scores of 81, 75, and 76 were ranked

Table 1: System Usability Scale (SUS) mean scores for Brainwave-based and Eyetracking-based authentication mechanisms. (*SD: Standard deviation)

Mechanism	Task	Mean	SD*	Median
Brainwaves	Slideshow	77.5	17.6	82.5
	Face	84.5	10.4	87.5
	Reading	76.8	13.8	78.8
Brainwaves	**All**	**79.6**	**14.3**	**82.5**
Eyetraking	Slideshow	83.8	11.5	85
	Dot	78.8	10.9	78.8
	Reading	73.2	15.4	76.2
Eyetraking	**All**	**78.6**	**13.3**	**80**

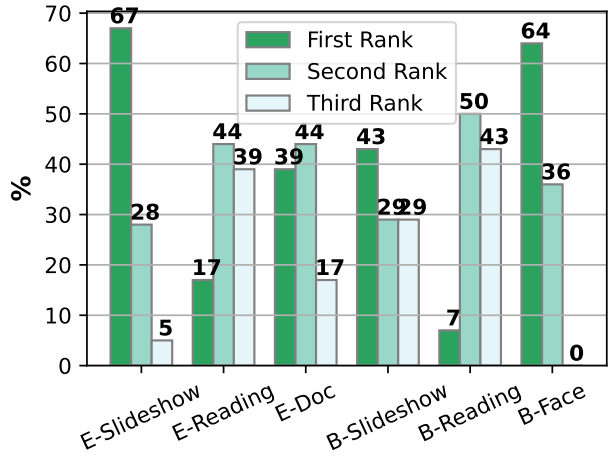


Figure 2: The plot displays the ranking percentages for each authentication task. (E: Eye-tracking mechanism, B: Brainwaves mechanism

as 1, 3, and 2, respectively. Figure 2 illustrates significant differences in user perceptions, particularly the lower usability of Reading tasks. Only 17% of participants with eye-tracking and 7% with brainwaves rated Reading tasks higher than others. In contrast, the brainwave Face task and eye-tracking Slideshow task were preferred, ranked highest by 64% and 67% of participants, respectively. These results align with prior research highlighting user preference for tasks with lower cognitive demand, such as visual over textual stimuli [1, 2].

RQ1-3: Are eye-tracking and brainwave-based authentication mechanisms easy to learn? To gain further insights into usability, we also calculated the **learnability scores** for both categories of mechanisms: brainwaves and eye-tracking. The learnability scores revealed that they both were easy for participants to learn, with high mean scores of 88.7 and 91.0 for brainwaves and eye-tracking, respectively. Interestingly, eye-tracking showed a slightly higher mean score and lower standard deviation, suggesting it may be easier to learn and use overall. Among the authentication tasks, the Dot task had the highest mean learnability score (93.1) and lowest standard deviation (7.7), indicating it was the easiest task for participants to learn. Similarly, within the brainwaves mechanisms, the Face task had the highest mean score (91.1) and lowest standard deviation (15.8). However, nonparametric tests did not reveal statistically significant differences between the mechanisms or among the tasks.

3.2 RQ2: Perception & Usage

Perceived Security, easy of use, effort, and reliability The results of the study indicate (Fig. 3) that a slightly higher proportion of participants agreed or strongly agreed that the authentication scheme was very secure when using brainwave-based authentication mechanisms (47.6%) compared to the eye-tracking mechanism (42.6%). However, it is worth noting that a high proportion of participants chose a neutral answer in both mechanisms (38.1%, 40.7%). The relatively high percentage of neutral responses may suggest that participants had some uncertainty about the level of security offered by the authentication schemes, as highlighted in the qualitative analysis (appendix D.2).

Regarding reliability, participants answered the question "I think the use of this authentication scheme generally causes no problems". Interestingly, the results for both brain-based and eye movement-based mechanisms showed a similar trend, with a significant number of participants expressing neutrality (Fig. 3). The findings indicate a lack of consensus on the absence of problems among the participants.

In terms of user effort, participants were asked "*How do you rate the effort for using this authentication scheme?*". The results, as depicted in Figure 3, indicate that 45.2% of participants perceived the brainwave-based mechanisms as demanding high or very high effort, whereas only 29.7% of participants reported similar perceptions regarding the eye movement mechanism. This suggests that brainwave-based mechanisms necessitate greater effort, potentially attributed to the additional overhead imposed by the headset used in this approach. Furthermore, participants expressed their opinions regarding the perceived balance between effort and benefits, as indicated in Figure 3. 45.2% and 44.8% of the participants disagreed or strongly disagreed with the statement "*In my opinion, the effort exceeds the gained benefits for this authentication scheme*" for brainwaves and eye movement mechanisms, indicating a substantial level of disagreement rate. Notably, despite the higher effort required by the brainwave-based mechanisms, this category exhibited a similar disagreement rate compared to the eye-tracking mechanisms.

Intended Usage. Participants' willingness to use the authentication schemes varied, with brainwave mechanisms achieving a 62% average approval rate and eye movement mechanisms slightly higher at 65% (Figure 4). The slideshow-based eye-tracking approach stood out, receiving an overwhelmingly positive response of 88.9%. For participants who answered 'No', we inquired about the reasons behind their decision via an open-ended question, key concerns included security (10 mentions), authentication time (8), performance (5), and the perceived burden of use (5). Additional feedback highlighted discomfort with the brainwave headset (3 mentions), a lack of detailed information (2), and the system's complexity. These findings correlate with trends observed in the System Usability Scale (SUS) scores.

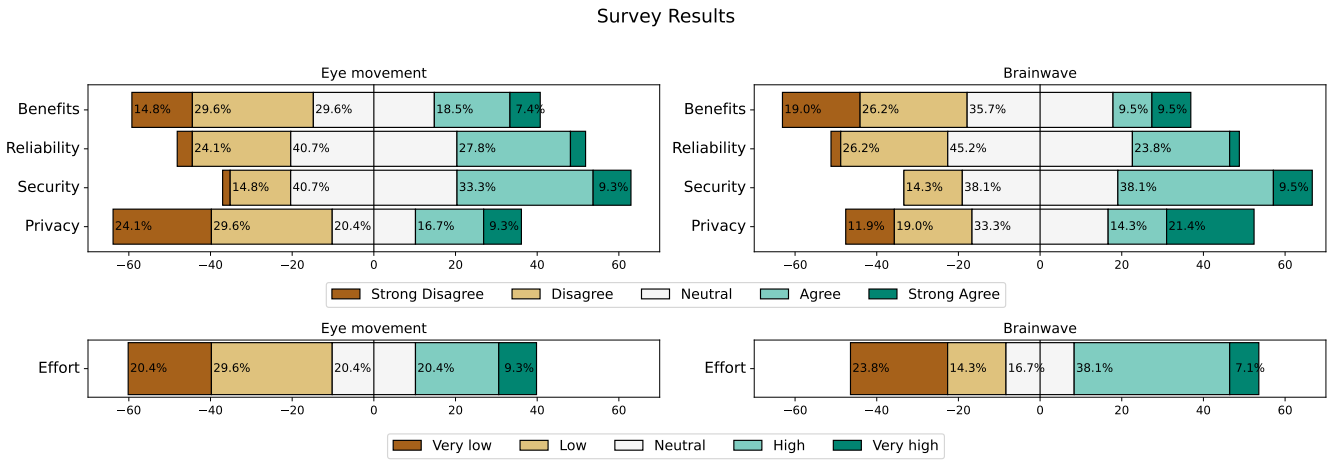


Figure 3: Subject perceptions on authentication scheme attributes for eye movement (left) and brainwave-based (right) mechanisms. Participants assessed: perceived Benefits ("*In my opinion, the effort exceeds the gained benefits for this authentication scheme.*"), Reliability ("*I think the use of this authentication scheme generally causes no problems.*"), Security ("*I think this authentication scheme is very secure, that is, it protects me against attacks*"), Privacy concerns ("*I have concerns to disclose eyegaze/brainwaves data for usage of an authentication scheme.*"), and Effort ("*How do you rate the effort for using this authentication scheme?*").

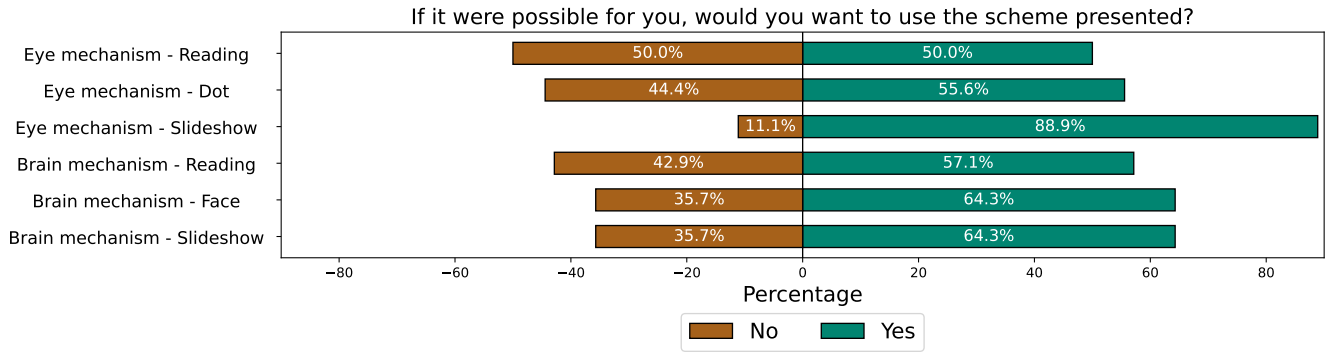


Figure 4: Participant Willingness to Use Different Authentication Schemes in Practice

3.3 RQ3: Benefits, Problems & Tradeoffs

To get richer insights into users' perspectives about the brainwave and eye-tracking authentication mechanisms, we utilized open questions aimed at identifying **benefits and problems**. In the following, we highlight the most important issues raised by participants, based on quantified results (inductive coding approach [30], More details in Appendix C).

Benefits. Participants highlighted several benefits of brainwave and eye-tracking authentication systems. Usability was a prominent advantage, with 34.59% (eye-tracking) and 38.05% (brainwaves) appreciating the ease of use without extensive training. Improved security was noted by 21.38% (eye-tracking) and 33.63% (brainwaves), emphasizing enhanced data protection. The passwordless feature, eliminating the need to remember passwords, was valued by 21.38% (eye-tracking) and 23.01% (brainwaves). Quick authentication times were appreciated by 8.81% (eye-tracking) and 3.54% (brainwaves). Additionally, 11.95% (eye-tracking) and 1.77% (brainwaves) found the system fun and futuristic. Only 1.89% of participants reported no perceived benefits, indicating overall positive reception. (Appendix Table 5)

Problems. Participants identified several potential challenges with brainwave and eye-tracking authentication systems. Key concerns included performance reliability (24.34% for eye-tracking, 20.61% for brainwaves), practical limitations like wearing the devices (15.79% eye-tracking, 26.72% brainwaves), and security risks (18.42% eye-tracking, 14.5% brainwaves). Usability issues such as task difficulty (14.47% eye-tracking, 7.63% brainwaves) and authentication time (14.47% eye-tracking, 13.74% brainwaves) were

also noted. Privacy concerns regarding sensitive data (4.61% eye-tracking, 12.98% brainwaves) and high equipment costs (2.63% eye-tracking, 2.29% brainwaves) were less frequent but significant. (Appendix Table 6)

Tradeoffs. Previous studies identified time to authenticate and privacy as prominent factors influencing acceptance of novel behavioral biometrics [2, 40]. We investigate how these factors are perceived by potential users of eye-tracking and brain-based authentication mechanisms.

Regarding **time**, we asked participants ' *'What would be an acceptable/preferred authentication time?"*. Surprisingly, five out of 32 participants expressed a range of 1-5 minutes (one user mentioned 5 minutes, another mentioned 2 minutes, and three subjects indicated up to 1 minute) as acceptable authentication time. Two participants simply mentioned "a few seconds," which could not be quantitatively converted. For the remaining participants, the average preferred authentication time was 13.14 ± 10.24 seconds. It is noteworthy that eight participants specifically emphasized a preference for a 5-second authentication time.

Regarding **privacy**, we asked participants whether they had concerns about disclosing their brainwave/eye-tracking data for the usage of an authentication scheme (see Fig. 3). The results of the study indicate that a higher percentage of participants disagreed or strongly disagreed with privacy concerns about disclosing their eye-tracking data for authentication purposes compared to their brainwave data, which is an interesting finding. In fact, most of the participants, 54%, who tried eye movement authentication are unconcerned versus 33% of participants in the brainwave condition. In turn, 35% of participants reported agreement or strong agreement to have privacy concerns in the brain case versus 26% for eye movement. This difference in responses could be due to the fact that the brainwave device requires wearing on the head, while the eye-tracking device is non-invasive and attached to a desktop monitor. Another possible explanation is that participants believe that brainwave data may contain more private information drop when compared to eye-tracking data. Furthermore, the proportion of participants who selected "neutral" was highest for Brainwaves (33%), compared to eye-tracking (20%). This suggests that participants may have had more uncertainty or ambiguity regarding their privacy concerns when it comes to Brainwave data. It may be worth considering additional measures to elicit more nuanced responses in future studies, such as open-ended questions or follow-up interviews to better understand participants' perspectives.

4 Limitations

The conducted study has some limitations that may impact the generalizability of the results. Specifically, the evaluation was conducted with a relatively small sample size, and participants were recruited from a specific population (college students). Therefore, caution should be taken when extrapolating the results to other populations or contexts and further studies should be conducted to get insights from other populations. Additionally, the study only examined participants' initial attitudes towards disclosing their biometric data, and it is possible that attitudes could change over time with more exposure and education about the technology.

5 Conclusion

In conclusion, our investigation into next-generation authentication methods based on behavioral biometrics, like eye movement and brainwave, reveals promising potential for user acceptance. Our study results on usability showed good to excellent scores in the System Usability Scale (SUS), with averages of 78.6 for eye mechanisms and 79.6 for brainwave-based. To improve usability, authentication tasks that require a low cognitive effort are preferred. When compared to the eye movement mechanisms, subjects perceive the brainwave mechanism to be more secure; however, they also express increased concerns regarding privacy and reliability of brainwaves, in both qualitative and quantitative questions. While attitudes are generally positive, concerns on privacy, security understanding, and efficient performance need to be further investigated.

Acknowledgments

This work was funded by the Topic Engineering Secure Systems of the Helmholtz Association (HGF) and supported by KASTEL Security Research Labs, Karlsruhe, and Germany's Excellence Strategy (EXC 2050/1 'CeTI'; ID 390696704). This work was also partially supported by the Spanish Government under the research project "Enhancing Communication Protocols with Machine Learning while Protecting Sensitive Data (COMPROMISE)" PID2020-113795RB-C32, and the research project "QUantum-based ReSistant Architectures and Techniques (QURSA)" TED 2021-130369B-C32, both funded by MCIN/AEI/10.13039/501100011033.

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* (2023).

[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 *Proceedings of the 30th {USENIX} Security Symposium ({USENIX} Security 21)*. 55–72.

[3] Sunpreet S Arora, Kai Cao, Anil K Jain, and Nicholas G Paulter. 2016. Design and fabrication of 3D fingerprint targets. *IEEE Transactions on Information Forensics and Security* 11, 10 (2016), 2284–2297.

[4] Lucas Ballard, Daniel Lopresti, and Fabian Monrose. 2007. Forgery quality and its implications for behavioral biometric security. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)* 37, 5 (2007), 1107–1118.

[5] Aaron Bangor, Philip Kortum, and James Miller. 2009. Determining what individual SUS scores mean: Adding an adjective rating scale. *Journal of usability studies* 4, 3 (2009), 114–123.

[6] John Brooke et al. 1996. SUS-A quick and dirty usability scale. *Usability evaluation in industry* 189, 194 (1996), 4–7.

[7] Michael Brooks, Cecilia R Aragon, and Oleg V Komogortsev. 2013. Perceptions of interfaces for eye movement biometrics. In *2013 International Conference on Biometrics (ICB)*. IEEE, 1–8.

[8] Attaullah Buriro, Bruno Crispo, Sandeep Gupta, and Filippo Del Frari. 2018. Dialerauth: A motion-assisted touch-based smartphone user authentication scheme. In *Proceedings of the eighth ACM conference on data and application security and privacy*. 267–276.

[9] 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, April 1, 2013, Revised Selected Papers 17*. Springer, 1–16.

[10] Jacob Cohen. 1960. A coefficient of agreement for nominal scales. *Educational and psychological measurement* 20, 1 (1960), 37–46.

[11] Alexander De Luca, Alina Hang, Emanuel Von Zezschwitz, and Heinrich Hussmann. 2015. I feel like I'm taking selfies all day! Towards understanding biometric authentication on smartphones. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. 1411–1414.

[12] Simon Eberz, Giulio Lovisotto, Kasper B Rasmussen, Vincent Lenders, and Ivan Martinovic. 2019. 28 blinks later: Tackling practical challenges of eye movement biometrics. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 1187–1199.

[13] 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.

[14] Steven Furnell and Konstantinos Evangelatos. 2007. Public awareness and perceptions of biometrics. *Computer Fraud & Security* 2007, 1 (2007), 8–13.

[15] Simon Hanisch, Patricia Arias-Cabarcos, Javier Parra-Arnau, and Thorsten Strufe. 2021. Privacy-protecting techniques for behavioral data: A survey. *arXiv preprint arXiv:2109.04120* (2021).

[16] Giles Hogben. 2010. ENISA Briefing: Behavioural Biometrics. *Computational Intelligence* (2010).

[17] Emotiv Inc. 2019. Emotiv EPOC X. https://www.emotiv.com/epoc-x/. Accessed: April 28, 2023.

[18] Ponemon Institute. 2019. The 2019 State of Password and Authentication Security Behaviors Report. https://resources.yubico.com/53ZDUYE6/at/q3tmql-974v8g-73e8p5/YubicoPonemon_2019_State_of_Password_and_Authentication_Security_Behaviors_Report.pdf?format=pdf.

[19] Laurie A Jones, Annie I Antón, and Julia B Earp. 2007. Towards understanding user perceptions of authentication technologies. In *Proceedings of the 2007 ACM workshop on Privacy in electronic society*. 91–98.

[20] Emiram Kablo and Patricia Arias-Cabarcos. 2023. Privacy in the Age of Neurotechnology: Investigating Public Attitudes towards Brain Data Collection and Use. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*. 225–238.

[21] Hassan Khan, Urs Hengartner, and Daniel Vogel. 2015. Usability and security perceptions of implicit authentication: convenient, secure, sometimes annoying. In *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*. 225–239.

[22] Belal Korany, Chitra R Karanam, Hong Cai, and Yasamin Mostofi. 2019. XModal-ID: Using WiFi for Through-Wall Person Identification from Candidate Video Footage. 15 pages.

[23] Sandeep Kumar, Sukhwinder Singh, and Jagdish Kumar. 2017. A comparative study on face spoofing attacks. In *2017 International Conference on Computing, Communication and Automation (ICCCA)*. IEEE, 1104–1108.

[24] Marta Kutas and Steven A Hillyard. 1980. Reading senseless sentences: Brain potentials reflect semantic incongruity. *Science* 207, 4427 (1980), 203–205.

[25] Chenhao Lin, Jingyi He, Chao Shen, Qi Li, and Qian Wang. 2022. CrossBehaAuth: Cross-Scenario Behavioral Biometrics Authentication Using Keystroke Dynamics. *IEEE Transactions on Dependable and Secure Computing* (2022).

[26] Feng Lin, Kun Woo Cho, Chen Song, Wenyao Xu, and Zhanpeng Jin. 2018. Brain password: A secure and truly cancelable brain biometrics for smart headwear. 296–309 pages.

[27] Dachuan Liu, Bo Dong, Xing Gao, and Haining Wang. 2015. Exploiting eye tracking for smartphone authentication. In *Applied Cryptography and Network Security: 13th International Conference, ACNS 2015, New York, NY, USA, June 2-5, 2015, Revised Selected Papers 13*. Springer, 457–477.

[28] Dillon Lohr and Oleg V Komogortsev. 2022. Eye Know You Too: Toward Viable End-to-End Eye Movement Biometrics for User Authentication. *IEEE Transactions on Information Forensics and Security* 17 (2022), 3151–3164.

[29] Sam McLellan, Andrew Muddimer, and S Camille Peres. 2012. The effect of experience on system usability scale ratings. *Journal of usability studies* 7, 2 (2012), 56–67.

[30] Matthew B Miles and A Michael Huberman. 1994. *Qualitative data analysis: An expanded sourcebook*. sage.

[31] Cristian Morosan. 2012. Voluntary steps toward air travel security: An examination of travelers' attitudes and intentions to use biometric systems. *Journal of Travel Research* 51, 4 (2012), 436–450.

[32] Wataru Oogami, Hidehito Gomi, Shuji Yamaguchi, Shota Yamanaka, and Tatsuru Higurashi. 2020. Observation study on usability challenges for fingerprint authentication using WebAuthn-enabled android smartphones. *Age* 20 (2020), 29.

[33] Chris Riley, Kathy Buckner, Graham Johnson, and David Benyon. 2009. Culture & biometrics: regional differences in the perception of biometric authentication technologies. *AI & society* 24 (2009), 295–306.

[34] Markus Röse, Emiram Kablo, and Patricia Arias-Cabarcos. 2023. Overcoming Theory: Designing Brainwave Authentication for the Real World. In *Proceedings of the 2023 European Symposium on Usable Security*. 175–191.

[35] Scott Ruoti, Brent Roberts, and Kent Seamons. 2015. Authentication Melee: A Usability Analysis of Seven Web Authentication Systems. In *Proceedings of the 24th International Conference on World Wide Web*. International World Wide Web Conferences Steering Committee, Florence Italy, 916–926. doi:10.1145/2736277.2741683

[36] Arpita Sarkar and Binod K Singh. 2020. A review on performance, security and various biometric template protection schemes for biometric authentication systems. *Multimedia Tools and Applications* 79 (2020), 27721–27776.

[37] Jeff Sauro. 2011. ARE BOTH POSITIVE AND NEGATIVE ITEMS NECESSARY IN QUESTIONNAIRES? online publication. Url: https://measuringu.com/positive-negative/, Accessed: 07.08.2018.

[38] Rachel Schomp. 2018. Behavioral Biometric Security: Brainwave Authentication Methods. (2018).

[39] 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.

[40] Chen Song, Aosen Wang, Kui Ren, and Wenyao Xu. 2016. Eyeveri: A secure and usable approach for smartphone user authentication. In *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*. IEEE, 1–9.

[41] Jinani Sooriyaarachchi, Suranga Seneviratne, Kanchana Thilakarathna, and Albert Y Zomaya. 2020. MusicID: A brainwave-based user authentication system for internet of things. *IEEE Internet of Things Journal* 8, 10 (2020), 8304–8313.

[42] Nancy K Squires, Kenneth C Squires, and Steven A Hillyard. 1975. Two varieties of long-latency positive waves evoked by unpredictable auditory stimuli in man. *Electroencephalography and clinical neurophysiology* 38, 4 (1975), 387–401.

[43] Giuseppe Stragapede, Ruben Vera-Rodriguez, Ruben Tolosana, Aythami Morales, Alejandro Acien, and Gaël Le Lan. 2022. Mobile behavioral biometrics for passive authentication. *Pattern Recognition Letters* 157 (2022), 35–41.

[44] Shari Trewin, Cal Swart, Larry Koved, Jacquelyn Martino, Kapil Singh, and Shay Ben-David. 2012. Biometric authentication on a mobile device: a study of user effort, error and task disruption. In *Proceedings of the 28th Annual Computer Security Applications Conference*. 159–168.

[45] Verizon. 2020. 2020 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/2020-data-breach-investigations-report.pdf.

[46] Frederick W Wheeler, Richard L Weiss, and Peter H Tu. 2010. Face recognition at a distance system for surveillance applications. In *2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*. IEEE, 1–8.

[47] Weitao Xu, Yiran Shen, Chengwen Luo, Jianqiang Li, Wei Li, and Albert Y Zomaya. 2020. Gait-Watch: A Gait-based context-aware authentication system for smart watch via sparse coding. *Ad Hoc Networks* 107 (2020), 102218.

[48] Xiaozhi Yang and Ian Krajbich. 2021. Webcam-based online eye-tracking for behavioral research. *Judgment and Decision Making* 16, 6 (2021), 1485–1505.

[49] Verena Zimmermann and Nina Gerber. 2020. The password is dead, long live the password–A laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies* 133 (2020), 26–44.

A Related Work

Several studies have investigated the **technical** and **user-perception** aspects of behavioral biometrics.

On the **technical studies** side, numerous works have evaluated the accuracy, efficiency, and security of behavioral authentication systems. For instance, *Xu et al.*[47], *Lin et al.*[25], *Fallahi et al.* [13], and *Eberz et al.* [12] have examined the performance of various behavioral biometric modalities in terms of Equal Error Rates (EER), including gait (EER=3.5%), keystroke dynamics (EER=5.35%), brainwaves (EER=0.14%), and eye movement (EER=1.88%). The promising results of these studies suggest that behavioral biometrics have the potential to be integrated into daily life. However, a crucial aspect that requires investigation is users' perceptions of these authentication mechanisms.

On the **user perception** stream of research, most works have focused on examining factors that affect user acceptance and adoption of physiological biometric authentication rather than behavioral biometrics. These factors include perceived security [49], privacy concerns [33], perceived ease of use [31], and social influence [11]. Several studies have shown that while users generally have a positive view of biometric authentication, they may still have concerns regarding privacy and data protection [14, 19, 49]. However, a limited number of laboratory studies have been conducted pertaining to behavioral biometrics in general and brainwaves and eye movement authentication in particular. The few studies in this area were constrained by the unavailability of real-world prototypes and their

evaluations rely on hypothetical scenarios or partial interface elements rather than on actual user interaction with a functional biometric system.

In the case of brainwave authentication, *Chuang et al.* [9], conducted a usability study asking participants (N=15) to rate authentication tasks according to how enjoyable, easy, or engaging they were. Building on this study, *Arias-Cabarcos et al.* [1] provided a more comprehensive evaluation (N=52), extending the questionnaire to cover both the usability of the EEG device and explore attitudes towards acceptance. However, in both studies, participants only evaluated authentication tasks, i.e., the activity performed by users while measured by a neuroheadset in order to get identified (e.g., resting, moving a hand, looking at images). But tasks are only a detached part of the whole authentication experience, so the insights regarding their usability provided limited value. However, recent research by Röse et al. [34] explored the usability of brainwave authentication by simulating its use as an authentication mechanism for a password manager. In their preliminary study, they achieved an excellent System Usability Scale (SUS) score of 85.28, based on surveys completed by 9 participants and simulating the ideal (but unrealistic) case where legitimate users are never rejected. Notably, this investigation was focused solely on a single authentication task, consisting of showing a slideshow of images.

In the case of eye movement-based authentication, the study by *Brooks et al.* [7] provides valuable insights into user perceptions (N=22) based on their interaction with a simulated biometric system. However, the simulation does not take into account the expected performance parameters of eye-based systems and the study did not capture the standardized system usability questionnaire (SUS), which may limit the ability to compare their results with other studies or assess the usability of the authentication schemes in a broader context. Additionally, while the study [7] focused on other factors that may influence user acceptance, it did not specifically address privacy concerns, which is an important consideration for biometric authentication.

We complement and extend existing research by comprehensively evaluating brainwaves and eye movement behavioral biometric systems, building high-fidelity interactive prototypes for the most promising interfaces in the literature, and considering their theoretical performance to simulate authentication. Furthermore, we address issues related to various aspects of user perception, conduct standardized usability tests, and investigate privacy concerns in order to gain a clearer understanding of the usability and potential acceptance of behavioral authentication methods.

B Authentication Prototypes

To enable realistic testing of authentication mechanisms, we implemented a news website that required registration and subsequent authentication to get access to extended content. This scenario is common and familiar to users, as it resembles the usual flow such as face detection. Here, users are required to provide biometric samples at the time of enrollment and then submit new samples during verification to either accept or deny authentication requests.

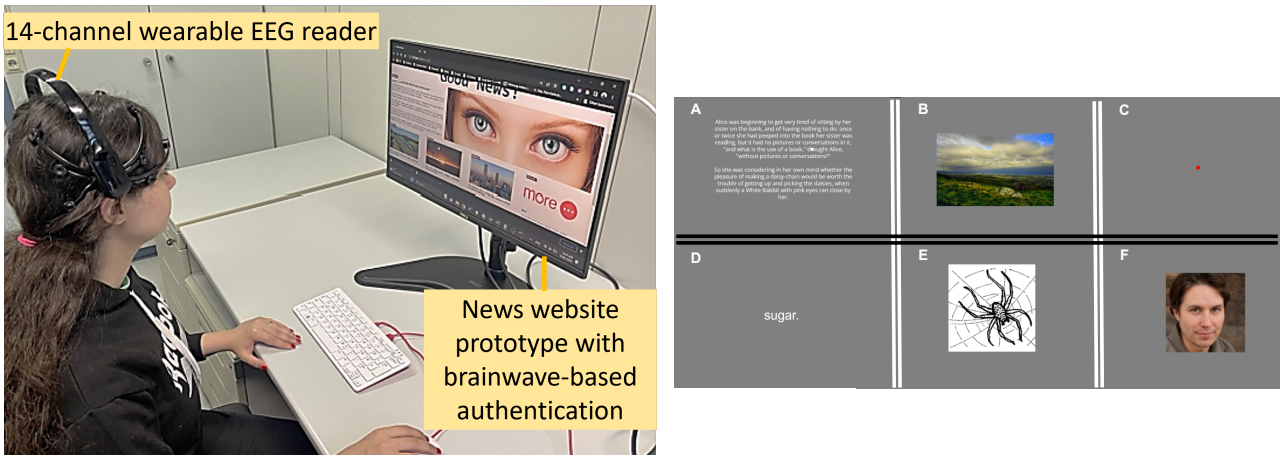
Authentication System Flow and Elements. In a behavioral biometric authentication system, users are granted access depending on their distinct traits, such as those we set up to study: brain activity and gaze. The full process involves collecting the data through specific hardware sensors, processing these data to extract relevant features, and comparing them to a previously stored sample or template from the user trying to authenticate, checking if it is a match or a mismatch. To acquire brainwave and gaze data for behavioral authentication, users should perform a specific task or be presented with certain stimuli, such as sounds or images. In our prototypes, we have developed interfaces for the authentication tasks and employed a simulated authentication decision algorithm. To enhance the realism of our experiment, even in the absence of actual user data collection, participants interact with the necessary hardware components as they would in a fully operational biometric system. Details on the prototype are given in the following.

Interfaces and Software Components. For our study, we implemented interfaces for six authentication tasks, comprising three brainwave-based tasks and three eye movement-based tasks. To ensure consistency, we selected tasks with similar formats in both categories, e.g., based on looking at images or reading text. The final selection includes the best-performing tasks in the literature, according to their authentication accuracy, for which detailed information on their implementation is available. These tasks were either not subjected to usability testing in the original works, or were evaluated in a limited fashion (Appendix A). All tasks were developed using PsychoPy[4] and the interfaces are visually summarized in Figure 5b.

We implemented our **Brain Interface Prototypes** based on *Arias-Cabarcos et al.'s* brainwave authentication experiment [1, 2], as follows:

- The **Slideshow task** utilizes a technique that involves presenting an infrequent stimulus among a sequence of common ones, thereby generating a distinct and uniquely identifying brain response [42], often referred to as the oddball design. In our interface implementation, a specific photo is assigned as the target stimulus. Participants are presented with a sequence of images in which the target image shows up infrequently (20% chance). Each photo is displayed for 200 milliseconds, followed by a random interval of 1 to less than 2 seconds before the next image appears. Furthermore, participants are instructed to count the targets, as this has proven useful in improving attention and increasing the amplitude of the brain signal of interest.
- The **Face task** is based on unique brain reactions that appear during face recognition, more specifically when observing an unfamiliar face after being primed with a series of familiar faces. Accordingly, our interface displays unfamiliar faces[5] amidst a stream of images featuring familiar faces (well established international celebrities), with an overall ratio of 1 unfamiliar face to every 3 familiar faces.
- The **Reading task** was designed to elicit uniquely identifying brain responses that appear in response to incongruent sentences. The interface shows sentences word by word, some of them ending in a semantically inconsistent manner [24].

[4]https://www.psychopy.org/
[5]We used fake faces generated with Artificial Intelligence



(a) Technical setup

(b) Authentication Interfaces

Figure 5: Left: Participant wearing the Emotiv EPOC X [17] neuroheadset while using our news website that required brainwave-based user authentication. Right: Interface screenshots of the authentication prototypes: A) Eye movement-Reading, B) Eye movement-Slideshow, C) Eye movement-Dot, D) Brainwaves-Reading, E) Brainwaves-Slideshow, and F) Brainwaves-Face.

For the **Eyetraking Interface Prototypes**, we base our implementations on the research works by *Eberz et al.* [12], and *Sluganovic et al.* [39], as follows:

- The **Slideshow task** involves displaying a series of images to users in a slideshow format. Each image is displayed for a fixed duration of two seconds before being replaced by the next image in the sequence. This task is designed to assess eye-gaze authentication based on how the user's gaze moves and fixates on each image in the slideshow.
- The **Dot task** displays a single red dot on a gray screen that changes position several times. Whenever the dot appears in the user's field of view, their reflexive "saccades" are triggered, causing a reorientation of their gaze towards the dot's new position. These reflexive eye movements have proven useful as a means of eye-gaze authentication.
- The **Reading task** prompts the user to read a passage from the novel "Alice in Wonderland". The text is displayed in a central column on a grey background. Authentication is based on unique eye fixation features, which are captured while the users read the text.

In this study, we utilized interactive mock-ups for each task to simulate the real-world operations of the examined biometric techniques. It is critical to note that our decision to not deploy an actual biometric authentication system was motivated by two primary reasons: the current unavailability of reliable prototypes for brainwave and eye movement authentication and concerns over user privacy risks [15, 20]. These limitations guided our choice to use simulated performance metrics, an approach that is consistent with established methodologies in prior biometric authentication user studies [21, 34, 44, 49]. We relied on performance data reported in the reference publications to configure the login failure rate, explicitly focusing on the False Rejection Rate (FRR), while setting the False Acceptance Rate (FAR) at 1%. Although this FAR value is higher than current industry norms, it aligns with specific contextual constraints and anticipates future advancements in biometric technology. Tables 2 and 3 provide a summary of the login failure rates or FRR for each authentication task, as reported in the literature. We implement these failure probabilities in the developed prototypes.

Hardware Components. The experiment used two devices: 1) the Emotiv EPOC X[6], a neuroheadset equipped with 14 electroencephalography electrodes (sensors) for brainwave data recording; and 2) the Tobii Pro Fusion[7], a compact screen-based eye tracker that can be plugged into a PC screen and captures gaze data at 128 frames per second. These devices were selected because they are higher-end consumer electronics, providing a good balance between accuracy, usability, and cost. Furthermore, this type of hardware has been used in the authentication research literature on which we base our prototype. Though we do not need the hardware for brain/eye data collection in our experiment, we use the devices to provide a realistic scenario, so the participants are convinced that the biometric mechanisms are fully implemented. Fig. 5a depicts a participant wearing the Emotiv headset while using our prototype [8].

C Implementation and Analysis

Recruitment & Ethical Aspects. Recruitment efforts were mainly focused on advertising through the official Instagram and Facebook of our university, distributing flyers around the university, and utilizing email lists of students, targeting participants over 18 years old. Participation was voluntary and could be aborted at any time without negative consequences. The participant remuneration, fixed at 18 Euro (for 75 minutes), slightly exceeds the minimum wage rate

[6] https://www.emotiv.com/epoc-x/
[7] https://www.tobii.com/products/eye-trackers/screen-based/tobii-pro-fusion
[8] The participant provided consent fot he picture to be taken and published

Table 2: Reported False Rejection Rates for Brainwave-based authentication tasks.

Mechanism	Task	FRR (%)
Brainwaves	Slideshow (count)	29.3 [1]
	Face	28.8 [1]
	Reading	38.5 [1]

Table 3: Reported False Rejection Rates for Eyetracking-based authentication tasks.

Mechanism	Task	FRR (%)
Eyetracking	Slideshow	12.37 [12]
	Dot	19.84 [39]
	Reading	6.86 [12]

in Germany (12 Euro/hour)[9]. This higher compensation accounts for the necessity of participants' physical presence in the lab. Participants received this amount in cash. Participants' survey data was only analyzed for research purposes and handled in an anonymized way to ensure confidentiality. We used the SoSci Survey platform[10] for this purpose, as it is a flexible, GDPR-compliant survey platform. Since the tested behavioral biometric systems were simulated, we did not collect any biometric data from our participants. Before taking part in the study, all participants provided their consent. While we did hide the fact that the authentication prototypes were not real, we consider this slight deception as harmless: it does not put users at risk and it provides high benefits for research on ecologically valid scenarios. Our study was approved by the Institutional Review Board (IRB) of our university.

Data Analysis. SUS responses were analyzed using targeted hypothesis testing with α =.05 , selecting the appropriate test based on the data type and distribution. We used the non-parametric Friedman test for within-subjects testing and independent samples t-test for the between-subject case. All statistical analyses were performed using the R programming language. In order to gain a comprehensive understanding of individuals' experiences and contextualize quantitative results, we collected answers to open-ended responses. These responses were analyzed following an iterative, inductive coding approach [30]. One researcher developed the codebook with thematic codes after reviewing responses, while another independently coded the entire data. The inter-coder reliability, assessed using Cohen's Kappa [10], showed satisfactory agreement ($\kappa > 0.7$). Discrepancies in codes were discussed and resolved.

Pilot Study. We piloted the study with a small group of participants (N=3) to test the overall feasibility of design, assess the clarity of the instructions and questions, and evaluate the functionality of the software prototype.

One valuable insight we gained was that one of the participants easily recognized that the prototype was not real. He noticed poor electrode-to-brain connectivity during the setup phase, and despite their successful login, he realized that this could not work so the system was not authentic. Based on this feedback, we modified the protocol to ensure at least 80% connectivity during the brainwave device setup. Additionally, for the eye-tracking mechanism, we focused on accurate calibration and allowed users to interact with their eye gaze on the screen for a few seconds, aiming to enhance their belief in the system's functionality.

As a result, during the debriefing phase of the main study, only three out of 35 participants (8.7%) admitted that they already knew the system was not real. To understand their discernment, we inquired about the cues that led them to this realization. Participant S1 cited the *"short process of determining a brain pattern"* as a clue, indicating skepticism towards the rapid authentication process. Participant S2's unfamiliarity with the system was evident as they remarked it was their *"first time"* using such technology, suggesting a lack of prior exposure as a factor in their suspicion. Meanwhile, S3 simply perceived the setup as *"just an experiment"* suggesting an inherent skepticism towards the authenticity of any setup within an experimental context. It is important to note that these responses do not point to a fundamental flaw in the experiment's design. Instead, they highlight individual experiences and perceptions, common in user studies involving both simulated and real systems. The high fidelity of our simulated system, therefore, remains credible, as these comments reflect isolated viewpoints rather than a collective assessment. Their surveys were subsequently excluded from our analysis to maintain the integrity of the data.

Additionally, the pilot study revealed some minor findings, such as ambiguity in some questions, typographical errors, the need for a country-specific layout for the keyboard, and a few technical issues. We addressed these concerns in the final version of the experiment.

D Results

D.1 Participants Background

The majority of participants (59.4%) fell into the 18-24 age range, while 31.3% were between 25-34, and 9.4% were between 35-44. In terms of gender, 53.1% identified as women, while 46.9% identified as men. When considering educational achievements, 46.9% of participants had a higher education level, with 28.1% holding a Bachelor's degree, 15.6% holding a Master's degree, and 6.3% with a Doctorate degree. From the 33 participants, 68.8% had heard of eye-tracking devices and 43.8% about brain–computer interfaces, but only 9.3% in both cases reported that already have used these devices. The rest of the participants had no prior knowledge about the technologies. Overall, the sample comprised a predominantly young and educated group of participants, with a slight gender imbalance favoring women. Limited familiarity with eye-tracking and brainwave devices was observed, as most participants reported only being aware of, but not used, these technologies. Full details of demographics per condition are given in Table 4.

D.2 Qualitative Analysis

The qualitative analysis is summarized in Tables 5 and 6.

[9]https://en.wikipedia.org/wiki/Minimum_wage_in_Germany
[10]https://www.soscisurvey.de/

Table 4: Study Participants' Background Information

	Brain Mechanisms(N=14)	Eye Mechanisms(N=18)	Overall(N=32)
Preceding knowledge and experience with eye tracking devices			
No knowledge about eye tracking devices	4 (28.6%)	3 (16.7%)	7 (21.9%)
Heard about eye tracking devices	8 (57.1%)	14 (77.8%)	22 (68.8%)
Used some kind of eye tracking	2 (14.3%)	1 (5.6%)	3 (9.4%)
Own some kind of eye tracking devices	0 (0%)	0 (0%)	0 (0%)
Preceding knowledge and experience with Brain Computer Interface technology			
No knowledge about Brain Computer Interfaces	6 (42.9%)	9 (50.0%)	15 (46.9%)
Heard about Brain Computer Interfaces	6 (42.9%)	8 (44.4%)	14 (43.8%)
Used some kind of Brain Computer Interface	2 (14.3%)	1 (5.6%)	3 (9.4%)
Own some kind of Brain Computer Interface	0 (0%)	0 (0%)	0 (0%)
Age			
35 - 44	0 (0%)	3 (16.7%)	3 (9.4%)
25 - 34	3 (21.4%)	7 (38.9%)	10 (31.3%)
18 - 24	11 (78.6%)	8 (44.4%)	19 (59.4%)
Gender			
Woman	8 (57.1%)	9 (50.0%)	17 (53.1%)
Man	6 (42.9%)	9 (50.0%)	15 (46.9%)
highest level of school you have completed or the highest degree			
Higher education entrance	8 (57.1%)	7 (38.9%)	15 (46.9%)
Completed vocational training	1 (7.1%)	0 (0%)	1 (3.1%)
Bachelor's Degree	3 (21.4%)	6 (33.3%)	9 (28.1%)
Master's Degree	1 (7.1%)	4 (22.2%)	5 (15.6%)
Doctorate	1 (7.1%)	1 (5.6%)	2 (6.3%)
Educational background or job field			
Education in, or work in, the field of computer science	12 (85.7%)	10 (55.6%)	22 (68.8%)
No education in, or work in, the field of computer science	2 (14.3%)	8 (44.4%)	10 (31.3%)
Prefer not to say	0 (0%)	0 (0%)	0 (0%)
English level			
B1 - Intermediate English	1 (7.1%)	2 (11.1%)	3 (9.4%)
B2 - Upper Intermediate English	7 (50%)	4 (22.2%)	11 (34.4%)
C1 - Advanced English	2 (14.3%)	10 (55.6%)	12 (37.5%)
C2 - Proficient	4 (28.9%)	2 (11.1%)	6 (18.8%)

Benefits: The most mentioned advantage was usability, which is backed up by the SUS scores in our quantitative analysis. Participants also value not having to deal with passwords and, interestingly, they mention improved security as a common positive aspect. The full list of topics that emerged contains:

- **Usability.** Participants found both the eye-tracking and brain mechanisms to be easy to use. They expressed that these mechanisms were effortless and straightforward. Additionally, some participants specifically mentioned that these methods could be performed hands-free, further emphasizing the ease of interaction and convenience:

  "*Very easy to use, and could be especially beneficial for example when trying to log into a service on a TV, it's a lot more comfortable than typing out your password with a TV remote*"- P26

  "*It can also prove handy when both the hands are already engaged and there is a need of authentication.*"- P10

- **Improve Security.** Several participants expressed a strong sense of security with both the eye-tracking and brain mechanisms. They viewed these authentication methods as highly unique and considered them to be potentially more secure than traditional methods such as fingerprints or regular passwords. Interestingly, the sense of security appeared to be even stronger in relation to brainwaves. They emphasized the difficulty of copying and stealing brainwave data:

  "*It can be more secure than a fingerprint because when you are asleep no one can login to your device.*"-P18

- **Passwordless.** Some participants highlighted the advantage of the eye-tracking and brain-based mechanisms by noting that they eliminate the need to memorize passwords. They

Table 5: What benefits do you see about using a brainwaves activity/eyetracking authentication scheme?

Codes	Representative Quote	Ratio
Usability	*Definition:* Ease of understanding and operation without extensive training.	
	Eye: "It's easy to understand and you don't need to learn how to use it."	34.59%
	Brain: "I can see the benefit of building a more reliable and user-friendly authentication system."	38.05%
Improve Security	*Definition:* Enhancements in safeguarding data and access.	
	Eye: "It seems to be more safe than a fingerprint or a face ID."	21.38%
	Brain:"The barrier to copying a password is very high. If it is only used locally for a password manager or similar, a lot of the attack surface vanishes."	33.63%
Passwordless	*Definition:* Elimination of traditional passwords, reducing the need to remember them.	
	Eye: "The benefits for me are not having to worry about forgetting passwords."	21.38%
	Brain:"Not having to remember a long secure password."	23.01%
Authentication Time	*Definition:* Concerns about the duration required for the system to authenticate a user.	
	Eye: "It's quick to register and log in."	8.81%
	Brain: "It didn't take a lot of time to log in".	3.54%
Fun and Futuristic	*Definition:* Perception of the system as engaging and innovative.	
	Eye: "It is a fun and entertaining way to enter a website (or else)."	11.95%
	Brain: "It is fun, I feel like being in the future."	1.77%
No benefit	*Definition:* users perceive no Problem.	
	Eye: "i dont see any benefits. It gives me a headache."	1.89%
	Brain: ""	0%

Table 6: What problems do you envision about using a brainwave activity/eyetracking authentication scheme?

Codes	Representative Quote/Definition	Ratio
Performance Concerns	*Definition:* Reliability and consistency of the authentication process.	
	Eye: "Hardship in logging in due to inconsistent reading patterns."	24.34%
	Brain: "There is no warranty you would be able to successfully login every time."	20.61%
Mechanism Limitations	*Definition:* Issues related to practical use of the technology.	
	Eye: "Eye-sight glasses and sunglasses could create hindrances..."	15.79%
	Brain: "I do not like to wear this headset..."	26.72%
Security Concerns	*Definition:* Potential risks regarding data safeguarding.	
	Eye: "Why exactly it will be safer..."	18.42%
	Brain: "People might not trust brain activity based authentication..."	14.5%
Authentication Time	*Definition:* Emphasizing quick and prompt user authentication.	
	Eye: "Not fast enough compared to just typing a password"	14.47%
	Brain: "That brainwave headset wouldn't function properly..."	13.74%
Task Usability	*Definition:* Challenges users face in interacting with authentication tasks.	
	Eye: "Concentrating on reading a text was a little bit hard for me."	14.47%
	Brain: "The images flashing is uncomfortable."	7.63%
Privacy Concerns	*Definition:* Issues related to the handling and potential misuse of sensitive personal data.	
	Eye: "Eye gaze data could be sensitive data"	4.61%
	Brain: "Information collected is sensitive and it may cause drastic problems if leaked."	12.98%
Cost of Equipment	*Definition:* Financial implications of implementing and using the technology.	
	Eye: "For now expensive hardware."	2.63%
	Brain: "I think the device would be too expensive."	2.29%
Transparency in Function	*Definition:* Understanding how the system operates and its mechanisms.	
	Eye: "I dont know how it works."	1.32%
	Brain: "Explaining the system to non-tech people could be more difficult."	1.53%
No Problem	*Definition:* users perceive no Problem.	
	Eye: "as long as the technical parts work I don't really see any problems at the moment"	3.95%
	Brain: "..."	0%

appreciated the convenience of not having to rely on remembering complex passwords and appreciated the alternative authentication approach offered by these methods.
- **Authentication Time.** A few participants mentioned that they found this type of authentication to be fast. However, they did not provide specific details with regard to other authentication methods or elaborated on why they considered it fast.
- **Fun and Futuristic.** A few participants expressed that they found this authentication method to be fun and futuristic. They appreciated the unique and innovative nature of the approach, which added an element of excitement and novelty to the authentication experience.

Problems: the most salient problems that emerged in the analysis are:

- **Performance Concerns.** Several participants worried that the system may not be able to accurately track their eye movements, which could lead to problems such as difficulty logging in or inaccurate results as a potential obstacle to successful logins. Similarly, users are concerned that the brain mechanism may not be accurate enough to reliably identify them, leading to login failures. These performance-related concerns highlight the importance of reliability and consistency in system performance.
- **Mechanism Limitations.** During the study, participants expressed several concerns regarding the limitations of the proposed mechanisms due to their inherent nature. For the brain authentication mechanism, the requirement of wearing a headset emerged as a potential hurdle for widespread adoption. Participants pointed out that this additional hardware could be inconvenient and restrict their mobility. On the other hand, the eye-tracking mechanism also presented its own set of limitations. Participants highlighted the challenges faced by individuals with specific needs, such as dyslexic people, blind individuals, and those with visual impairments who rely on alternative methods for authentication. The mechanism's performance was also questioned in conditions such as dark environments and outdoor settings, where accuracy might be compromised. Furthermore, the presence of eyeglasses and sunglasses was found to obstruct or interfere with the accurate tracking of eye movements, adding another layer of complexity. Camera malfunctions were mentioned as a potential reliability issue for the eye-tracking system.
- **Security Concerns.** Users expressed security concerns regarding both types of authentication mechanisms. Concerning brainwaves mechanisms, users highlighted a lack of trust in its security compared to traditional password-based authentication. They emphasized the need for robust security measures and questioned the system's ability to provide sufficient protection. In relation to the eye-tracking mechanism, users expressed even higher levels of security concern. They were worried about the ease of copying or recognizing their eye gaze data, raising doubts about its security. These security concerns underscore the importance of addressing user trust and ensuring the effectiveness and safety of both authentication methods.
- **Authentication Time.** Participants also raised concerns about the time required for authentication using the proposed schemes. Some participants felt that the system was not as fast as conventional methods such as typing passwords. Additionally, the possibility of repeated login attempts due to malfunctioning headsets was mentioned, indicating potential delays in the authentication process. These concerns emphasize the importance of efficient and swift authentication procedures to ensure user satisfaction.
- **Task Usability:** Participants reported encountering challenges related to task difficulty while utilizing the brainwave/eye-tracking scheme. Some participants expressed difficulties in concentrating on reading the text, indicating potential obstacles in effectively engaging with the system. Furthermore, a few participants found the flashing images uncomfortable, suggesting that the visual stimuli associated with the scheme may impede a seamless user experience. These findings underscore the significance of considering task demands and designing visual stimuli in order to optimize usability and minimize cognitive load for users interacting with the system. Additionally, concerns were raised regarding the mechanism's effectiveness for individuals who are illiterate or have difficulty reading. Moreover, A few participants expressed concerns regarding the potential exhaustion associated with frequent use of the system. The notion of the system becoming monotonous and boring over extended periods was mentioned, indicating the need to consider user engagement and system design elements that mitigate fatigue.
- **Privacy Concerns.** Privacy concerns emerged in the participants' responses, with a higher frequency for the brain mechanisms. Participants emphasized the importance of preventing the availability of their brain activity data to government entities and authentication providers, highlighting a desire to avoid any potential leaks or misuse of this sensitive information. The sensitivity of the collected brainwave data underscored the need for robust privacy measures and heightened awareness regarding the potential implications of unauthorized access or disclosure.
- **Cost of Equipment.** Some participants mentioned concerns about the cost associated with the required hardware. The perceived expense of the devices could pose a barrier to widespread adoption. Considering cost implications and exploring ways to make the system more affordable could enhance its accessibility and usability.
- **Transparency in Function.** A few participants expressed uncertainty about how the system functions. They highlighted the need for clear explanations, particularly for non-technical individuals, to facilitate understanding and acceptance.

D.3 Comparative Analysis

We compared the usability of our two mechanisms, eye-tracking and brainwaves, with eight different authentication mechanisms from other papers. We selected works that focused on biometrics

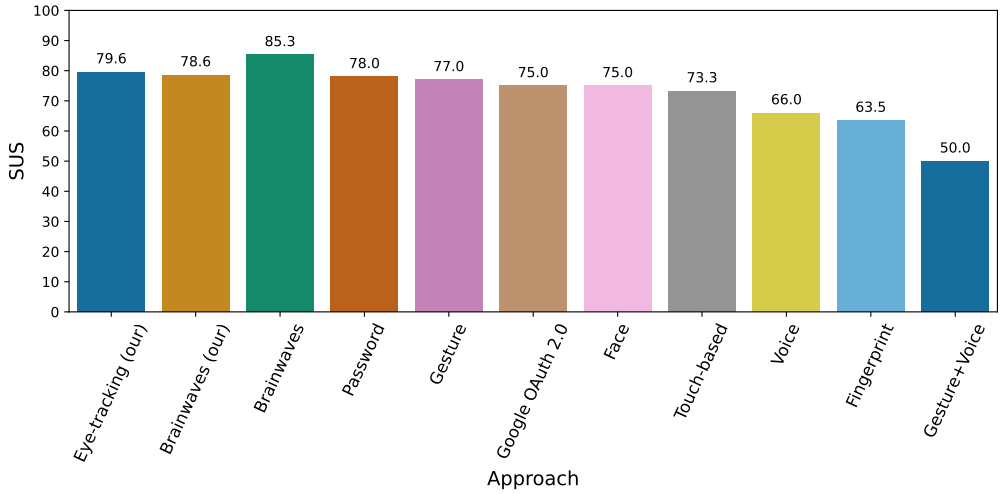


Figure 6: SUS scores for authentication with Eye-tracking (our), Brainwaves(our), Brainwaves [34] Password [44], Gesture, [44], Google OAuth 2.0 [35], Face [44], Touch[8], Voice [44], Fingerprint [32], and Gesture+Voice [44].

and reported the System Usability Scale (SUS) score. We also considered the evaluation of passwords and single sign-on (SSO) as a baseline. The final set of authentication mechanisms available for comparison according to these criteria include: passwords, SSO (Google OAuth)[35] [44], as well as five biometric methods: Gesture [44], face [44], touch-based [8], fingerprint [44], and voice [44]. As it can be seen in Figure 6, our eye-tracking and brainwave mechanisms achieved on average higher SUS scores than all of the other mechanisms. Comparatively, the traditional password-based authentication method obtained a SUS score of 78, demonstrating similar usability to our mechanisms. Furthermore, it is to note that most of our participants had no previous experience with the tested technologies and studies have shown that unfamiliar users rate new solutions 15-16% lower in the SUS scale [29].

When comparing the SUS scores with our work, it is important to consider that *Trewin et al.* [44] primarily focused on smartphone usability rather than the desktop scenario we examined in our study, and conducted the evaluation in 2012. Future work testing under the same conditions would be interesting to better assess comparative usability. The closest work, from *Ruoti et al.* [35] compared seven non-biometric schemes in 2015, confirming that users prefer single sign-on vs the other secret and token-based solutions evaluated. Interestingly, their participants would like biometrics to be part of their ideal authentication system.

In our comparative analysis, we also consider the work of *Röse et al.* [34], who reported an 85.28 System Usability Scale (SUS) score based on a brainwave slideshow task, though measured with a smaler sample (9 participants). Their findings closely align with ours, employing a similar survey process in their experiment. The slightly higher SUS score in their study could be attributed to the use of a more convenient and easy to wear brainwave recorder with only 4 dry sensors, the Muse 2[11]. When assessing perceptions of security, 55% of participants in *Röse et al.'s* study agreed or strongly agreed that their scheme was secure, compared to 47.6% in our research. Regarding the ease of use, both studies observed a similar trend, with 55% of their participants and 45.2% of ours reporting neutral opinions. Additionally, when evaluating the benefit-effort trade-off, 55% in *Röse et al.'s* study disagreed or strongly disagreed that the effort outweighed the benefits, closely paralleling our finding of 45.2% disagreement. Finally, when asked about the willingness to adopt the scheme if available, 66.6% of participants in their study responded positively, compared to an average of 61.9% in ours.

[11]https://choosemuse.com/products/muse-2