A Literature Review on Virtual Reality Authentication

John M. Jones, Reyhan Duezguen, Peter Mayer, Melanie Volkamer, Sanchari Das

A Literature Review on Virtual Reality Authentication

John M. Jones[1], Reyhan Duezguen[2], Peter Mayer[2], Melanie Volkamer[2], Sanchari Das[1]

[1] University of Denver
firstname.lastname@du.edu
[2] Karlsruhe Institute of Technology, SECUSO - Security, Usability, Society
firstname.lastname@kit.edu

Abstract

As virtual reality (VR) sees an increase in use in several domains such as retail, education, military; a secure authentication scheme for VR devices is necessary to keep users' personal information safe. A smaller section of research focuses on the authentication schemes of VR devices. To further the understanding of this topic, we conducted a detailed literature review of VR authentication by exploring papers published till October 2020. A total of $N = 29$ papers were found. While many papers evaluate the accuracy of authentication methods, few conduct detailed user studies. In the user studies done, we found a lack of focus on diverse populations such as the elderly, with the mean age of the participants being 25.11. Our findings from the literature review give a detailed overview of VR-based authentication schemes and highlight trends as well as current research gaps. These findings drive future research direction to create robust and usable authentication strategies.

Keywords

Virtual Reality, Authentication, Literature Review, User Studies.

1 Introduction

Over the past five years Virtual Reality (VR) use has grown to encompass many new areas outside of recreation [1]. With the rise of VR technologies, a secure method of authenticating users has become a pressing issue [2]. Due to the nature of VR it leaves the user prone to observation attacks, in which a malicious user may observe them inputting a traditional password into their device [3, 4]. As such, prior research shows that the solution exists in leveraging the unique benefits of the VR Head Mounted Device (HMD) by gathering biometric information from the user [5]. However, this collection of biometric data leaves the user at risk of exposure of biometric data attack vectors. Thus, we aim to analyze the current research on VR authentication through a detailed literature review.

In order to better understand the field of VR authentication, we conducted a literature review where the initial online database search yielded a total of $4,300,000$ publications focusing on VR, out of which only $N = 57$ were articles focused on the security aspects of VR devices. For an in-depth analysis we thereafter performed an analysis of the 29 articles among the 57 which detailed VR-based authentication. In this analysis we found that the papers primarily focused on two broad categories, including biometric-based authentication and knowledge-based authentication. While conducting our review, we recognized significant gaps in the research in the field of VR authentication including a lack of diverse population samples.

2 Methods

Our review is composed of three steps: (1) article collection from multiple digital libraries, (2) abstract and then full text screening, and finally (3) thematic analysis of the collected papers. Papers were included in our analysis corpus if they met the following criteria: (1) written in English; (2) provided some form of analysis or technique regarding VR authentication; (3) peer-reviewed workshop, conference, or journal papers, i.e., any work in progress papers or poster abstracts were excluded from our corpus.

Data Collection and Duplicate Removal: We collected the papers for our analysis using the research tool Publish or Perish[3]. We performed a keyword-based search on the platform to collect papers that were published in several digital libraries including, ACM, IEEE eXplore, SSRN, ScienceDirect, and ResearchGate. This initial search included the following keywords: "Authentication for VR", "Authentication VR", "Authentication in VR", "VR user authentication", "VR authentication". For each keyword the word VR was used both abbreviated and written out. We did not perform any time-based filtering on the article collection, however, we found that the earliest published paper was in 2008.

This initial search helped us to obtain a corpus of $N = 123$ articles which was further reduced to $N = 91$ by removing the duplicate articles that appeared in our keyword searches. Thereafter, we wanted to focus primarily on any published research, thus any patents were removed from the corpus; leaving us with a total of $N = 57$ articles on which we performed the abstract and full text screening for quality control.

Abstract and Full Text Screening: After the paper collection process was completed we read through the abstract of the articles. Thereafter, we continued with reading the full text of all 57 articles. We carefully assessed whether the published research met the criteria to be included in the final corpus. This process resulted in $N = 29$ articles on which our analysis was performed. We noticed that the other half of the articles talked about the technical details of the VR tools and devices, and mentioned authentication is needed for these devices.

[3] https://harzing.com/resources/publish-or-perish

However, their research was not focused on VR-based authentication.

Analysis: We focused our analysis of VR authentication on the following aspects: (1) the types of authentication schemes applied or discussed by the researchers on VR tools and technologies; (2) any security evaluation of the proposed protocols they have done; (3) pros and cons of the authentication scheme the article was covering; (4) methods used by the researchers to look at any user studies done; and (5) the participant details of the user studies done to test the VR authentication scheme. Two researchers conducted thematic analysis on the work (inter-coder reliability score = 86.7%). Such techniques include collecting the pros and cons of each proposed VR authentication scheme, and collecting data that is relevant to the accuracy of the scheme.

3 Findings

We primarily evaluated the type of authentication, the security analyses of the proposals in the articles, and the user studies conducted to evaluate the properties of the proposals. Out of the overall 29 articles, $N = 26$ included at least one user study and seven of these conducted multiple user studies [2,4,6–10], leading to the analysis of 34 user studies across all articles. Therefore, in sections 3.1 and 3.2, the percentages are calculated off of $N = 29$ articles, while in section 3.3 they are calculated off of $N = 34$ user studies.

3.1 Types of Authentication

In our analysis, we expanded on the authentication methodologies and found majorly three styles of authentication proposed by the researchers, including biometric, knowledge-based, and multi-modal authentication.

Knowledge-based Authentication: The most prevalent form of VR authentication implemented by the researchers has been the classical mode of password-based authentication. Overall, our corpus contains $N = 8$ (27.5%) [2, 4, 7, 8, 10–13] papers which covered knowledge-based authentication schemes. While using the knowledge-based authentication scheme, the commonly used technique implemented by the researchers has been to enter a PIN or an alphanumeric password before being allowed access to the VR device [2, 4, 8]. For example, Yu et al. [4] study the potential usability of PIN systems in VR, finding that they have an average entry time of 10.5 seconds, but leave the user prone to shoulder surfing attacks. Another article which covers PINs and patterns was written by George et al. [2], in which they find both PINs and patterns are well suited to VR, because of their high usability and security in authentication.

Biometric Authentication: Another form of authentication employed by the researchers uses biometric factors of the VR headset user. Our corpus contains $N = 15$ (51.7%) [3, 14–26] papers that cover biometric authentication systems.

The types of biometric data utilized for the authentication varied between different studies, but the general principle of biometric authentication remains. Types of data collected in such schemes include, electroencephalogram (EEG) readings [17, 27], body movements [3, 14, 16, 18, 20, 21, 23, 24], and Electrooculography (EOG) readings [26]. A paper by Li et al. collects EEG signals in two ways, first subjects would view a video in VR and then on a laptop. They then extracted the EEG data from both the VR and non-VR sections and used it to later authenticate the users, achieving an accuracy of 80.91% [17]. An example of a study which authenticates based of off body movement data is the work by Kupin et al. In this paper they authenticate users based on how they complete the task of throwing a ball, as they throw the HMD measures the position of their dominant hand controller [23]. One of the key weaknesses of biometric authentication is that it requires users' personal biometric data increasing the susceptibility to security attacks increasing user privacy concerns.

Multi-model Authentication: Multi-model authentication schemes utilize two or more separate techniques in order to authenticate users. This helps improve the accuracy of the system as multiple things are being checked. It also improves the security of the system, as an attacker must bypass two systems instead of one. A prime example of this is RubikBiom, an authentication scheme designed by Mathis et al. which combines the knowledge-based system of entering a password on a Rubik's cube, with the gesture biometric data collected as you enter the password [3]. Thus, knowing the password is not enough to gain entry to the system, the password must also be entered in a way that matches the users biometric gesture data. These multi-model systems help to negate some of the downsides found in any of the individual type of authentication. However, they can also be plagued by similar weaknesses.

Gaze-based authentication: Another section of VR authentication research is found within systems that utilize the human gaze, known as gaze-based authentication methods. Gaze-based authentication can combine or use both biometric and knowledge based approaches given its implementation. Among our corpus, $N = 5$ (17.2%) [6, 9, 28–30] articles cover gaze-based schemes. Gaze-based schemes authenticate the user based off their eye gaze, such as measuring eye saccades as a user observes a video [22]. This can be combined with a knowledge-based system, where the user enters the password by looking at a PIN pad [9, 28]. The concept revolves around your eye movements being tracked by the HMDs and then having the spot where you are looking at being displayed on the screen or tracked and analysed by the HMDs. This method helps to mitigate the possibility of observational attacks, as the user of the HMDs can authenticate without any outward body movements that could give away the password. George et al. [9] propose such a system in which the user selects a number of objects in a room by looking at them. Overall, this approach has a mean entry time of 5.94 seconds, with very few errors in entries.

3.2 Security Evaluation of Proposed Authentication Protocols

When evaluating the security of a given authentication scheme there are many different things to consider given the type of the system. In our corpus, $N = 12$ (41.38%) papers did the security evaluation of their protocol [2,4,7,9,10,14–16,24,26,27,31]. For biometric schemes, a clear indicator of security is a low equal error rate (EER). The biometric schemes in our corpus had an average EER of 8.67%, with the minimum being 1.4% from the study by Olade et al. [16]. The average accuracy amongst the biometric schemes was 92.34% with the highest being 99% accuracy obtained by Sivasamy et al. [20]. George et al. conducted and described two security studies in their paper which cover potential attacks on the system. Even when attackers were provided with video of the user entering their password, they were unable to guess the password indicating the schemes resilience to observational attacks [10]. Of the articles which covered knowledge-based schemes ($N = 8$ papers), $N = 5$ (62.5%) provided an additional study which analyzed potential attack threats and determined whether or not the system was resilient [2,4,7,9,10].

3.3 User Studies

The articles included in our further analysis had a resounding amount of user studies, with $N = 26$ (89.65%) of articles including some form of user study. Among these, seven articles included two or more user studies [2,4,6–10]. The articles which included multiple studies tended to work with knowledge-based authentication schemes [2,4,7,8,10–13], as multiple studies are needed to observe attacking patterns of the systems. Studies which covered biometric schemes had the highest average user study population size of 69.8 participants [3,5,14–22,24,26,31], and gaze-based [6,9,28] as well as knowledge-based schemes had average sizes of 35 and 20 participants respectively. Across all user studies, the average sample size was 44.18.

Age: We noticed a significant gap in literature where the studies were mostly based of convenient samples, such as university students. For other populations, such as the elderly, their security perspective or VR usage was understudied. The mean age of participants in user studies was 25.11 years. Furthermore, the eldest participant amongst our the studies in our literature corpus was 57 [9].

Gender: In our literature corpus we found more male participants in the user studies (49%) than females (35.9%). 14.71% studies did not report the gender in their analysis [8,15,19,25,27]. This gap is most noticeable in articles which cover gaze-based schemes, with a 3 to 1 ratio [6,9,28]. Table 1 shows the gender distribution of the different types of studies analyzed in this paper.

Study duration: The majority ($N = 24$, 70.59%) of the studies were conducted in a single session [3,4,7,10,14,15,17,19–22,27,28,31]. However, some studies conducted multiple phase user studies [11,16,18,23–26]. While others implied both single session and multiple phase user studies [6,8,9]. There is a vast difference in the duration of studies, with the longest study taking 2 months to conclude while most are only single session.

Gender			
Authentication method	Male	Female	Not Reported
Biometric	467(44.6%)	397(37.9%)	183(17.5%)
Multi-Modal (Gaze-based)	128(74%)	45(24%)	0(0%)
Knowledge	149(52.84%)	104(36.88%)	29(10.28%)
Total	744(49.53%)	546(36.4%)	212(14.1%)

Table 1. Showcases the Gender of Participants for Each Type of Authentication-based Studies on VR Devices

Type of User Studies: We split the studies into four different categories that adequately describe the purpose of each study. Table 2 mentions the type of user studies we have found in our literature corpus. Dataset creation studies' primary goal was to build a dataset which they could then use to test out their authentication scheme, and tune their authentication mechanism [6, 15, 17–20, 22, 23, 25, 31]. Authentication evaluation studies sought to test out the proposed authentication scheme and its working principle for VR devices [8, 14, 16, 23, 24, 26–28]. Usability studies are studies which tested the usability or memorability of their proposal [2–4, 7, 9–11]. Security studies measured the effective security of their proposed scheme using participants, whether they were able to hack the system [2, 4, 7, 9, 10]. There was one notable study conducted by George et al. which covered both security and usability domains [2]. So, this study appears in our table under both the usability and security evaluation sections.

Type of Study		
Type of Study	Number of Studies	Average Study Duration (Days)
Dataset Creation	10(28.57%) [6, 15, 17–20, 22, 23, 25, 31]	1.1
Authentication Evaluation	9(25.71%) [8, 14, 16, 21, 23, 24, 26–28]	12.44
Usability	10(28.57%) [2–4, 7–11]	2.8
Security Evaluation	6(17.14%) [2, 4, 7, 9, 10]	1

Table 2. Showcases the Types of User Studies Done by Researchers, Along with the Number of Studies and Average Duration. The Percentages are Calculated on a Total of 34 User Studies in 26 Papers:

4 Discussions and Implications

The various advantages and disadvantages of proposed authentication schemes vary greatly depending on many factors.

Knowledge-based: Knowledge-based authentication schemes offer an advantage by having arguably the greatest familiarity to users. Also, knowledge-based authentication does not require any personal data from the user to work (i.e. users might still choose secrets including their personal data, but in contrast

to biometrics this is not required). However, the studies we found regarding such schemes point towards security problems, indicating e.g. a susceptibility to shoulder-surfing which is a bigger issue in VR as users don't see the real world when having their HMDs on.

Biometric: Biometric authentication schemes proposed for VR environments utilise a wide variety of user characteristics (e.g. EEG or body movements). These are less familiar to the users. Therefore, users might be reluctant to accept them as replacement alternative for the better-known schemes. Furthermore, authentication based on body movement might be challenging for elderly or people with handicaps. Thus, user groups with physical constraints need to be taken in consideration when investigating the usability of such schemes. Yet, biometric authentication offers in the proposed configurations a high level of security, in particular resilience to shoulder-surfing attacks. On the other hand, biometric authentication has the downside of needing to collect and store users' biometric data.

Multi-modal: Multi-modal authentication schemes offer the highest security. When combining knowledge-based schemes with gaze-based elements, the risk of shoulder-surfing attacks can be partly mitigated, as the attacker can not see what the user is inputting. For example, by combining a knowledge-based scheme with biometric readings, Mathis et. al created a secure authentication mechanism that negates the possibility of an observation attack [3]. On the other hand, low acceptance of one scheme might not be completely mitigated by combining it with a better-accepted one, but instead have the inverse effect.

Implications for future research: Firstly, we identified a potentially very low acceptance, which might hinder adoption of these schemes. In particular, since the VR market is currently still somewhat niche, this might have serious impacts. Yet, very few user studies actually explored this space and future studies should explore the acceptance of potentially more exotic schemes. Secondly, the long-term usability (in particular memorability) is a space mostly unexplored. Conducting these studies is of the essence to properly assess the real-world deployability of the schemes in the VR context. If using these schemes can aggravate issues which are specific to the VR context, such motion sickness or eye strain, otherwise suitable schemes might not be deployable in the VR context. Thirdly, the usability studies reported for the authentication schemes we found in our literature review mostly relied on convenience samples. While this problem is not specific to studies investigating authentication schemes for use with VR, this leads to a strong skew in the samples. Therefore, future studies must strive for more diverse samples. Especially elderly people are underrepresented in the user studies. Finally, multi-modal authentication seems to be under-researched in the VR context. Specifically, how multi-modal authentication can be best integrated into the VR context and work for users when wearing VR headsets is an open question. The few works done in this area (e.g., combining eye-gaze and a secret for knowledge-based authentication) seem promising, but alternatives and how easy proposals can be translated from a non-VR context should be investigated

to harness the full potential of existing proposals and guide the design of new proposals specifically tailored to the VR context.

Limitations: This literature review reflects the current work in the field of VR authentication. It is possible that in gathering these articles some were missed. However, the corpus we gathered provides detailed representation of all major aspects of VR authentication.

5 Conclusion

This literature review reports on 29 papers within the field of VR authentication schemes. We found that certain gaps in literature exist, such as including elderly participants in user studies. We also provide in depth statistics on the current methods of authentication and the potential each system holds. We conclude that there should be more investigation into multi-model schemes, as they combine the advantages of both knowledge-based and biometric authentication and have been relatively unstudied yet.

6 Acknowledgement

This work was supported by the Helmholtz Association (HGF) through the subtopic Engineering Secure Systems (ESS) at Karlsruhe Institute of Technology. Furthermore, this research was supported through the Secure and Privacy Research in New-Age Technology (SPRINT) Lab, University of Denver. Any opinions, findings, and conclusions or recommendations expressed in this material are solely those of the author(s).

References

1. Tsun-Ju Lin and Yu-Ju Lan. Language learning in virtual reality environments: Past, present, and future. *Journal of Educational Technology & Society*, 18(4):486–497, 2015.
2. Ceenu George, Mohamed Khamis, Emanuel von Zezschwitz, Marinus Burger, Henri Schmidt, Florian Alt, and Heinrich Hussmann. Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality. In *The 2017 Network and Distributed System Security Symposium (NDSS)*. NDSS, 2017.
3. Florian Mathis, Hassan Ismail Fawaz, and Mohamed Khamis. Knowledge-driven biometric authentication in virtual reality. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–10, 2020.
4. Zhen Yu, Hai-Ning Liang, Charles Fleming, and Ka Lok Man. An exploration of usable authentication mechanisms for virtual reality systems. In *2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, pages 458–460. IEEE, 2016.
5. Brook Bowers, Andrew Rukangu, and Kyle Johnsen. Making it simple: Expanding access and lowering barriers to novel interaction devices for virtual and augmented reality. In *2020 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pages 1–6. IEEE, 2020.

6. Karan Ahuja, Rahul Islam, Varun Parashar, Kuntal Dey, Chris Harrison, and Mayank Goel. Eyespyvr: Interactive eye sensing using off-the-shelf, smartphone-based vr headsets. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(2):1–10, 2018.
7. Florian Mathis, John Williamson, Kami Vaniea, and Mohamed Khamis. Rubikauth: fast and secure authentication in virtual reality. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–9, 2020.
8. Ilesanmi Olade, Hai-Ning Liang, Charles Fleming, and Christopher Champion. Exploring the vulnerabilities and advantages of swipe or pattern authentication in virtual reality (vr). In *Proceedings of the 2020 4th International Conference on Virtual and Augmented Reality Simulations*, pages 45–52, 2020.
9. Ceenu George, Daniel Buschek, Andrea Ngao, and Mohamed Khamis. Gazeroomlock: Using gaze and head-pose to improve the usability and observation resistance of 3d passwords in virtual reality. In *International Conference on Augmented Reality, Virtual Reality and Computer Graphics*, pages 61–81. Springer, 2020.
10. Ceenu George, Mohamed Khamis, Daniel Buschek, and Heinrich Hussmann. Investigating the third dimension for authentication in immersive virtual reality and in the real world. In *2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*, pages 277–285. IEEE, 2019.
11. Jonathan Gurary et al. *Improving the Security of Mobile Devices Through Multi-Dimensional and Analog Authentication*. PhD thesis, Cleveland State University, 2018.
12. Jonathan Gurary, Ye Zhu, and Huirong Fu. Leveraging 3d benefits for authentication. *International Journal of Communications, Network and System Sciences*, 10(8):324–338, 2017.
13. Reyhan Duezguen, Peter Mayer, Sanchari Das, and Melanie Volkamer. Towards secure and usable authentication for augmented and virtual reality head-mounted displays. *arXiv preprint arXiv:2007.11663*, 2020.
14. Sarah Morrison-Smith, Aishat Aloba, Hangwei Lu, Brett Benda, Shaghayegh Esmaeili, Gianne Flores, Jesse Smith, Nikita Soni, Isaac Wang, Rejin Joy, et al. Mmgatorauth: A novel multimodal dataset for authentication interactions in gesture and voice. In *Proceedings of the 2020 International Conference on Multimodal Interaction*, pages 370–377, 2020.
15. Henry K Griffith and Oleg V Komogortsev. Texture feature extraction from free-viewing scan paths using gabor filters with downsampling. In *ACM Symposium on Eye Tracking Research and Applications*, pages 1–3, 2020.
16. Ilesanmi Olade, Charles Fleming, and Hai-Ning Liang. Biomove: Biometric user identification from human kinesiological movements for virtual reality systems. *Sensors*, 20(10):2944, 2020.
17. Sukun Li, Sonal Savaliya, Leonard Marino, Avery M Leider, and Charles C Tappert. Brain signal authentication for human-computer interaction in virtual reality. In *2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, pages 115–120. IEEE, 2019.
18. Ashwin Ajit, Natasha Kholgade Banerjee, and Sean Banerjee. Combining pairwise feature matches from device trajectories for biometric authentication in virtual reality environments. In *2019 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR)*, pages 9–97. IEEE Computer Society, 2019.

19. Robert Miller, Ashwin Ajit, Natasha Kholgade Banerjee, and Sean Banerjee. Realtime behavior-based continual authentication of users in virtual reality environments. In *2019 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR)*, pages 253–2531. IEEE, 2019.
20. Manimaran Sivasamy, VN Sastry, and NP Gopalan. Vrcauth: Continuous authentication of users in virtual reality environment using head-movement. In *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, pages 518–523. IEEE, 2020.
21. Yujun Lu, BoYu Gao, Jinyi Long, and Jian Weng. Hand motion with eyes-free interaction for authentication in virtual reality. In *2020 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pages 715–716. IEEE, 2020.
22. Julie Iskander, Ahmed Abobakr, Mohamed Attia, Khaled Saleh, Darius Nahavandi, Mohammed Hossny, and Saeid Nahavandi. A k-nn classification based vr user verification using eye movement and ocular biomechanics. In *2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)*, pages 1844–1848. IEEE, 2019.
23. Alexander Kupin, Benjamin Moeller, Yijun Jiang, Natasha Kholgade Banerjee, and Sean Banerjee. Task-driven biometric authentication of users in virtual reality (vr) environments. In *International conference on multimedia modeling*, pages 55–67. Springer, 2019.
24. Tahrima Mustafa, Richard Matovu, Abdul Serwadda, and Nicholas Muirhead. Unsure how to authenticate on your vr headset? come on, use your head! In *Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics*, pages 23–30, 2018.
25. Robert Miller, Natasha Kholgade Banerjee, and Sean Banerjee. Within-system and cross-system behavior-based biometric authentication in virtual reality. In *2020 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pages 311–316. IEEE, 2020.
26. Shiqing Luo, Anh Nguyen, Chen Song, Feng Lin, Wenyao Xu, and Zhisheng Yan. Oculock: Exploring human visual system for authentication in virtual reality head-mounted display. In *2020 Network and Distributed System Security Symposium (NDSS)*, 2020.
27. Vrishab Krishna, Yi Ding, Aiwen Xu, and Tobias Höllerer. Multimodal biometric authentication for vr/ar using eeg and eye tracking. In *Adjunct of the 2019 International Conference on Multimodal Interaction*, pages 1–5, 2019.
28. Mohamed Khamis, Carl Oechsner, Florian Alt, and Andreas Bulling. Vrpursuits: interaction in virtual reality using smooth pursuit eye movements. In *Proceedings of the 2018 International Conference on Advanced Visual Interfaces*, pages 1–8, 2018.
29. Rosa Iglesias, Mauricio Orozco, Fawaz A Alsulaiman, Julio J Valdes, and Addulmotaleb El Saddik. Characterizing biometric behavior through haptics and virtual reality. In *2008 42nd Annual IEEE International Carnahan Conference on Security Technology*, pages 174–179. IEEE, 2008.
30. Dillon Lohr, Samuel-Hunter Berndt, and Oleg Komogortsev. An implementation of eye movement-driven biometrics in virtual reality. In *Proceedings of the 2018 ACM Symposium on Eye Tracking Research & Applications*, pages 1–3, 2018.
31. Dillon J Lohr, Samantha Aziz, and Oleg Komogortsev. Eye movement biometrics using a new dataset collected in virtual reality. In *ACM Symposium on Eye Tracking Research and Applications*, pages 1–3, 2020.