

Review

Recent Trends of Authentication Methods in Extended Reality: A Survey

Louisa Hallal^{1,*}, Jason Rhinelanders¹  and Ramesh Venkat²¹ Division of Engineering, Saint Mary's University, Halifax, NS B3H 3C3, Canada; jason.rhinelanders@smu.ca² Sobey School of Business, Saint Mary's University, Halifax, NS B3H 3C3, Canada; ramesh.venkat@smu.ca

* Correspondence: louisa.hallal1@smu.ca

Abstract: Extended Reality (XR) is increasingly gaining momentum in industries such as retail, health, and education. To protect users' personal data, establishing a secure authentication system for XR devices becomes essential. Recently, the focus on authentication methods for XR devices has been limited. To further our understanding of this topic, we surveyed authentication schemes, particularly systems and methods deployed in XR settings. In this survey, we focused on reviewing and evaluating papers published during the last decade (between 2014 and 2023). We compared knowledge-based authentication, physical biometrics, behavioral biometrics, and multi-model methods in terms of accuracy, security, and usability. We also highlighted the benefits and drawbacks of those methods. These highlights will direct future Human–computer Interaction (HCI) and security research to develop secure, reliable, and practical authentication systems.

Keywords: authentication; biometrics; extended reality; virtual reality; augmented reality; head-mounted displays



Citation: Hallal, L.; Rhinelanders, J.; Venkat, R. Recent Trends of Authentication Methods in Extended Reality: A Survey. *Appl. Syst. Innov.* **2024**, *7*, 45. <https://doi.org/10.3390/asi7030045>

Academic Editor: Christos Douligeris

Received: 3 April 2024

Revised: 17 May 2024

Accepted: 20 May 2024

Published: 28 May 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Engagement in various online activities, such as education and meetings, has heightened during the COVID-19 pandemic. However, it has limitations in terms of real-world experiences, physical expression, and collaboration since online environments only provide simple interaction services using microphones, cameras, and screens. In the recent past, Metaverse environments—interconnected virtual spaces where users could interact using Extended Reality (XR), a general term for immersive technologies namely Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR)—have attracted interest to unravel these limitations. However, the realization of a fully functional metaverse is still complicated by the fact that it requires the integration of different technologies. Many advanced technologies, such as 5G, Web 3.0, Blockchain, and Artificial Intelligence (AI), are becoming more promising and feasible to make the metaverse a reality, which marks a fundamental change in terms of human–computer interactions (HCI), ubiquity, and decentralization. This has caught the attention of numerous large tech corporations, which are investing billions in developing various metaverse platforms and XR technologies. For instance, Microsoft offers Microsoft Mesh for live virtual collaborations, Meta offers Horizon Workrooms for immersive virtual workspaces, Nvidia offers Omniverse for the development of advanced 3D applications, and Decentraland which is owned by its users and developers, among many others. As a result, XR innovative solutions naming AR developing platforms (e.g., Google ARCore, Apple ARKit), VR headsets (e.g., HTC Vive Pro 2), and MR glasses (e.g., Microsoft HoloLens) have progressed into marketable and affordable technologies. Furthermore, the numbers of XR users are anticipated to increase, and XR experiences are expected to become more immersive. Given the future potential of the Metaverse, there are significant cybersecurity threats that need to be resolved before the metaverse can be put to practical use. Sensitive user data such as identity, passwords, and biometric information is likely to become vulnerable to privacy and security breaches.

Extended reality devices collect massive amounts of sensitive biometric information about their users. Various privacy and security risks stemming from this considerable data collection, inputs, outputs, and user interactions have been identified by researchers. Another difficulty that applies to XR wearables is that of user authentication, which is used as a first barrier for technology devices and systems. Efficient authentication techniques and strong access control models aim to identify authorized and unauthorized access. Less reliable authentication systems lead to users risking their security. The absence of a physical keyboard in XR makes it challenging to authenticate users and secure user profiles and the data generated by XR devices. Therefore, additional safety measures will be needed to ensure users' privacy in the future. In essence, to further understand authentication and its related privacy risks in the XR ecosystem, it became crucial to study XR authentication as a whole instead of segmented AR, MR, and VR technologies as it has been typically practiced.

The evolution of authentication in XR has been marked by a shift from traditional methods to more advanced and context-aware approaches. At first, XR authentication relied heavily on conventional methods like passwords and PINs, leading to usability challenges within immersive environments. As XR technologies developed, biometric authentication methods gained attention due to their convenience and added layers of security. Behavioral biometrics such as eye tracking and gait recognition seem promising considering users' unique interactions in XR environments. This allows for smoother and more robust authentication solutions suitable for the immersive nature of XR, enhancing both security and user experience across various applications and sectors.

Despite the current efforts to improve authentication in the field of XR, it is still evolving, putting both users' privacy and data security at risk. Thus, we strongly believe that it is time to review existing research to guide the design and creation of innovative XR authentication systems. Therefore, we aim to comprehensively evaluate and compare recent proposed authentication systems. To the best of our knowledge, a survey targeting both traditional knowledge-based and biometric-based techniques used in XR environments is lacking. This survey makes the following contributions:

- An in-depth exploration of recent research on authentication aspects in XR.
- An overview of various authentication approaches used within XR.
- A taxonomy outlining the diverse authentication techniques applied in XR.
- A critical analysis of recent research outcomes and evaluation of usability and security studies regarding authentication systems in XR

Before proceeding to the review of the different user authentication schemes, we clarify that we do not focus on network security or any related topics. This paper is organized as follows: Our methodology is presented in Section 2. Related research and how it differs from our survey are discussed in Section 3. Next, Sections 4 and 5 present an overview of authentication methods in XR. Section 6 presents a discussion and future research directions. This paper concludes in Section 7.

2. Methods

In this work, we survey and summarize the most recent research that highlights authentication schemes for XR over the last decade. The adopted approach was a two-stage process to review authentication in XR. The initial stage was collecting and identifying relevant papers published between 2014 and July 2023. As such, papers containing the XR-related index terms "Augmented Reality" OR "Virtual Reality" OR "Mixed Reality" OR "Extended Reality" OR "Metaverse" OR "Head-mounted Displays" and authentication-related terms "Authentication" OR "Identification" OR "Security and Privacy" in the title, keywords, and abstract fields were collected using five major scientific databases naming Scopus, IEEE Xplore, Web of Science, ScienceDirect, and ACM. A total of 1186 journal and conference publications were the outcome of this search. In the second stage, we performed an abstract and full text screening to make sure that the content of our selection included papers related to our index terms search from the first stage. This allowed us to define a taxonomy of the different sub-topics that researchers in the field of authentication in

XR are currently focusing on. Then, we specified our review sub-topics, further selected publications that contributed to these sub-topics, and presented summaries of the studies' findings. Regarding XR and the metaverse, those publications' specific emphasis was on the technical and security aspects of authentication systems (data collection studies, deployed schemes, proposed techniques, and usability and security evaluations). This stage resulted in 197 publications. To reflect current trends, we only included recent publications in our review. We also did not exclude articles based on the number of citations alone, to ensure we did not overlook any potentially innovative ideas. Figure 1. presents a PRISMA flow model of the process of selecting relevant papers for our survey.

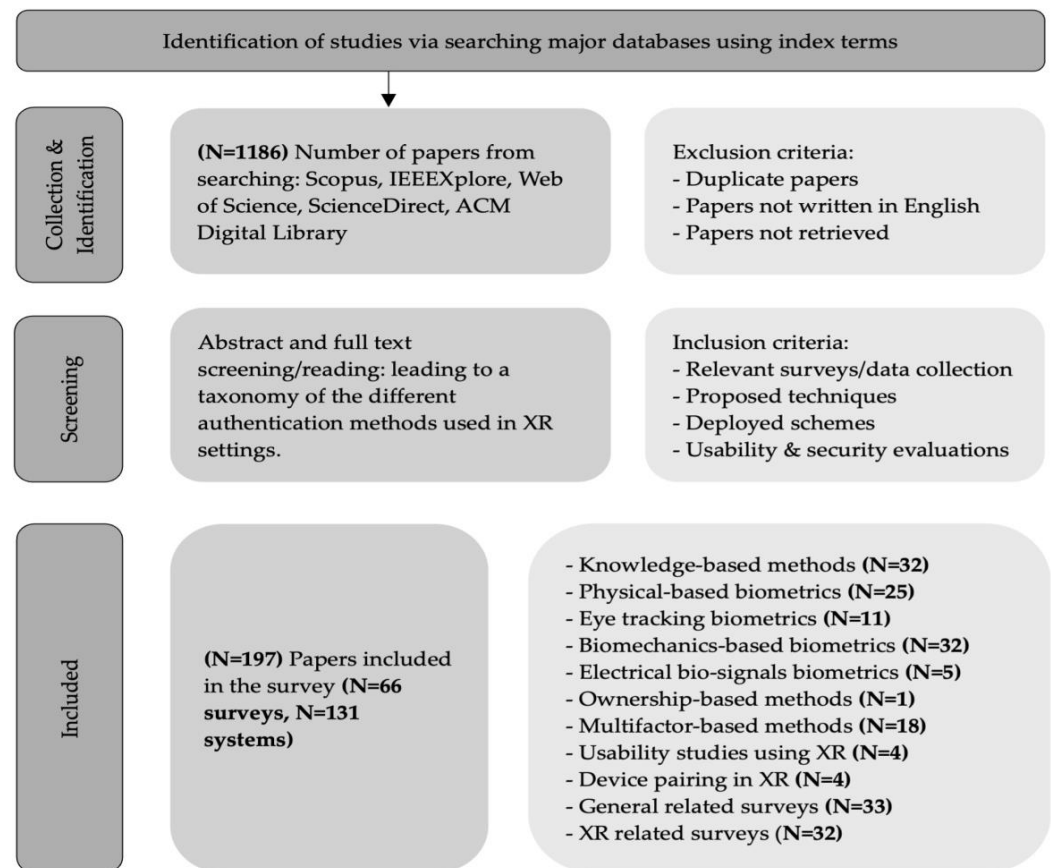


Figure 1. Methodology process.

3. Related Work

Computing systems in general and XR systems in particular require safe and accurate authentication. Several traditional authentication mechanisms, naming passwords, cards, and security keys, are subject to being lost, stolen, or hacked, resulting in security breaches. Thus, cybersecurity researchers have recently placed a significant focus on biometric authentication. Biometric attributes such as fingerprints, iris, and signatures provide an excellent choice for user authentication. Physiological and behavioral traits are the two main categories of those biometric attributes. The physiological category includes characteristics relating to physical structures like face, palm, and feet, while the behavioral category is associated with the user's behavior like keystroke, speech, and gait. Table 1 lists the latest surveys on biometric authentication methods.

Table 1. Summary of recent surveys on biometric authentication, security, and privacy methods in general.

<i>Biometric Authentication</i>				
Ref.	Year	Biometrics	Title	Contribution
[1]	2023	Various Blockchain	Combining blockchain and biometrics: A survey on technical aspects and a first legal analysis	Provides a survey of the technical literature on the integration of blockchain and biometrics including a first legal analysis.
[2]	2021	Various Blockchain	Authentication mechanisms and classification: A literature survey	Surveys and classifies various methods of authentication based on particular criteria.
[3]	2022	Various	A Comprehensive overview on biometric authentication systems using artificial intelligence techniques	Discusses the different Artificial Intelligence techniques used in biometric user authentication.
[4]	2022	Various	Biometrics: Going 3D	Provides a taxonomy of 3D biometrics since 2011, presents the related work, the hardware used, and the available datasets.
[5]	2021	Various	Attacks and defenses in user authentication systems: A survey	Reviews attacks and corresponding defense mechanisms in authentication systems.
[6]	2021	Various	User authentication schemes using machine learning methods—A review	Examines the different machine learning user authentication schemes proposed to increase the security of different devices.
[7]	2020	Various	Biometric authentication systems towards secure and privacy identification: A review	Indicates the types of biometric authentication measurements, and their applications.
[8]	2019	Various	Process of biometric authentication and its application—A review	Presents a review on many biometric authentication processes and devices.
[9]	2018	Various	A Survey on Biometric Authentication: Toward secure and Privacy-Preserving Identification	Classifies the existing biometric authentication systems by focusing on the security and privacy solutions.
[10]	2018	Various	Multi-factor authentication: A survey	Sheds the light on the evolution of multi-factor authentication and the emerging sensors used for authenticating a user.
[11]	2016	Various	Biometric authentication technologies and applications	Investigates biometric authentication technologies, their utilization, and their underlying issues.
[12]	2015	Various	Biometric: Types and its applications	Classifies biometric authentication factors and applications.
[13]	2015	Various	Surveying the development of biometric user authentication on mobile phones	Creates a taxonomy of existing biometric authentication techniques on mobile phones.
[14]	2022	Behavioural Continuous	Continuous user authentication on smartphone via behavioral biometrics: A survey	Systematizes literature and public datasets in continuous authentication using behavioral biometrics for smartphones.
[15]	2016	Behavioural Continuous	A review of continuous authentication using behavioral biometrics	Presents a literature review on the topic of Continuous Authentication using behavioral biometrics.
[16]	2021	Behavioural	Behavioral biometrics & continuous user authentication on mobile devices: A survey	Surveys on behavioral biometrics and continuous authentication technologies for mobile devices.
[17]	2017	Behavioural	A survey on behavioral biometric authentication on smartphones	Overviews the behavioral biometric traits used to develop active authentication systems for smartphones.
[18]	2022	Gait	Gait recognition based on deep learning: A survey	Summarizes gait recognition with a focus on deep learning approaches, their architectures, and available datasets.
[19]	2021	ECG	Electrocardiogram signals-based user authentication systems using soft computing techniques.	Presents a taxonomy of ECG-based authentication, its key contributions, applied algorithms, and possible drawbacks.
[20]	2021	EEG	User authentication and cryptography using brain signals—A systematic review	Examines the need for a bio-cryptographic system for user authentication and data security through brainwave signals.
[21]	2019	EEG	A Survey on brain biometrics	Provides a detailed survey of the current literature and scientific work conducted on brain biometric systems.
[22]	2020	Eye gaze	The role of eye gaze in security and privacy applications: Survey and future HCI research directions	Presents a holistic view on gaze-based security applications and discusses the opportunities and challenges of eye tracking.
[23]	2016	Eye gaze	Eye movement analysis for human authentication: A critical survey	Reviews gaze analysis methods for biometric identification when behavioral, and dynamic biometrics are warranted.
[24]	2019	Keystroke	A survey paper on keystroke dynamics authentication for current applications	Investigates keystroke dynamics authentication systems, their applications, and benchmarking datasets for current applications to improve security in online learning environment.
[25]	2022	Facial	Facial liveness detection in biometrics: A multivocal literature review	Examines the importance, advantages, and limitations of liveness facial detection using a multivocal literature review.
[26]	2020	Facial	Face recognition: Past, present, and future	Systematizes image/video/deep learning-based face recognition methods and facial biometric data classification.
[27]	2019	Iris	A comprehensive review on iris image-based biometric system	Reviews iris biometric systems and their segments, features, approaches, and techniques.
[28]	2022	Palmprint	Contactless palmprint recognition system: A survey	Overviews and evaluates contactless palmprint recognition systems, their performance, and algorithms.
[29]	2018	Palmprint	The fundamentals of unimodal palmprint authentication based on a biometric system: A review	Investigates palmprint biometric systems and technology with existing recognition approaches and datasets.
[30]	2015	Finger vein	A survey of mathematical techniques in finger vein biometric	Presents a survey of important mathematical techniques used in finger vein biometrics.
[31]	2022	Audiovisual	Multimodal authentication system based on audio-visual data: A review	Examines recent advancements in multimodal identification systems based on auditory and visual input.
[32]	2021	Graphical passwords	A taxonomy of multimedia-based graphical user authentication for green internet of things	Summarizes existing approaches of graphical password authentication to highlight Green IoT challenges.
[33]	2019	Fingerprint Password	A survey of biometric approaches of authentication	Presents fingerprint and password biometric authentication approaches.

Various: Includes several biometric methods.

With the popularity of the metaverse, various publications have reviewed studies focusing on many facets of the metaverse. An overview of recent surveys that looked at several security and privacy vulnerabilities within the metaverse as well as authentication of XR systems (AR, VR, and MR) is provided in this section. An outline of recent surveys on authentication, security, and privacy in the metaverse and XR is presented in Table 2.

From Table 2, it can be seen that not many [34–41] existing surveys discussed authentication methods in both AR and VR environments. In recent work by [34–37], authors focused on surveying miscellaneous methods of authentication. Stephenson et al. [34] systematized authentication methods in both AR and VR based on properties concluded from user experience studies and interviews [42]. In [35], Duezguen et al. focused solely on reviewing knowledge-based authentication methods in AR and VR worlds. In [36], Jones et al. gave a simple overview of VR-based authentication schemes and then highlighted trends and research gaps. In [37], Kurtunluoglu et al. compared the main authentication methods used in VR worlds in terms of security. On the other hand, [38–41] presented surveys about only biometric authentication in AR and VR. In their work, Heruatmadja et al. [38] conducted a VR-based biometric authentication review and pointed out the literature gaps. In [39], Liu et al. classified biometric authentication methods for wearable devices based on their processing techniques and classification methods. In [40], Olade et al. reviewed state-of-the-art camera-based multimodal facial biometric authentication research for mobile devices and examined its potential to be implemented on Head-mounted Displays (HMDs). In [41], Liebers et al. reviewed gaze-based authentication research in VR.

Table 2. Summary of recent surveys on authentication, security, and privacy in the Metaverse and XR.

Ref.	Year	Contribution/Title
<i>Authentication</i>		
[34]	2022	SoK: Authentication in augmented and virtual reality
[35]	2022	SoK: A Systematic Literature Review of Knowledge-Based Authentication on Augmented Reality Head-Mounted Displays
[36]	2022	A literature review on virtual reality authentication
[37]	2022	Security of Virtual Reality Authentication Methods in Metaverse: An Overview
[38]	2023	Biometric as Secure Authentication for Virtual Reality Environment: A Systematic Literature Review
[39]	2021	Recent advances in biometrics-based user authentication for wearable devices: A contemporary survey
[40]	2018	A Review of multimodal facial biometric authentication methods in mobile devices and their application in Head mounted displays
[41]	2020	Gaze-based authentication in virtual reality
<i>Security & Privacy</i>		
[43]	2023	A Survey on metaverse: fundamentals, security, and privacy
[44]	2023	Security and privacy in metaverse: A comprehensive survey
[45]	2023	Identity Threats in the Metaverse and Future Research Opportunities
[46]	2022	Visualization and cybersecurity in the metaverse: A Survey
[47]	2022	Cybersecurity in the AI-based metaverse: A Survey
[48]	2022	Metaverse security and privacy: An overview
[49]	2021	Metaverse: Security and privacy issues
[50]	2022	Vision: Usable privacy for XR in the era of the metaverse
[51]	2022	Implications of XR on privacy, security, and behaviour: Insights from experts
[52]	2019	Security and privacy approaches in mixed reality: A literature survey
[53]	2023	Security and Privacy Evaluation of Popular Augmented and Virtual Reality Technologies
[54]	2022	A systematic literature review on Virtual Reality and Augmented Reality in terms of privacy, authorization, and data-leaks
[55]	2022	Overview of vulnerabilities of decision support interfaces based on virtual and augmented reality technologies
[56]	2023	SoK, Data Privacy in Virtual Reality
[57]	2022	Security and privacy in virtual reality—A literature survey
[58]	2022	Security and privacy in virtual reality: A literature review
[59]	2022	Virtually secure: A taxonomic assessment of cybersecurity challenges in virtual reality environments
[60]	2022	Digital body, identity, and privacy in social virtual reality: A systematic review
[61]	2014	Security and privacy for augmented reality systems
<i>Technology</i>		
[62]	2022	Artificial intelligence for the metaverse: A survey
[63]	2022	The Eye in Extended Reality: A Survey on Gaze Interaction and Eye Tracking in Head-worn Extended Reality
[64]	2022	Eye tracking in virtual reality: A broad review of applications and challenges
[65]	2017	Hand posture and gesture recognition techniques for virtual reality applications: a survey

Moreover, several recent surveys focused on the different security and privacy concerns that the metaverse faces and their solutions. For example, in [43–49], the authors presented the architecture, technologies, and characteristics of the metaverse and discussed its different security challenges and their associated countermeasures. Other related works focused on only the security and privacy of sub-fields of the metaverse, like XR [50,51], MR [52], VR/AR [53–55], VR [56–60], and AR [61].

In addition, there are few surveys that concentrate on the numerous technologies embodied in the metaverse and its sub-fields. For instance, Huynh-The et al. [62] explored the role of AI, its branches, and its primary areas of application in the establishment and advancement of the metaverse. The work conducted by [63,64] focused on eye-tracking research. Plopski et al. [63] reviewed eye gaze and eye-tracking techniques and their uses in XR, while Adhanom et al. [64] investigated eye-tracking fields of application in detail. Other surveys [65] also studied hand posture and gesture recognition techniques and provided a comparative study of the different Machine Learning (ML) models used for motion classification.

Based on the summary of relevant literature provided above, it appears that current surveys do not specifically address authentication within the framework of XR. In order to bridge this gap, this study will look into authentication methods and security issues faced by immersive technologies. To date, there has not been much focus on XR security. Therefore, as the metaverse's development progresses, it is anticipated that authentication systems protecting immersive technologies against attacks will become more crucial. This paper's motivation stems from this.

4. Authentication Methods in XR

User authentication is the process of confirming a user's identity and legitimacy to use secure resources prior to giving him access. There are three types of authentication methods: naming, Knowledge-based Authentication (KBA), Biometric-based Authentication (BBA), and Object-based Authentication (OBA). Only a very few authentication methods were specifically designed for usage in XR, and traditional authentication methods have been implemented for XR applications. Figure 2 represents a taxonomy of the different authentication methods.

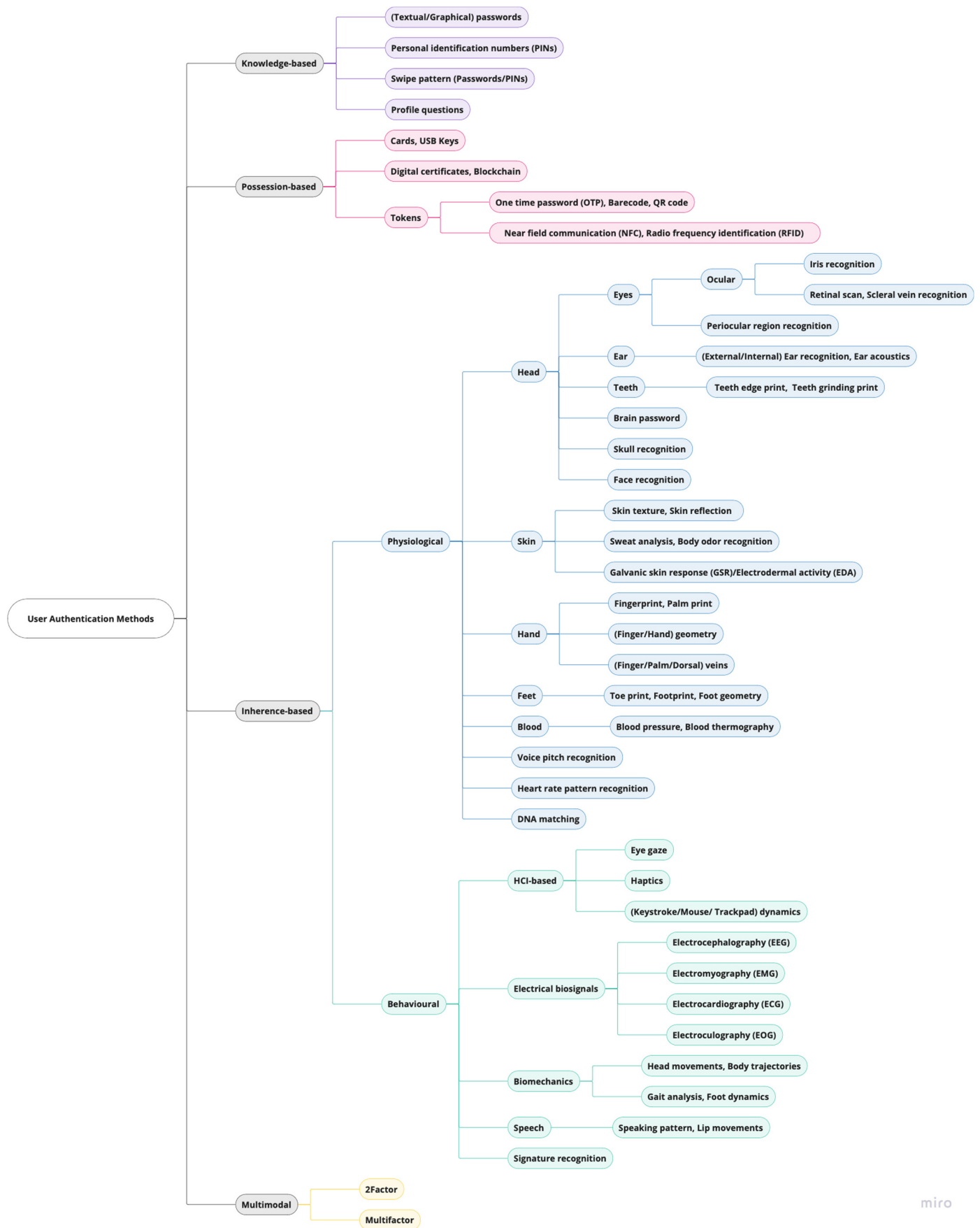


Figure 2. Taxonomy of user authentication techniques.

4.1. Knowledge-Based Authentication

Knowledge-based authentication is among the dominant types of user authentication in XR. It is based on a knowledge factor—something the user knows and recalls, such as textual passwords, graphical passwords, personal identification numbers (PIN codes), patterns, etc. Knowledge-based authentication can be classified into three categories: recall-based, cue-based, and recognition-based authentication.

Many researchers proposed knowledge-based methods for XR, adopting already existing techniques. After studying 30 knowledge-based approaches naming PINs and textual and graphical passwords, we generally conclude that seminal authentication methods in this category, such as PINS and patterns, offer secure solutions for authentication in XR. However, the main disadvantage of such methods is physical observation by attackers (shoulder surfing). In contrast, subsequent methods proposed shoulder-surfing-resistant methods that were based on the concept of immersiveness, which offers a safe space between the users and the system. This space is a hidden channel from real-world attackers, which makes it perfect for password cues that only users can observe. In addition, several proposed knowledge-based methods that implement traditional techniques retained all deployment benefits. They can be considered platform-agnostic and appealing to developers. This is crucial to developers adapting existing applications to an XR context, except for certain 3D-based passwords built differently than traditional PINs. Furthermore, techniques based on eye gaze, speech recognition, and head and hand gestures as input modalities are high-power-consuming but seem effortless and usable, which is not the case for other techniques where usability is greatly affected by the inconvenient nature of entering passwords on virtual keyboards or PIN pads. Thus, some methods are either considered visually accessible or hearing accessible because they work for one input modality but not the other. Finally, the unfamiliarity and complicated concepts of these new XR authentication techniques make them difficult to learn [34].

Several knowledge-based systems in XR systems have been explored. We categorized the password schemes into four groups: Alphanumeric, graphical, haptic pattern, and semantic. Alphanumeric passwords can include elements like digits, characters, and symbols.

In [66], Abdelrahman et al. studied the use and effect of cue-based authentication input modalities on security and usability in VR environments. They explored the impact of laserpointer, trackpad, and motion controller input modes on authentication time using a two-way ANOVA test. Their results showed that the trackpad modality outperforms the motion controller option; however, they are both slower than the laserpointer baseline modality, which matches traditional PIN-input methods, meaning that cue-based modalities improve security at the expense of usability. Their study also showed that the trackpad and motion controller methods are resilient to shoulder-surfing by design because they rely on visual cues delivered to the user through the headset, unlike the laserpointer modality, which is vulnerable to observations by bystanders. They recommended the use of cue-based modalities only when there is a high risk of observation attack due to their long authentication times; otherwise, using laserpointers would be a better option in terms of usability–security balance.

In [67,68], Mathis et al. presented RubikAuth, an authentication method for VR using a manipulable 5-faced 3D cube (the back face is omitted due to unreachability; the other faces have 1 color each and 9 digits per face, translating to 45^n password possibilities). To authenticate themselves, users wear a Head-mounted Display (HMD) and hold a Hand-held Controllers (HHC) to manipulate the 3D cube. They use eye gaze, head pose, or tapping with the right-hand controller to select n digits for their password and use the left controller for confirmation. The authors compared pointing using eye gaze, head pose, and controller tapping and assessed RubikAuth's usability, memorability, and observation resistance against threat models. The observers in their user studies used (1) written annotations, (2) a 3D copy of the cube, and (3) recordings as means to mimic the password. They found that (a) for usability, a 4-symbol RubikAuth password us-

ing controller tapping is highly faster than head pose and eye gaze; (b) a memorability study indicated that passwords are as memorable as previous work; (c) observation resistance showed that passwords are highly resilient to observations: 98.52% of attacks were unsuccessful, and gaze input outperformed head pose and controller tapping. RubikAuth is promising against shoulder-surfing attacks due to the possibility of applying fake face switches and changing the cube angle without rotating it to trick observers. Gaze-based interaction for RubikAuth scored highly among participants based on usability and security.

Most eavesdropping password entry schemes used in AR smart glasses require additional devices connected to them. In [69,70], Li et al. addressed the non-practicability of entry schemes on Smart Glasses (SG) such as the Google Glass (GG). They designed and implemented gTapper, gRotator, and gTalker, three authentication schemes based on touch pad, gyroscope, and speech recognition input modalities, respectively. For interaction, users enter a 6-digit PIN by performing gestures on the touchpad, rotating the head, and speech by reading the hidden information on the GG display. They concluded that their schemes are resilient to password leakage and are very cost-effective because they require no extra hardware beyond what is available on GG.

In [71], Khamis et al. extensively studied the use of smooth pursuits in VR. After an in-depth analysis to derive the different guidelines for pursuit selection design considering trajectory size, target size, and distance to target, they designed an Automated Teller Machine (ATM) sample application for authentication in VR and conducted usability interviews and questionnaires. Their authentication scheme considers a 4-digit PIN and eyes' smooth pursuits as an input modality, and it reached 79% accuracy. They concluded that larger trajectory sizes result in better accuracy and faster selections, but target size and distance have little to no effect on the overall performance. They highlighted their plan to investigate pursuits with other modalities and scenarios.

In [72], Zhang et al. proposed AugAuth, a gesture-based AR authentication framework resistant to shoulder surfing attacks. AugAuth users securely authenticate themselves while bystanders are present by randomly entering a PIN on the device's display coupled with finger movements' detection using a MYO armband (MYO). For registration, users wearing a MYO perform 20 taps for each finger on the display to build a finger movements' profile, then set up a PIN that they use later for authentication. They collected EMG (Electromyography) signals from 8 volunteers and used Support Vector Machine (SVM) classifier for finger movement classification. AugAuth accuracy reached 86%.

Similarly, in order to address the shoulder surfing issue in PIN-based authentication methods in AR, Seo et al. [73] introduced two PIN-entry methods for GG by exploiting the hidden overlay screen in GG to display secret values. They proposed two masked-PIN schemes that make use of voice and touch. Users choose a 4-digit PIN for enrollment, and then to authenticate, they must put the randomized PIN given by the server in order by speech or touchpad. Once the PIN is correct, they may confirm. Their voice-based method is effective when users cannot use their hands, and the touch-based method is more useful in loud environments or where users are at risk of eavesdropping from bystanders. The authors implemented and evaluated the prototypes, and their results reached a very high accuracy rate with a very short entry time.

George et al. [74] proposed the integration of well-established concepts (PIN, Android unlock patterns) into VR. Through both a pilot study and a lab study, they showed that the current real-world authentication methods are transferable into VR. Particularly, they showed that the usability of both PIN and swipe patterns in VR matched the usability in the physical world. Furthermore, they illustrated that the hidden channel offered by VR makes such authentication mechanisms harder to attack and hack.

In [75], Gheorghe et al. proposed a new input approach aiming to overcome the lack of available touch surface in modern SG by using a thermal camera embedded in the front of the SG. Users enter a 4-digit-based PIN on a touchpad that faces the virtual pad while the

thermal camera captures the residual heat from the fingertip on the touchpad. They used the Simple Blob Detector (SBD) algorithm to detect the blob pixels left by finger touch. They pointed out the technical issues of their approach, such as the SBD algorithm's effectiveness in detecting other touch gestures in non-laboratory situations.

In their original work, Yu et al. [76] implemented well-developed authentication methods such as pattern swiping and PINs within a VR environment while attempting to build a 3D password for VR. The authors conducted usability and security experiments to provide some insight into the strength of the three techniques against observation attacks. In the experiment, participants using the three authentication techniques were recorded, watched other participants' recordings, and then asked to guess the passwords. The results suggested that the 3D password system was considerably harder to guess and had a higher security level than 2D swipes and PINs, likely as a result of introducing a complex third dimension. Two-dimensional swipes and PIN systems were perceived as more usable.

With the same purpose as previously mentioned PIN-based schemes, Yadav et al. [77] addressed the shoulder surfing and eavesdropping issues of PIN-based authentication schemes in AR. They implemented two PIN-based authentication schemes for GG and compared their effectiveness with the built-in option available on GG. The schemes employ voice and touch input modalities. For registration, a 4-digit PIN is assigned to the user by the server. For the voice-based scheme, the user is shown a plain pad with random colored digits, and the user speaks the digits that match the registered PIN. GG captures the spoken digits, matches the digit with the corresponding real PIN, and grants access. For the touch-based scheme, the user is assigned a randomly assigned PIN pad that changes with each instance, and the user must navigate to the correct digit by swiping and selecting the digit by tapping. The system grants access when the PIN matches the stored one. Through a usability study with 30 subjects, they concluded that users perceived the proposed schemes as faster and more secure than the built-in schemes. They also recommended the use of different authentication schemes on the same device because users tend to use them in different contexts.

In [78], Winkler et al. presented Glass Unlock, a novel PIN-based framework that used GG to authenticate smartphones. By outsourcing the near-eye display, they introduced a randomized secret digit layout that shows on the near-eye display while the user enters the PIN on an empty layout on the smartphone screen. Through a usability study with 18 participants, their concept was tested with three input methods (10-key PIN, 6-key PIN, and swipe), and it proved robust against all visual attacks. The 6-key modality scored lowest in authentication time, and the swipe modality was favored by participants, and they recommend reducing it to 6 keys instead of 10 keys for lower input times.

In [79], Bailey et al. discussed speech-based solutions to the eavesdropping issue in AR authentication schemes. They recommended both PIN-based, textual passwords, and graphical solutions. For the PIN-based solutions, (1) users calculate the sum of the PIN digit and a random number displayed on the GG private display, then speak the result mod 10 for each digit and (2) users pronounce a letter associated with each PIN digit that is displayed on the GG private display. For the graphical-based solution, the users select grids of pictures that are assigned random labels by speaking out the label using head movements, blinks, or a touchpad.

In addition, Olade et al. [80] extensively studied the portability of popular SWIPE lock mobile device authentication systems to VR. They compared the speed and usability of the SWIPE authentication system in both mobile and VR environments through a 3-phase study: (1) a web experiment to gather and examine possible SWIPE password patterns; (2) a mobile device experiment; and (3) a VR experiment. The VR experiment entailed creating a VR replica of the mobile SWIPE authentication mechanism. The VR authentication system interaction was in terms of using an HHC, an HMD, a Leap Motion (LM) hand-tracking sensor, and an aGlass eye-tracking device (aGlass). Since shoulder-surfing is recognized

as a vulnerability on mobile devices, they also looked at how effective it was in a VR context. The study findings showed that, whereas mobile swipe authentication was the quickest and easiest to use, the HHC and LM versions were similarly quick and easy to use. According to the shoulder-surfing evaluation, attackers have a considerably lower success rate, and SWIPE in VR has a significantly high resistance to shoulder-surfing attacks. This makes this technique extremely safe to use in public settings where there may be a number of bystanders.

In [81], Düzgün et al. applied “Things”, an authentication scheme proposed by [82] to protect against shoulder surfing attacks for the Microsoft HoloLens (MH) headset. Their scheme is a gesture recognition-based graphical scheme where users select randomly displayed images on the private display of the HMD. They conducted usability studies to investigate usability and security aspects such as efficiency, satisfaction, and perceived security. They concluded that the scheme showed a high effectiveness due to easiness of memorizing graphical passwords; however, the long authentication duration needs to be improved by replacing gesture input with speech or eye gaze.

In [83], Hadjidemetriou et al. designed HoloPass, an MR gesture-based authentication prototype that requires users to mark patterns on a hologram image. Users register their passwords by drawing three patterns on the hologram image using gestures. Then, to authenticate, they must enter the same patterns by using elements on the image as a cue or reference. They designed an in-lab study to investigate the aspects of their MR prototype in terms of likeability, task execution, and guessing attacks and compared their results with the results of the desktop version to check if their prototype is platform-agnostic or not. The result of the study revealed a non-significant difference between both prototype versions in terms of password creation time and the number of password guesses needed to crack the password. The result also showed that users had a positive preference for the MR version of the prototype.

Funk et al. [84] proposed LookUnlock, a graphical authentication technique based on head-gaze tracking and spatial awareness. LookUnlock authorizes authentication on HMDs without requiring any extra devices by using spatially and virtually built passwords, namely, spatial passwords, virtual passwords, and hybrid passwords. Users select spatial targets in the environment by dragging the HMD’s cursor over an object and pressing the enter key to set a spatial password. To unlock the procedure, users insert the spatial password by focusing their head gaze over the designated spatial targets. Binding spatial passwords to the environment adds a layer of security against observers. Unlike spatial passwords, virtual passwords’ positions might be randomized because they are not aligned with any physical object. The process of setting and unlocking a password is identical to that for spatial passwords; however, virtual targets in the form of 3D models of objects are necessary. The virtual targets spawn at different locations within the 3D world each time a virtual password is entered. This adds an extra layer of security against bystanders but makes the task of finding the right virtual unlock target more challenging. Hybrid passwords permit users to merge spatial and virtual targets and only work in environments where passwords are defined because they depend on the position of previously defined spatial targets. The authors implemented a prototype and carried out a user study to evaluate LookUnlock. They demonstrated that this mechanism can be efficiently used by people and that the three password types are resistant to observation attacks. Out of 135 attempts, virtual passwords were resilient to guessing, whereas spatial passwords were the most susceptible. Compared to other graphical and textual authentication techniques, LookUnlock passwords may be prone to users’ favoritism for some targets over others.

In [85], Turkmen et al. proposed VoxAuth, a graphical authentication mechanism for VR, with the aim of minimizing observation threats. During authentication, users’ avatars wear sunglasses as an eye-gaze obscuration technique and to warn bystanders of the ongoing activity. Users pick their voxel-based pattern from a previously chosen image transformed into a 3D voxel image. The target voxels get selected using a multimodal input

method that involves eye gaze pointing and HHC selection. The authors suggested future usability studies to investigate the learnability and memorability of the voxel pattern as well as testing a unimodal eye gaze input method for both pointing and selection instead of a multimodal input method.

In [86], Han et al. designed Ninja Locker, a hand-gesture-enabled knowledge-based authentication system for VR. Ninja Locker uses the difference between the virtual environment view and the bystander perspective view to create confusion in detecting the gesture password. For registration, a user selects a hand gesture from a list of gestures as his password; the same gesture will be displayed, spawning in a different direction each time the user enters the virtual environment. To authenticate, the user uses one hand to copy the gesture displayed in the virtual view, and they use the remaining hand to make a confounding gesture. The confounding gesture adds a layer of security to the gesture password.

In [87], Bologna et al. implemented SPHinX, a pattern-based authentication scheme for XR environments that enables users to authenticate by pattern tracing on a 3D object (pyramid or cube). Each object's face is divided into grid positions (9 for cubes and 6 for pyramids), and users can choose a continuous pattern or a group of sub-patterns that get concatenated at the end in a sole pattern. Their usability study with 16 volunteers indicated that the highest security level against shoulder surfing attacks was reached when patterns were composed from the four sides of the objects. In terms of login speed and error rates, the cube design scored better than the pyramid design. They pointed out their interest in studying the robustness of their scheme against other types of attacks and in experimenting with other 3D shapes.

In order to demonstrate the potential of existing authentication mechanisms in terms of usability and security, George et al. [88] carried on their work in [86] and investigated the effect of pointing and selection choices on usability and security for 3D passwords in VR. They presented GazeRoomLock, an authentication mechanism similar to RoomLock [86] that leverages other interaction modalities instead of only using HHC. GazeRoomLock utilizes eye gaze and head pose for pointing, dwell time, and HHC tactile input for selection. Their usability study regarding entry time, error rate, and memorability revealed that the interaction modality does not have a significant effect on memorability. However, multimodal mechanisms (eye gaze or head pose with tactile input) are notably quicker and less error-prone than unimodal ones (eye gaze or head pose with dwelling). Additionally, the results of their security study in terms of robustness against both real-world and offline observations showed that multimodal mechanisms (eye gaze or head pose with tactile input) are resilient against real-world observations, while only the multimodal mechanism (eye gaze with tactile input) is robust against offline observations.

In [89], George et al. presented RoomLock, an authentication mechanism that leverages the 3D virtual space. Users authenticate by selecting 3D objects from their virtual environment. The usability studies of RoomLock indicated that it is usable and memorable, and security studies showed that RoomLock is highly secure against shoulder surfing attacks. Results also showed that despite longer authentication times in the virtual environment in comparison with the real world, users' perceptions of the workload are the same in both environments, meaning RoomLock is transferable. They indicated that with slight changes to the interaction modality, they are certain about the applicability of RoomLock to MR and AR devices, as well as its robustness against shoulder surfing attacks in those environments due to their closeness to the real world.

In [90], Gurary et al. defined both the physical and physiological advantages of 3D authentication and introduced 3Dpass, a 3D authentication scheme. Users generate a password by navigating the virtual environment and performing a set of actions and interactions with the objects present in the scene. To authenticate, they must perform the same actions and navigations with a level of tolerance toward distances and angles. In a controlled laboratory setting with 20 participants, their longitudinal usability study to test the memorability and usability of 3Dpass in comparison with a monitor version of an

alphanumeric password showed that 3Dpass scored higher in memorability and preference but lower for entry times and hotspots.

In [91], Yu et al. proposed a 3D-cube-based authentication system for virtual environments as a solution against shoulder surfing attacks. The user's hand gets detected by the LM and visually displayed in the virtual environment to facilitate interaction and navigation. Then, the user virtually touches a cube in a sequential way. Each time a cube is touched, it displays a number on it. The system registers the sequence of the cubes' numbers and generates a unique password. The authors suggested adding more interactive elements to their system's 3D environment to enhance interactivity, increase the theoretical password space, and thus increase security.

In [92], Wazir et al. developed an AR recognition-based authentication scheme for mashing up a doodle password with the AR environment. Users draw a doodle password five times to create the password, and they recreate the same password for authentication. The system then matches the recreated password with the five registered passwords according to size, coordinates, and content. Users get granted access only if the coordinates and size of the passwords match. The authors evaluated their authentication scheme, considering usability, security, and usefulness measures. The results of their evaluation demonstrated the ease and effectiveness of the scheme and that doodle-based passwords are highly secure due to the wide variety of possibilities that make them hard to crack.

Current PIN-based and password-based authentication techniques are considered unsuitable for wearable SG due to their limited input space. In [93], Islam et al. designed GlassPass, a tapping gesture-based user authentication scheme, to address that problem. They designed a set of ten symbol-based tapping gestures that get captured by a custom-made touchpad attached to the side of the Epson Moverio (EM) SG and that can differentiate between gesture types. They evaluated two versions of their scheme: a standard version that displays a black highlight on the private display and a disclosed version that displays the input symbols of the password. Their evaluations' results showed that tapping gestures boosts the accuracy and rapidity of the scheme and reported that the disclosed version helps with password memorization. They suggested further work to obfuscate observable physical inputs on GlassPass to improve resistance against observation attacks.

In [94], Hutchins et al. developed Beat-PIN, a touch-based authentication scheme for wearable devices. The scheme's rhythm-based password is a set of beats marked by their timing. Users enter the beat-PIN via taps on a touchpad several times for training and enter the same password to authenticate. They get authorized if the tapped password matches the training sample. Through experimental evaluations with 124 participants, they collected data and extracted tapping time instances, tapping intervals, and relative interval features. Then, they proposed a classification algorithm, Vector Comparison Algorithm (VCA), and compared the results with those of an SVM classifier. Their scheme achieved a 7.2% Equal Error Rate (EER) with a low input time and outperformed the SVM classifier.

In [95], Duezguen et al. proposed a shoulder-surfing-resistant authentication scheme for AR and VR devices. They based their proposed scheme on their previous work, the Zero-Trust Authentication Protocol explained in [96]. For registration, the users receive a secret assigned to them by the server through a private channel. Then, to authenticate, users answer a series of semantic challenges related to the registration phase secret without disclosing the secret by using speech, touchpad, or head movements as input modalities. The server then checks the accuracy of the answers and grants access. The authors did not evaluate the usability of their proposal.

In [97], Li et al. studied users' perceptions toward the usability and security of authentication interaction modalities in VR. They designed four authentication technology probes (PIN, virtual card, and signature) for a VR environment and embedded them in an archery VR game for evaluation. They evaluated the probes in terms of interaction experience, security and privacy perception, and meeting user expectations. Among their prominent findings, users face usability challenges such as motion control and space

awareness while performing authentication; the gamified VR context affects users' sense of security and privacy; improving interaction factors such as designing flexible and engaging interfaces.

The suggested knowledge-based methods are generally satisfactory but do not always seem to be the ideal option for XR devices. It is possible that other approaches could yield greater advantages than knowledge-based approaches. Table 3 shows an overview of the selected papers with each scheme type, technical equipment, and conducted usability and security studies.

Table 3. Summary of knowledge-based authentication mechanisms and schemes in XR.












































Concept	Ref.	Year	Scheme Name	Input Method/Equip.	Equip.	US	SS	A% (EER)
<i>Password type: Alpha-numerical password</i>								
	[66]	2022	CueVR	Lasepointer Trackpad Motion controller	HTC-V	20		
	[67] [68]	2021 2020	RubikAuth RubikAuth	Eye gaze Head pose Tapping	HTC-V	23	15	
	[69] [70]	2020 2017	gTapper gRotator gTalker	Touch pad Touch pad, gyroscope Speech recognition	GG	57		98.3 98.2
	[71]	2017	VRPursuits	Eye smooth pursuits	HTC-V PLab	26		79
	[72]	2017	AugAuth	Gesture recognition armband	MYO	8		86
	[73]	2017	MaskedVoice * MaskedTouch *	Speech recognition Touch pad	GG	10		100 100
	[74]	2017	PinVR *	Pointers Tapping VR Stylus	HTC-V	30 #	30	
	[75]	2016	ThermalTouch *	Thermal touch front camera				
	[76]	2016	PinSystem *	Touch pad Hand tracking/Leap Motion	OR-DK2	15 #	15	
	[77]	2015	VoicePIN * (VBP) TouchPIN * (TBP)	Speech recognition Touch pad	GG	30 #	30	83 87
	[78]	2015	Glass Unlock	Tapping & swiping on an empty button lock screen	GG	18		
	[79]	2014	SecretRandomPIN * HiddenRandomPIN * HiddenTextPWD *	Speech recognition	GG			
<i>Password type: Graphical password</i>								
	[80]	2020	SwipeVR *	Hand-Held-Controller Head-Mounted-Display Hand tracking/Leap Motion Eye tracking/aGlass	HTC-V	15 #	15	
	[74]	2017	PatternVR *	Pointers Tapping VR Stylus	HTC-V	30 #	30	
	[76]	2016	PatternLock *	Touch pad Hand tracking/Leap Motion	OR-DK2	15 #	15	
	[81]	2022	PictureAR *	Gesture recognition	MH	16 #	16	
	[83]	2019	HoloPass	Gesture tracking	MH	15 #	15	
	[84]	2019	LookUnlock	Head gaze tracking	MH		15	
	[79]	2014	HiddenPictureAR *	Speech recognition Gesture recognition/blinking Gesture recognition/tapping Head movements recognition	GG			
	[85]	2023	VoxAuth	Gaze pointing/Controller trigger	MQ-P			
	[86]	2023	Ninja Locker	Hand gesture recognition	MQ-2			
	[87]	2023	SPHinX	Controller's trigger button	SG	16		
	[88]	2021	GazeRoomLock	Gaze pointing & dwelling Gaze pointing & controller's trigger Head pose pointing & dwelling Head pose pointing & controller's trigger	HTC-V	48	26	
	[89]	2019	RoomLock	Laser pointing & HHC' trackpad and trigger press	HTC-V	48	75	
	[90]	2017	3DPass	Xbox 360 controller Head tracking	OR	20		
	[76]	2016	3DPassword *	Touch pad Hand tracking/Leap Motion	HTC-V	30 #	30	
	[91]	2016	3DCubePWD *	Hand tracking/Leap Motion				
	[92]	2020	DoodleAR *	Smartphone touch gesture recognition		20 #	20	

Table 3. Cont.

Concept	Ref.	Year	Scheme Name	Input Method/Equip.	Equip.	US	SS	A% (EER)
<i>Password type: Haptic pattern password</i>								
	[93]	2018	Standard Glass pass Disclosed Glass pass	Tapping on a special touch pad	EM	33	12	93–96 96
	[94]	2018	Beat-PIN	Touch pad		124	49	(7.2)
	[77]	2015	Built-In-Mechanism	Touch pad	GG	30 #	30	
<i>Password type: Semantic password</i>								
	[95]	2020	Zeta	Touch pad Speech recognition Gyroscope	GG OR			
	[97]	2023	ProbeVR *	Hand-Held-Controller Head-Mounted-Display	OQ	24 #	24	

Ref.: Reference, Equip.: Equipment, US: Usability Study sample size, SS: Security Study sample size, A%: Accuracy, EER: EqualError Rate, * Scheme name not given by the author but given depending on the method used, # The study includes a security study, GG: Google Glass, SG: Smart Glasses, HTC-V: HTC Vive, OQ: Oculus Quest, OR: Oculus Rift, OR-DK2: Oculus Rift DK2, MQ-P/2: Meta Quest Pro/2, MH: Microsoft Hololens, EM: Epson Moverio, PLab: Pupil Lab Eye

Tracker, MYO: Myo Armband.  = PIN,  = Swipe,  = Graphical,  = 3D,  = 4D,  = Doodle,  = Touch,  = Protocol,  = Token,  = Signature.

4.2. Inherence-Based (Biometric) Authentication

Inherence authentication is based on factors referring to something you ARE or something YOU DO, such as DNA or gestures (gait). Primarily, biometric data of any kind is an example of an inherence factor.

4.2.1. Physical Biometrics

Physical biometrics refers to physiological traits in the human body, such as a fingerprint or iris. Authentication using physical biometrics has been researched in miscellaneous applications long before XR took hold. For the scope of this paper, we focus only on physical biometric authentication research conducted in the XR field.

Iris is considered a gold standard biometric modality. Boutros et al. [98–102] extensively studied the possibility of using iris and periocular images captured by HMD-integrated cameras for biometric authentication while taking into consideration the low computation of such devices. Using the open-source dataset (OpenEDS, captured using HMDs) and several deep-learning recognition approaches, they concluded that iris and periocular images captured during HMD device use might be utilized for biometric authentication. In [98,102], the authors suggested a lightweight and precise segmentation solution for the ocular region images taken by HMDs and benchmarked many well-studied iris and periocular region verification approaches in terms of sample size effect on accuracy. In particular, deep learning approaches resulted in encouraging results, with a high EER of 6.35% for iris verification and 5.86% for periocular verification.

They made note of the necessity of more investigations tested in real-world use-case scenarios due to the suboptimal results achieved by both the segmentation and authentication models. To further investigate and improve their findings, Boutros et al. [99] presented a novel multi-modal fusion model that combines iris and periocular modalities using many deep learning models. The fusion model achieved the highest performance, reaching an EER of 6.47%. In [100], the authors focused on continuous iris authentication under the same settings as in their previous works while using different deep-learning recognition models. Their results show that a 5% EER performance can be achieved. In addition, and under the same settings, Boutros et al. [101] re-studied authentication employing the periocular region using different deep learning models. They observed that the variation in periocular images due to the uncontrolled way of capturing images leads to inaccurate authentication, and they proposed new sample selection and normalization methods to address the issue. However, they showed that the deep learning models used in their experiments can still learn from the randomly taken, non-ideal periocular images. Their work resulted in a 9.84% EER.

Sehee et al. [103] proposed a periocular region method as a biometric for personal authentication in HMDs. Unlike iris recognition, their method did not use high-frequency features of the image; thus, it offered fast and efficient recognition with minimal effect on image quality. It showed excellent performance, with an EER of 6.83%.

Varkarakis et al. [104,105] presented a proof-of-concept to target the segmentation of off-axis iris images taken by frontal embedded cameras in HMDs. Particularly, they used advanced data augmentation techniques on publicly available iris datasets and designed a novel Convolutional Neural Network (CNN) architecture with minimal complexity for embedded devices' deployment. The segmentation results of their method were compared with advanced segmentation models and showed great performance for both frontal and off-axis iris regions, despite the lightweight nature of the suggested model. Thus, it is a suitable choice for deployment on HMDs.

In [106,107], John et al. addressed the issue of anonymizing iris images during eye tracking in HMDs. The authors suggested a hardware-based optical defocus solution to conceal the iris biometric from the stream of eye-tracking images. Both their pilot study with 5 participants and the study with 15 participants, respectively, produced an average Correct Recognition Rate (CRR) of 0% and 7% compared to 91% and 79% before defocus was applied.

Li et al. [108] were among the first researchers who tried to solve the problem of user authentication in wearable smart glasses. They designed an innovative iris recognition mechanism and proposed an efficient and accurate iris segmentation algorithm to be used on smart glasses. The accuracy of their iris recognition system on smart glasses reached 100%.

Many researchers have investigated other physical biometrics besides the iris. Zhu et al. [109] proposed SoundLock, an innovative biometric user authentication system for VR systems based on auditory-pupillary responses. SoundLock authenticates users by using carefully crafted features extracted from variations in pupil size captured by an integrated eye tracker in response to auditory stimuli presented via the VR headset. The response is compared to the template created at the enrollment stage to verify the user's legitimacy. The solution offers an essential direction for choosing efficient auditory stimuli and establishing their appropriate durations. Through comprehensive in-field studies, the authors demonstrated that their proof-of-concept accuracy surpasses the performance of cutting-edge biometric systems with an EER as low as 1.5% and is well-liked by the study participants. Similar work based on the core idea of using pupil light reflex (PLR) for biometric authentication by Yan et al. [110] confirmed the feasibility of the PLR signal for authentication through experiments. Their authentication experiments were designed based on three different authentication light intensities. The results of their authentication system turned out promising and achieved quick and effective authentication with 99% accuracy, showing that the system can be integrated into a more secure biometric authentication system. To the best of our knowledge, this work on PLR for smart helmet device authentication is original.

Gao et al. [111] proposed EarEcho, a novel acoustic biometric authentication scheme that takes advantage of the unique characteristics of in-ear sound. They validated that user authentication on wearable devices can be achieved using acoustic features extracted from audio emitted from an integrated earbud speaker combined with the reflected echoes of those audios recorded by a microphone. Their implemented and tested proof-of-concept on 20 participants attained a 97.57% precision rate for continuous authentication. EarEcho also showed that it is stable and resilient enough to handle ambiguities related to background noise, body movements, and sound pressure levels.

Lin et al. [112,113] explored the potential practicality of neurofeedback-based biometrics for head wearables. For all we know, their work is the first to investigate using cancelable Event Related Potential (ERP) biometrics for secure user authentication. They addressed the issue of generating consistent brain reactions from complex visual stimuli and how to change those brain biometrics when the used credentials get divulged.

They demonstrated the feasibility of their solution through a pilot study with an EER of 2.503%, thus validating the feasibility of using visual stimuli to generate brainwave responses for user authentication on smart headwear devices. They additionally performed longitudinal and cancelability studies to demonstrate the success and practicality of the suggested approach.

Schneegass et al. [114] presented SkullConduct, a biometric mechanism that uses the user's skull to conduct sound waves in order to authenticate users of SG. They reported on a user study with 10 subjects showing that the frequency resulting from the user's cranium is person-specific and stable despite moving the eyewear, which makes it a robust biometric. Their method brings to light biometric user authentication for SG with bone conduction technology, and it authenticates users with an accuracy of 97.0% and an EER of 6.9% without requiring explicit user input.

Zhang et al. [115,116] introduced a facial recognition authentication solution for a remote student proctoring virtual laboratory system. In their system, a Kinect camera scans student faces and captures their facial expressions and head movements to determine questionable behaviors. If suspicious behaviors are detected, the system records and analyzes more videos for further investigation. The authors concluded that the virtual proctor system could provide high accuracy in detecting sketchy behavior and identifying and tracking users' faces. They also revealed that their future work on virtual lab proctoring would expand to not only facial recognition but also speech and gesture recognition.

Tran et al. [117] introduced a finger-vein-based recognition mechanism for VR HMDs. They argued that finger veins are hard to duplicate, which makes them a more secure physical authentication solution than other hand-based characteristics. They developed a model using CNNs and Anti-Aliasing Technique (AAT) and evaluated the model using three publicly available finger vein datasets. The results of their experiments surpassed those of well-established methods, with a high accuracy reaching 99.94% on the SDUMLA dataset (Shan-Dong University finger vein public dataset), making their model a reliable choice for authentication on VR headsets.

Bader et al. [118] addressed the issue of virtual worlds' platforms being equipped with only password-based authentication mechanisms by proposing a methodology to design a virtual world platform to implement a biometrical authentication mechanism. They used a 3D toolkit to build a complete virtual space and opted for a client-server configuration. In their proposal, the user provides their fingerprint at the client stage for enrollment and authentication purposes. Then, at the server stage, the user's identity is identified and confirmed to be genuine or not.

Chen et al. [119] explored the use of Electric Muscle Simulation (EMS) for biometric authentication due to its inter-subject variability. They engineered ElectricAuth, a mechanism that conducts users' involuntary finger movements by stimulating their forearm with electrical impulses. They showed that ElectricAuth is robust against impersonation attacks, replay attacks, and data breaches since it uses new challenges in each instance of authentication. ElectricAuth's longitudinal study results showed its stability under different humidity and muscle conditions. The authors stated that ElectricAuth would offer practical authentication for devices that use motion tracking, like VR headsets, and for users with motor impairments.

Given that the propagation of vibration signals through the human head results in unique patterns between individuals, Li et al. [120] suggested VibHead, a vibration-based authentication technique for HMDs. Extracted features from the vibration signals were used to classify registered legitimate users and also distinguish between legitimate and illegitimate users using CNN-based classification and authentication schemes. Their results from their experiments revealed a 92% accuracy for login user authentication.

Similar to the work conducted in [111,114,117,119,120] focusing on hard-to-imitate biometrics, Bianco et al. [121] investigated multimodal physiological biometric recognition by combining Heart Rate (HR), Breathing Rate (BR), Palm Electrodermal Activity (P-EDA), and Perinasal Perspiration (PER-EDA) signals. These multimodal signals acquired from

open-source datasets were stacked and used as input for a mono-dimensional CNN, and experiments on a driving simulator show an accuracy close to 99.69%. The authors suggested that an increase in the data sample size, the types of physiological signals used, and the exploitation of deeper architectures would contribute to more robust biometric recognition.

In [122], Liebers et al. introduced a novel class of biometric authentication systems called “functional biometrics” with the intention of disproving some of the drawbacks of traditional physiological and behavioral biometrics. In their proposal, they regarded the body as a robust function that transforms any stimuli applied to it into a secret reflection that cannot be stolen, lost, or leaked. Their approach overcomes both the lack of changeability seen in physiological traits and the loss or leak of the secret reflection since it can easily be regenerated. Their proposal was inspired by the work conducted in [114].

Table 4 presents a summary of the selected papers addressing physiological biometric mechanisms and schemes in XR.

Table 4. Summary of physiological biometric mechanisms and schemes in XR.

































Concept	Ref.	Year	Scheme Name	Classifier	Features	Equip.	Sample	A% (EER)
	[98]	2020	DenseNet-201-Iris	CNNs	Handcrafted and DL features	HMD	123	(6.35)
			DenseNetBC-100-Iris					(7.25)
			DCT-SHD-Iris					(31.13)
			LG-SHD-Iris					(31.78)
			CSBCA-Iris					(34.34)
			DCT-HD-Iris					(36.44)
			LG-HD-Iris					(34.80)
			DenseNet-201-Peri					(5.86)
			DenseNetBC-100-Peri					(12.33)
			BSIF-Peri					(34.77)
			LBP-Peri					(35.58)
			TreeLBP-Peri					(31.27)
	[99]	2020	HOG-Peri	CNNs	Handcrafted and DL features	HMD	123	(28.51)
			DeepIrisNet-Iris					(17.42)
			MobileNetV3-Iris					(16.18)
			MobileNetV3-Peri					(9.40)
			ResNet-Peri					(12.79)
			Fusion					(6.98)
	[100]	2020	DeepIrisNet	CNNs	Handcrafted and DL features	HMD	123	(12.48)
			DenseNet					(5.80)
			MobileNet					(13.32)
			ResNet					(7.74)
			DCT-SHD					(31.66)
			LG-SHD					(31.32)
			CSBCA					(34.58)
			DCT-HD					(34.97)
	[101]	2020	LG-HD	CNNs	Handcrafted and DL features	HMD	123	(33.47)
			VGG19					(9.18)
			VGG19-SS					(7.06)
			MobileNetV3					(10.44)
			MobileNetV3-SS					(9.84)
			BSIF					(23.80)
			BSIF-SS					(22.25)
			Tree.LBP					(27.38)
	[102]	2019	Tree.LBP-SS	CNNs	256 features 32 features	HMD	152	(24.97)
			Eye-MM					92.75
			Eye-MMS80					90.68
	[103]	2018	Peri-BIO *	L1 LBP SIFT		HMD		(6.83)
			CASIA Thousand					1000
			Bath800					800
	[104] [105]	2020	UBIRIS-v2	CNNs	Iris patterns	HMD		99.13
								800
								261
	[106]	2020	Iris-Focus *	GK LG HD	Iris patterns Glint Pupil edge	PLab MH-2	15	79 (CRR)
			Iris-Defocus *					7 (CRR)
	[107]	2019	EyeVEIL-Focus	GK LG HD	Iris patterns Glint Pupil edge	PLab HMD	5	91 (CRR)
			EyeVEIL-Defocus					0 (CRR)

Table 4. Cont.

Concept	Ref.	Year	Scheme Name	Classifier	Features	Equip.	Sample	A% (EER)
	[108]	2017	RB-HD-Collect	RB-HD GMM-HD PGM	Haar features	SG-D	62	98.54 (4.6)
			GMM-HD-Collect					98.54 (3.2)
			PGM-Collect					98.54 (1.5)
			RB-HD-MICHE					(19)
			GMM-HD-MICHE					(19)
	[109]	2023	SoundLock	k-NN SVMs LR GNB RF	60 features reduced to 20: Morphological features (dilation rates, peak & 2nd valley magnitude), Statistical features (pupil size)	HTC-V	76 ~	(0.84, 1.5)
								(3.4, 4.3)
	[110]	2020	LightLock * (PLR)	SVMs	Pupil contraction Pupil recovery Inverse magnitude Mean, variance, Standard Deviation	SM-VR	20	(4.6)
								(7.8)
	[111]	2019	EarEcho	SVMs k-NN DT NB MLP	Ear acoustics data features (output sound, echo)	BSS	20	(3.6)
								99 (3.43)
	[112] [113]	2019 2018	Brain password	SVMs	840 features	HMD EEG	177	97.57
								95.46 (2.503)
	[114]	2016	SkullConduct	1-NN	(MFCC) data features	GG	10	97 (6.9)
	[115] [116]	2016 2016	VirtualLAB * VirtualLAB *	Haar-C k-NN	Haar features (6000 features)	Kinect	108 30	91
	[117]	2022	DenseNET-FVUSM * DenseNET-SDUMLA * DenseNET-THUFV2 *	CNNs	Vein patterns data features	HTC-V	123 106 610	97.66 (2.03)
								99.94 (0.24)
	[118]	2017	3DVR-Fingerprint *		Proposal			88.19 (12.61)
	[119]	2021	ElectricAuth	CNNs VAE	Finger's inertial movements data features (acceleration, rotation)	EMS 9-IMU D435 OQ	13	99.78–99.89
	[120]	2023	VibHead	CNNs SVMs RF	IMU data features (MFCC) data features	MH-2 IMU PICO-3	20	92–100 <80 <80
	[121]	2019	MultiSignal *	1D-CNN k-NN ANN SVMs STACK	21 statistical features from HR, BR, P-EDA, & PER-EDA	DS	37	90.54–99.69 78.97–94.80 82.90–98.24 82.74–97.02 85.50–98.17
	[122]	2020	BodyReflect *		Proposal			

Ref.: Reference, **HMD:** Head-mounted Display, **Equip.:** Equipment, **Sample:** User/Usability/Security Study sample size, **A%:** Accuracy, **EER:** Equal Error Rate, * Scheme name not given by the author but given depending on the method used, ~ The study includes a usability and/or a security study, **GG:** Google Glass, **HTC-V:** HTC Vive, **OQ:** Oculus Quest, **MH-2:** Microsoft Hololens 2, **SG:** Smart Glasses, **SM-VR:** Storm Mirror Smart VR Glasses, **PICO-3:** PICO Neo3, **PLab:** Pupil Lab Eye Tracker, **D435:** Intel RealSense Depth Camera D435, **9-IMU:** 9 Inertial Measurement Units, **IMU:** Inertial Measurement Unit, **BSS:** Bose SoundSport in-ear headphone, **DS:** Driving Simulator, **Kinect:** Kinect Camera, **SG-D:** Designed Smart Glasses, **ResNet:** Residual Network, **EMS:** Electric Muscle Stimulator, **EEG:** Electroencephalogram, **VAE:** Variational Auto-Encoder, **HR:** Heart Rate, **BR:** Breathing Rate, **P-EDA:** Palm Electrodermal Activity, **PER-EDA:** Perinasal Perspiration, **MFCC:** Mel Frequency Cepstral Coefficient, **LG:** Log-Gabor Features, **DCT:** Discrete Cosine Transform Coefficients, **HD:** Hamming Distance, **SHD:** Shifted Hamming Distance, **CSBCA:** Cumulative-Sum-based Change Analysis, **LBP:** Local Binary Pattern, **BSIF:** Binarized Statistical Independent Features, **TreeLBP:** Tree Local Binary Patterns, **HOG:** Histogram of Oriented Gradients, **GK:** Gaussian Kernel, **L1:** L1 distance, **LBP:** Local Binary Pattern, **SIFT:** Scale Invariant Feature Transform, **GMM:** Gaussian Mixture Models, **PGM:** Probabilistic Graphical Model, **Haar-C:** Haar Cascade, **RB:** Rule Based Haar Features, **STACK:** Stack Algorithm.

 = Periocular,  = Iris,  = Pupil,  = Ear,  = Brain,  = Skull,  = face,  = Finger veins,  = Fingerprint,  = EMS,  = Head vibrations,  = Heart rate,  = Breathing rate,  = Palm electrodermal activity,  = Perinasal perspiration,  = Body signal.

4.2.2. Behavioral Biometrics

Eye Tracking Sensors

For decades, eye tracking technology has been available on desktop displays and smartphones. Several technologies that enable eye tracking on XR HMDs have been recently created. Hence, work on eye tracking in HMDs has increased and expanded. Many researchers have investigated the use of eye-tracking technologies for authentication purposes on HMDs. Lohr et al. [123–127] are among those who did extensive work in this area. Firstly, in [127], they implemented an eye movement VR authentication framework

using a previously proposed framework for an ocular biometric system. For optimization purposes, they used focused rendering techniques in the stimuli to collect the eye-tracking data, and only low-frequency signals were considered. Many statistical methods were used for feature extraction and matching. They pointed out many difficulties in terms of calibration issues, the required number of stimuli, and 3D eye movement data classification. They demonstrated their future intent to test their framework on a larger pool of data using complex 3D eye movement features and to compare different ML classifiers in terms of authentication results. Next, they realized their intent, elaborated on their previous work in [126], and introduced a novel 2D and 3D eye movement dataset. The dataset was collected in a VR environment with over 400 participants. They used both statistical and ML models to evaluate the suitability of the dataset for authentication. Their results were compared with results from an open-source dataset and showed worse performance. The authors argued that the poor performance might be linked to the way features were extracted and classified. They showed their interest in collecting more dataset recordings, using more features, and performing a longitudinal study in their future research. Furthermore, in [124,125], the authors proposed a lightweight and easy-to-train DenseNet-based architecture for end-to-end eye movement authentication. They trained and evaluated their model using the open-source eye movement dataset (GazeBase) collected from 322 subjects using the EyeLink 1000 eye tracker (EL1000) over a 37-month period. Data recordings from only 59 participants were used to verify and test the model across several eye-tracking tasks. The authentication results achieved a 3.66% EER. They also attempted to reach the level of spatial precision that exists in current VR HMDs such as the HTC Vive Pro (HTC-VP) by using artificial degradation techniques; however, their technique's performance dropped significantly. Thus, they left the issue for future studies on eye tracking to design proper methods for artificially degrading high-quality signals to imitate low-quality signals. Their technique was compared with other state-of-the-art techniques using different eye movement tasks for training and validation and other open-source datasets such as JuDo 1000 (which contains recordings of 150 subjects captured using similar equipment to GazeBase). To the best of our knowledge, their technique is the first to reach a level of authentication performance suitable for practical applications. Finally, in [123], the authors employed the previously proposed Deep Learning (DL) CNN architecture [124] and evaluated the performance of their model through a user study by collecting data from 5 participants using the HTC-VP VR headset. Their verification results from the user study revealed an EER of 0.2%. To achieve better outcomes, they suggested the use of larger VR datasets in future work.

Zhang et al. [128] proposed and evaluated a continuous authentication system to deal with impersonation attacks from insider threats who have physical access to HMD devices. They based the system on Sparse Representation Classification (SRC) using eye movement data. First, they developed a prototype of SG that allows them to apply both implicit and explicit stimuli to the user and collect eye movement data from the user at the same time. Their longitudinal verification study supported the stability of the system and showed that a user can be identified with an EER of 6.9 for a one-day dataset vs. an EER of 9.7% for a two-week dataset. Furthermore, their comparative study results revealed that the SRC classifier outperformed SVMs and Nearest Neighbour (k-NN) classifiers. In addition, they carried out impersonation attack experiments where the attackers learned to imitate the users' eye movements. The results of the impersonation experiments show that a successful attack can be reached after an average of 5.67 attempts, and they argue that successful attempts can be prevented by using complex scenes. Lastly, they finalized their studies by evaluating the acceptance of the implicit stimuli among 50 participants through a questionnaire survey. A minimum of 60% of participants expressed satisfaction with the used stimuli.

Asish et al. [129] presented a system that uses minimal eye-gaze-based features to authenticate users. They designed an educational power production VR environment for the purpose of data collection and gathered eye gaze data from 34 subjects without applying any stimuli. A recursive feature elimination algorithm was used to minimize

the number of needed features in order to reduce computation costs. They tested and compared many ML and deep DL, such as Random Forest (RF), k-NN, Long Short-Term Memory (LSTM), and CNNs, using different sets of features (12 and 6 feature sets); all models reached 98% accuracy. They additionally ran the same models using different data features and sessions; the overall results did not show a significant difference, meaning that using the smallest set of features (6 feature sets) would be an optimal cost-effective solution. At the end, participants in the study were surveyed about the usability of the VR tutorial.

In [130], Friström et al. investigated gaze-trajectory-based passwords as a replacement for fixation-gaze-based passwords. After enrolling, users authenticate by using the same free-form-gaze password saved during enrollment, which is then compared to the password they have previously saved, leading to a binary authentication decision. The gaze direction captured by the eye-facing cameras placed on the SG is obtained from pupil movements instead of gaze points; this represents a gaze password in the shape of a horizontal and vertical eye movement time series. They used Dynamic Time Wrapping (DTW) to match time series samples, and their authentication results reached an EER of 16. An interesting finding of the collected dataset with 19 participants was that most passwords can be partially described as well-known geometrical shapes instead of free-form passwords, but knowing the shape of the password is not sufficient information to reconstruct a password, and more details are needed, such as the end and start points of the password. Their spoofing attack evaluation resulted in a total failure to crack the password, and the user study results indicated that users believe it would be challenging for hackers to speculate on the password without seeing it at the enrollment stage.

Peng et al. [131] focused on incorporating linguistic features into eye movement-based authentication. They used an eye movement dataset collected from participants performing poem reading tasks in the Gazebase database used in [124,125]. After extracting fixation features and filtering short ones, they associated each eye movement fixation with its underlying token and added word features for each token from the open-source CELEX database. For a total of eight metrics (first-order metrics vs. linguistics metrics), they trained and tested nine known ML classifiers to obtain authentication accuracy rates. Their best results were from the AdaBoost classifier (AdaBoost) with a 76.6% F1 score accuracy for linguistics metrics and the RF classifier with a 61% F1 score.











Iskander et al. [132] suggested a VR biometric model based on eye movements and extraocular muscle activations. They developed a simple open-horizon VR scene with a cube acting as a target. During the experiment, data from one eye was collected using the Tobii eye tracker (Tobii) integrated into an HTC-V headset. The data was processed using biomechanical analysis and used to investigate three distance metrics using a k-NN algorithm for classification. The classification resulted in almost a 90% accuracy rate. They concluded that the k-NN classifier presents a feasible and non-invasive user verification solution to be integrated into VR devices. They also pointed out their interest in using DL methods and datasets collected from both eyes in their future work.

Ahuja et al. [133] described EyeSpyVR, an inexpensive software-only eye-sensing implementation. They developed a prototype using a VR Box headset and an iPhone to test four different sensing modalities. They started by detecting if a headset is worn or not using a linear-kernel SVM classifier to detect if an eye image is present in the sensing field. After image detection and segmentation, eye gaze features were extracted and computed using CNN classifiers. A well-established CNN model (MicheNet, used for periocular-based smartphone authentication and trained using two open-source databases (VISOB and MICHE)) was used as a foundation model to build custom CNN models. The custom CNN classifiers were custom trained as a binary classifier, a multiclass classifier, and both a classifier and regressor for blink detection, user verification and identification, and gaze estimation, respectively. Usability and accuracy evaluation experiments to test the different-four sensing modalities were run using 70 participants; their verification and identification results, conducted including 60 participants, show an EER of 20.9% and an 81.4% accuracy, respectively. Finally, they concluded that despite the low cost and







promising accuracy of EyeSpyVR, the verification and identification accuracy is still far from levels seen in conventional eye-sensing systems, meaning that inexpensive options come with a low-performance cost.

Table 5 sums up the schemes that uses eye tracking techniques to authenticate users.

Table 5. Summary of Eye tracking mechanisms and schemes in XR.

Concept	Ref.	Year	Scheme Name	Classifier	Features	HMD	S	A% (EER)
	[123]	2022	Eye Know You Too	DenseNet-CNN	Horizontal and vertical velocities	HTC-VP	5	(20)
	[124] [125]	2022	Eye Know You Too	DenseNet-CNN	Horizontal and vertical velocities	EL1000 HTC-VP	472	(3.66)
	[126]	2020	STAT-VREM-R1 STAT-SBA-ST RBFN-VREM-R1 RBFN-SBA-ST	CD + SWT RBF	Over 1000 features (fixations, saccades, oscillations) dimensionally reduced using PCA 12 features from each fixation and 46 features from each saccade	HTC-VP	356 208 356 208	(9.98) (2.04) (14.37) (5.12)
	[127]	2018	EyeMoveBio *	CVM + SWM	Fixation features (start time, duration, centroid), saccades features (start time, duration, amplitude, mean velocity, max velocity) 12 CEM-B features in all.	FOVE		
	[128]	2017	VisualStimuli-SRC VisualStimuli-SVMs VisualStimuli-k-NN MinimalGaze-CNN MinimalGaze-LSTM MinimalGaze-RF MinimalGaze-k-NN MinimalGaze-CNN MinimalGaze-LSTM MinimalGaze-RF MinimalGaze-k-NN	SRC SVMs k-NN CNNs LSTM RF k-NN CNNs LSTM RF k-NN	8 fixation features (pupil diameter and pairwise velocity), saccades (horizontal and vertical velocities) 12 features ((Left-eye diameter, Right-eye diameter, Left-eye openness, Right-eye openness, Left-eye wideness, Right-eye wideness) + 6 features below).	VM100	30	(6.7–9.7) (11.1–14.1) (15.8–18.8) 98.57 98.58 98.96 99.62 98.29 98.34 98.41 98.46
	[129]	2022			6 features (Left-eye gaze origin(X,Y,Z), Right-eye gaze origin(X,Y,Z))	HTC-VP	34	
	[130]	2019	SmartGlass *	DTW	Gaze direction and pupil movements timeseries.	SG PLab	25	(16)
	[131]	2022	LinguisticsEyeAuth *	k-NN Linear-SVMs RBF-SVMs GP DT RF NN AdaBoost NB	8 eye movement features, duration metrics (single fixation duration, first fixation duration, total time, gaze duration), probability features (fixation probability, probability of making exactly one fixation, probability of making two or more fixations, probability of skipping), Linguistics features (reading rate, word length, and word frequency)	EL1000	322	≈60, ≈55 ≈58, ≈75 ≈60, ≈70 ≈45, ≈50 ≈55, ≈55 61, ≈75 ≈60, ≈70 ≈55, 76.4 ≈60, ≈75
	[132]	2019	EyeBiomechanics *	ED-k-NN WED-k-NN CD-k-NN ED-k-NN WED-k-NN CD-k-NN	11 features (3 joint angles of the eye + 9 features below) 9 features (Cube ID, Cube Depth, (lateral rectus, medial rectus, superior rectus, inferior rectus, superior oblique, and inferior oblique muscle activations))	HTC-V	26	89.4 (9.79) 89.3 (9.78) 89 (9.977) 76.9 (9.79) 78 (9.78) 77.2 (9.97)
			EyeSpyVR-Identify					81.4
	[133]	2018	EyeSpyVR-Verify	CNNs	Gaze angles features	VR-BH iPhone7	60	20.9 23.6

Ref.: Reference, **HMD:** Head-mounted Display, **S:** User/Usability/Security Study sample size, **A%:** Accuracy, **EER:** Equal Error Rate, * Scheme name not given by the author but given depending on the method used, **HTC-V:** HTC Vive, **HTC-VP:** HTC Vive Pro, **SG:** Smart Glasses, **PLab:** Pupil Lab Eye Tracker, **PLab-IC:** Pupil Lab Infrared Cameras, **FOVE:** FOVE Head-mounted Display, **EL1000:** EyeLink 1000 Eye Tracker, **VR-BH:** VR Box Headset, **VM100:** Vuzix M100 Smart Glasses, **iPhone7:** iPhone7, **NN:** Neural Network, **RF:** Random Forest, **DT:** Decision Tree, **NB:** Naive Bayes, **SVMs:** Support Vector Machines, **LSTM:** Long Short-term Memory, **DTW:** Dynamic Time Wrapping, **k-NN:** Nearest Neighbour, **SNN:** Siamese Neural Network, **RBF:** Radial Basis Function, **CNNs:** Convolutional Neural Networks, **DenseNet:** CNNs feature models, **SRC:** Sparse Representation Classification, **CVM:** Cramér–Von Mises, **SWM:** Simple Weighted Mean, **SWT:** Shapiro–Wilk Test, **CD:** Cosine Distance, **ED:** Euclidean Distance,

WED: Weighted Euclidean Distance, **AdaBoost:** AdaBoost Classifier.  = Eye movement,  = Eye gaze,  = Linguistics,  = Eye muscle,  = Blinking,  = Sensing.

Biomechanics

Researchers always find it challenging to transport well-established authentication mechanisms to XR environments because of both the complexity of the XR environment and the complexity of the data collection process. The majority of biomechanical authentication research in XR focuses on the head movement trait due to the easy data collection process since most HMDs are equipped with Inertial Measurement Units (IMUs) devices. Hand and eye gaze movements come in second place for similar reasons. However, there is a lack of contribution to the gait authentication category because of data unavailability.

Mai et al. [134] suggested a head-tilt-based user authentication approach. They established their study, selected their task, and chose features from previous findings [135,136]. Both works in [135,136] concluded that head movements are among the most accurate features to distinguish users' movements during walking tasks. Mai et al. designed a within-subject study and collected data from 10 recruited participants by directing them to move freely in a VR space for 5 min. They used four ML classifiers for training; SVMs and k-NN models' accuracy results were poor due to insufficient sample size. However, RF and Decision Tree (DT) classifiers resulted in high identity authentication accuracy, reaching above 95%.

Sivasamy et al. [137] implemented VRCAuth, a novel continuous authentication scheme for VR HMDs using head movements' information. In their experimental setup, they studied two tasks for a VR driving simulator and a VR video-watching open-source datasets. The head movement information in both datasets was used to extract unique user signatures. Five binary ML classifiers were used for classification, and a comparative study was performed. The authentication accuracy results were promising and reached 99% with all ML classifiers when using the VR video-watching dataset. Similar results were achieved using the Logistic Model Tree (LMT) classifier for the VR driving simulator. They indicated their future interest in implementing a lightweight online version of their continuous authentication mechanism using a Capsule Neural Network (CapsNet) classifier.

Mustafa et al. [138] experimented with using head movement data for user authentication in VR. They built a VR application where users have to collect 25 balls from one target point to another and used it for data collection from 23 subjects. ML algorithms were used for authentication, and the Logistic regression (LR) model manifested a 7% EER outperforming the SVM model. Their approach used only head movement data without incorporating hand movement data, which represents realistic interactions. Hence, using a full range of body movement data in future works would more likely provide a closer representation of real-world interactions. They highlighted that their authentication approach is app-specific due to head movement data changes from one setting to another and pointed out their current efforts to design alternative frameworks based on DL techniques.

Most of today's authentication mechanisms lack usability and are cumbersome due to the need for 2F authentication through smartphone use. Li et al. [139] designed Headbanger, a lightweight authentication system for head-worn devices, with the aim of providing a more usable and efficient alternative to the current authentication solutions. Headbanger monitors the distinctive patterns in head movement data after exposure to an outer phonographic stimulus. The authors collected head movement data from 28 participants performing head nodding activity in response to a short audio music cue. They custom-built a distance-based classifier and evaluated the accuracy and robustness of Headbanger through a series of usability and security evaluations. The results showed that Headbanger authenticates users with a 4.43% EER and is robust against imitation attacks.

Liebers et al. [140] investigated both AR and VR user identification using user unimanual and bimanual hand-tracking data. The authors collected data from 16 volunteers interacting in AR and VR environments using eight different interaction modalities: button, slider, slate, context menu, reposition, rescale, unimanual keyboard, and bimanual keyboard. They used an RF classifier to implement their approach. Their best identification accuracy results reached 95% vs. 88% for the bi-manual keyboard AR and VR prototypes, respectively. They finally used the System Usability Scale (SUS) questionnaire and the NASA Raw Task Load Index (NASA Raw-TLX) questionnaire to assess the usability of their prototypes. From the participants' feedback, the VR prototype scored higher in terms of usability and interaction preference.

Chauhan et al. [141] implemented a touch-based continuous authentication system for smart wearables. Considering the accuracy and computational load of wearable devices, their work assesses the portability of touch-based authentication mechanisms, from smartphones to GG. They modeled the touch gestures in a novel way and extracted new touch features. The authors utilized an SVM classifier with a Gaussian Kernel-Radial Basis Function (GK-RBF) and designed a custom-built Chebyshev classifier (Chebyshev) based

on Chebyshev concentration inequality to perform classification. Their motivation to use a new Chebyshev classifier is to support prior works' findings on touch-based smartphone authentication, indicating that using a block of successive touch gestures is more effective than a single gesture. The Chebyshev showed a 99% classification accuracy, nearly comparable to SVM results. They suggested continuously adjusting and training the classifier with recent data to alleviate the effects of data drift on the classifier's accuracy.

Lu et al. [142] suggested FMHash, a user identification prototype using deep hashing of in-air handwriting. The framework generates a compressed binary hash code from in-air written ID strings that facilitates users' database indexing and searching. They first carried out a data collection experiment with 100 subjects who wrote an ID string and implemented their framework using CNN classifiers. The evaluation of the FMHash showed a precision of ≥ 99.5 , making it a robust in-air handwriting identification solution for wearable devices. They juxtaposed their framework with another deep hashing framework used for image retrieval and highlighted that their framework is better optimized. The authors pointed out their future interest in investigating the prototype's long-term performance through a longitudinal study.

Lu et al. [143] presented an eye-free interaction approach seeking to address the non-secure process of simultaneously performing authentication and task execution. They proposed a hand-motion VR authentication system without eye motion involved to shift attention from concentrating on authentication to performing other tasks. They collected data from 10 participants who were asked to draw a 3D trajectory using their dominant hand's HHC. Their work-in-progress accomplished the data collection pilot study and the feature extraction phase, and the authors pointed out their future plans to implement the SVM classifier to validate their approach.

Peng et al. [144] examined the effectiveness of voice commands and touch gestures for continuous user authentication on wearable devices, utilizing the GG case. They proposed GlassGuard, a non-invasive authentication mechanism that uses seven simple interaction modalities (touch gestures (single-tap, swipe forward, swipe backward, swipe down, two-finger swipe forward, and two-finger swipe backward) and voice commands). GlassGuard is composed of five modules (event monitor, feature extraction, classifiers, aggregator, and power control). The event monitor monitors the type of event (touch or voice) and extracts the data, then forwards the data to the feature extraction module. The classifiers module contains 7 classifiers for each interaction modality, and the classifier corresponding to the event makes an independent decision if the event features belong to the owner. The aggregator is custom-built based on Threshold Random Walking (TRW), a spam detection algorithm, and it combines the classifier results to improve authentication accuracy. The power control module communicates between the aggregator and the event monitor, and in the event of a negative classification decision by the aggregator, it pauses feature extraction and classification until the security risk is low. Data collection during the evaluation involved 32 college students, and their mechanism accuracy reached 99% using SVM classifiers. The authors also compared their accuracy results with the work in [141] and concluded that their mechanism achieved better performance. They mentioned their future plan to deploy GlassGuard on GG and evaluate long-term performance using other daily tasks.

Wang et al. [145] developed Nod to Auth, a nodding-based authentication technique, to address the issue of current cumbersome AR and VR input modalities. In a study with 10 participants using GC, the authors extracted bio-features using the embedded IMU device in a Huawei smartphone. Using an RF classifier, their authentication accuracy indicated an average accuracy of 97.01%, supporting the robustness of the model. They showed their interest in (1) deploying Nod to Auth for long-term evaluations, (2) considering the neck's elasticity features, and (3) using cameras for multi-model sensing in their future work.

Miller et al. [146,147] focused on user identifiability through motion data in VR. In [146], they specifically investigated privacy risks in social VR and the effect of duration and delay on identifiability by using a social interactions dataset of 232 subjects, ML methods, and a comparative study with different methods that resulted in high accuracy

rates. They concluded that both the number and durability of recorded interaction sessions increase identifiability. However, lengthy delays between training and testing sessions decrease identifiability. In their subsequent work [147], they aimed at testing users' identifiability under typical VR conditions, unlike previous work where body motion was tested under custom-designed circumstances. Their system reached a 95% accuracy rate when trained and tested with a pool of 511 participants. They concluded that the limitation of their work is the loss of features due to dimensionality reduction and their non-generality to more complicated tasks. Thus, they recommended including other previously successfully used features like velocity, rotation, and acceleration to improve their work.

Bhalla et al. [148] proposed, investigated, and evaluated the potential of head movement-based continuous authentication in AR. Data collection involved only 5 participants to collect holographic head gaze data of AR users interacting with their environment, and ML algorithms were used to extract unique signatures from these AR users. They used ML models that are time series-based or feature-based and experimented with many feature extraction techniques. They evaluated their prototype, and the best accuracy results were achieved with the RF classifiers, with 92.675% accuracy and an 11% EER. They highlighted their interest in deploying their prototype and considering other holographic spatial interaction tasks.

Based on work conducted by Miller [147], Nair et al. [149] demonstrated the extent to which head and hand motion data can uniquely identify a large number of users in VR. First, they used telemetry data from BeatLeader, an open-source dataset of over 50,000 users, for both motion and context feature extraction. Using a hybrid featurization technique that combines both motion and context features, several ML and DL classifiers were tested for pre-identification, and the best classifier was selected. The Light Gradient Boosting Machine (LightGBM) classifier outperformed other classifiers and reached 100% accuracy with a full hybrid featurization approach on 500 users. Due to the infeasibility of training LightGBM for very large datasets such as BeatLeader, the authors constructed a multi-layer hierarchal classifier for the purposes of training facilitation, scalability, and practicality. The hierarchal architecture boosted the identification accuracy to 94.3% from 90.1% with only one layer. They additionally performed analysis about the impact of the metadata, such as country and type of device used when playing the game, etc. present in the BeatLeader dataset on the accuracy results. Also, an effect analysis of the telemetry data (static, motion, and context) on the system's entropy was performed. They finally expressed their future hope to use DL models to address similar issues.

Many researchers investigated VR user authentication using full HMD data (headsets and controllers). Various works used ball throwing as their experimental task, where an imposter tries to mimic a genuine user. Initially, Kupin et al. [150] argued the uniqueness of biomechanical movement from one user to another and used the 3D trajectories of the dominant hand controller for user authentication in VR. In their study, users threw a ball at a target, and their hand trajectories data was compared to the dataset of other users. Using the Symmetric Nearest Neighbor (S-NN) algorithm, their system was proven efficient, as its accuracy reached 92.86%. They pointed out their intention to include head trajectory data and to create more tasks in their future works, such as physically swinging a golf club or cognitively solving a puzzle. Using a similar case study and task as Kupin et al. [150], Ajit et al. [151] improved their authentication results by using pairwise relationships between 3D trajectories data from not only the dominant hand but also the recessive one and the head. They also used a 33-participant dataset, exceeding similar previous biometric works. Their mechanism was based on Perceptron Neural Networks (PNN) and reached 93.03% accuracy. They believed similar results could be achieved using other VR headsets, such as Oculus Rift (OR) and Samsung Gear VR (SGVR). Additionally, Miller et al. [152] provided a real-time version of the [151] case study, and the difference lies in distinguishing between imposters within and outside the training set using a threshold-based method. The new number of trajectories used to train and test the model was $N = 330$ pairs. Moreover, Miller et al. [153] made several contributions to prior work.

They noted that VR users do not always use the same type of HMD and that changing the headset comes with high time consumption in terms of training to perform authentication. They were the pioneers of task-driven biometrics using different VR headsets (Oculus Quest (OQ), HTC Vive (HTC-V), and HTC Vive Cosmos (HTC-VC)) and the first to perform cross-system authentication. They collected a multi-system dataset using the previously mentioned headsets with 46 users, a number higher than prior studies by [150–152] (14 and 33 users, respectively). They also introduced linear and angular velocity features to prior work [150–152] and analyzed a significantly higher number of features compared to [151]. They restated the findings in [151] about the feasibility and impact of feature diversification on user authentication. Using the same study settings and dataset used in [153], and in order to improve their earlier work, Miller et al. [154] suggested using a Siamese Neural Network (SNN) to perform across-systems authentication. For the purpose of avoiding user enrollment each time a user changes the VR device, they used an SNN to learn the distance metric between the headset/controller trajectories of the VR enrollment device and the trajectories of the new VR device. Their system performs identification by providing the user with a minimal distance and authentication by comparing the distance to a threshold. Their authentication findings indicate a 1.39% EER when OQ is used for enrollment and HTC-V for new use, with an average range of 1.38–3.86%. The identification accuracy results reached 98.53%. As per DL training requirements, Miller et al. [146,155] addressed the issue of using small datasets to perform authentication and identification using DL models. Normalization, spatial, and smoothing techniques were used to preprocess input data. Similar study settings as [154,156] and DL algorithm architecture were used in their first model to perform matching, while an N-class Fully Convolutional Networks (FCN) architecture similar to the work in [157,158] was used in their second model to perform classification. Both models take position, orientation, and displacement vector features from input and enrollment trajectories and return a match distance between both trajectories. The lowest distance represents an identification match, and a positive match between the trajectories distance and a threshold represents successful authentication. They compared their method to different baseline methods, and their results reached a 2.08% improvement. Their identification results showed success for 36 users out of 42. They showed their interest in creating and investigating VR applications that represent daily activities such as office visits, doctor visits, etc. In addition, Miller et al. [159] performed a temporal effect study on behavioral authentication. They used the same model used in [154] and data from [152–154] to study the relationship between enrollment and input trajectories over short, medium, and long timescales. Their results suggested that both short and medium timescales have an insignificant impact on VR behavior for day-to-day tasks. However, data collected during a period of 8 to 17 months showed that long timescales result in varying user behaviors. Their best results' performance in the long timescales category was achieved by using long timescales data to train the model since it contains both the baseline behavior and the changed behavioral data.

To amend the issue of data security in XR systems, Shen et al. [135] proposed Gaitlock, an AR gait authentication mechanism based on users' gait signatures. The study was founded on the tasks of short indoor walks and arbitrary outdoor walks while wearing GG. The gait data was collected from 20 subjects using the IMU device embedded in the HMD, and the noisy head movements data was filtered. The authors custom-built a model using DTW and Sparse Representation Classification (SRC) techniques for authentication and compared their evaluation results with the best alternative techniques. A total of 98% accuracy was achieved, and it outperformed its rivals. They additionally evaluated the performance of Gaitlock on zero-effort and mimicry attacks; the prototype scored 0.021 vs. 0.029 for zero-effort and mimicry attacks, respectively. Thus, we conclude that mimicking the user's gait pattern increases the risk of the attacker being authenticated. Despite evaluating Gait Lock using only GG, they noted the possibility of transporting it to a VR environment. They highlighted their future interest in considering multimodal gait tasks, such as running, since they are ruled by more complicated constraints.

Liu et al. [160] looked into body interaction usability in VR. They established their work on the importance of skeleton-tracking technology in motion recognition and proposed a hybrid approach using skeleton-tracking techniques and depth cameras as a new interaction modality in VR to replace HHC. They pointed out their future plans to incorporate speech recognition techniques into their future work. Implementing novel interaction methods lays the foundation for practical authentication solutions.

Wierzbowski et al. [161] explored user identification in VR using gaze and head movement dynamics instead of body size, proportions, and position of users. In an experiment with 43 volunteers watching a 360° video, the authors collected gaze and head movement datasets. A statistical-based classifier and a DL-based classifier were used to test the performance of their approach. Accuracy results revealed 74.4% with the Gaussian Mixture Models (GMM) classifier and 80.1% with a CNN classifier. They pointed out that they excluded the contribution of physical characteristics for the purpose of avoiding classification confusion between users with similar physical measurements within the class sample. They also highlighted that, for the purposes of ecological validity and identification robustness, using multi-session videos recorded days apart instead of one video session would have been more suitable.

Based on the uniqueness of eye gaze movements as a biometric trait, Liebers et al. [156] proposed a user identification system by using fixations, smooth pursuit, saccadic movement, and head orientation as dependent reactions to visual stimuli. Following the VR design presented in [127], the authors built a VR stimulus scene represented by a counter-clockwise moving sphere on an elliptical path and collected eye gaze and head rotation data from a small pool of 11 individuals using an HTC-V HMD modified with additional infrared cameras. They used a 1-NN ML model and eight mainly CNN-based DL models to classify the users. The highest identification accuracy results in both classifier categories reached 75% vs. 100% for the ML and DL models, respectively.

In [162], Rogers et al. introduced an approach for user identification from among a set of HMD users using blinking and head movement data. They used a series of images as stimuli to collect data from 20 subjects, utilizing infrared, accelerometer, and gyroscope sensors integrated into the HMD. They extracted 162 features; blinking features were classified into five classes (IR peaks, rising IR, falling IR, IR peak interval, and IR floor); head-movement features were classified into three categories (Gyroscope peaks, accelerometer peaks, and movement time); then the features were reduced to 96 features. These features were used to examine many ML classifiers, and an RF classifier with 100 trees was selected and achieved 94% user identification accuracy.

Work by Pfeuffer et al. [136] looked into the application of behavioral biometrics and body motion to user identification in VR. They implemented their study based on tasks such as typing, walking, grabbing, and pointing by utilizing head and hands data collected using an HTC-V HMD equipped with a Pupil Lab Eye Tracker (PLab). They used RF and SVM classifiers and high-level features like max, min, mean, and standard deviation derived from low-level features, namely distance, motion, rotation, and motion. Their most accurate results achieved only 44.44% within the task of typing and the feature set of distance. The head motion feature set scored second best among feature sets overall, while the head movement feature set was more suitable for the task of walking. For the hand movement feature set, the pointing task scored better than the grabbing task. Their low score results warrant the need for further research and investigation.

Olade et al. [163] presented BioMove, a VR user identification study of 15 participants performing controlled tasks such as grabbing, rotating, and dropping tasks. They particularly extracted eye gaze, head, and hand positional (elevating, strafing, surging) and rotational (rolling, pitching, yawing) movement data patterns and dimensionally reduced the features for efficiency purposes. Using ML classification techniques, mainly k-NN, both user identification and authentication were investigated. Two identification models were implemented, one for task identification and another for participant identification. They concluded that the k-NN model had the best user identification accuracy of 98.6% out of

all classifiers. The authentication results showed a 0.0032% false positive rate and a 1.3% false negative rate, making the system biased toward rejecting valid users instead of giving invalid users access to the system. The authors argued that the authentication results can be improved, although it is out of the scope of their research. They further investigated BioMove's vulnerabilities through a security evaluation against malicious attacks using the Whitebox Penetration Testing (WPT) framework. The impersonation results indicated a 50% accuracy value, insufficient for positive user identification outcomes. They also highlighted that attackers with similar heights and genders to valid users score higher than other impersonators. They expressed interest in evaluating the robustness of BioMove across multiple subject groups while considering the effect of age on users' kinesiological movements.

Following the approach used in [154], Schell et al. [164] proposed an embedding-based approach for user identification in XR using motion data. Their approach overcomes the limited applicability of previously proposed distance-based approaches [135,139,150] and the costly deployability of classification-based approaches [158,159]. They studied the use of Deep Metric Learning (DML) models known to produce continuous vector representations called embeddings. The DML models used are not limited to the user motion data they were trained on but can also generate unique embeddings from the motion data newly fed to the model. Their models learn to represent known users as close to their motion data, while they compare new users with existent motion data and retrieve the best similarities. The authors used the public database "Who is Alyx?"—a motion data dataset collected from 63 users while playing a VR game on an HTC-VP. They selected a Gated Recurrent Units (GRU) architecture for the DML model and trained it to embed the motion data. Evaluations of their model and comparisons with classification-based models were performed. The embedding-based approach performed better in situations where there was less enrollment data, while the classification-based model outperformed the embedding-based method in situations where there existed at least 20 min of enrollment data. Given that many use cases of prior works mainly allow for only a few seconds or minutes to enroll, the embedding-based approach became a compelling substitute.

Moore et al. [165] looked into the limitations of user identification work conducted by [147], such as stationary data collected over a single period of time, by exploring some of the improvements identified in the approach proposed in [136], which considers feature data generated over time and identification obtained by aggregated data from several sessions. To address that, they built their case study using a training task for operating room assists in a VR environment, where assists are involved in a series of motion tasks over a multiple-day span. The task is uncontrolled, as opposed to work in [147], resulting in non-stationary motion datasets. The data consists of a training session dataset and a retention session dataset. Using k-NN, RF, and Gradient Boosting Machine (GBM) classifiers, the authors investigated identification in two settings (within and between) sessions using positional features of the motion data. The highest user identification results for the within-setting showed a 95.50% accuracy rate with the RF classifier, while the between-settings results showed a 42.33% accuracy rate with the same classifier. They attributed the decline in results to the different circumstances of data collection between the training and retention sessions, such as psychological changes and a change in the VR device position. Moreover, they attempted a user anonymization study by interpolating the positional motion data used in the previous study with velocity data. Their velocity-based obfuscation study results showed worse accuracy than the prior study, with 35.17% vs. 13.83% for within and between settings, respectively. They assumed that the decrease in identification accuracy results was caused by the classifiers not being able to embed anatomical data such as user height and arm length. They highlighted that between-session identification is more difficult to implement than within-session identification and their future intentions to conduct similar research using different classifiers considering different data parameters. They recommended analyzing their approach in the context of authentication.

Liebers et al. [157] conducted a lab study to investigate body normalization effects on task-driven biometric user identification in VR environments. Using archery and bowling as

their chosen VR tasks, they compared different scenarios where body height normalization and arm length normalization were applied vs. no normalization. They achieved 90% user identification results with height normalization using DL algorithms. They pointed out the non-necessity of including physical features while performing behavioral user identification, despite their overall importance. They also argued that physical features enlarge the noise window when using DL models; thus, it is feasible to exclude them for a better accuracy outcome. The drawback of their normalization technique is the need for a pre-enrollment phase to measure body and arm sizes, and this phase might affect usability and be cumbersome for the users. Additionally, the authors conducted a NASA Raw TLX questionnaire and semi-structured interviews about the model's usability; most participants did not notice the change in body measurements and expressed no opposition to the idea of normalization.

Table 6 below systematically summarizes biomechanical-based schemes based on the corresponding papers.

Table 6. Summary of biomechanical mechanisms and schemes in XR.











Concept	Ref.	Year	Scheme Name	Classifier	Activity/Task, Features	Equip.	S	A% (EER)
	[134]	2023	Head-Tilt *	RF DT	Freely move in VR space, Head Tilt Head angular velocity, head rotation angle, headset position, head motion distance, virtual point speed	HTC-V	10	94.633 98.023
	[137]	2020	VRCAuth	NB PART LF MLP LMT	1. VR driving simulator 2. VR spherical video streaming Head movement direction, head movement magnitude, movement duration (90 features reduced to 3 categories)	HMD	40/48	78 99 99 99 80 99 92 99 99 99
	[138]	2018	HeadVR *	LR SVMs	Freely interacting with a moving ball in a VR game Head movements (178 features dimensionally reduced to 70)	GC	23	(7.39) (10)
	[139]	2016	Headbanger	(DTW) (Built)	Nodding after an audio stimulus (music cue) Head movement patterns	GG	95 ~	(4.43) 95.57
	[140]	2022	FingerAR-VR *-button FingerAR-VR *-slider FingerAR-VR *-slate FingerAR-VR *-menu FingerAR-VR *-reposit FingerAR-VR *-rescale FingerAR-VR *-uni-key FingerAR-VR *-bi-key	RF	Hand interaction with 8 interfaces: Button, slider, slate, context menu, reposition, rescale, unimanual keyboard, bimanual keyboard Rotational and positional coordinates for all fingers, palm, and wrists 12 feature sets	MQ MH	16	63, 64 53, 57 72, 51 51, 69 55, 64 61, 66 73, 64 95, 88
	[150]	2019	ThrowTraject *	S-NN (matching)	Ball throwing VR game Dominant hand trajectories	HTC-V	14	92.86
	[141]	2016	GlassTouch *	Chebyshev SVMs	Tap or swipe gesture on touch pad 13 Tap features (point (x,y) coordinates, downward force, duration) and swipe features (start point (x,y) coordinates, end point (x,y) coordinates, angle, downward force, planar force, duration, and length)	GG	30	99
	[142]	2019	FMHash	CNNs	In air handwriting of an ID string 3D velocity, 3D acceleration, position, hand pose, and amplitude	LM	100	≥99.5
	[143]	2020	HandMotion *	SVMs	Draw a define trajectory as a password 2 features (trajectory, distance)	HHC	10	
	[144]	2017	GlassGuard-Tap GlassGuard-Swipe-F GlassGuard-Swipe-B GlassGuard-Swipe-D GlassGuard-2F-Swipe-F GlassGuard-2F-Swipe-B GlassGuard-Voice GlassGuard-All-Touch GlassGuard-Touch-Voice	SVMs TRW	1. Swipe to view the application list one by one, 2. Swipe to view the options in the settings menu one by one 3. Take pictures with touch gestures 4. Take pictures with voice commands 5. Google search with voice commands 6. Delete pictures one by one 7. Use an app to asks the user to perform a series of randomly selected touch gestures Duration, distance, speed, pressure, min, max, median, and standard deviation 99 features for one-finger touch gestures, 156 features for two-finger touch gestures (81 sensor data, 75 touch data) 19 voice features for user voice commands.	GG	32	≈93 (≈16) ≈94 (≈15) ≈93 (≈15) ≈95.5 (≈12) ≈96.5 (≈8) ≈97 (≈10) ≈99.8 (4.88) 98.7 99.2 Average EER: 16.43 (11 Features), 16.56 (9 Features)

Table 6. Cont.






































Concept	Ref.	Year	Scheme Name	Classifier	Activity/Task, Features	Equip.	S	A% (EER)	
	[145]	2021	Nod to Auth-Nodding	RF	1. Nodding, 2. Turning, 3. Tilting. Head-Neck radius, angular velocity magnitude, irrelevant orientation changes, properties of trajectory projections, power spectral density of linear acceleration magnitude (Mean, pitch, roll, yaw, skewness, kurtosis, and Std.Dev)	GC IMU H-WEI	10	98	
			Nod to Auth-Turning					98	
			Nod to Auth-Tilting					>98	
	[146]	2023	BodyVR *-within	RF	Virtual group discussions in VR while walking, creating 3D drawings and writing Body-space coordinates and speed, 840 features	OQ-2	232	98.43	
			BodyVR *-between					85.48	
	[147]	2020	MotionVR *	RF k-NN GBM	1. A 360-degree video observation task 2. A questionnaire-answering task Statistic (maximum, minimum, median, mean, and standard deviation), body part (head, left hand, right hand), and dimension (x, y, z, yaw, pitch, and roll)	HTC-V	511	90.7	91.1
								85.6	92.7
	[148]	2021	MoveAR-TimeSeries-RF	RF k-NN SVMs BOSS AdaBoost	Perform a “spatial interaction task” typing the word: “Apple” using a holographic keyboard. Roll, yaw, and pitch Head gaze distance and position Max, mean, and Std.Dev	MH	5	78.293	
			MoveAR-TimeSeries-k-NN					74.326	
			MoveAR-TimeSeries-SVMs					76.776	
			MoveAR-TimeSeries-BOSS					83.526, 9.2	
			MoveAR-Features-Ada-RF					92.675 (11)	
			MoveAR-Features-Others					88–93 (11–12)	
			MoveAR-Features-PCA					90–93 (11–12)	
	[149]	2023	Single-L-GBM	LightGBM	Beat Saber game where players slice musical beats blocks with a pair of sabers 22 context features ((position, orientation, type, and color of the block), (the angle, speed, location, and accuracy of the cut), and (the relative error of the cut in both space and time)), 105 motion features (min, max, mean, median, and Std.Dev)	HMD HHC	55,541	100	
			Hierarchical-L-GBM					94.3	
	[159]	2022	TrajectVR *-short	SNN	Ball throwing Position and orientation of time trajectories from headset and controllers	OQ HTC-V HTC-VC	74	80.62–100 (0.05–3.86)	
			TrajectVR *-medium					91.25–100 (0.14–1.85)	
			TrajectVR *-long					31.25–100 (0.06–29.25)	
	[155]	2022	TrajectVR *-within	SNN FCNs	Ball throwing Normalized position and orientation, displacement vectors 128 features	OQ HTC-V HTC-VC	41	98.05 (1.75) 97.56 (1.3)	
			TrajectVR *-across					87.81 (3.38) 82.02 (9.68)	
	[154]	2021	TrajectVR *	SNN	Ball throwing Positions, orientations, linear & angular velocities, and trigger grab or release for headset and controllers	OQ HTC-V HTC-VC	46	87.82–98.53 (1.38–3.86)	
	[153]	2020	TrajectVR *-within	SSD PNN	Ball throwing Positions, orientations, linear & angular velocities, and trigger grab or release for headset and controllers, 5 features, 8192 (2 ¹³) subsets of 13 feature matches	OQ HTC-V HTC-VC	46	58–85	
			TrajectVR *-across					91–97	
	[152]	2019	ThrowVR *	PNN	Ball throwing Position and orientation of headset and controllers	HTC-V	33		
	[151]	2019	ThrowVR *	PNN	Ball throwing Position and orientation of headset and controllers, 21 feature sets	HTC-V	33	93.03	
	[135]	2019	GaitLock-DTW-SRC	DTW-SRC	Indoor controlled walking and outdoor uncontrolled walking Unique gait patterns from walking inertial signals	GG	20	>98	
			SRC-SF	SRC-SF				≈95	
			SRC-MV	SRC-MV				≈93	
			SRC-ZP	SRC-ZP				≈93	
			DTW-k-NN	DTW-NN				≈85	
			TDE-TM	TDE-TM				≈93	
	[160]	2018	SkeletonVR *	SVMs	HOG features, joint angle features	HTC-V Kinect		≈77	

Table 6. Cont.

Concept	Ref.	Year	Scheme Name	Classifier	Activity/Task, Features	Equip.	S	A% (EER)	
	[161]	2022	Identify-360 *	GMM CNNs	Freely watch a 360° videos displayed in VR 8 Time series features (gaze angular (velocity, acceleration & path curvature), duration (fixation & non-fixation), intervals (fixation & non-fixation)). 32 Statistical features (min, max, mean, median, Std.Dev, kurtosis, skewness, 9 ten-step percentiles and 16-bin histogram)	HTC-VP	43	74.4 80.1	
		[156]	2021	1-NN	1-NN	A sphere moving counterclockwise on 1. elliptical path 1, 2. elliptical path 2 Six features (onset time, amplitude, duration, peak velocity, median velocity, and average velocity) for each user gaze type (fixations, smooth pursuits, and saccades). Head rotational coordinates (x, y, and z) from HMD. All aggregated to 21 features.	HTC-VP PLab-IC	11	45
Time-CNN				T-CNN	≈94				≈88
Encoder				CNN	≈97				100
FCN				FCN	≈88				≈97
Inception				Inception	≈94				100
MCDCNN				MCDCNN	≈94				≈97
MLP				MLP	≈91				≈82
ResNet				ResNet	≈94				100
TWIESN	TWIESN	≈94	100						
	[162]	2015	BlinkHeadAR *	RF	View a sequence of rapidly changing images of numbers and letters on the HMD display 70 blink features + 90 head-movement features = 162 features reduced to 95 features overall.	GG	20	94	
		[136]	2019	PointingVR *	Controlled VR tasks (pointing, grabbing, walking, typing) Position, movement, and spatial relations between body segments (head, hands), eye gaze, ray, and target. Distance, rotation, motion, velocity, and angular velocity (6 feature categories)	HTC-V	22	41.39	
GrabbingVR *				31.25					
WalkingVR *				43.42					
TypingVR *				44.44					
	[163]	2020	BioMove	k-NN	Interacting with Balls in VR environment Interacting with Cubes in VR environment. Static metrics (arm length, body, and waist height). HMD and HHC positional and rotational coordinates, acceleration, and velocity. Eye tracking gaze positional data	HTC-V	15	98.6 (1.4)	
		[164]	2023	XR-Embedding *	GRU DML	Playing the VR game “Half-Life: Alyx” Positional (x,y,z) and orientational (quaternion: x,y,z,w) coordinates from the HMD and both HHC (21 features)	HTC-VP	63	99 98
XR-Classification *									
	[165]	2021	PositionF-within-k-NN	k-NN RF GBM	Using an ecologically valid VR app to train first assists how to troubleshoot a surgical robot in a robotic operating room Positional data (6-DOF (x, y, z, roll, pitch, yaw)) from HMD and HHC was interpolated to a velocity Combined as (min, max, mean, median, and standard deviation) vector	HTC-V	61	89.42	
			PositionF-within-RF					95.50	
			PositionF-within-GBM					95	
			PositionF-between-k-NN					28	
			PositionF-between-RF					42.33	
			PositionF-between-GBM					41.5	
			Velocity-Features-k-NN					31.17	
			Velocity-Features-RF					32.67	
Velocity-Features-GBM	25.67								
	[157]	2021	BodyNorm *	LSTM (RNNs) MLP	1. Archery, 2. Bowling 3D position, 3D rotation, and vectors 4 feature sets	OQ	16	90 78	68 63

Ref.: Reference, **Equip.:** Equipment, **Sample:** User/Usability/Security Study sample size, **A%:** Accuracy, **EER:** Equal Error Rate, **HMD:** Head-mounted Display, **HHC:** Handheld Controller, * Scheme name not given by the author but given depending on the method used, ~ The study includes a usability and/or a security study, **GG:** Google Glass, **GC:** Google Cardboard, **HTC-V:** HTC Vive, **HTC-VC:** HTC Vive Cosmos, **HTC-VP:** HTC Vive Pro, **MQ-2:** Meta Quest 2, **MQ:** Meta Quest, **OQ:** Oculus Quest, **OQ-2:** Oculus Quest 2, **MH:** Microsoft HoloLens, **PLab-IC:** Pupil Lab Infrared Cameras, **IMU:** Inertial Measurement Unit, **LM:** Leap Motion, **H-WEI:** Huawei CAZ-TL10, **Kinect:** Kinect Camera, **NN:** Neural Network, **RF:** Random Forest, **DT:** Decision Tree, **NB:** Naïve Bayes, **LF:** Logistic Functions, **PNN:** Perceptron Neural Networks, **MLP:** Multi-Layer Perceptron, **LR:** Logistic Regression, **SVMs:** Support Vector Machines, **RNNs:** Recurrent Neural Networks, **LSTM:** Long Short-term Memory, **DTW:** Dynamic Time Wrapping, **k-NN:** Nearest Neighbour, **SNN:** Siamese Neural Network, **S-NN:** Symmetric Nearest Neighbor, **CNNs:** Convolutional Neural Networks, **ResNet:** Residual Network, **FCNs:** Fully Convolutional Networks, **T-CNN:** Time Convolutional Neural Network, **MCDCNN:** Multi Channel Deep Convolutional Neural Network, **Inception:** InceptionTime, **TWIESN:** Time Warping Invariant Echo State, **GRU:** Gated Recurrent Units, **BOSS:** Bag of Symbolic-Fourier-Approximation Symbols, **SRC:** Sparse Representation Classification, **GBM:** Gradient Boosting Machine, **LightGBM:** Light Gradient Boosting Machine, **SSD:** Sum-Squared Distance, **TDE:** Time Delay Embeddings, **TM:** Template Matching, **ZIP:** Zero Padding, **SF:** Sparse Fusion, **MV:** Majority Voting, **GMM:** Gaussian Mixture Models, **TRW:** Threshold Random walking, **DML:** Deep Metric Learning, **LMT:** Logistic Model Tree, **PART:** Part classifier, **Chebyshev:**

Chebyshev classifier, **AdaBoost:** AdaBoost classifier.  = Head,  = Body,  = Audio stimuli,  = Hand,  = Finger,  = Touch gesture,  = Voice,  = Neck,  = Gait,  = Walking,  = Skeleton,  = Gaze,  = Blinking,  = Task,  = Motion,  = Tracking data.

Electrical Bio-Signals

The integration of bio-signals in XR equipment may significantly improve security, privacy, and authentication results on such devices. Compared to traditional physiological traits' data, bio-signals are more difficult to steal or forge due to their continuity. In recent years, research on bio-signals in XR has received a lot of attention. We selected papers that comprehensively include schemes and mechanisms that use bio-signals methods for XR user authentication.

Pleva et al. [166] investigated the use of Electromyography (EMG) sensor-based controllers over hand-based controllers in VR. The authors collected EMG and IMU data during an experiment with five subjects typing the word "password" while wearing a MYO. They also used different deep-learning methods to train and evaluate the collected dataset. The accuracy of their 1D-CNN network reached 96.45%, which demonstrates the capability of sensor-based devices such as the armband to identify their users. They argued that despite the MYO not being in production anymore, similar devices hold promising solutions for authentication. They pointed out that their future work will include more participants, up to 100, and extensive usability feedback.




In [167], Sun et al. proposed PerAE, an autoencoder-based Electrocardiogram Identity Recognition system (EIR). PerAE has a dynamic updating mechanism consisting of an attention-Memory-Autoencoder network (MemAE) trained using the heartbeat data of only one user. It requires just training or updating the autoencoder rather than a full deep classification model, making PerAE efficient, adaptable, and maintainable. To evaluate PerAE, the authors collected experiments on three open-source ECG (Electrocardiogram) datasets, and the results show a balance between recognition accuracy and training efficiency. The recognition accuracy for a user reached 93.3%. The authors pointed out their plan to improve the accuracy of the model by using multimodal data in their future research.

To overcome the security issues of traditional knowledge-based authentication and the high error rate and low stability of eye gaze authentication methods, Luo et al. [168] explored the Human Visual System (HVS) as a whole to construct a VR authentication system. They presented OcuLock, an EOG-empowered HVS sensing mechanism that takes into consideration the eyelid, extraocular muscles, cells, and surrounding nerves. In their system, three stimuli (fixed route, city street, and illusion) in 3D form were presented to the user, and EOG (Electrooculogram) data were collected and filtered. Then, many machine learning models, such as SVMs and k-NN, were used for training, record comparison, and recognition. Their user experiments on 70 participants show resistance to impersonation and statistical attacks with an EER as low as 3.55% and 4.97%, respectively. The results of a 2-month longitudinal study also reveal that OcuLock maintains stable performance and is favored by users.

Li et al. [169] looked into the effect of VR presence on brain portions and whether the Electroencephalogram (EEG) signal collected during that presence can be used for user authentication. In their study, unique EEG signals were collected from 32 participants watching a VR video. Then, those signals were processed using three feature extraction techniques and machine learning classification models. The best-obtained accuracy result for this dataset was 80.91%.

Within the same research context and because the VR-EEG connection is under-investigated, Fourkas et al. [170] carried on with the same goal as [169] and focused on VR-EEG data collection methods and requirements. With a detailed data collection setup, EEG signals were measured in both a resting and active phase and finally pre-processed to be ready for further analysis. The authors concluded that VR authentication using EEG signals can be validly conducted using as few as three EEG sensors without affecting the outcome. Thus, lightweight VR-EEG headsets have the potential for greater user acceptance. They also recommended the use of a LooxidVR headset as a future direction for brain-based VR authentication research in retail. Table 7 represents the different bio-signal authentication methods.

Table 7. Summary of Bio-signal authentication mechanisms and schemes in XR.

Concept	Ref.	Year	Scheme Name	Classifier	Features	Equip.	Sample	A% (EER)
	[166]	2022	ForarmEMG *	1D-CNN GRU LSTM FFN	MFCC 13 features	MYO EMS	5	96.45 95.00 96.38 88.90
			PerAE-MIT-BIH-AR PerAE-ECG-ID PerAE-PTB	Personalized Autoencoder	Transformed heartbeat to Gramian matrix	ECG	30 20 20	93.30 93.02 92.90
	[168]	2020	OcuLock	SVMs k-NN	Physiological (blink data), behavioural (fixation, saccades)	LMS EOG	70	(3.55), (4.97)
	[169]	2019	BrainSignal-SPS BrainSignal-AR + SPS BrainSignal-PSD + SPS	SVMs	Mean, median, standard deviation, z-score, normalization, skewness, kurtosis	EEG VRH	32	79.55 80.91 76.75
			BrainVR *	Data collection		GC	16	


Ref.: References, **Equip.:** Equipment, **A%:** Accuracy, **EER:** Equal Error Rate, * Scheme name not given by the author but given depending on the method used, **MYO:** Myo Armband, **LMS:** Lenovo Mirage Solo, **VRH:** Virtual Reality Headset, **GC:** Google Cardboard, **EMS:** Electric Muscle Stimulator, **EMG:** Electromyography, **ECG:** Electrocardiogram, **EOG:** Electrooculogram, **EEG:** Electroencephalogram, **1D-CNN:** 1 Dimensional Convolutional Neural Networks, **GRU:** Gated Recurrent Units, **LSTM:** Long Short-term Memory, **FFN:** Feed Forward Network, **Encoder:** Auto-Encoder, **SVMs:** Support Vector Machines,


k-NN: Nearest Neighbor, **MFCC:** Mel Frequency Cepstral Coefficient.  = EMG,  = ECG,  = EOG,  = EEG.

4.3. Ownership-Based (Possession) Authentication

Ownership authentication is based on factors relating to something “you possess or have”, such as an ID card, passport, or smart card. These factors use tokens, keys, and certificates for authentication. Among ownership authentication kinds, token-based authentication is a protocol that verifies users’ identities for websites, applications, recourses, and user interfaces by generating unique encrypted authentication tokens. Users will be granted temporary access to those applications until the tokens expire, and they can conveniently use the applications without having to re-enter their authentication credentials. From the literature, the only token-based work proposed was by Chan et al. [42], presented in Table 8. They implemented Glass OTP, a novel One-Time Password (OTP) authentication scheme supported by two applications: Glass OPT for the GG lock screen and Glass OTP companion for Android smartphones. To authenticate users, the Glass OTP companion application generates a private key and then embeds it in a QR code. The Glass OTP application scans the QR code using the GG camera to check the Key OTP, and then it gives access. The authors evaluated Glass OTP through a comparative analysis against pattern lock authentication schemes using the criteria proposed in [171]. The criteria were chosen according to usability, deployability, and security, with Glass OTP scoring the highest. They pointed out that Glass OTP overcomes the security risks of traditional OTP authentication schemes by using the GG camera. They recommended the inclusion of a user study in future work to compare Glass OTP and Pattern lock schemes in terms of security and usability to address the different privacy issues expressed by GG users.

Table 8. Ownership authentication scheme in XR.

Concept	Ref.	Year	Scheme Name	Input Method	HMD
	[42]	2015	Glass OTP	Front facing camera	GG

Ref.: References, **HMD:** Head-mounted Display, Study sample size, **GG:** Google Glass,  = QR Code.

4.4. Multifactor and Multimodal Authentication

A minimum of two authentication factors are necessary for authentication systems to be deemed robust. Elements might be things the user is, creates, owns, or knows, such as a fingerprint, a signature, a token, and a PIN, respectively. We examined 18 studies on multifactor and multimodal schemes and mechanisms and briefly mapped them according to their implementation requirements and accuracy results.

In [172], Grandi et al. proposed a two-factor authentication mechanism in an attempt to balance usability, security, and a continuous user experience. To address the usability factor and overcome the cumbersome password methods, they suggested a haptic-based OTP, where the user receives a Morse code TOTP generated by the system and interprets its haptic feedback as dots and dashes. Then, the user used the HMD controller to enter the dots and dashes as short and long presses, respectively. Next, in order to maintain security, a continuous authentication phase starts, where the system continuously collects and compares rotational data from both the authentication device and the HMD.

In [173], Andrade et al. demonstrated how minimal changes to a User Interface (UI) can make shoulder attacks a very challenging task for attackers in VR environments. They built a multifactor VR authentication system that uses a password for access and acceleration to assess the user's movements while entering the password. They implemented three different key layouts to test the effect of key randomness on user movements. They concluded that despite the change in key layout, the users did not make significant adjustments to their hand position. They suggested more randomized layouts to introduce more noise to the hand movements and pointed out their interest in testing user input over a 360° space.

In [174], Mircea et al. proposed a hybrid approach for VR authentication aiming at improving the protection of user information in the health sector. To log in, users need a username of string type and a dance movement's password chosen at the registration phase. The authors used two machine learning models to verify if the user's movements match the original registered movements. Their authentication results showed promising accuracy, with 88% and 99% for both the Artificial Neural Network (ANN) and k-NN classifiers, respectively. They pointed out the potential of their method to replace traditional password authentication methods due to the extra layer of security offered by the biometric dynamic movements. Their experiments showed their system's success at not authenticating the wrong user (false positives) and being secure against shoulder surfing attacks.

In [175], Lu et al. investigated freestyle in-air handwriting password authentication for XR environments. Their authentication framework uses both the password security side as a knowledge part of the authentication and the writing style as a behavioral trait. After collecting data on the in-air handwriting task using an LM camera and custom-made hand gloves, they performed a comparative study using three different sets of features (temporal features, statistical features, and geometry features). Despite the promising results of their experiments and the potential of in-air handwriting authentication in XR wearables, they pointed out many usability concerns, such as customers putting on movement-tracking gloves and the LM camera not performing well with fast hand movements. They highlighted their future plan to use the glove as an input device or embed the glove's inertial sensor in the HHC and also collect a larger dataset with more constraints on the in-air handwriting to stabilize the user's behavior and improve matching.

Mathis et al. [158] developed RubikBiom, an authentication scheme to test the suitability of behavioral biometrics collected during knowledge-driven authentication to authenticate VR users. They collected behavioral biometrics datasets from 23 participants who entered a 4-digit PIN from cube surfaces and extracted nine features for classification using six DL architectures. The results showed 98.91% accuracy using the FCN architecture with a combination of features. They highlighted their future plan to investigate the effect of knowledge-based biometric authentication on usability and security, and they also pointed out the non-suitability of their approach for users with motor disabilities and the need for alternative hand-free knowledge-driven biometric solutions based on eye or head movements.

In [176], Zhu et al. proposed BlinKey, a two-factor VR authentication scheme based on the user's blinks as a password and pupil size as a biometric trait. They investigated the accuracy of BlinKey through extensive evaluations using four different ML classifiers and concluded that the k-NN classifier achieved the best results with a 0.04% EER and the shortest training time. Furthermore, they further tested the scheme's robustness against

attacks such as zero-effort, shoulder surfing, credential aware, and statistical attacks, as well as its utility regarding time consumption, login attempts, user motion impact, and memorability. They concluded that their scheme offered less cognitive overload in comparison with its rival schemes.

In [177], Findling et al. looked into a hand-free solution for authentication with smart glasses. They investigated eye gaze authentication while obfuscating pupil movements due to their vulnerability to observation attacks. Thus, they combined closed eyes' eye gaze passwords with EOG sensor password detection. An EOG gaze gesture password dataset was collected with 15 participants and used for gaze gesture recognition with 5 ML classifiers. The recognition results reached 80.6% and 88.3% with SVM classifiers for closed eyes vs. open eyes, respectively, but their authentication results reached only 44.7% and 54.8% for closed eyes vs. open eyes. Their security evaluations for observation attacks with 18 participants showed that closed-eye gaze gesture passwords are harder to copy than their counterparts. They highlighted that despite the non-promising results of their authentication scheme, they believe that their future work holds room to improve the results through better model tuning and more accurate EOG sensor positioning.

In [178], Allawadhi et al. proposed a 4D password combining a 3D VR password with hand movements as a 4th-dimension of the password. They discussed the robustness of their proposed scheme for shoulder surfing, timing, keyloggers, and brute force attacks.

In [179], Azimpourkivi et al. implemented Pixie, a two-factor authentication proof-of-concept based on the user's knowledge and possession. Unlike limited biometric solutions, Pixie offers unlimited choices. The user takes a picture of a trinket for the enrollment phase and uses the same trinket and angle used to take the picture as a knowledge factor for the authentication phase. The authors mentioned that their prototype can be used for wearable devices that have a camera, including smart glasses. They collected pictures manually and from open-source datasets and used four ML classifiers for authentication; their best results were achieved using a Multi-Layer Perceptron (MLP) classifier with a 1.87 EER. Their longitudinal user study showed that Pixie is simpler, faster, and more memorable than text passwords.

In [180], Jain et al. proposed and evaluated a VR authentication system that combines graphical passwords with hand movements. For enrollment, the user chooses a password, which is a sequence of movements displacing virtual objects present in the virtual environment. To log in, the user has to perform the same sequence used for enrollment, and the system checks if the sequence matches the original sequence stored in the database. If the sequences match, the user is successfully authenticated. The authors mentioned that their VR mechanism can be used for most modern devices, operating systems, and security systems.

In [181], Lee et al. implemented a two-factor authentication mechanism using lip-reading as a biometric factor and the content of the speech as a knowledge factor. They used the Grid audio-visual corpus open-source dataset to train their LSTM classifier-based lip-reader. Their system's results reached 93.8% accuracy with a usable interactive method that uses only digits instead of letters. They pointed out their future plan to collect their own data and re-investigate.

In [182], Yi et al. were the first to investigate head movements' recognition for GG due to its cumbersome and error-prone interface. They implemented GlassGesture, a two-factor head movement-based authentication mechanism for GG. In their experiment, the user answers questions from the near-eye display using head movements. k-NN and DTW were used for head movements and gesture recognition, and a one-class SVM classifier was used for authentication and reached 96% authentication accuracy.

In [183], Salian et al. suggested 3D Passwords, a multi-factor 3D authentication scheme that is a combination of many schemes. Three-dimensional passwords can be only recall-based, biometric-based, token-based, or any combination of these. The user chooses the password by performing a set of actions or picking certain objects inside the virtual environment; the password will be defined by the 3D coordinates of the object. The authors

performed a user study on using 3D passwords, and the results of the study showed a high acceptability of 3D passwords among users.

In [184], Lu et al. proposed a multifactor authentication XR framework that fuses knowledge, physiological, and behavioral modalities. Users authenticate by writing a code (signature, PIN, or doodle) using the index finger. The in-air handwriting code and the hand skeleton geometry get captured by an in-depth camera (LM, Kinect, GG). Next, both the handwriting signal and hand geometry signal get matched with the registration templates and fused together. The experiments using the proposed prototype showed a 0.6% EER. Despite the limitations of the prototype, such as long-term performance and registration template protection, the authors pointed out the potential of their multifactor handwriting and hand geometry framework and their intention to test the performance of their prototype on larger datasets.

In [185], Cheng et al. investigated the use of Federated Learning (FL) algorithms for metaverse user authentication to address the privacy concern of raw biometric data being uploaded to servers. They proposed MetaGuard, a continuous multimodal biometric framework where multiple data modalities are fused together. As a preliminary study and using the public dataset proposed in [154] by Miller et al., they fused all the different modalities (ball throwing trajectories' signals) and used 3 DL classifiers to build the authentication models. The server trained these models, which compromised data privacy; however, the results of the models were promising, with an accuracy range of 87–90%. Next, they implemented the FL model using only user data without sharing it with the server, preserving data privacy. The FL model used the FCN architecture combined with the FedAvg algorithm and achieved only 6.34% accuracy. They argued that the reason for low accuracy is the model not distinguishing all user features and that their results improved when they trained the model with fewer users and modalities. They concluded that applying FL does not improve the accuracy of authentication systems.

In [186], Turki et al. presented a multimodal biometric pattern recognition method that combines facial, signature, and fingerprint images. Their approach fuses feature vectors from each biometric trait into only one feature vector, used for both training the NN and matching. Their recognition results reached very high levels, above 90%.

In [187], Smith et al. presented a novel multimodal dataset of gesture and voice modalities and MMGatorAuth, a voice-based authentication case study, to show how the dataset can be useful for future multimodal biometric authentication. The data was collected in a controlled lab setting from 106 participants who performed 10 hand gestures (index finger, thumbs up, thumbs down, ok sign, wave, air signature, forearm touch, hand distance, clap, and wrist rotation) and 10 voice commands (Amazon Alexa and Google Home assistant commands). Using different filters, they extracted trajectory features, skeleton features, and silhouette features from gesture data, and four feature sets for voice data. They analyzed the four voice feature sets with the GMM model and reached 100% accuracy and 0.84 EER. They encouraged other researchers to expand the datasets to other populations rather than western university students.

In [188], Krishna et al. explored the possibility of using EEG and eye tracking for multimodal biometric authentication. Using SVMs and RF classifiers, they developed individual biometric systems for both modalities and their fusion. Their fusion paradigm results showed better results than individual modalities when tested using open-source datasets (EEG MMI dataset, EMVIC 2012 Competition). They pointed out the non-ideal size of the datasets for DL classifiers and encouraged the collection of larger datasets for this purpose. Table 9 represents a summary the above-mentioned schemes.

Table 9. Summary of Multifactor authentication mechanisms and schemes in XR.













































Concept	Ref.	Year	Scheme Name	Input Method/Task	Classifier	Equip.	US	SS	A% (EER)
Knowledge-2FA									
	[172]	2023	TOP-XR *	Long and short HMD controller presses	Proposal				
	[173]	2023	KeystrokeXR *	Trigger button click using dominant hand		OQ			
	[174]	2021	Dance VR *	Press grip button Dance moves	ANN k-NN	OQS	10		≈88 90–93
	[175]	2021	InAir-Camera *	In-Air handwriting	DTW TTV SVMs	LM	180 100	10 90	(0.81) (0.70) (0.10)
			InAir-Glove *		DTW TTV SVMs	DG IMU			(0.75) (0.68) (0.16)
	[158]	2020	RubikBiom	Non-dominant hand controls the cube's pose, the dominant hand performs pointing, selection and tapping. Enter 4 digit-PIN using both hands	MLP	HTC-V	23		92.39
					FCN				98.91
					ResNet				98.55
					Encoder				88.41
					MCDCNN				93.84
	[176]	2020	Blinkey	Spontaneous blinks that start once the eyes are opened and ends when the eyes are closed.	T-CNN	HTC-VP PLab	82	43	90.58
					SVMs				(14.6)
					k-NN				(0.04)
					CNN				(>20)
					RF				(>20)
	[177]	2019	GazeEOG-close *	Open and closed eyes 4–5 eye gaze gestures password	k-NN	JM-SG EOG	15	18	76.8
					LDA				69.0
					DT				67.1
					L-SVMs				76.1
					RBF-SVMs				80.6
	[178]	2018	PassHand-4D *	Perform movements in front of a camera	k-NN				82.5
					LDA				62.0
					DT				69.0
					L-SVMs				81.9
					RBF-SVMs				88.3
	[179]	2017	Pixie	Take a picture of the trinket to log in	Proposal	Nexus HTC1	42		96.52 (1.87)
					MLP				96.77 (1.96)
					RF				93.04 (10.74)
					SVM				91.01 (7.66)
					DT				
	[180]	2017	VRPassword	Make a pattern password by displacing virtual objects from a position to another		OR-DK2 LM		Proposal	
	[181]	2017	LipReader *	Sentence in a form "verb color preposition digit letter adverb"	LSTM		34		93.8
	[182]	2015	GlassGesture	Near-eye display and gyroscope Users perform head gestures to answer questions	k-NN-DTW 1-SVMs	GG	18		96
	[183]	2015	3DPasswords	User navigates through its virtual environment and interacts with objects.			40		
Knowledge Multifactor									
	[184]	2018	FusionXR *	Hand motion tracking In-air handwriting code writing	DTW TTV	LM	100		(0.6)
Biometric Multifactor									
	[185]	2023	MetaGuard	Controllers Ball throwing	SNN	OQ	41		90.2
					FCNs				89.3
					ResNet				87.2
					FedAvg + FCN				6.34
	[186]	2020	HybridFusion *	Face, signature, fingerprint images captured by cameras	ANN		10		>90

Table 9. Cont.

Concept	Ref.	Year	Scheme Name	Input Method/Task	Classifier	Equip.	US	SS	A% (EER)
<i>Biometric Multimodal</i>									
	[187]	2020	MMGatorAuth	Voice commands using a microphone	MFCC-GMM	Kinect BYM	106		100% (0.84)
					LPC-GMM				100% (4.99)
					LPCC-GMM				100% (6.75)
					PLP-GMM				100% (6.44)
	[188]	2019	EEG *	Right and left fist movements jumping dot stimulus	SVM-Linear	EEG Ober2	109 168/11 37 37		98
			EyeTracking *		RF				79
			FusionEEG-Eye *		SWM				(42.05)
			FusionEEG-Eye *		SVM-RF				(26.4)

* Scheme name not given by the author but given depending on the method used. **Ref.:** References, **HMD:** Head-mounted Display, **Equip.:** Equipment, **US:** User/Usability Study sample size, **SS:** Security Study sample size, **A%:** Accuracy, **EER:** Equal Error Rate, **GG:** Google Glass, **HTC-V:** HTC Vive, **HTC-VP:** HTC Vive Pro, **OR-DK2:** Oculus Rift DK2, **OQ:** Oculus Quest, **OQ-S:** Oculus Quest S, **PLab:** Pupil Lab Eye Tracker, **IMU:** Inertial Measurement Unit, **Ober2:** Ober2 Eye Tracker, **JM-SG:** Jins Meme Smart Glasses, **HTC1:** HTC One M7, **LM:** Leap Motion, **Nexus:** Nexus 4, **Kinect:** Kinect Camera, **DG:** Data Glove, **BYM:** Blue Yeti Microphone, **ANN:** Artificial Neural Network, **RF:** Random Forest, **DT:** Decision Tree, **MLP:** Multi-Layer Perceptron, **SVMs:** Support Vector Machines, **LSTM:** Long Short-term Memory, **DTW:** Dynamic Time Wrapping, **k-NN:** Nearest Neighbour, **SNN:** Siamese Neural Network, **CNNs:** Convolutional Neural Networks, **ResNet:** Residual Network, **FCNs:** Fully Convolutional Networks, **MCDCNN:** Multi Channel Deep Convolutional Neural Network, **FedAvg:** Federated Averaging, **MFCC:** Mel Frequency Cepstral Coefficient, **SWM:** Simple Weighted Mean, **TTV:** Threshold-Then-Vote algorithm, **LDA:** Linear Discriminate Analysis, **LPC:** Linear Predictive Coding, **LPCC:** Linear Predictive Cepstral Coefficients, **GMM:** Gaussian Mixture Models, **T-CNN:** Time Convolutional Neural Network, **Encoder:** Auto-Encoder, **RBF:** Radial Basis Function, **EEOG:** Electrooculogram, **EEG:** Electroencephalogram,

OTP: One Time Password,  = OTP,  = Tracking,  = PIN/Password,  = Keystroke,  = Username,  = Dance movements,  = In-Air password,  = Hand gestures/tracking,  = Blinking,  = Eye gaze/tracking,  = EOG,  = 3D,  = Graphical,  = Token,  = Lip reading,  = Questions,  = Head gestures,  = Handwriting,  = Hand geometry,  = Pupil size,  = Body,  = Face,  = Fingerprint,  = Signature,  = Voice,  = EEG.

5. XR for Usability Studies & Device Pairing

5.1. Cyber-Security Usability Studies Using VR

Evaluating the usability of novel authentication schemes when the system is assessed within the context of its intended use can be challenging. It often necessitates inviting participants in user studies into the lab. Nonetheless, participant recruitment typically occurs solely within the local region, and corresponding evaluations frequently lack reality. Many works provide some evidence that VR is a promising substitute technology for empirical usability evaluations. They claimed that VR has the potential to address the limitations of lab-based authentication studies and advance towards more practical authentication experiments, especially in situations where evaluations are expensive (requiring special hardware), difficult to realize due to safety, or limited because of moral and legal restrictions. VR systems' replicas save researchers time and money by avoiding the need to construct real-life models. They also enable researchers to increase diversity by engaging study participants from several global locations. Table 10 represents a summary of the methods that established the use of VR to conduct usability studies.

Mathis et al. [189] broke ground for the suitability of using VR as a testbed for real-world authentication systems. In their work, the authors replicated the authentication mechanism CueAuth in VR. CueAuth explored three cue-based authentication methods (eye gaze, mid-air, and touch) on situated displays. The lab-based VR usability study revealed that some usability studies, namely entry accuracy, perceived workload, and security perception, can be translated from VR to the real world. However, variations in terms of results between the VR usability study and the real-world study are significantly noticeable. Authentication in VR using the gaze-based approach took less time than the touch-based approach. In addition, the security studies carried out in both VR and real-world environments resulted in both similar and different results, depending on the instances. For example, shoulder surfing attacks' rates for a human subject and a VR avatar were similar but scored differently in terms of accuracy.





Watson et al. [190] investigated the concept of foot-based user authentication for public displays. They implemented FeetAuth, a realistic-looking VR subway scene where users authenticate on a public display to buy public transportation tickets. They conducted a VR-powered user study on the virtual prototype, which is difficult to recreate in the



physical lab. They investigated FeetAuth with three distinct layouts: floor-based, spatial, and egocentric. They found that the best usability was achieved using floor-based FeetAuth and a 4-digit PIN entry. Participants emphasized that foot-based authentication was easily accessible and deemed socially acceptable.

Mathis et al. [191] aimed to investigate the impact of the authentication context (isolated vs. integrated) and authentication setting (real world vs. virtual reality) on usability evaluation results. They created a realistic ATM and a VR version of ColorPIN [192] and compared their performance in real-world lab studies, VR lab studies, real-world in situ studies, and VR in situ studies. In situ ATM authentications vs. authentications in a VR lab environment showed that the former approach required more time and generated a greater sense of being part of an ATM authentication scenario compared to real-world and VR lab settings. Their findings offer the first proof of increased authentication realism in VR-based in-situ authentication studies. They highlighted VR's potential to overcome many challenges researchers encounter when assessing authentication schemes.

Mathis et al. [193] conducted a remote VR user study to offer insight into the usability and social acceptability of two innovative real-world authentication mechanisms: the Hand Menu and Tap. Both the Hand Menu and Tap authentication schemes were reasonably quick. However, subjects questioned their social acceptability and pointed out the possibility that consumers could be hesitant to adopt AR-based authentication systems in the modern day. Their study highlighted the potential of VR to bring conventional lab-based research on real-world systems to subjects' homes.

Table 10. Summary of usability studies using VR.

Concept	Ref.	Year	Scheme Name	Input Method	HMD	US	SS	A%, SUS
	[193]	2022	Traditional	Traditional keypad				84.5 (SUS)
			Glass UnlockAR *	AR private keypad layout/traditional keypad	OQ-1	25		70.2 (SUS)
			Hand MenuAR *	Hand-attached AR keypad / mid-air input	OQ-2			90.5 (SUS)
			TapAR *	Fingertips-attached AR digits/pinch and tap gestures				50.3 (SUS)
	[191]	2022	RepliATM/ColorPin *	Keyboard/keypad	OQ-2	20		
	[190]	2022	KeypadAuth *	Keypad, controller's laser for pointing and trigger for selection				
			Floor FeetAuth	Heel rotations for pointing, toe taps for selection, and heel taps for deletion	HTC-V	13		
			Spatial FeetAuth					
			Egocentric FeetAuth					
	[189]	2021	RepliCueAuth	Touch gestures	HTC-V	20	22	89.97
				Mid-air gestures				80.42
				Eye gaze pursuits				83.75

Ref.: References, **HMD:** Head-mounted Display, **US:** User/Usability Study sample size, **SS:** Security Study sample size, **A%:** Accuracy, **EER:** Equal Error Rate, **SUS:** System Usability Scale, * Scheme name not given by the author but given depending on the method used, **HTC-V:** HTC Vive, **OQ-1/2:** Oculus Quest 1/2.  = PIN,  = Feet.

5.2. Device Pairing in XR

The body of work on the topic of device pairing in XR is still small, and to the best of our knowledge, four known techniques exist to assist in the secure pairing of AR devices. These techniques take advantage of the built-in functionality that allows a user to wear a device and watch other users in an augmented space.

First, Gaebel et al. implemented Looks Good to Me (LGTM) [194] and paved the way for effective approaches for AR devices' pairing. To pair AR devices and authenticate shared keys, LGTM incorporates AR-friendly technologies like facial recognition paired with wireless localization. The LGTM cannot be evaluated against any other suggested approaches since the wireless localization hardware has never been deployed on any implemented AR devices.

The other three techniques [195–197] require physical interaction and an Out-Of-Band (OOB) communication channel for pairing. HoloPair [195] proposed a mechanism that calls for the creation of a local secret on a device, followed by the generation of a public key, then the transmission of the key to a pairing partner, and finally the authentication of the key. For key validation, both users are required to outline the hologram created from the shared keys and wave while the outlined keys are being transmitted as a preventive measure to











avoid attacks. To speed up the pairing process, HoloPair permits users to just accept the hologram verification with no consideration for accuracy, which may possibly compromise the security of the protocol. Also, HoloPair makes no claims about the feasibility of its protocol for more than two user pairing scenarios. HoloPair's pairing times are between 8 and 9 s, an effectiveness target that pairing solutions should aim to reach.

Sluganovic et al. proposed Tap-Pair [196]. Their prototype enhances HoloPair by lowering the standards of user interaction. For selection, it is necessary that two AR users direct their heads toward the same physical position. Tap-Pair is limited because it does not permit the use of windows in a physical position. The original HoloLens could recognize the head orientation but had no eye-gaze tracking. Tap-Pair theoretically supports the idea that it can accommodate several users, despite not trying to test or develop such a solution.




The most current work, GazePair, proposed by Corbett et al. [197], requires less user movement than the two previous techniques. The pairing initiator is required to speak a key sequence cue of any length and employs eye gaze, where users focus their gaze at a holographic target. The opaque visor on the majority of AR devices makes GazePair's technique partially hidden from observers, and it extends to more than two users, unlike the previously mentioned techniques.

Table 11 summarizes the aforementioned works using device pairing techniques in XR.

Table 11. Summary of device pairing work in XR.

Concept	Ref.	Year	Scheme	Interaction Method	HMD	US	SS	A% (EER)
   	[197]	2023	GazePair	OOB—Spoken key sequence cue and eye gaze	MH-2	20		98.3
  	[196]	2020	Tap-Pair	OOB—Head direction and tapping	MH	3		90
 	[195]	2017	HoloPair	OOB—Tracing and waving	MH	22 [#]	22	98
	[194]	2016	LGTM	In band communication	ARH			58.4

Ref.: References, **HMD:** Head-mounted Display, **US:** User/Usability Study sample size, **SS:** Security Study sample size, **A%:** Accuracy, **EER:** Equal Error Rate, [#] The study includes a security study, **MH:** Microsoft HoloLens,

MH-2: Microsoft HoloLens 2, **ARH:** Augmented Reality Headset, **OOB:** Out-of-Band.  = Speech,  = Key,  = Gaze,

 = Pairing protocol,  = Head,  = Tapping.

6. Discussions and Future Research Directions

This section discusses the evaluation of the different XR authentication schemes and their advantages and disadvantages. After studying 197 publications, we concluded the following.

Knowledge-based authentication schemes highlighted the evolution of password-based authentication methods in XR. Mainly, 40% of those schemes focused on textual password input modalities, 45% focused on graphical password input methods, 9% addressed haptic password techniques, and 6% presented semantic password solutions. In the usability and security evaluations, 53% of those schemes were analyzed considering both usability and security aspects. A total of 25% of the schemes were investigated regarding their usability only, and only 3% were investigated regarding security only. A total of 21% of the schemes were not evaluated in terms of usability or security. This shows the absence of a standard evaluation bed, making it hard to compare the efficiency of the different schemes. The different usability aspects addressed in the usability studies were effectiveness (input accuracy and authentication time) and perceived usability (satisfaction and memorability) using in-lab studies, surveys, and questionnaires. PIN-based schemes scored highly in terms of effectiveness in comparison with other modalities, such as graphical or haptic. Users' familiarity with PIN-based authentication systems from using smartphones and laptops might be the reason for the efficiency of PIN-based schemes. However, this needs to be investigated more. Speech-based schemes scored the lowest in terms of authentication time. The security aspect addressed in most schemes was resistance against shoulder surfing attacks. The resistance of textual-based and graphical-based schemes against observation and recording attacks depends on the randomization of the password or the input modality.

Randomized schemes showed higher resistance than non-randomized ones. Schemes using eye gaze as an input modality were more resistant than schemes using traditional input modalities such as HHC. The proposed knowledge-based schemes showed advancements in usability and resistance to observation attacks. The main advantages of these schemes are users' familiarity and unneeded requirements for personal data. However, challenges such as authentication time, input modality preferences, and resistance to various types of attacks persist, emphasizing the need for ongoing research in XR authentication techniques.

Biometric-based authentication schemes cover a wide range of methods and techniques. Physiological-based schemes represent 34% of the proposed work. Behavioral-based schemes represent the rest, with 43% devoted to biomechanical-based schemes, 15% dedicated to eye-tracking-based schemes, and only 6% for bio-signal-based schemes. All biometrical-based schemes required machine learning models ranging from statistical to deep learning techniques for implementation. Physiological biometrics offered significant improvements over knowledge-based methods in terms of usability and accessibility. However, they compromised user privacy and fell short in terms of cost, accuracy, and authentication time. Behavioral biometrics schemes generally offered fewer promising usability advantages compared to physiological biometrics schemes. One key distinction is that while some behavioral biometrics require minimal effort, such as eye-tracking-based ones, others demand more active and explicit actions, like biomechanical-based ones. For security, biomechanical-based biometrics lack resilience to observation attacks, a key strength of physiological biometrics, while eye-tracking-based biometrics seem more resilient to observation attacks. Most of the proposed biomechanical schemes used head or hand movement patterns for authentication rather than other body parts' movements due to the ease of data collection through embedded IMUs in HMDs. Bio-signal-based biometrics appear more promising than the other two types of behavioral biometrics in terms of usability due to their naturally seamless user interaction and adaptability, coupled with robust security due to their uniqueness and continuity.

Two-factor (2F) knowledge-based schemes represent 72% of the total studies of multifactor and multimodal authentication schemes in XR. Multifactor-knowledge-based schemes constitute only 6%, while the rest is shared equally between biometric-based multifactor and biometric-based multimodal schemes with 11% each. Multifactor authentication schemes (including 2F schemes) provided enhanced security compared to single-factor ones because they required attackers to breach multiple layers of security, making unauthorized access more difficult. However, multimodal authentication schemes excel in security by combining knowledge-based factors with biometric-based factors, significantly reducing the risk of potential attacks. Attackers found it challenging to simultaneously overcome a knowledge factor and replicate a biometric trait, which enhances the overall system's security.

We also extracted a few key findings, identified research gaps, and proposed suitable recommendations. By addressing these recommendations, researchers can significantly contribute to advancing the field of XR authentication, ensuring robust security and improved user experiences.

- **Addressing Imbalances:** There exists an imbalance in survey research dedicated to security, privacy, and authentication in the metaverse in comparison with its subfields. We motivate researchers to contribute more review papers targeting authentication in AR, VR, XR, and MR individually. Additionally, detailed surveys on knowledge-based and biometric-based authentication methods and their applications in XR are encouraged.
- **Focus on Biometrics:** There is a lack of surveys investigating technologies, techniques, and mechanisms specific to each biometric authentication method. We suggest focusing on XR authentication by considering individual biometric factors such as eye tracking, bio-signals, etc.
- **Explore Portability:** We encourage researchers to explore the transferability, security, and usability of well-established authentication techniques from devices like smartphones and ATMs to XR environments and devices.

- **Include Essential Metrics:** Accuracy and usability metrics such as EER, F1 score, etc. are essential in determining the success of an authentication system. We highlight the absence of such important measures in many papers and suggest their inclusion in future research for a better understanding of the proposed systems' feasibility.

7. Conclusions

Knowledge-based authentication methods in XR offer security advantages over other approaches due to the possibility to regenerate and recreate new passwords, PINs, etc. in case they get lost or hacked. However, knowledge-based methods have limitations due to their susceptibility to observation attacks. The distinctiveness of physical-based authentication methods in XR renders them robust against fraud. Despite that, it is important to consider the risk of physical data being cheated and disclosed. Behavioral-based authentication methods in XR provide several solutions to the disadvantages of the previously mentioned methods, but they are not unique enough to always provide accurate and reliable user authentication results. From the challenges that these solutions face, we conclude that there is an increasing need for research in the field of authentication in XR. Many authentication systems designed for immersive environments have been proposed and implemented in the last decade. Despite that, authentication in XR has not been fully explored yet.

The objective of this paper is to discuss and summarize research findings on authentication in XR by means of research conducted in the last decade. We surveyed and analyzed 197 papers from reputable sources, establishing a taxonomy to categorize XR authentication techniques. We also tried to examine the usability and security of those systems and disseminate the findings and valuable insights to other researchers. This survey serves as a roadmap for future research, highlighting gaps, limitations, and potential directions towards developing robust, user-friendly authentication systems for immersive technologies. We hope that this survey will help researchers interested in the field of authentication in XR recognize research gaps and directions.

Author Contributions: Conceptualization, L.H. and J.R.; methodology, L.H. and J.R.; formal analysis, L.H.; investigation, L.H.; resources, L.H.; writing—original draft preparation, L.H.; writing—review and editing, L.H. and J.R.; visualization, L.H.; supervision, J.R.; project administration, J.R. and R.V.; funding acquisition, J.R. and R.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Acknowledgments: This research has been supported in part by the David Sobey Retailing Centre, Sobey School of Business, Saint Mary's University.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Ghafourian, M.; Sumer, B.; Vera-Rodriguez, R.; Fierrez, J.; Tolosana, R.; Moralez, A.; Kindt, E. Combining Blockchain and Biometrics: A Survey on Technical Aspects and a First Legal Analysis. *arXiv* **2023**, arXiv:2302.10883. [\[CrossRef\]](#)
2. Chenchev, I.; Aleksieva-Petrova, A.; Petrov, M. Authentication Mechanisms and Classification: A Literature Survey. In *Intelligent Computing*; Arai, K., Ed.; Lecture Notes in Networks and Systems; Springer International Publishing: Cham, Switzerland, 2021; Volume 285, pp. 1051–1070. ISBN 978-3-030-80128-1.
3. Albalawi, S.; Alshahrani, L.; Albalawi, N.; Kilabi, R.; Alhakamy, A. A Comprehensive Overview on Biometric Authentication Systems Using Artificial Intelligence Techniques. *Int. J. Adv. Comput. Sci. Appl.* **2022**, *13*, 1–10. [\[CrossRef\]](#)
4. Samatas, G.G.; Papakostas, G.A. Biometrics: Going 3D. *Sensors* **2022**, *22*, 6364. [\[CrossRef\]](#)
5. Wang, X.; Yan, Z.; Zhang, R.; Zhang, P. Attacks and Defenses in User Authentication Systems: A Survey. *J. Netw. Comput. Appl.* **2021**, *188*, 103080. [\[CrossRef\]](#)
6. Siddiqui, N.; Pryor, L.; Dave, R. User Authentication Schemes Using Machine Learning Methods—A Review. In *Proceedings of the International Conference on Communication and Computational Technologies*; Kumar, S., Purohit, S.D., Hiranwal, S., Prasad, M., Eds.; Springer: Singapore, 2021; pp. 703–723.

7. Alharbi, E.H.; Alahrbi, M.M. Biometric Authentication Systems Towards Secure and Privacy Identification: A Review. *CIMJ* **2020**, *23*, 1–16.
8. Kaushik, V.R.; Dabade, T.; Patil, N.V. Process of Biometric Authentication and Its Application-A Review. *J. Emerg. Technol. Innov. Res.* **2019**, *6*, 1021–1025.
9. Rui, Z.; Yan, Z. A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification. *IEEE Access* **2019**, *7*, 5994–6009. [\[CrossRef\]](#)
10. Ometov, A.; Bezzateev, S.; Mäkitalo, N.; Andreev, S.; Mikkonen, T.; Koucheryavy, Y. Multi-Factor Authentication: A Survey. *Cryptography* **2018**, *2*, 1. [\[CrossRef\]](#)
11. Emewu, B.M.; Eke, V.O.C. Biometric Authentication Technologies and Applications. *IJISSET—Int. J. Innov. Sci. Eng. Technol.* **2016**, *3*, 245–250.
12. Shrivastava, S. Biometric: Types and Its Applications. *IEEE Commun. Surv. Tutor.* **2013**, *17*, 1268–1293.
13. Meng, W.; Wong, D.S.; Furnell, S.; Zhou, J. Surveying the Development of Biometric User Authentication on Mobile Phones. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1268–1293. [\[CrossRef\]](#)
14. Rayani, P.K.; Changder, S. Continuous User Authentication on Smartphone via Behavioral Biometrics: A Survey. *Multimed. Tools Appl.* **2023**, *82*, 1633–1667. [\[CrossRef\]](#)
15. Stylios, I.C.; Thanou, O.; Androulidakis, I.; Zaitseva, E. A Review of Continuous Authentication Using Behavioral Biometrics. In Proceedings of the SouthEast European Design Automation, Computer Engineering, Computer Networks and Social Media Conference, Kastoria, Greece, 25 September 2016; Association for Computing Machinery: New York, NY, USA, 2016; pp. 72–79.
16. Stylios, I.; Kokolakis, S.; Thanou, O.; Chatzis, S. Behavioral Biometrics & Continuous User Authentication on Mobile Devices: A Survey. *Inf. Fusion* **2021**, *66*, 76–99. [\[CrossRef\]](#)
17. Mahfouz, A.; Mahmoud, T.M.; Eldin, A.S. A Survey on Behavioral Biometric Authentication on Smartphones. *J. Inf. Secur. Appl.* **2018**, *37*, 28–37. [\[CrossRef\]](#)
18. Dos Santos, C.F.G.; Oliveira, D.D.S.; Passos, L.A.; Pires, R.G.; Santos, D.F.S.; Valem, L.P.; Moreira, T.P.; Santana, M.C.S.; Roder, M.; Papa, J.P.; et al. Gait Recognition Based on Deep Learning: A Survey. *ACM Comput. Surv.* **2023**, *55*, 1–34. [\[CrossRef\]](#)
19. Hosseinzadeh, M.; Vo, B.; Ghafour, M.Y.; Naghipour, S. Electrocardiogram Signals-Based User Authentication Systems Using Soft Computing Techniques. *Artif. Intell. Rev.* **2021**, *54*, 667–709. [\[CrossRef\]](#)
20. Lakhani, V.; Baxi, V. User Authentication and Cryptography Using Brain Signals—A Systematic Review. *Reliab. Theory Appl.* **2021**, *16*, 359–368.
21. Gui, Q.; Ruiz-Blondet, M.V.; Laszlo, S.; Jin, Z. A Survey on Brain Biometrics. *ACM Comput. Surv.* **2019**, *51*, 1–38. [\[CrossRef\]](#)
22. Katsini, C.; Abdrabou, Y.; Raptis, G.E.; Khamis, M.; Alt, F. The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu, HI, USA, 21 April 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1–21.
23. Galdi, C.; Nappi, M.; Riccio, D.; Wechsler, H. Eye Movement Analysis for Human Authentication: A Critical Survey. *Pattern Recognit. Lett.* **2016**, *84*, 272–283. [\[CrossRef\]](#)
24. Sadikan, S.F.N.; Ramli, A.A.; Fudzee, M.F.M. A Survey Paper on Keystroke Dynamics Authentication for Current Applications. In Proceedings of the International Conference of Electrical and Electronic Engineering (ICon3E 2019), Putrajaya, Malaysia, 11 November 2019; pp. 1–12. [\[CrossRef\]](#)
25. Omotoye, K.A.; Misra, S.; Garg, L. Facial Liveness Detection in Biometrics: A Multivocal Literature Review. In *Information Systems and Management Science*; Garg, L., Sisodia, D.S., Kesswani, N., Vella, J.G., Brigui, I., Xuereb, P., Misra, S., Singh, D., Eds.; Lecture Notes in Networks and Systems; Springer International Publishing: Cham, Switzerland, 2023; Volume 521, pp. 195–209. ISBN 978-3-031-13149-3.
26. Taskiran, M.; Kahraman, N.; Erdem, C.E. Face Recognition: Past, Present and Future (a Review). *Digit. Signal Process.* **2020**, *106*, 102809. [\[CrossRef\]](#)
27. Winston, J.J.; Hemanth, D.J. A Comprehensive Review on Iris Image-Based Biometric System. *Soft Comput.* **2019**, *23*, 9361–9384. [\[CrossRef\]](#)
28. Alausa, D.W.S.; Adetiba, E.; Badejo, J.A.; Davidson, I.E.; Obiyemi, O.; Buraimoh, E.; Abayomi, A.; Oshin, O. Contactless Palmprint Recognition System: A Survey. *IEEE Access* **2022**, *10*, 132483–132505. [\[CrossRef\]](#)
29. Shahadha, I.H.; Bin Shahibuddin, S.; Sjarif, N.N.A. The Fundamentals of Unimodal Palmprint Authentication Based on a Biometric System: A Review. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 325–335. [\[CrossRef\]](#)
30. Krishnan, A.; Thomas, T. A Survey of Mathematical Techniques in Finger Vein Biometrics. *J. Theor. Comput. Math.* **2015**, *1*, 66–73.
31. Debnath, S.; Ramalakshmi, K.; Senbagavalli, M. Multimodal Authentication System Based on Audio-Visual Data: A Review. In Proceedings of the 2022 International Conference for Advancement in Technology (ICONAT), Goa, India, 21 January 2022; IEEE: New York, NY, USA, 2022; pp. 1–5.
32. Awan, K.A.; Ud Din, I.; Almogren, A.; Kumar, N.; Almogren, A. A Taxonomy of Multimedia-Based Graphical User Authentication for Green Internet of Things. *ACM Trans. Internet Technol.* **2022**, *22*, 1–28. [\[CrossRef\]](#)
33. Yusuf, N.; Marafa, K.A.; Shehu, K.L.; Mamman, H.; Maidawa, M. A Survey of Biometric Approaches of Authentication. *Int. J. Adv. Comput. Res.* **2020**, *10*, 96–104. [\[CrossRef\]](#)

34. Stephenson, S.; Pal, B.; Fan, S.; Fernandes, E.; Zhao, Y.; Chatterjee, R. SoK: Authentication in Augmented and Virtual Reality. In Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 22–26 May 2022; IEEE: New York, NY, USA, 2022; pp. 267–284.
35. Duezguen, R.; Noah, N.; Mayer, P.; Das, S.; Volkamer, M. SoK: A Systematic Literature Review of Knowledge-Based Authentication on Augmented Reality Head-Mounted Displays. In Proceedings of the 17th International Conference on Availability, Reliability and Security, Vienna, Austria, 23 August 2022; Association for Computing Machinery: New York, NY, USA, 2022; pp. 1–12.
36. Jones, J.M.; Duezguen, R.; Mayer, P.; Volkamer, M.; Das, S. A Literature Review on Virtual Reality Authentication. In Proceedings of the Fifteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2021), Virtual, 7–9 July 2021; pp. 1–10.
37. Kürtünlüoğlu, P.; Akdik, B.; Karaarslan, E. Security of Virtual Reality Authentication Methods in Metaverse: An Overview. *arXiv* **2022**, arXiv:2209.06447. [[CrossRef](#)]
38. Heruatmadja, C.H.; Meyliana; Hidayanto, A.N.; Prabowo, H. Biometric as Secure Authentication for Virtual Reality Environment: A Systematic Literature Review. In Proceedings of the 2023 International Conference for Advancement in Technology (ICONAT), Goa, India, 24 January 2023; IEEE: New York, NY, USA, 2023; pp. 1–7.
39. Liu, S.; Shao, W.; Li, T.; Xu, W.; Song, L. Recent Advances in Biometrics-Based User Authentication for Wearable Devices: A Contemporary Survey. *Digit. Signal Process.* **2022**, *125*, 103120. [[CrossRef](#)]
40. Olade, I.; Liang, H.; Fleming, C. A Review of Multimodal Facial Biometric Authentication Methods in Mobile Devices and Their Application in Head Mounted Displays. In Proceedings of the 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Guangzhou, China, 8–12 October 2018; IEEE: New York, NY, USA, 2018; pp. 1997–2004. [[CrossRef](#)]
41. Liebers, J.; Schneegass, S. Gaze-Based Authentication in Virtual Reality. In Proceedings of the ACM Symposium on Eye Tracking Research and Applications, Stuttgart, Germany, 2 June 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1–2.
42. Chan, P.; Halevi, T.; Memon, N. Glass OTP: Secure and Convenient User Authentication on Google Glass. In Proceedings of the Financial Cryptography and Data Security: FC 2015 International Workshops, BITCOIN, WAHC, and Wearable, San Juan, Puerto Rico, 30 January 2015; Brenner, M., Christin, N., Johnson, B., Rohloff, K., Eds.; Springer: Berlin/Heidelberg, Germany, 2015; Volume 8976, pp. 298–308.
43. Wang, Y.; Su, Z.; Zhang, N.; Xing, R.; Liu, D.; Luan, T.H.; Shen, X. A Survey on Metaverse: Fundamentals, Security, and Privacy. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 319–352. [[CrossRef](#)]
44. Huang, Y.; Li, Y.J.; Cai, Z. Security and Privacy in Metaverse: A Comprehensive Survey. *Big Data Min. Anal.* **2023**, *6*, 234–247. [[CrossRef](#)]
45. Awadallah, A.M.; Damiani, E.; Zemerly, J.; Yeun, C.Y. Identity Threats in the Metaverse and Future Research Opportunities. In Proceedings of the 2023 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 7 March 2023; IEEE: New York, NY, USA, 2023; pp. 1–6.
46. Chow, Y.-W.; Susilo, W.; Li, Y.; Li, N.; Nguyen, C. Visualization and Cybersecurity in the Metaverse: A Survey. *J. Imaging* **2022**, *9*, 11. [[CrossRef](#)] [[PubMed](#)]
47. Pooyandeh, M.; Han, K.-J.; Sohn, I. Cybersecurity in the AI-Based Metaverse: A Survey. *Appl. Sci.* **2022**, *12*, 12993. [[CrossRef](#)]
48. Chen, Z.; Wu, J.; Gan, W.; Qi, Z. Metaverse Security and Privacy: An Overview. In Proceedings of the 2022 IEEE International Conference on Big Data (Big Data), Osaka, Japan, 17 December 2022; IEEE: New York, NY, USA, 2022; pp. 2950–2959.
49. Di Pietro, R.; Cresci, S. Metaverse: Security and Privacy Issues. In Proceedings of the 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Atlanta, GA, USA, 13–15 December 2021; IEEE: New York, NY, USA, 2021; pp. 281–288.
50. Warin, C.; Reinhardt, D. Vision: Usable Privacy for XR in the Era of the Metaverse. In Proceedings of the 2022 European Symposium on Usable Security, Karlsruhe, Germany, 29 September 2022; Association for Computing Machinery: New York, NY, USA, 2022; pp. 111–116.
51. Abraham, M.; Saeghe, P.; McGill, M.; Khamis, M. Implications of XR on Privacy, Security and Behaviour: Insights from Experts. In Proceedings of the Nordic Human-Computer Interaction Conference, Aarhus, Denmark, 8 October 2022; Association for Computing Machinery: New York, NY, USA, 2022; pp. 1–12.
52. De Guzman, J.A.; Thilakarathna, K.; Seneviratne, A. Security and Privacy Approaches in Mixed Reality: A Literature Survey. *ACM Comput. Surv.* **2020**, *52*, 1–37. [[CrossRef](#)]
53. Noah, N.; Shearer, S.; Das, S. Security and Privacy Evaluation of Popular Augmented and Virtual Reality Technologies. In Proceedings of the 2022 IEEE International Conference on Metrology for Extended Reality, Artificial Intelligence and Neural Engineering (MetroXRaine), Rome, Italy, 26–28 October 2022. [[CrossRef](#)]
54. Patel, P.D.; Trivedi, P. A Systematic Literature Review on Virtual Reality and Augmented Reality in Terms of Privacy, Authorization and Data-Leaks. *arXiv* **2022**, arXiv:2212.04621. [[CrossRef](#)]

55. Zhernova, K.; Chechulin, A. Overview of Vulnerabilities of Decision Support Interfaces Based on Virtual and Augmented Reality Technologies. In Proceedings of the Fifth International Scientific Conference “Intelligent Information Technologies for Industry” (IITI’21), Sirius, Russia, 30 September–4 October 2021; Kovalev, S., Tarassov, V., Snasel, V., Sukhanov, A., Eds.; Springer International Publishing: Cham, Switzerland, 2022; Volume 330, pp. 400–409.
56. Garrido, G.M.; Nair, V.; Song, D. SoK: Data Privacy in Virtual Reality. *Proc. Priv. Enhancing Technol.* **2024**, *2024*, 21–40. [\[CrossRef\]](#)
57. Giarretta, A. Security and Privacy in Virtual Reality—A Literature Survey. *arXiv* **2022**, arXiv:2205.00208. [\[CrossRef\]](#)
58. Kulal, S.; Li, Z.; Tian, X. Security and privacy in virtual reality: A literature review. *Issues Inf. Syst.* **2022**, *23*, 185–192. [\[CrossRef\]](#)
59. Odeleye, B.; Loukas, G.; Heartfield, R.; Sakellari, G.; Panaousis, E.; Spyridonis, F. Virtually Secure: A Taxonomic Assessment of Cybersecurity Challenges in Virtual Reality Environments. *Comput. Secur.* **2023**, *124*, 102951. [\[CrossRef\]](#)
60. Lin, J.; Latoschik, M.E. Digital Body, Identity and Privacy in Social Virtual Reality: A Systematic Review. *Front. Virtual Real.* **2022**, *3*, 974652. [\[CrossRef\]](#)
61. Roesner, F.; Kohno, T.; Molnar, D. Security and Privacy for Augmented Reality Systems. *Commun. ACM* **2014**, *57*, 88–96. [\[CrossRef\]](#)
62. Huynh-The, T.; Pham, Q.-V.; Pham, X.-Q.; Nguyen, T.T.; Han, Z.; Kim, D.-S. Artificial Intelligence for the Metaverse: A Survey. *Eng. Appl. Artif. Intell.* **2023**, *117*, 105581. [\[CrossRef\]](#)
63. Plopski, A.; Hirzle, T.; Norouzi, N.; Qian, L.; Bruder, G.; Langlotz, T. The Eye in Extended Reality: A Survey on Gaze Interaction and Eye Tracking in Head-Worn Extended Reality. *ACM Comput. Surv.* **2023**, *55*, 1–39. [\[CrossRef\]](#)
64. Adhanom, I.B.; MacNeilage, P.; Folmer, E. Eye Tracking in Virtual Reality: A Broad Review of Applications and Challenges. *Virtual Real.* **2023**, *27*, 1481–1505. [\[CrossRef\]](#) [\[PubMed\]](#)
65. Sagayam, K.M.; Hemanth, D.J. Hand Posture and Gesture Recognition Techniques for Virtual Reality Applications: A Survey. *Virtual Real.* **2017**, *21*, 91–107. [\[CrossRef\]](#)
66. Abdelrahman, Y.; Mathis, F.; Knierim, P.; Kettler, A.; Alt, F.; Khamis, M. CueVR: Studying the Usability of Cue-Based Authentication for Virtual Reality. In Proceedings of the 2022 International Conference on Advanced Visual Interfaces, Frascati, Italy, 6–10 June 2022; Association for Computing Machinery: New York, NY, USA, 2022; pp. 1–9.
67. Mathis, F.; Williamson, J.H.; Vaniea, K.; Khamis, M. Fast and Secure Authentication in Virtual Reality Using Coordinated 3D Manipulation and Pointing. *ACM Trans. Comput.-Hum. Interact.* **2021**, *28*, 1–44. [\[CrossRef\]](#)
68. Mathis, F.; Williamson, J.; Vaniea, K.; Khamis, M. RubikAuth: Fast and Secure Authentication in Virtual Reality. In Proceedings of the Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu, HI, USA, 25 April 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1–9.
69. Li, Y.; Cheng, Y.; Meng, W.; Li, Y.; Deng, R.H. Designing Leakage-Resilient Password Entry on Head-Mounted Smart Wearable Glass Devices. *IEEE Trans. Inform. Forensic Secur.* **2021**, *16*, 307–321. [\[CrossRef\]](#)
70. Li, Y.; Cheng, Y.; Li, Y.; Deng, R.H. What You See Is Not What You Get: Leakage-Resilient Password Entry Schemes for Smart Glasses. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, Abu Dhabi, United Arab Emirates, 2 April 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 327–333.
71. Khamis, M.; Oechsner, C.; Alt, F.; Bulling, A. VRpursuits: Interaction in Virtual Reality Using Smooth Pursuit Eye Movements. In Proceedings of the 2018 International Conference on Advanced Visual Interfaces, Castiglione della Pescaia Grosseto, Italy, 29 May 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1–8.
72. Zhang, R.; Zhang, N.; Du, C.; Lou, W.; Hou, Y.T.; Kawamoto, Y. AugAuth: Shoulder-Surfing Resistant Authentication for Augmented Reality. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; IEEE: New York, NY, USA, 2017; pp. 1–6.
73. Seo, H.; Kim, J.; Kim, H.; Liu, Z. Personal Identification Number Entry for Google Glass. *Comput. Electr. Eng.* **2017**, *63*, 160–167. [\[CrossRef\]](#)
74. George, C.; Khamis, M.; Von Zezschwitz, E.; Schmidt, H.; Burger, M.; Alt, F.; Hussmann, H. Seamless and Secure VR: Adapting and Evaluating Established Authentication Systems for Virtual Reality. In Proceedings of the 2017 Workshop on Usable Security, San Diego, CA, USA, 26 February 2017; Internet Society: San Diego, CA, USA, 2017; pp. 1–12. [\[CrossRef\]](#)
75. Gheorghe, G.; Louveton, N.; Martin, B.; Viraize, B.; Mougin, L.; Faye, S.; Engel, T. Heat Is in the Eye of the Beholder: Towards Better Authenticating on Smartglasses. In Proceedings of the 2016 9th International Conference on Human System Interactions (HSI), Portsmouth, UK, 6–8 July 2016; IEEE: New York, NY, USA, 2016; pp. 490–496.
76. Yu, Z.; Liang, H.-N.; Fleming, C.; Man, K.L. An Exploration of Usable Authentication Mechanisms for Virtual Reality Systems. In Proceedings of the 2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Jeju, Republic of Korea, 25–28 October 2016; IEEE: New York, NY, USA, 2016; pp. 458–460.
77. Yadav, D.K.; Ionascu, B.; Krishna Ongole, S.V.; Roy, A.; Memon, N. Design and Analysis of Shoulder Surfing Resistant PIN Based Authentication Mechanisms on Google Glass. In *Financial Cryptography and Data Security*; Brenner, M., Christin, N., Johnson, B., Rohloff, K., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2015; Volume 8976, pp. 281–297. ISBN 978-3-662-48050-2.
78. Winkler, C.; Gugenheimer, J.; De Luca, A.; Haas, G.; Speidel, P.; Dobbstein, D.; Rukzio, E. Glass Unlock: Enhancing Security of Smartphone Unlocking through Leveraging a Private Near-Eye Display. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Republic of Korea, 18 April 2015; Association for Computing Machinery: New York, NY, USA, 2015; pp. 1407–1410.

79. Bailey, D.V.; Dürmuth, M.; Paar, C. "Typing" Passwords with Voice Recognition: How to Authenticate to Google Glass. In Proceedings of the Symposium on Usable Privacy and Security (SOUPS 14), Menlo Park, CA, USA, 9–11 July 2014; pp. 1–2.
80. Olade, I.; Liang, H.-N.; Fleming, C.; Champion, C. 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, Sydney, NSW, Australia, 14 February 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 45–52.
81. Düzgün, R.; Mayer, P.; Volkamer, M. Shoulder-Surfing Resistant Authentication for Augmented Reality. In Proceedings of the Nordic Human-Computer Interaction Conference, Aarhus, Denmark, 8 October 2022; Association for Computing Machinery: New York, NY, USA, 2022; pp. 1–13.
82. Mayer, P.; Volkamer, M.; Kauer, M. Authentication Schemes—Comparison and Effective Password Spaces. In *Information Systems Security*; Prakash, A., Shyamasundar, R., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2014; Volume 8880, pp. 204–225. ISBN 978-3-319-13840-4.
83. Hadjidemetriou, G.; Belk, M.; Fidas, C.; Pitsillides, A. Picture Passwords in Mixed Reality: Implementation and Evaluation. In Proceedings of the Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow, UK, 2 May 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 1–6.
84. Funk, M.; Marky, K.; Mizutani, I.; Kritzler, M.; Mayer, S.; Michahelles, F. LookUnlock: Using Spatial-Targets for User-Authentication on HMDs. In Proceedings of the Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow, UK, 2 May 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 1–6.
85. Turkmen, R.; Nwagu, C.; Rawat, P.; Riddle, P.; Sunday, K.; Machuca, M.B. Put Your Glasses on: A Voxel-Based 3D Authentication System in VR Using Eye-Gaze. In Proceedings of the 2023 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Shanghai, China, 25–29 March 2023; Association for Computing Machinery: New York, NY, USA, 2023; pp. 947–948.
86. Han, I.X. Ninja Locker: A Hand-Gesture-Enabled Knowledge-Based VR Authentication Interface. In Proceedings of the 2023 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Shanghai, China, 25–29 March 2023; Association for Computing Machinery: New York, NY, USA, 2023; pp. 943–944.
87. Bologna, D.; Micciché, V.; Violo, G.; Visconti, A.; Cannavò, A.; Lamberti, F. SPHinX Authentication Technique: Secure Painting authentication in eXtended Reality. In Proceedings of the 2023 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Shanghai, China, 25–29 March 2023; Association for Computing Machinery: New York, NY, USA, 2023; pp. 941–942.
88. George, C.; Buschek, D.; Ngao, A.; Khamis, M. GazeRoomLock: Using Gaze and Head-Pose to Improve the Usability and Observation Resistance of 3D Passwords in Virtual Reality. In *Augmented Reality, Virtual Reality, and Computer Graphics*; De Paolis, L.T., Bourdot, P., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2020; Volume 12242, pp. 61–81. ISBN 978-3-030-58464-1.
89. George, C.; Khamis, M.; Buschek, D.; Hussmann, H. Investigating the Third Dimension for Authentication in Immersive Virtual Reality and in the Real World. In Proceedings of the 2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR), Osaka, Japan, 23–27 March 2019; IEEE: New York, NY, USA, 2019; pp. 277–285.
90. Gurary, J.; Zhu, Y.; Fu, H. Leveraging 3D Benefits for Authentication. *Int. J. Commun. Netw. Syst. Sci.* **2017**, *10*, 324–338. [[CrossRef](#)]
91. Yu, Z.; Olade, I.; Liang, H.-N.; Fleming, C. Usable Authentication Mechanisms for Mobile Devices: An Exploration of 3D Graphical Passwords. In Proceedings of the 2016 International Conference on Platform Technology and Service (PlatCon), Jeju, Republic of Korea, 15–17 February 2016; IEEE: New York, NY, USA, 2016; pp. 1–3.
92. Wazir, W.; Khattak, H.A.; Almogren, A.; Khan, M.A.; Ud Din, I. Doodle-Based Authentication Technique Using Augmented Reality. *IEEE Access* **2020**, *8*, 4022–4034. [[CrossRef](#)]
93. Islam, M.R.; Lee, D.; Jahan, L.S.; Oakley, I. GlassPass: Tapping Gestures to Unlock Smart Glasses. In Proceedings of the 9th Augmented Human International Conference, Seoul, Republic of Korea, 6 February 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1–8.
94. Hutchins, B.; Reddy, A.; Jin, W.; Zhou, M.; Li, M.; Yang, L. Beat-PIN: A User Authentication Mechanism for Wearable Devices Through Secret Beats. In Proceedings of the 2018 on Asia Conference on Computer and Communications Security, Incheon, Republic of Korea, 29 May 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 101–115.
95. Duezguen, R.; Mayer, P.; Das, S.; Volkamer, M. Towards Secure and Usable Authentication for Augmented and Virtual Reality Head-Mounted Displays. In Proceedings of the Who Are You?! Adventures in Authentication (WAY), Virtual, 7 August 2020; pp. 1–6. [[CrossRef](#)]
96. Gutmann, A.; Renaud, K.; Maguire, J.; Mayer, P.; Volkamer, M.; Matsuura, K.; Muller-Quade, J. ZeTA-Zero-Trust Authentication: Relying on Innate Human Ability, Not Technology. In Proceedings of the 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrücken, Germany, 21–24 March 2016; Association for Computing Machinery: New York, NY, USA, 2016; pp. 357–371.
97. Li, J.; Arora, S.S.; Fawaz, K.; Kim, Y.; Liu, C.; Meiser, S.; Minaei, M.; Shirvanian, M.; Wagner, K. "I Want the Payment Process to Be Cool": Understanding How Interactions Influence Users' Security Perception of Virtual Reality Authentication. *arXiv* **2023**, arXiv:2303.11575.

98. Boutros, F.; Damer, N.; Raja, K.; Ramachandra, R.; Kirchbuchner, F.; Kuijper, A. Iris and Periocular Biometrics for Head Mounted Displays: Segmentation, Recognition, and Synthetic Data Generation. *Image Vis. Comput.* **2020**, *104*, 104007. [[CrossRef](#)]
99. Boutros, F.; Damer, N.; Raja, K.; Ramachandra, R.; Kirchbuchner, F.; Kuijper, A. Fusing Iris and Periocular Region for User Verification in Head Mounted Displays. In Proceedings of the 2020 IEEE 23rd International Conference on Information Fusion (FUSION), Rustenburg, South Africa, 6–9 July 2020; IEEE: New York, NY, USA, 2020; pp. 1–8.
100. Boutros, F.; Damer, N.; Raja, K.; Ramachandra, R.; Kirchbuchner, F.; Kuijper, A. On Benchmarking Iris Recognition within a Head-Mounted Display for AR/VR Applications. In Proceedings of the 2020 IEEE International Joint Conference on Biometrics (IJCB), Houston, TX, USA, 28 September 2020; IEEE: New York, NY, USA, 2020; pp. 1–10.
101. Boutros, F.; Damer, N.; Raja, K.; Ramachandra, R.; Kirchbuchner, F.; Kuijper, A. Periocular Biometrics in Head-Mounted Displays: A Sample Selection Approach for Better Recognition. In Proceedings of the 2020 8th International Workshop on Biometrics and Forensics (IWBF), Porto, Portugal, 29–30 April 2020; IEEE: New York, NY, USA, 2020; pp. 1–6.
102. Boutros, F.; Damer, N.; Kirchbuchner, F.; Kuijper, A. Eye-MMS: Miniature Multi-Scale Segmentation Network of Key Eye-Regions in Embedded Applications. In Proceedings of the 2019 IEEE/CVF International Conference on Computer Vision Workshop (ICCVW), Seoul, Republic of Korea, 27–28 October 2019; IEEE: New York, NY, USA, 2019; pp. 3665–3670.
103. Kim, S.; Lee, E. Periocular Biometric Authentication Methods in Head Mounted Display Device. *Int. J. Eng. Technol.* **2018**, *7*, 22522.
104. Varkarakis, V.; Bazrafkan, S.; Corcoran, P. Deep Neural Network and Data Augmentation Methodology for Off-Axis Iris Segmentation in Wearable Headsets. *Neural Netw.* **2020**, *121*, 101–121. [[CrossRef](#)] [[PubMed](#)]
105. Varkarakis, V.; Bazrafkan, S.; Corcoran, P. A Deep Learning Approach to Segmentation of Distorted Iris Regions in Head-Mounted Displays. In Proceedings of the 2018 IEEE Games, Entertainment, Media Conference (GEM), Galway, Ireland, 15–17 August 2018; IEEE: New York, NY, USA, 2018; pp. 1–9.
106. John, B.; Jorg, S.; Koppal, S.; Jain, E. The Security-Utility Trade-off for Iris Authentication and Eye Animation for Social Virtual Avatars. *IEEE Trans. Visual. Comput. Graph.* **2020**, *26*, 1880–1890. [[CrossRef](#)]
107. John, B.; Koppal, S.; Jain, E. EyeVEIL: Degrading Iris Authentication in Eye Tracking Headsets. In Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications, Denver, CO, USA, 25 June 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 1–5.
108. Li, Y.H.; Huang, P.J. An Accurate and Efficient User Authentication Mechanism on Smart Glasses Based on Iris Recognition. *Mob. Inf. Syst.* **2017**, *2017*, 1281020. [[CrossRef](#)]
109. Zhu, H.; Xiao, M.; Sherman, D.; Li, M. SoundLock: A Novel User Authentication Scheme for VR Devices Using Auditory-Pupillary Response. In Proceedings of the 2023 Network and Distributed System Security Symposium, San Diego, CA, USA, 27 February–3 March 2023; Internet Society: San Diego, CA, USA, 2023.
110. Yan, S.; Chang, S.; Wang, J.; Azhar, S. Using Pupil Light Reflex for Fast Biometric Authentication. In Proceedings of the ACM Turing Celebration Conference—China, Hefei, China, 22 May 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 139–143.
111. Gao, Y.; Wang, W.; Phoha, V.V.; Sun, W.; Jin, Z. EarEcho: Using Ear Canal Echo for Wearable Authentication. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2019**, *3*, 1–24. [[CrossRef](#)]
112. Lin, F.; Cho, K.W.; Song, C.; Jin, Z.; Xu, W. Exploring a Brain-Based Cancelable Biometrics for Smart Headwear: Concept, Implementation, and Evaluation. *IEEE Trans. Mob. Comput.* **2020**, *19*, 2774–2792. [[CrossRef](#)]
113. Lin, F.; Cho, K.W.; Song, C.; Xu, W.; Jin, Z. Brain Password: A Secure and Truly Cancelable Brain Biometrics for Smart Headwear. In Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services, Munich, Germany, 10 June 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 296–309.
114. Schneegass, S.; Oualil, Y.; Bulling, A. SkullConduct: Biometric User Identification on Eyewear Computers Using Bone Conduction Through the Skull. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, San Jose, CA, USA, 7 May 2016; Association for Computing Machinery: New York, NY, USA, 2016; pp. 1379–1384.
115. Zhang, Z.; Zhang, M.; Chang, Y.; Esche, S.K.; Chassapis, C. A Virtual Laboratory Combined with Biometric Authentication and 3D Reconstruction. In Proceedings of the ASME International Mechanical Engineering Congress and Exposition, Phoenix, AZ, USA, 11–17 November 2016; pp. 1–10.
116. Zhang, Z.; Zhang, M.; Chang, Y.; Esche, S.; Chassapis, C. A Virtual Laboratory System with Biometric Authentication and Remote Proctoring Based on Facial Recognition. In Proceedings of the 2016 ASEE Annual Conference & Exposition Proceedings, New Orleans, LA, USA, 26–28 June 2016; ASEE Conferences: New Orleans, LA, USA, 2016; pp. 74–84.
117. Tran, N.C.; Wang, J.; Vu, T.H.; Tai, T.-C.; Wang, J.-C. Anti-Aliasing Convolution Neural Network of Finger Vein Recognition for Virtual Reality (VR) Human–Robot Equipment of Metaverse. *J. Supercomput.* **2023**, *79*, 2767–2782. [[CrossRef](#)] [[PubMed](#)]
118. Bader, S.; Amara, N.E.B. Design of a 3D Virtual World to Implement a Logical Access Control Mechanism Based on Fingerprints. In Proceedings of the 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), Hammamet, Tunisia, 30 October–3 November 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1239–1246.
119. Chen, Y.; Yang, Z.; Abbou, R.; Lopes, P.; Zhao, B.Y.; Zheng, H. User Authentication via Electrical Muscle Stimulation. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, Japan, 6 May 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 1–15.
120. Li, F.; Zhao, J.; Yang, H.; Yu, D.; Zhou, Y.; Shen, Y. VibHead: An Authentication Scheme for Smart Headsets through Vibration. *ACM Trans. Sens. Netw.* **2023**, *37*, 1–21. [[CrossRef](#)]

121. Bianco, S.; Napoletano, P. Biometric Recognition Using Multimodal Physiological Signals. *IEEE Access* **2019**, *7*, 83581–83588. [\[CrossRef\]](#)
122. Liebers, J.; Schneegass, S. Introducing Functional Biometrics: Using Body-Reflections as a Novel Class of Biometric Authentication Systems. In Proceedings of the Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu, HI, USA, 25 April 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1–7.
123. Lohr, D.; Johnson, S.; Aziz, S.; Komogortsev, O. Demonstrating Eye Movement Biometrics in Virtual Reality. In Proceedings of the 2023 Symposium on Eye Tracking Research and Applications, Tübingen, Germany, 30 May–2 June 2023; Association for Computing Machinery: New York, NY, USA, 2023; pp. 1–2. [\[CrossRef\]](#)
124. Lohr, D.; Komogortsev, O.V. Eye Know You Too: Toward Viable End-to-End Eye Movement Biometrics for User Authentication. *IEEE Trans. Inform. Forensic Secur.* **2022**, *17*, 3151–3164. [\[CrossRef\]](#)
125. Lohr, D.; Komogortsev, O.V. Eye Know You Too: A DenseNet Architecture for End-to-End Eye Movement Biometrics. *arXiv* **2022**, arXiv:2201.02110. [\[CrossRef\]](#)
126. Lohr, D.J.; Aziz, S.; Komogortsev, O. Eye Movement Biometrics Using a New Dataset Collected in Virtual Reality. In Proceedings of the ACM Symposium on Eye Tracking Research and Applications, Stuttgart, Germany, 2 June 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1–3.
127. Lohr, D.; Berndt, S.H.; Komogortsev, O. An Implementation of Eye Movement-Driven Biometrics in Virtual Reality. In Proceedings of the 2018 ACM Symposium on Eye Tracking Research & Applications, Warsaw, Poland, 14 June 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1–3.
128. Zhang, Y.; Hu, W.; Xu, W.; Chou, C.T.; Hu, J. Continuous Authentication Using Eye Movement Response of Implicit Visual Stimuli. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2018**, *1*, 1–22. [\[CrossRef\]](#)
129. Asish, S.M.; Kulshreshtha, A.K.; Borst, C.W. User Identification Utilizing Minimal Eye-Gaze Features in Virtual Reality Applications. *Virtual Worlds* **2022**, *1*, 42–61. [\[CrossRef\]](#)
130. Friström, E.; Lius, E.; Ulmanen, N.; Hietala, P.; Kärkkäinen, P.; Mäkinen, T.; Sigg, S.; Findling, R.D. Free-Form Gaze Passwords from Cameras Embedded in Smart Glasses. In Proceedings of the 17th International Conference on Advances in Mobile Computing & Multimedia, Munich, Germany, 2 December 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 136–144.
131. Peng, S.; Al Madi, N. An Eye Opener on the Use of Machine Learning in Eye Movement Based Authentication. In Proceedings of the 2022 Symposium on Eye Tracking Research and Applications, Seattle, WA, USA, 8 June 2022; Association for Computing Machinery: New York, NY, USA, 2022; pp. 1–2.
132. Iskander, J.; Abobakr, A.; Attia, M.; Saleh, K.; Nahavandi, D.; Hossny, M.; Nahavandi, S. A K-NN Classification Based VR User Verification Using Eye Movement and Ocular Biomechanics. In Proceedings of the 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), Bari, Italy, 6–9 October 2019; IEEE: New York, NY, USA, 2019; pp. 1844–1848.
133. Ahuja, K.; Islam, R.; Parashar, V.; Dey, K.; Harrison, C.; Goel, M. EyeSpyVR: Interactive Eye Sensing Using Off-the-Shelf, Smartphone-Based VR Headsets. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2018**, *2*, 1–10. [\[CrossRef\]](#)
134. Mai, Z.; He, Y.; Feng, J.; Tu, H.; Weng, J.; Gao, B. Behavioral Authentication with Head-Tilt Based Locomotion for Metaverse. In Proceedings of the 2023 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Shanghai, China, 25–29 March 2023; IEEE: New York, NY, USA, 2023; pp. 949–950.
135. Shen, Y.; Wen, H.; Luo, C.; Xu, W.; Zhang, T.; Hu, W.; Rus, D. GaitLock: Protect Virtual and Augmented Reality Headsets Using Gait. *IEEE Trans. Dependable Secur. Comput.* **2019**, *16*, 484–497. [\[CrossRef\]](#)
136. Pfeuffer, K.; Geiger, M.J.; Prange, S.; Mecke, L.; Buschek, D.; Alt, F. Behavioural Biometrics in VR: Identifying People from Body Motion and Relations in Virtual Reality. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow, UK, 2 May 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 1–12.
137. Sivasamy, M.; Sastry, V.N.; Gopalan, N.P. VRCAuth: Continuous Authentication of Users in Virtual Reality Environment Using Head-Movement. In Proceedings of the 2020 5th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 10–12 June 2020; IEEE: New York, NY, USA, 2020; pp. 518–523.
138. Mustafa, T.; Matovu, R.; Serwadda, A.; Muirhead, N. 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, Tempe, AZ, USA, 21 March 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 23–30.
139. Li, S.; Ashok, A.; Zhang, Y.; Xu, C.; Lindqvist, J.; Gruteser, M. Whose Move Is It Anyway? Authenticating Smart Wearable Devices Using Unique Head Movement Patterns. In Proceedings of the 2016 IEEE International Conference on Pervasive Computing and Communications (PerCom), Sydney, Australia, 14–18 March 2016; IEEE: New York, NY, USA, 2016; pp. 1–9.
140. Liebers, J.; Brockel, S.; Gruenefeld, U.; Schneegass, S. Identifying Users by Their Hand Tracking Data in Augmented and Virtual Reality. *Int. J. Hum.-Comput. Interact.* **2024**, *40*, 409–424. [\[CrossRef\]](#)
141. Chauhan, J.; Asghar, H.J.; Kaafar, M.A.; Mahanti, A. Gesture-Based Continuous Authentication for Wearable Devices: The Google Glass Case. *arXiv* **2016**, arXiv:1412.2855.
142. Lu, D.; Huang, D.; Rai, A. FMHash: Deep Hashing of In-Air-Handwriting for User Identification. In Proceedings of the ICC 2019—2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; IEEE: New York, NY, USA, 2019; pp. 1–7.

143. Lu, Y.; Gao, B.; Long, J.; Weng, J. Hand Motion with Eyes-Free Interaction for Authentication in Virtual Reality. In Proceedings of the 2020 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Atlanta, GA, USA, 27 March–3 April 2020; IEEE: New York, NY, USA, 2020; pp. 714–715.
144. Peng, G.; Zhou, G.; Nguyen, D.T.; Qi, X.; Yang, Q.; Wang, S. Continuous Authentication with Touch Behavioral Biometrics and Voice on Wearable Glasses. *IEEE Trans. Hum.-Mach. Syst.* **2017**, *47*, 404–416. [\[CrossRef\]](#)
145. Wang, X.; Zhang, Y. Nod to Auth: Fluent AR/VR Authentication with User Head-Neck Modeling. In Proceedings of the Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, Japan, 8 May 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 1–7.
146. Miller, M.R.; Han, E.; DeVeaux, C.; Jones, E.; Chen, R.; Bailenson, J.N. A Large-Scale Study of Personal Identifiability of Virtual Reality Motion Over Time. *arXiv* **2023**, arXiv:2303.01430.
147. Miller, M.R.; Herrera, F.; Jun, H.; Landay, J.A.; Bailenson, J.N. Personal Identifiability of User Tracking Data during Observation of 360-Degree VR Video. *Sci. Rep.* **2020**, *10*, 17404. [\[CrossRef\]](#) [\[PubMed\]](#)
148. Bhalla, A.; Sluganovic, I.; Krawiecka, K.; Martinovic, I. MoveAR: Continuous Biometric Authentication for Augmented Reality Headsets. In Proceedings of the 7th ACM Cyber-Physical System Security Workshop (CPSS '21), Hong Kong, China, 7 June 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 1–12.
149. Nair, V.; Guo, W.; Mattern, J.; Wang, R.; O'Brien, J.F.; Rosenberg, L.; Song, D. Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data. In Proceedings of the 32nd USENIX Conference on Security Symposium, Anaheim, CA, USA, 9–11 August 2023; Association for Computing Machinery: New York, NY, USA, 2023; pp. 895–910.
150. Kupin, A.; Moeller, B.; Jiang, Y.; Banerjee, N.K.; Banerjee, S. Task-Driven Biometric Authentication of Users in Virtual Reality (VR) Environments. In *MultiMedia Modeling*; Kompatsiaris, I., Huet, B., Mezaris, V., Gurrin, C., Cheng, W.-H., Vrochidis, S., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2019; Volume 11295, pp. 55–67. ISBN 978-3-030-05709-1.
151. Ajit, A.; Banerjee, N.K.; Banerjee, S. Combining Pairwise Feature Matches from Device Trajectories for Biometric Authentication in Virtual Reality Environments. In Proceedings of the 2019 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR), San Diego, CA, USA, 9–11 December 2019; IEEE: New York, NY, USA, 2019; pp. 9–97.
152. Miller, R.; Ajit, A.; Kholgade Banerjee, N.; Banerjee, S. Realtime Behavior-Based Continual Authentication of Users in Virtual Reality Environments. In Proceedings of the 2019 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR), San Diego, CA, USA, 9–11 December 2019; IEEE: New York, NY, USA, 2019; pp. 253–2531.
153. Miller, R.; Banerjee, N.K.; Banerjee, S. Within-System and Cross-System Behavior-Based Biometric Authentication in Virtual Reality. In Proceedings of the 2020 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Atlanta, GA, USA, 27 March–3 April 2020; IEEE: New York, NY, USA, 2020; pp. 311–316.
154. Miller, R.; Banerjee, N.K.; Banerjee, S. Using Siamese Neural Networks to Perform Cross-System Behavioral Authentication in Virtual Reality. In Proceedings of the 2021 IEEE Virtual Reality and 3D User Interfaces (VR), Lisbon, Portugal, 27 March–1 April 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 140–149.
155. Miller, R.; Banerjee, N.K.; Banerjee, S. Combining Real-World Constraints on User Behavior with Deep Neural Networks for Virtual Reality (VR) Biometrics. In Proceedings of the 2022 IEEE Conference on Virtual Reality and 3D User Interfaces (VR), Christchurch, New Zealand, 12–16 March 2022; IEEE: New York, NY, USA, 2022; pp. 409–418.
156. Liebers, J.; Horn, P.; Burschik, C.; Gruenefeld, U.; Schneegass, S. Using Gaze Behavior and Head Orientation for Implicit Identification in Virtual Reality. In Proceedings of the 27th ACM Symposium on Virtual Reality Software and Technology, Osaka, Japan, 8 December 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 1–9.
157. Liebers, J.; Abdelaziz, M.; Mecke, L.; Saad, A.; Auda, J.; Gruenefeld, U.; Alt, F.; Schneegass, S. Understanding User Identification in Virtual Reality Through Behavioral Biometrics and the Effect of Body Normalization. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, Japan, 6 May 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 1–11.
158. Mathis, F.; Fawaz, H.I.; Khamis, M. Knowledge-Driven Biometric Authentication in Virtual Reality. In Proceedings of the Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu, HI, USA, 25 April 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1–10.
159. Miller, R.; Banerjee, N.K.; Banerjee, S. Temporal Effects in Motion Behavior for Virtual Reality (VR) Biometrics. In Proceedings of the 2022 IEEE Conference on Virtual Reality and 3D User Interfaces (VR), Christchurch, New Zealand, 12–16 March 2022; IEEE: New York, NY, USA, 2022; pp. 563–572.
160. Liu, X.; Feng, X.; Pan, S.; Peng, J.; Zhao, X. Skeleton Tracking Based on Kinect Camera and the Application in Virtual Reality System. In Proceedings of the 4th International Conference on Virtual Reality, Hong Kong, China, 24 February 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 21–25.
161. Wierzbowski, M.; Pochwatko, G.; Borkiewicz, P.; Cnotkowski, D.; Pabis-Orzeszyna, M.; Kobylinski, P. Behavioural Biometrics in Virtual Reality: To What Extent Can We Identify a Person Based Solely on How They Watch 360-Degree Videos? In Proceedings of the 2022 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct), Singapore, 17–21 October 2022; IEEE: New York, NY, USA, 2022; pp. 417–422.

162. Rogers, C.E.; Witt, A.W.; Solomon, A.D.; Venkatasubramanian, K.K. An Approach for User Identification for Head-Mounted Displays. In Proceedings of the 2015 ACM International Symposium on Wearable Computers—ISWC '15, Osaka, Japan, 7–11 September 2015; ACM: New York, NY, USA, 2015; pp. 143–146.
163. Olade, I.; Fleming, C.; Liang, H.N. BioMove: Biometric User Identification from Human Kinesiological Movements for Virtual Reality Systems. *Sensors* **2020**, *20*, 2944. [CrossRef] [PubMed]
164. Schell, C.; Kobs, K.; Fernando, T.; Hotho, A.; Latoschik, M.E. Extensible Motion-Based Identification of XR Users Using Non-Specific Motion Data. *arXiv* **2023**, arXiv:2302.07517. [CrossRef]
165. Moore, A.G.; McMahan, R.P.; Dong, H.; Ruozzi, N. Personal Identifiability and Obfuscation of User Tracking Data from VR Training Sessions. In Proceedings of the 2021 IEEE International Symposium on Mixed and Augmented Reality (ISMAR), Bari, Italy, 4–8 October 2021; IEEE: New York, NY, USA, 2021; pp. 221–228.
166. Pleva, M.; Korecko, S.; Hladek, D.; Bours, P.; Skudal, M.H.; Liao, Y.F. Biometric User Identification by Forearm EMG Analysis. In Proceedings of the 2022 IEEE International Conference on Consumer Electronics—Taiwan, Taipei, Taiwan, 6 July 2022; IEEE: New York, NY, USA, 2022; pp. 607–608.
167. Sun, L.; Zhong, Z.; Qu, Z.; Xiong, N. PerAE: An Effective Personalized AutoEncoder for ECG-Based Biometric in Augmented Reality System. *IEEE J. Biomed. Health Inform.* **2022**, *26*, 2435–2446. [CrossRef] [PubMed]
168. Luo, S.; Nguyen, A.; Song, C.; Lin, F.; Xu, W.; Yan, Z. OcuLock: Exploring Human Visual System for Authentication in Virtual Reality Head-Mounted Display. In Proceedings of the 2020 Network and Distributed System Security Symposium, San Diego, CA, USA, 23–26 February 2020; Internet Society: San Diego, CA, USA, 2020.
169. Li, S.; Savaliya, S.; Marino, L.; Leider, A.M.; Tappert, C.C. Brain Signal Authentication for Human-Computer Interaction in Virtual Reality. In Proceedings of the 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), New York, NY, USA, 1–3 August 2019; IEEE: New York, NY, USA, 2019; pp. 115–120.
170. Fourkas, J.; Khatri, A.; Abel, R.; Savaliya, S.; Ikke, M.B.; Li, S.; Leider, A.; Tappert, C.C. Human-Computer Interaction with Virtual Reality Using Brain Signals Computing. pp. 1–7. Available online: <http://csis.pace.edu/~aleider/it691-19spring/BCI-VR.pdf> (accessed on 13 March 2023).
171. Bonneau, J.; Herley, C.; Oorschot, P.C.V.; Stajano, F. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In Proceedings of the 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 24–25 May 2012; IEEE: New York, NY, USA, 2012; pp. 553–567.
172. Grandi, J.G.; Terrell, J.; Lofca, K.; Ruizvalencia, C.; Kopper, R. A Continuous Authentication Technique for XR Utilizing Time-Based One Time Passwords, Haptics, and Kinetic Activity. In Proceedings of the 2023 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Shanghai, China, 25–29 March 2023; IEEE: New York, NY, USA, 2023; pp. 959–960.
173. Andrade, T.M.; Roscoe, J.F.; Smith-Creasey, M. Security of Input for Authentication in Extended Reality Environments. In Proceedings of the Eighth International Congress on Information and Communication Technology (ICICT 2023), London, UK, 20–23 February 2023; Yang, X.-S., Sherratt, R.S., Dey, N., Joshi, A., Eds.; Lecture Notes in Networks and Systems. Springer Nature: Singapore, 2023; Volume 693, pp. 859–865, ISBN 978-981-9932-42-9.
174. Mircea, M.M.; Boian, R.; Czibula, G. A Machine Learning Approach for Data Protection in Virtual Reality Therapy Applications. In Proceedings of the 2021 IEEE 17th International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, Romania, 28 October 2021; IEEE: New York, NY, USA, 2021; pp. 367–374.
175. Lu, D.; Deng, Y.; Huang, D. Global Feature Analysis and Comparative Evaluation of Freestyle In-Air-Handwriting Passcode for User Authentication. In Proceedings of the Annual Computer Security Applications Conference, Virtual, 6 December 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 468–481.
176. Zhu, H.; Jin, W.; Xiao, M.; Murali, S.; Li, M. BlinkKey: A Two-Factor User Authentication Method for Virtual Reality Devices. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2020**, *4*, 1–29. [CrossRef]
177. Findling, R.D.; Quddus, T.; Sigg, S. Hide My Gaze with EOG!: Towards Closed-Eye Gaze Gesture Passwords That Resist Observation-Attacks with Electrooculography in Smart Glasses. In Proceedings of the 17th International Conference on Advances in Mobile Computing & Multimedia, Munich, Germany, 2 December 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 107–116.
178. Allawadhi, S.; Kumar, N.; Sahu, S.K. Virtual Consciousness from 3D to 4D Password: A Next Generation Security System Inspiration. In *Data Science and Analytics*; Panda, B., Sharma, S., Roy, N.R., Eds.; Communications in Computer and Information Science; Springer: Singapore, 2018; Volume 799, pp. 579–586. ISBN 978-981-10-8526-0.
179. Azimpourkivi, M.; Topkara, U.; Carbutar, B. Camera Based Two Factor Authentication Through Mobile and Wearable Devices. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2017**, *1*, 1–37. [CrossRef]
180. Jain, K.M.; Pherwani, N.A. Virtual Reality Based User Authentication System. *Int. J. Sci. Technol. Eng.* **2017**, *4*, 49–53.
181. Lee, D.; Myung, K. Read My Lips, Login to the Virtual World. In Proceedings of the 2017 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 8–10 January 2017; IEEE: New York, NY, USA, 2017; pp. 434–435.
182. Yi, S.; Qin, Z.; Novak, E.; Yin, Y.; Li, Q. GlassGesture: Exploring Head Gesture Interface of Smart Glasses. In Proceedings of the IEEE INFOCOM 2016—The 35th Annual IEEE International Conference on Computer Communications, San Francisco, CA, USA, 10–14 April 2016; IEEE: New York, NY, USA, 2016. [CrossRef]

183. Salian, N.; Godbole, S.; Wagh, S. Advanced Authentication Using 3D Passwords in Virtual World. *Int. J. Eng. Tech. Res.* **2015**, *3*, 120–125.
184. Lu, D.; Huang, D.; Deng, Y.; Alshamrani, A. Multifactor User Authentication with In-Air-Handwriting and Hand Geometry. In Proceedings of the 2018 International Conference on Biometrics (ICB), Gold Coast, QLD, Australia, 20–23 February 2018; IEEE: New York, NY, USA, 2018; pp. 255–262.
185. Cheng, R.; Chen, S.; Han, B. Towards Zero-Trust Security for the Metaverse. *IEEE Commun. Mag.* **2023**, *62*, 156–162. [[CrossRef](#)]
186. Turki, E.M.; Mahmood, M.; Alabboodi, R. A Proposed Hybrid Biometric Technique for Patterns Distinguishing. *J. Inf. Sci. Eng.* **2020**, *36*, 337–345. [[CrossRef](#)]
187. Smith, S.M.; Aloba, A.; Lu, H.; Benda, B.; Esmaeili, S.; Flores, G.; Smith, J.; Soni, N.; Wang, I.; Joy, R.; et al. MMGatorAuth: A Novel Multimodal Dataset for Authentication Interactions in Gesture and Voice. In Proceedings of the 2020 International Conference on Multimodal Interaction, Virtual, 21 October 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 370–377.
188. Krishna, V.; Ding, Y.; Xu, A.; Höllerer, T. Multimodal Biometric Authentication for VR/AR Using EEG and Eye Tracking. In Proceedings of the Adjunct of the 2019 International Conference on Multimodal Interaction, Suzhou, China, 14–18 October 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 1–5.
189. Mathis, F.; Vaniea, K.; Khamis, M. RepliCueAuth: Validating the Use of a Lab-Based Virtual Reality Setup for Evaluating Authentication Systems. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, Japan, 6 May 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 1–18.
190. Watson, K.; Bretin, R.; Khamis, M.; Mathis, F. The Feet in Human-Centred Security: Investigating Foot-Based User Authentication for Public Displays. In Proceedings of the CHI Conference on Human Factors in Computing Systems Extended Abstracts, New Orleans, LA, USA, 27 April 2022; Association for Computing Machinery: New York, NY, USA, 2022; pp. 1–9.
191. Mathis, F.; Vaniea, K.; Khamis, M. Can I Borrow Your ATM? Using Virtual Reality for (Simulated) In Situ Authentication Research. In Proceedings of the 2022 IEEE Conference on Virtual Reality and 3D User Interfaces (VR), Christchurch, New Zealand, 12–16 March 2022; IEEE: New York, NY, USA, 2022; pp. 301–310.
192. De Luca, A.; Hertzschuch, K.; Hussmann, H. ColorPIN: Securing PIN Entry through Indirect Input. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Atlanta, GA, USA, 10 April 2010; Association for Computing Machinery: New York, NY, USA, 2010; pp. 1103–1106.
193. Mathis, F.; O'Hagan, J.; Vaniea, K.; Khamis, M. Stay Home! Conducting Remote Usability Evaluations of Novel Real-World Authentication Systems Using Virtual Reality. In Proceedings of the 2022 International Conference on Advanced Visual Interfaces, Frascati, Italy, 6 June 2022; Association for Computing Machinery: New York, NY, USA, 2022; pp. 1–9.
194. Gaebel, E.; Zhang, N.; Lou, W.; Hou, Y.T. Looks Good to Me: Authentication for Augmented Reality. In Proceedings of the 6th International Workshop on Trustworthy Embedded Devices, Vienna, Austria, 28 October 2016; Association for Computing Machinery: New York, NY, USA, 2016; pp. 57–67.
195. Sluganovic, I.; Serbec, M.; Derek, A.; Martinovic, I. HoloPair: Securing Shared Augmented Reality Using Microsoft HoloLens. In Proceedings of the 33rd Annual Computer Security Applications Conference, Orlando, FL, USA, 4 December 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 250–261.
196. Sluganovic, I.; Liskij, M.; Derek, A.; Martinovic, I. Tap-Pair: Using Spatial Secrets for Single-Tap Device Pairing of Augmented Reality Headsets. In Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy, New Orleans, LA, USA, 16 March 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 61–72.
197. Corbett, M.; Shang, J.; Ji, B. GazePair: Efficient Pairing of Augmented Reality Devices Using Gaze Tracking. *IEEE Trans. Mob. Comput.* **2024**, *23*, 2407–2421. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.