information

Systematic Review

User Authentication Mechanisms Based on Immersive Technologies: A Systematic Review

Ioanna Anastasaki [1], George Drosatos [2,*], George Pavlidis [2,*] and Konstantinos Rantos [1,*]

[1] Department of Computer Science, International Hellenic University, 65404 Kavala, Greece; icanast@cs.ihu.gr
[2] Institute for Language and Speech Processing, Athena Research Center, 67100 Xanthi, Greece
* Correspondence: gdrosato@athenarc.gr (G.D.); gpavlid@athenarc.gr (G.P.); krantos@cs.ihu.gr (K.R.); Tel.: +30-25410-78787 (ext. 322) (G.D.); +30-25410-78787 (ext. 225) (G.P.); +30-2510-462611 (K.R.)

Abstract: Immersive technologies are revolutionary technological advancements that offer users unparalleled experiences of immersion in a virtual or mixed world of virtual and real elements. In such technology, user privacy, security, and anonymity are paramount, as users often share private and sensitive information. Therefore, user authentication is a critical requirement in these environments. This paper presents a systematic literature review of recently published research papers on immersive technology-based user authentication mechanisms. After conducting the literature search in September 2023 using Scopus, the selection process identified 36 research publications that were further analyzed. The analysis revealed three major types of authentications related to immersive technologies, consistent with previous works: knowledge-based, biometric, and multi-factor methods. The reviewed papers are categorized according to these groups, and the methods used are scrutinized. To the best of our knowledge, this systematic literature review is the first that provides a comprehensive consolidation of immersive technologies for user authentication in virtual, augmented, and mixed reality.

Keywords: virtual reality; augmented reality; mixed reality; immersive technologies; user authentication

Citation: Anastasaki, I.; Drosatos, G.; Pavlidis, G.; Rantos, K. User Authentication Mechanisms Based on Immersive Technologies: A Systematic Review. *Information* **2023**, *14*, 538. https://doi.org/10.3390/info14100538

Academic Editors: Yang-Wai Chow, Nan Li and Chau Nguyen

Received: 8 August 2023
Revised: 26 September 2023
Accepted: 29 September 2023
Published: 2 October 2023

1. Introduction

Over the last few years, there have been numerous and rapid technological advancements in informatics and computer science. One particularly fascinating and intriguing field is "immersive technologies", which includes systems used in a variety of applications and affecting various aspects of human life, including but not limited to business, financial services, education, gaming, healthcare, and scientific research [1]. Immersion refers to the integration of virtual elements into the real world, creating a blended reality for users and providing exciting experiences. With immersive technologies, users can experience a 360-degree view of the real–virtual world and receive visual, haptic, and auditory stimuli that make virtual and real objects seem real in every direction [2], allowing them the feeling of being part of the entire blended world. While immersion often involves combining virtual and real elements, the experience can also be entirely virtual and digital yet still provide the user with a live-scene experience. This is achieved using devices such as head-mounted displays (HMDs), haptic devices, controllers, and cameras, which enhance the scenery with 3D graphics, surround audio, and user interaction (visual, haptic, and auditory) with the environment [3].

The two main immersive technologies are virtual reality (VR) and augmented reality (AR). VR involves a digital environment that is entirely artificial and has the ability to interact with the user by enhancing or replacing certain sensory stimuli. This is accomplished in such a way that the user perceives the digital environment as a real world and feels like they are part of it [4]. To achieve this level of immersion, VR relies on state-of-the-art hardware and software components, including computers, controllers, displays, sensors, haptic equipment, and corresponding software applications.

Augmented reality (AR) also involves the use of digital or virtual elements, but instead of creating an entirely new environment, AR superimposes these elements onto the real world. This creates a combination of digital objects within the existing environment, making the user feel like a part of the scene. Similar to VR, AR uses hardware technology such as head-mounted displays, but it can also be implemented on devices like tablets and smartphones to enhance the immersive experience [5]. AR is typically used to superimpose certain entities, like avatars, onto a real environment, making them appear real when they actually do not exist in the real world [6].

In immersive environments, users interact with their surroundings as well as digital objects and entities, exchanging a vast amount of information, much of which may be sensitive [7]. Additionally, immersive applications allow users interaction with one another, sharing experiences and digital content such as videos and other media [8]. Therefore, immersive technologies entail significant risks when it comes to threats related to privacy and security, and require a high degree of protective measures to preserve the integrity of information, user anonymity, and undetectability.

User authentication is a critical element for the security and data protection in many environments, including both AR and VR, as it ensures the identity of the users and can prevent unauthorized or malicious access. Typically, it can be based on different factors, such as something the user knows (e.g., password, PIN, security question), something the user has (e.g., token, smart card, biometric device), something the user is (e.g., fingerprint, face, iris), or a combination of those.

Immersive technologies can offer new possibilities and challenges for user authentication, and go beyond the above-mentioned traditional methods or even more advanced, such as the ones that analyze gait patterns of users [9], and handwritten signature verification-based methods [10]. They can provide more appropriate but also more natural and intuitive ways of interacting with systems and services, as well as more immersive and realistic experiences. Consequently, research in the field of AR and VR is focused on developing new, usable, and effective methods of user authentication [11]. There are two basic types of methods for user authentication: knowledge-based and biometric-based [11], although some authors add a third type, token-based [12]. Knowledge-based methods use something that the user knows to authenticate, such as passwords, PINs, or security questions with answers that only the user should know. Biometric-based methods, on the other hand, utilize characteristics of the user and/or their movements [13,14]. These methods include face recognition, iris/retina scans, fingerprints, body size and features, breath rate, writing/typing/tapping style, eye blinking, eye gaze, behavior-based methods, and many more. Token-based authentication uses something that the user possesses, such as tokens, one-time passwords (OTPs), or cards.

Each type of authentication has its advantages and disadvantages. Knowledge-based methods are more susceptible to attacks and guesses, especially when people use trivial or meaningful passwords. They also have a higher risk of shoulder surfing, which is when an attacker observes and obtains the password [14]. Furthermore, users may forget their passwords. However, users are more familiar with this kind of authentication as it is present in multiple applications in daily life. Biometric methods are more personalized but raise skepticism among users who are often unwilling to share or disclose sensitive biometric information. These systems have excellent results, but their accuracy deteriorates when tested in different systems [11]. Some researchers suggest that biometric-based technologies should be used in combination with other methods and not solely relied upon [15]. The disadvantages of biometric methods also include the requirement for additional equipment, as well as the difficulty or impossibility of changing the biometric settings once they are set [11]. Token-based authentication is widely used in various applications, such as e-banking [12], and is typically combined with knowledge-based authentication, such as passwords.

This paper presents a systematic literature review of recent research on the use of immersive technologies for user authentication in virtual reality, augmented reality, and mixed

reality. Specifically, we reviewed papers published within the past 16 years to investigate the various types of user authentication methods explored and utilized in immersive technology applications. Our aim is to contribute to the existing knowledge in this field by incorporating state-of-the-art methods and techniques found in the literature. Our main contributions can be summarized as follows:

- We provide a comprehensive consolidation of immersive technologies for user authentication in virtual, augmented and mixed reality (compared to previous work).
- The present work is the first systematic review that tried to identify authentication methods related to VR, AR, and MR, while limiting the scope of the research to papers presenting immersive technologies as a solution.
- In addition to grouping authentication methods into categories, we also focus on the success and error rate, the tools/devices/techniques used, and the main strengths and weaknesses of each method.

The remainder of the paper is organized as follows: Section 2 presents related work in the field of this review paper and the differences between them and our work. Section 3 outlines the research methodology, which includes the scope and aim of this systematic literature review (SLR), the research questions, the search strategy, and the eligibility criteria. Section 4 presents the findings and analysis of the review, organized by user authentication methods. Finally, Section 5 discusses the results in the context of the research conducted in the field.

2. Related Work

In recent years, research on the use of immersive technologies for user authentication has focused on developing novel methods that ensure access security, privacy, and information protection. User authentication mechanisms help prevent various cybersecurity threats, but also address major privacy concerns, as analyzed by Odeleye et al. [16] in their work. Various schemes are used in immersive technologies, which can be categorized into knowledge-based (requiring information already known to the user, such as passwords or PINs), biometric-based (using characteristics of the user, such as gestures, eye gaze, face or iris identification), possession-based (using an object such as a card, a token or a One-Time Password—OTP), or combinations of the above methods.

Only a few literature reviews were found that consolidate recent research and applications in the field of immersive technologies for authentication purposes. The literature review conducted by Jones et al. [17] in 2021 included 29 papers on VR authentication. This review also categorizes the papers by type of authentication, to knowledge-based, biometric data and multi-model authentication, adding a category of Gaze-based authentication. The authors found eight papers with knowledge-based authentication techniques with a PIN or alphanumeric passwords, which are characterized as of high usability, but not high security due to shoulder-surfing risks. Fifteen papers refer to biometric authentication methods, including electroencephalogram, body motion (for example, throwing a ball) and electrooculography. Five papers refer to gaze-based authentication methods, as ones of combining knowledge-based as well as biometric techniques. In principle, such methods process eye gaze of the user and can be combined with password or PIN authentication methods. These technologies track eye movements. Finally, only one paper [18] addressed to multi-model authentication incorporating the use of passwords (on a Rubik's cube) combined with gesture information.

In 2022, Duezguen et al. [7] made a review of published work in the field, focusing only on knowledge-based authentication applications in augmented reality environments (therefore not including other types of authentication, neither VR nor mixed reality). Their review included 18 papers, which incorporated 31 authentication schemes and was concentrated on the type of user knowledge/secret being used, system requirement in terms of equipment (mainly for the head mounted devices HMD), security considerations and usability considerations. In terms of equipment, the reviewed papers utilized Google Glass (45% of the papers), Microsoft HoloLens (13%) and Epson Moverio BT-200 (6%), while

the rest of the articles reviewed did not provide specific equipment information. User input for providing information (e.g., passwords, PINs, etc.) includexd touch pad, speech recognition, gyroscope and accelerometer, eye tracking devices, gesture tracking devices, camera, and electrooculography (EOG). Apparently, these are not all knowledge-based input devices, but they were mentioned within the researched papers, since few of them considered multiple authentication methods. The types of knowledge/secrets identified in this review included text passwords, graphical representations of passwords, haptic designs, semantic-knowledge elements/passwords and combined/two-factor elements. In terms of security in the form of resistance against recording and shoulder-surfing, the included solutions utilized randomized keypads, without PIN repetitions, most of which are visible only by the user and depend on the input method. Overall, security was mainly considered only at a PIN level according to the aforementioned literature review [7].

In addition, the systematic literature review (SLR) conducted by Heruatmadja et al. [19] focused on biometric authentication research publications for virtual reality environments. This study answered research questions such as which biometrics and HMDs, but also examined which machine learning models are used, and how accurate individual identification is. Finally, another closely related work on AR and VR authentication was conducted by Stephenson et al. [20]. However, this work is not a systematic literate review, and it focuses on surveying users and developers about their experience with current authentication methods used on AR/VR with the ultimate goal of evaluating these authentication schemes.

To the best of our knowledge, the literature reviews conducted thus far provide a comprehensive consolidation of authentication research papers, although they are limited to either AR [7] or VR [17,19] applications or restrict the research to knowledge-based authentication [7] and biometric authentication [19]. In this review, we evaluated all papers related to VR, AR and MR as well as all authentication methods, while limiting the scope of the research to papers presenting immersive technologies (AR, VR, and MR) for user authentication in immersive applications. Therefore, the present work provides a more holistic and focused perspective compared to the above referenced works.

3. Research Methodology

This section includes a description of the Systematic Literature Review (SLR) method and the methodological procedures followed to conduct the review and the analysis of articles studying the use of immersive technologies in user authentication.

3.1. Research Scope

The scientific field of the present work is immersive technologies, a division of computer science. As mentioned in the introduction, immersive technologies include virtual reality (VR) and augmented reality (AR) components and the term immersive is used to describe the integration of a virtual component in a real environment, producing a blended reality for the human/user. In addition, the use of immersive technologies is limited to user authentication and the applications specifically developed and used in this purpose. The type of data used in this research is secondary information, retrieved from published research, referring to empirical applications (in this respect, excluding theoretical publications or theories in the topic area). The scope of the present research, i.e., the use of immersive technologies for user authentication in immersive applications, is depicted in Figure 1.

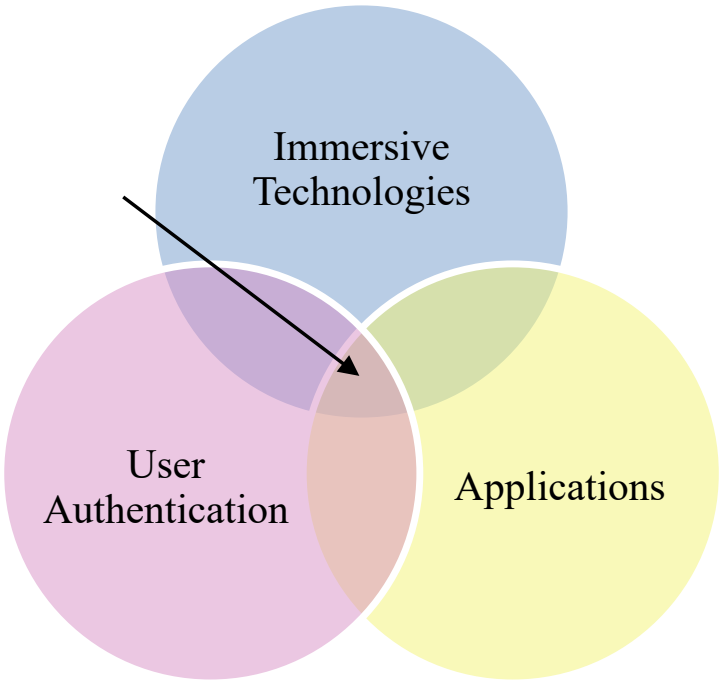

Figure 1. Scope of this research.

3.2. Research Aim and Research Question

Although research in the field of immersive technologies has been considerably growing during the last years, there is a scarcity of works consolidating the underlined methods and tools used to assure user authentication within this field. Therefore, the aim of the present analysis is to present a comprehensive and systematic bibliographic review of related work published during the last fifteen years regarding user authentication within the field of virtual reality, augmented reality and mixed reality.

The research questions which this analysis endeavors to answer are:

RQ1. Which are the state-of-the-art user authentication mechanisms based on immersive technology?
RQ2. What types of authentication schemes are mostly investigated in the reviewed literature?
RQ3. What is the success and error rate of the proposed schemes?
RQ4. Which tools/devices/techniques are elaborated in these methods?
RQ5. What are the main strengths and weaknesses of each of these methods?

3.3. SLR Method

For accomplishment of the research aims of this paper, the method of SLR was selected. SLR is currently used in a variety of research fields and research subjects, including computer science and technology [21]. It is a systematic, stand-alone process, following certain steps and methods, explicit and comprehensive [22]. Taking into account these features, SLR, and more specifically the PRISMA methodology [23], was chosen as the research method of this paper, targeting to include all published articles related to the research question based on a bias-free process and predefined criteria. The transparency provided by SLR provides the basis for developing a process and results of the required quality standards. It needs, however, to be mentioned at this point that SLR also has certain limitations, as the search for material is made in specific databases, leading to the risk of missing a part of the published research. In the following sections, all the steps of the research and analysis are described.

The process steps in this paper include the definition of the research scope, the research strategy (including the selection of the data sources, research string and selection criteria), the initial screening of titles and abstracts, the extraction of the relevant information,

the analysis and synthesis of the information and the composition of the final report of the study [24].

3.4. Search Strategy and Eligibility Criteria

The search strategy for conducting the SLR included the selection of the data sources, the formation of the search string and the inclusion/exclusion criteria. Searching for published articles was performed in the Scopus database, as it is the most comprehensive database in the field of the present research, including the main volume of published material.

The research string for the database search was the following:

```
TITLE-ABS-KEY ( ( immersive AND technologies ) OR ( augmented AND
reality) OR ( extended AND reality ) OR ( virtual AND reality ) OR
       ( mixed AND reality ) ) AND TITLE ( authentication )
```

The selection/inclusion criteria for the articles were the language (English) and availability of the whole article (not only parts). Reviews were not included in the reviewed articles. In addition, during the search process, it was decided that articles related to the use of immersive technologies for user authentication in immersive applications are only included (excluding in this respect articles which referred to use of immersive technologies for user authentication in other types of applications, as, for example, in e-banking and also excluding other types of identification such as passwords in immersive applications).

The first criterion (language) was set in the Scopus search engine, the rest of the criteria were applied during article screening.

4. Results

4.1. Selection of Relevant Publications

A total of 167 research publications were initially retrieved from the Scopus search in September 2023. In the initial screening of the papers, 78 were accepted as within the scope of the research and 89 were rejected. The excluded papers, at this stage, refer to:

- 28 papers which were only partly within the scope of the research,
- 27 papers which were not related to immersive technologies (for example, some were mentioning virtual machines),
- 23 papers which were out of the scope of the research,
- 3 papers which were not related to user authentication,
- 6 papers which were excluded as literature reviews, and
- 2 papers which were rejected as lecture notes and book chapters.

In the next stage, the 78 initially accepted papers were further evaluated (using full-text), and the following were found to be excluded:

- 12 papers related to research on the use of immersive technologies in authentication (only, but for general applications, not for immersive applications).
- 15 papers related to technologies for authentication in immersive applications (but not immersive technologies).
- 14 papers were excluded for low quality, as they did not provide adequate information for the process and results.
- 1 paper was not accessible online.

From this evaluation process, 36 research publications were ultimately accepted for further analysis in the current systematic literature review. The source selection process is shown in Figure 2. Furthermore, Figure 3 shows the distribution of these papers by year, and as you can see, most of them were published after 2019.

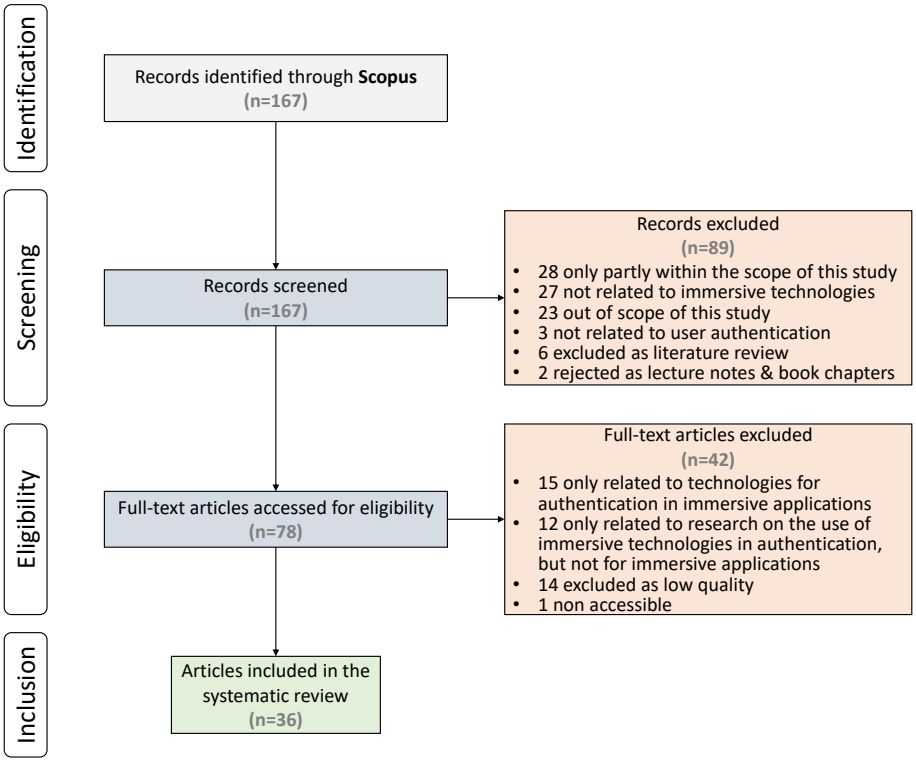

Figure 2. Source selection process from the Scopus search engine (PRISMA flowchart).

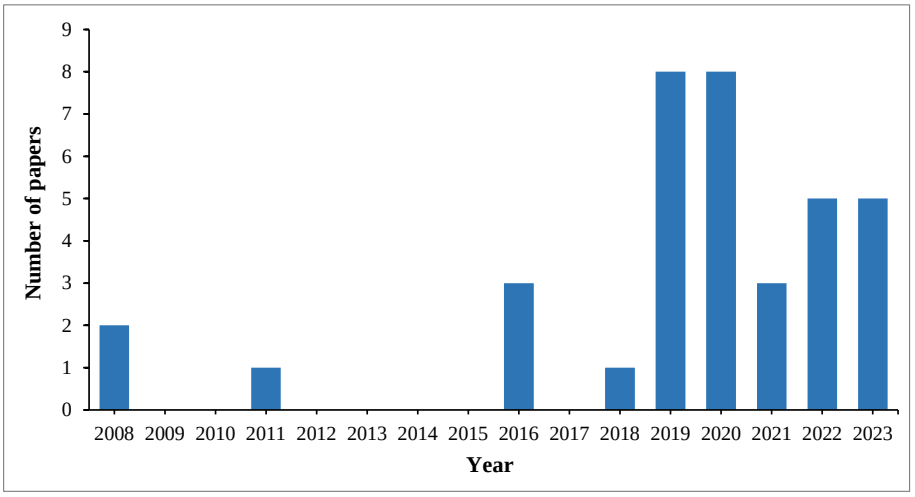

Figure 3. Yearly distribution of papers included in our systematic review.

4.2. Immersive Technology-Based Authentication Methods

In line with prior literature and relevant research [7,17], this literature review follows the approach of categorizing reviewed papers by type of authentication. As discussed earlier, the primary types of user authentication are knowledge-based and biometric methods, as well as their combination. Additionally, in the current analysis, a motion-based type of authentication was identified, which is classified under biometric methods. Of the total 36 papers reviewed, 6 (17%) contained knowledge-based methods, 19 (53%) contained biometric methods and 11 (30%) contained multi-factor methods (Figure 4). Token-based methods (authentication with something that the user possesses, such as a card, a token or a one-time-password (OTP)) were found only in combination with other methods [25].

The analysis of the reviewed papers follows this pattern, providing enrollment and authentication procedures, where available. The characteristics and data chart for each of the 36 research papers included in the systematic review are presented in Table 1.

Table 1. Research papers included in the systematic review according to their characteristics.

Reference (RQ1)	Year	Type of Authentication (RQ2)	System Name	Immersive Technology	User Sample Size	Success Rate (RQ3)	Error Rate/Attack Success (RQ3)	Tools/Hardware Used (RQ4)	Main Strengths and Weaknesses (RQ5)
Knowledge-based methods									
Micallef et al. [26]	2011	Knowledge-based (avatar)		VR		100%		Not applicable	Ability of participants to recall information associated with their Avatar
George [27]	2019	Knowledge-based (3D graphical password)	RoomLock	VR	48		0% post hoc attacks 12.5% immediate attacks 12.5% shoulder surfing rate	Oculus Go HTC VIVE controller	High level of security, usability, and memorability
Mathis et al. [15]	2020	Knowledge-based (Rubik cube)	RubikAuth	VR	23	98.91%	1.48% attack 0% eye gaze 2.22% head pose	HTC VIVE controller and HMD	Controller tapping is significantly faster than head pose and eye gaze
Mathis et al. [13]	2021	Knowledge-based (Rubik cube)	RubikAuth	VR	15 + 23	90.80% correct entries		HTC VIVE controller and HMD	3D passwords in a cube offer large password space, and high resistance of RubikAuth to observation attacks
Kumar et al. [28]	2022	Knowledge-based (body-centric graphical password)	PassWalk	MR (AR, VR)	22		1.1% observation attacks	Microsoft HoloLens 1	A keyboard-less authentication system that offers a new combination of multi-modal inputs, i.e., head-gazes and footsteps, highly accurate, secure to observation attacks (98.9% resistance)
Wang et al. [29]	2023	Knowledge-based (3D graphical password)		VR	36	97.78% enter accuracy 97.92% memory accuracy	0% shoulder surfing attack 4.17% MITR (Man-In-The-Room) attack	HTC VIVE Pro	Utilization of a dynamic combination of multi-attribute authentication methods (3D objects and their attributes) for VR
Biometric methods									
Orozco et al. [30]	2008	Biometric (haptic based)		VR	45	86.6–90.9%	0.4% false identification	Haptic interface (not specified)	Haptic methods that will become more common in the near feature
Zhang et al. [31]	2016	Biometric (facial recognition)		VR	30	63–100% according to criteria		Depth camera (not specified)	Macroscopic authentication is more suitable for virtual proctoring than microscopic authentication
Zhou et al. [32]	2016	Biometric (facial recognition)		VR		63–100% according to criteria		Camera (not specified)	The virtual proctor can provide high accuracy in detecting suspicious behavior—the value of the threshold needs to be appropriately configured
Miller et al. [33]	2019	Biometric (ball throwing)		VR	33	80% accuracy 84.36% attack resistance		Oculus Quest, HTC VIVE, and HTC VIVE Cosmos	Protection against session hijacking and external intruder detection
Ajit et al. [34]	2019	Biometric (ball throwing)		VR	33	93.03%		HTC VIVE	Study provides results for position and orientation—using orientation only provides the best results
Kupin et al. [35]	2019	Biometric (ball throwing)		VR	14	90% to 92.86%		HTC VIVE headset and hand controllers	Work can be extended with more controllers, not unique trajectories and cognitive components

Table 1. *Cont.*

Reference (RQ1)	Year	Type of Authentication (RQ2)	System Name	Immersive Technology	User Sample Size	Success Rate (RQ3)	Error Rate/Attack Success (RQ3)	Tools/Hardware Used (RQ4)	Main Strengths and Weaknesses (RQ5)
Li et al. [36]	2019	Biometric (brain signal)		VR	32	79.22%, 79.55%, 80.91% for different methods		8-channel EEG sensors 2 reference sensors with Cyton board	No significant difference between the accuracy rates for VR and Non-VR EEG data
Islam et al. [37]	2019	Biometric (breathing patterns)		VR	6	100%		Microwave Doppler radar	A valuable method to overcome limitations of existing traditional authentication systems
John et al. [38]	2019	Biometric (eye gaze)		VR	5	80%		Pupil Labs eye tracker (Pupil Pro 2016, 30 Hz)	Easy-to-use method with a good ease/security trade-off
Miller et al. [39]	2020	Biometric (ball throwing)		VR	41	90% and higher		Oculus Quest, HTC VIVE, and HTC VIVE Cosmos	High within-system accuracy—cross-system accuracy is lower
John et al. [40]	2020	Biometric (eye gaze)		VR	15	60.1% true positive rate 39.9% false negative rate		Pupil Labs Pro glasses-based eye tracker	Recognition rate from 79% dropped to 7% with defocus
Sivasamy et al. [41]	2020	Biometric (head movement)	VRCAuth	VR	40 + 48	99.6–99.98%		HMD (not specified) with accelerometer and gyroscope	LMT and PART classifiers/algorithms work more effectivelu and efficiently
Bhalla et al. [42]	2021	Biometric (head movement)	MoveAR	AR	5	92.675% accuracy score	11% EER	Microsoft HoloLens	It is possible to authenticate AR head-mounted display users from their head movements and gestures
Lohr et al. [43]	2022	Biometric (eye gaze)	EKYT (Eye Know You Too)	MR (AR, VR)	59	1-in-10,000 false accept. rate	3.66% EER on a reading task with 5 s long	EyeLink 1000 eye tracker	The first to approach a level of authentication performance using eye gaze acceptable for real-world use
Islam et al. [44]	2022	Biometric (breathing patterns)		VR	20	98.33% and 97.5% for single- and two-subject experiments		Microwave Doppler radar	This work demonstrates its efficacy in the presence of two equidistant subjects in the radar field of view, a major hurdle for practical authentication applications
Chang et al. [45]	2022	Biometric (ultrasonic-based mapping—ear)	MetaEar	AR	17	96.48% average accuracy		Smartphone (Android)	Modeling and authenticating human ear ERTF (Ear Related Transfer Function) biometrics using FMCW (Frequency-Modulated Continuous Wave) ultrasonics
Jang et al. [46]	2023	Biometric (brain signals)		AR	20	100% accuracy using LSVM and KNN models		Microsoft HoloLens 2	Demonstrates the feasibility of using EEG-based event-related potentials (ERPs) in combination with augmented reality (AR) glasses for highly secure and reliable biometric authentication
Seok et al. [47]	2023	Biometric (Photo-plethysmogram)		VR	35	97.23% accuracy	3.57% EER	Photoplethysmogram sensor	Noise reduction and information preservation through multicycle averaging; system accuracy not affected by the number of enrolled subjects; potential significant performance deterioration when using noisy data

Table 1. *Cont.*

Reference (RQ1)	Year	Type of Authentication (RQ2)	System Name	Immersive Technology	User Sample Size	Success Rate (RQ3)	Error Rate/Attack Success (RQ3)	Tools/Hardware Used (RQ4)	Main Strengths and Weaknesses (RQ5)
Wang et al. [48]	2023	Biometric (ultrasonic-based mapping—head)		VR	30	98.87% (99.33% for the mobile phone VR)		Meta Quest (Samsung Galaxy S8)	Low-effort authentication system leveraging head-reverberated sounds, for current VR headsets, without kernel or hardware modifications
Multi-factor methods									
Alsulaiman et al. [49]	2008	Multi-factor		VR	30			Any input device: mouse, keyboard, fingerprint scanner, iris scanner, stylus, card reader, and microphone	High user acceptance and huge password space
Gaebel et al. [8]	2016	Multi-factor	LGTM	AR	100	1m: 60–100% 2m: 30–75% 3m: 23–50%	1m: 0.722m (mean err.) 2m:1.654m (mean err.) 3m: 2.321m (mean err.)	AR headsets SpotFi	Wireless localization can be a useful tool for authentication
Lu et al. [50]	2018	Multi-factor		VR	100		0.6% EER (without spoofing attack) 3.4% EER (with spoofing)	Leap Motion controller	Hand gesture has a potential in user authentication
Funk et al. [51]	2019	Multi-factor	LookUnlock	AR	15		3.7–5.9%	HMD (not specified)	High level of resistance to shoulder-surfing attacks
Zhu et al. [14]	2020	Multi-factor	BlinKey	VR	50		14.6% EER	HTC VIVE Pro with a Pupil Labs eye tracker	Robust against various types of attacks—high usability
Mathis et al. [52]	2020	Multi-factor	RubikBiom	VR	23	98.91%		HTC VIVE (2160 × 1200 px) and SteamVR Plugin for controller communication	Knowledge-driven behavioral biometric authentication increases security
Lu et al. [53]	2020	Multi-factor		VR	10	Not mentioned		Not mentioned	The user can authenticate the VR system while performing another task simultaneously
Wazir et al. [54]	2020	Multi-factor		AR	20 + 20	50%		Smartphone	Satisfactory results in terms of ease to use, interaction, effectiveness, and security
Nahar et al. [12]	2021	Multi-factor		MR (AR, VR)	20	84.36%		IRIS imaging device (not specified)	System can be used in surgical telepresence
Abdelrahman et al. [11]	2022	Multi-factor	CueVR	VR	20		$1/10^n$ to $1/5^n$ successful attacks (n = PIN length)	HTC VIVE Pro headset, using the SteamVR plugin Laserpointer Trackpad Motion Controller	Among the 3 pointing methods Laserpointer, two-handed Trackpad and two-handed Motion Controller, the Laserpointer was the least secure input method, but the most preferred by the users
Yang et al. [55]	2023	Multi-factor		VR	iris public datasets			Raspberry Pi 4B for simulation	A two-factor authentication framework which guarantees the virtual–physical traceability that tracks an avatar in virtual space to its manipulator in the physical world

Note: EER—Equal Error Rate.

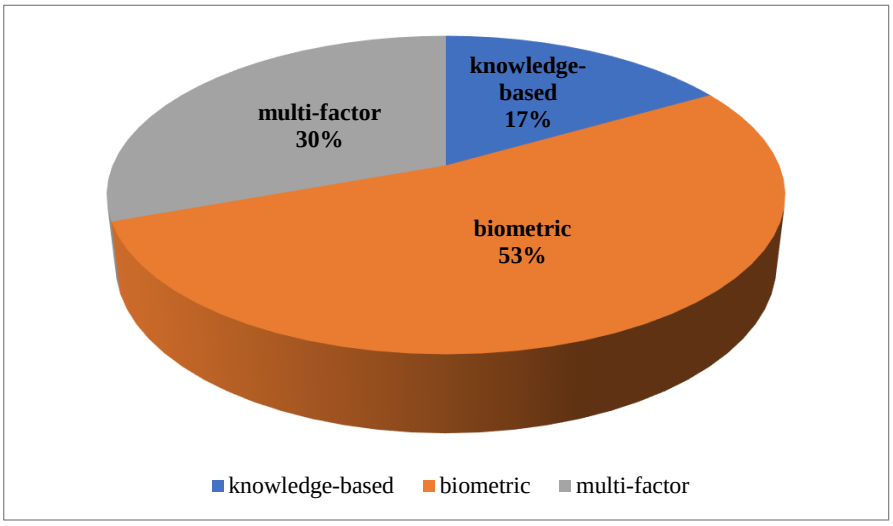

Figure 4. Distribution of papers according to the user authentication method.

4.2.1. Knowledge-Based Methods

Knowledge-based methods typically require the user to enter a password or a PIN that they know and is secret. In the present review, we found four papers that exclusively employed knowledge-based authentication methods; two of them use a Rubik cube, one a 3D graphical password, and one an avatar.

Rubik cube: Mathis et al., in [13,15,52], use a version of a Rubik cube for authentication in VR applications. We note, however, that RubikBiom [52] is classified as a multi-factor method in this review, as the authors describe it as "human behavioral biometrics collected during knowledge-based authentication". These schemes present to the user a cube ($3 \times 3 \times 3$ dimensions) with colored surfaces. In this respect, the method makes use of 2D grids on 3D objects. The user needs to select a digit–color combination to authenticate themself. Mathis et al. [13,52] developed a scheme (RubikAuth) based on the above colored-cube concept. In fact, their work in 2021 [13] is an extension of the previous 2020 [15] development. A matrix of nine digits is depicted on each of the five out of six surfaces of the cube (the sixth is not used) and each surface has a different color. The authentication process consists of the user selecting a digit-color combination. In Mathis et al. [13,15], the user points to the specific digit during the authentication process (from the desired color) with three different methods and presses a trigger button on the hand device to select it. The selection device (HTC VIVE controller) is held in the dominant hand, while the cube pose is controlled by the non-dominant hand (with an HTC VIVE controller). The concept has three modes: the first uses eye gaze to point the desired digit (they use a prefab called VRGazeTrail enabled by Tobii Pro VR SDK) that identifies user gaze at the digit. The second pointing method is the head pose pointing technique, for which the head position is identified as it is linked to an HTC VIVE HMD and tracked by an HTC VIVE Lighthouse tracking system. The third pointing method is performed with a controller, with the dominant hand, using the SteamVR Plugin.

In Mathis et al. [15], hand movement-related data are collected from 23 users. The system is evaluated with 15 users regarding security and with 23 users for usability, and shows high security levels (successful attack rate 1.48%). The evaluation process (13 participants) in [13] shows that the accuracy of the system is 90.80% on average, without significant differences among different pointing methods. Regarding speed, the fastest enter mode is the pointing method, while the other two do not differ significantly from one another. Security strengths according to the authors include a large PIN space, quick access to the target digits with minimum movements, difficulty for attackers who need to watch both hands of the user, and ease of use.

Graphical passwords: Another application of knowledge-based authentication in immersive virtual reality and in the real world is developed by George et al. [27] by selecting objects in a virtual room to create a 3D graphical password. Users point to a predefined number of objects (four objects in the prototype) in a virtual room; selection should be in the correct order. Selection of objects is performed by pointing the object with a laser and pressing a button. A visual path in the form of a blue line connecting the selected objects is presented to the user. Users are allowed selectiion of the same object more than once, but not consecutively. If the attempt is successful, the blue line turns to green upon completion, or it turns to red if the attempt does not succeed. In addition, haptic feedback is provided in the form of controller vibration (two short times for success and two slow times for failure). The system is evaluated for memorability with 27 users (100% success), for usability with a sample of 48 participants, for security against post hoc attacks with 15 participants and for security against immediate attacks with 25 participants. Post hoc attacks have a success rate of 0% and immediate attacks have a success rate of 12.5%.

Kumar et al. [28] introduce PassWalk to address the challenge of secure and user-friendly authentication on mobile headsets with limited interaction options. It introduces PassWalk, a novel keyboard-less authentication system that leverages multi-modal inputs. PassWalk combines the user's gaze and lateral foot movements to authenticate, allowing users the input of graphical passwords using digital overlays and physical objects. Through an evaluation involving 22 participants, including both legitimate users and attackers, PassWalk demonstrates high security, with only a 1.1% success rate for observation attacks, outperforming traditional virtual keyboard methods. Additionally, PassWalk reduces user workload and enhances security by introducing randomness into the authentication process. This paper presents a valuable contribution to the field by offering a usable and shoulder-surfing resistant authentication mechanism for mobile headsets, implemented on Microsoft Hololens 1.

Wang et al. [29] propose an authentication method in VR using dynamic combinations of 3D objects as a 3D graphical password against shoulder surfing and Man-In-The-Room (MITR) attacks. To evaluate their approach, they conduct three studies on usability (N = 36), memorability (N = 36) and security (N = 12). The first two studies reveal that the complexity of setting the password and authentication interface (within a certain range) has no significant impact on either usability or memorability, providing a 97.78% enter accuracy and a 97.92% memory accuracy. Accordingly, the security study reveals that high security could be achieved without specifying highly complex passwords and authentication objects, providing 0% for the shoulder surfing attacks and 4.17% for the MITR attacks.

Avatar: A novel method of knowledge-based authentication is presented by Micallef et al. [26] based on the creation of an avatar representing a fictitious person with pseudo-randomly assigned characteristics. The avatar undertakes the role of a known person with the user entering its features to the systems authentication's questions. This scheme overcomes the problem of attackers guessing the answers to questions like "What is your Mother's Maiden Name?" (and replaces them with questions like "What was your Avatar's secondary school?") as information of the avatar is only known to the user. The avatar's information is not connected to the user personally, but the user has a bond with the avatar, in an attempt to deal with psychological issues of using it. The user is presented with the avatar's profile when logging into the system as a method to maintain this bond.

The enrollment phase includes creation of the avatar, with a name, address, city and postcode, email address, phone number, birthday, occupation, maiden name and some additional information. The user can select the characteristics from a drop-down menu, while some information is created using Fake Name Generator. Then, the user fills in the personality characteristics (pets, vacation places, family, friends, etc.). The user can select questions for authentication or a list of features. At authentication phase, the user should correctly answer these questions in order to be authenticated. The authors do not provide usability and/or security testing results.

4.2.2. Biometric Methods

Biometric-based methods for user identification elaborate several biometric characteristics of the user, including iris scan, fingerprints, breathing patterns, tapping patterns, movement and more. In the present review, most of the papers make use of this method of authentication, as it is claimed to have high security levels, based on its nature that makes attacks harder and shoulder surfing not possible. On the other hand, biometric authentication methods are often approached with skepticism by users, who do not wish to disclose sensitive personal, biometric information. Another weakness of these methods is that information (biometric data/passwords) cannot be revoked or altered (in the way that a user can change a textual password).

In the present review, we found thirteen papers that employed biometric authentication methods, two of them are based on head movement/motion, two on eye gaze, four on ball throwing, one on brain signal, one on breathing patterns, two on facial recognition, and one on haptic.

Head movement: The work of Bhalla et al. [42] and Sivasamy et al. [41] uses head movement for user authentication. Both systems are based data regarding position, movement, and rotation of the head, forming unique motion patterns, of the user.

Bhalla et al. [42] provide a scheme for a continuous biometric authentication system, which uses the different ways people move their heads and interrelate with AR objects and virtual environments. The aim of their system was to develop a model which authenticates the user and distinguishes the legitimate one from a potential attack, based on signals created with interaction they have with the environment and their head movements.

The system uses the HoloLens headset and two types of data: from IMU (inertial measurement unit consisting of an accelerometer, gyroscope, and magnetometer), for the physical features of the user, and from an AR headset, for the interaction of the user with the environment. There are two types of processing, according to the different input: A time series with raw time series input and a feature-based model for the computation of individual feature vectors.

Their evaluation of the system compares various methods including k-Nearest Neighbors, Random Forest, Support Vector Machine (SVM), and Bag of Symbolic-Fourier-Approximation Symbols (BOSS), a balanced accuracy score of 92.675% and an Equal Error Rate of 11% with the participation of five users.

Sivasamy et al. [41] use inertial sensors (accelerometer and gyroscope) on the VR headset, to measure position, direction and rotation of the user head in the 3D space. Two types of data are also collected: position–rotation (driving simulator dataset) and position–quaternion (head tracking). The system collects 90 features in those datasets classified into three categories: (a) movement direction, (b) movement magnitude for abrupt head- movements, and (c) movement time as duration between head movements. The system is evaluated with 40 users for driving behavior and 48 users watching videos. Comparison of methods (Naive Bayes, PART, Logistic functions, Multilayer Perception and LMT) LMT has the highest accuracy for the driving set 99.6% and PART for the video watching set 99.98%).

Eye gaze: John et al. [38,40] use eye gaze information, with defocus/subtraction of iris information. Iris recognition is one of the best identifiers for a person, being unique for each person. Therefore, it is highly sensitive information that may be vulnerable, and its use or misuse is a major concern. In John et al. [40], defocus methodology is a Gaussian blur. The researchers evaluate the system with a sample of 15 users. They use a Pupil Labs Pro glasses-based eye tracker to collect eye tracking data and remove frames with eye blinks and motion. They also use virtual avatars for the eye gaze detection. Evaluation results showed that defocus deteriorates correct recognition rate and eye contact of avatars. An element in the work of John et al. [38] adds the possibility to the user to toggle iris track on and off, according to the specific use so as to choose whether to perform iris defocus to prevent attacks by hackers. The iris defocus retains gaze estimation level, while it reduces iris authentication.

Lohr et al. [43] introduce EKYT (Eye Know You Too), a novel DenseNet-based architecture for eye movement biometrics (EMB), and evaluates it on the GazeBase dataset, which contains high-quality eye movement data from 322 subjects. The study primarily focuses on authentication scenarios, measuring performance with an Equal Error Rate (EER) metric. Notably, their model achieves an impressive 3.66% EER when using just 5 s of eye movement data for authentication, a time frame comparable to entering a four-digit PIN. The authors claim that their work stands out as the first EMB study to achieve a 5% False Rejection Rate (FRR) at a False Acceptance Rate (FAR) of 10^{-4} with only 30 s of eye movement data, indicating its potential for real-world authentication. Additionally, it explores the feasibility of EMB at low sampling rates, down to 50 Hz, making it suitable for VR/AR devices. Lastly, it introduces a modern convolutional architecture for EMB, advancing the state-of-the-art in eye-based biometric authentication.

Ball throwing: Miller et al. [33,39], Ajit et al. [34] and Kupin et al. [35] investigate user movement as an authentication method, tracing the movement of the user when throwing a ball in a VR environment. Miller et al. [39] use three VR systems, Oculus Quest, HTC VIVE, and HTC VIVE Cosmos and a sample of 41 users (from a sample of 46, excluding left-handed users). The users have to lift one ball from the pedestal and throw it to a predefined target in the VR environment, using each one of the VR systems. Enrollment is considered as the training phase, which is compared to test use after the training with 10 training samples and 10 test samples per user. Comparisons are made on the features of the trajectories of the movement as within system (train session with second session) and cross-system (among the three used systems) with matches of the left controller and right controller orientations and headset position. Within-system comparisons show that accuracy above 0.90. In the cross-system accuracy, the VIVE system scores better than the other two at 0.85.

Settings for the research of the Miller et al. [33] study are similar with a training session and an authentication session, using HTC VIVE and a NVIDIA GTX systems in a sample of 33 users. The authentication phase is performed with users providing a classic PIN and then being authenticated by performing a ball throw. Matches of headset and controller position and orientation at this phase against training phase in the form of distances of the trajectories are used to authenticate the user and the system announced to the user whether they are identified and granted permission or rejected.

Similarly, Ajit et al. [34] use the motion and position of left hand and right hand controllers and the headset (HTC VIVE system) to authenticate the user. A sample of 33 users is used in two sessions, 10 throws in a training session and 10 throws in an authentication session 24 h later. Authentication success is estimated by calculating the proximity between training throw trajectories and test ones. The tests reach a maximum accuracy of 93.03% for the matches between training and test data, using the nearest neighbor matching algorithm and an HTC VIVE system.

Kupin et al. [35] use a similar setting for ball throwing activity in a VR environment. They match a 3D trajectory of the dominant hand movement of a user with a head mounted VR system. They use a sample of 14 users throwing a ball towards a target in a VR setting, recording s maximum accuracy of 92.86% after comparisons with metrics of a library with 10 trajectories of participants in the training session.

Brain signal: Li et al. [36] use biometric data from brain signals to authenticate the user, in a VR and a natural environment. The researchers use electroencephalography (EEG) to record brain signals of a sample of 32 volunteer participants. The users watch videos in a virtual environment (with a VR headset) and non-virtual environment (using a laptop) while they start from a resting stage. The brain wave data collection device is an EEG with eight channel sensors and e reference sensors with a Cyton board. Authentication test results show an accuracy rate of 75.08% and 71.66% for the Non-VR and VR environments, respectively, when a Statistical Parameters of Signals (SPS) method is used, an accuracy rate of 76.73% and 73.68% when an Autoregressive (AR) model is used and 70.92% for both

VR and non-VR when a combination of SPS and the Power Spectral Density (PSD) method is used. Better accuracy rate (80.91%) results are found for 10 s length EEG data with a 75% session overlapping when using the AR and SPS model combination.

Jang et al. [46] propose a biometric authentication system using EEG and AR glasses. The system leverages the rapid serial visual presentation (RSVP) paradigm with photographs of familiar and unfamiliar individuals to detect event-related potentials (ERPs). The study demonstrates that the amplitude of certain ERPs, such as P3a, P3b, and late positive potential (LPP), is higher when subjects are exposed to familiar photographs. Classification results using machine learning models achieve perfect accuracy, highlighting the potential of EEG-based biometric authentication, especially in high-security applications. The authors suggest that EEG could be combined with traditional biometrics to create hybrid systems. The use of AR glasses makes EEG-based authentication portable and mobile, with potential applications in fields such as medicine, education, and the military.

Breathing patterns: Islam et al. [37] base their research for a continuous authentication on respiration patterns, which are distinct for each individual. Measurements of non-contact cardio-respiratory motion can provide an accurate measurement of cardiopulmonary activity, different among people. They use a Doppler radar motion-sensing transceiver to track and transmit a continuous microwave signal and demodulate the echo from the target and dynamic segmentation methods to identify the subjects from their breathing patterns. Experimental trials with six participants result in a 100% classification accuracy overall success rate.

Islam et al. [44] elaborate on [37] which can only authenticate a single subject, and they present a pioneering approach to identifying individuals in scenarios involving two equidistant subjects in front of a radar system. The proposed scheme adapts the Independent Component Analysis with the Joint Approximation of Diagonalization of Eigenmatrices (ICA-JADE) method and introduces a novel dynamic segmentation algorithm to extract distinctive respiratory features. Machine learning classifiers, including k-nearest neighbor (KNN) and support vector machine (SVM), are employed to achieve high accuracy rates in subject authentication. Their work is notable for successfully implementing non-contact identity authentication for two subjects within a radar antenna pattern, expanding the possibilities of radar-based authentication systems. In the experiments conducted for this method, 20 different participants are used to assess the feasibility of identifying individuals when two equidistant subjects are present. The results demonstrate impressive accuracy rates, with a 97.5% success rate for two-subject experiments and a 98.33% success rate for single-subject experiments.

Facial recognition: Facial recognition techniques for virtual/remote proctoring are used by Zhang et al. [31] and Zhou et al. [32].

Zhang et al. [31] experiment with authentication via facial recognition/expressions and head motions, using virtual proctoring. Virtual proctors have similar functionality with that of physical/in-person ones, having to administer a test and validate the identity of the students/people taking the test. Virtual proctors authenticate users using biometric information such as facial control, fingerprint, iris or retina, and hand geometry. Macroscopic authentication (such as face recognition) is more suitable for virtual proctoring settings compared to microscopic authentication (e.g., iris scan).

The authors of [31] describe a prototype for facial recognition in a virtual laboratory of a mechanical engineering course. For the purposes of proctoring, the authors define two types of "suspicious" behaviors based on head movement, namely "rotating head" (movement in X or Y axis) and "moving relative to webcam" (movement in X, Y and/or Z axes). Their system performs facial recognition in terms of suspicious behaviors of the students. They evaluate the system with the participation of 30 students in a test of six questions. Real-time face tracking is captured with a video with 15 frames per second. Analysis is based on threshold criteria for rotation (in degrees) and movement (in millimeters) and cheating behavior is identified if students record actions above the thresholds. System accuracy

is 100% for rotation threshold $\leq |3|$ and movement $\leq |10|$, accuracy $\leq 91\%$ for rotation threshold $\leq |5|$ and movement $\leq |20|$, accuracy $\leq 63\%$ for rotation threshold $\leq |10|$ and movement $\leq |40|$ and accuracy $\leq 30\%$ for rotation threshold $\geq |10|$ and any movement.

Zhou et al. [32] implement a virtual laboratory (VL) and apply face recognition methods for remote proctoring. The design of the system has a registration, where the picture of the user is taken and stored. In the testing phase, as a first time matching, the user is allowed entering the VL on a successful match of face recognition or failing to enter otherwise. During examination in the VL, suspicious movements are identified in a manner similar to that of [31], as rotations and movement relative to the camera, with similar accuracy rates.

Haptic-based authentication: Orozco et al. [30] develop a haptic-based authentication system which uses haptic biometric information to authenticate the user in three types of tasks: dialing from a virtual phone, signing a virtual check and solving a virtual maze problem. Their system comprises main subsystems of data acquisition, feature creation and selection and evaluation.

In the data acquisition phase, the process creates a profile database during a 4-week period with the use of different haptic devices. Data parameters include the haptic output in terms of e-axes position, orientation), time, force and torque. For the creation of the profile database, users dial seven numbers using a virtual telephone and record data containing 3D world coordinates, the force and torque of the stylus and the rotation ankle of the pen. The virtual check signature task records parameters related to the way of signing in terms of pen position, force exerted, and velocity (not the signature itself). The maze problem-solving task records hand movements (the maze is on a 3D side of a 3D cube and the success in solving the maze is not relevant).

Feature selection is based on Gaussian distribution functions. For feature extraction, the force and torque are represented in 3D world axes resulting in six distinct distributions. For feature clustering, a k-means algorithm is applied. The system is further evolved using neural networks technology, with five features as vector dimensions and a sixth representing the identity of the user. Authentication process compares database features with user test features. Signature authentication tests are conducted with 16 users, providing 144 signatures (the overall number of users is 45). In the virtual signature task authentication, success is defined in cases where the test signature features matches at least two of the database reference samples. The system evaluation shows that there is a probability of successful virtual signature verification of 92% at a False Acceptance Rate of 25%.

Ultrasonic-based mapping: Chang et al. [45] introduce MetaEar, an innovative system for continuous biometric authentication using ultrasonic signals sent by head-mounted devices to the human ear. The system leverages the Ear Related Transfer Function (ERTF) to model the unique biometrics of the human ear, including auricle and ear canal characteristics. These characteristics are extracted from the inaudible ultrasonic signals reflected from the ear and are used for user authentication. MetaEar addresses challenges related to static ear features, signal synchronization, and self-interference, proposing solutions such as differential denoising and modeling the ERTF. To ensure user security and prevent replay attacks, it employs a traditional SVM for one-class authentication, achieving an impressive average accuracy over 96.8%.

Wang et al. [48] introduce a novel approach to simplifying user authentication in VR headsets. By leveraging acoustic sensing, the system emits ultrasonic signals through the VR device's speakers, capturing unique biometric information based on the user's head size, skull shape, mass, and facial characteristics. These data are then analyzed using a Convolutional AutoEncoder (CAE) and a Convolutional Neural Network (CNN) to authenticate users. Despite challenges related to echo cancellation and hardware limitations, the system successfully distinguishes users, supports both single-user verification and multi-user identification, and implements security measures to prevent acoustic replay

attacks. In the performance evaluation of the system, two types of VR headset devices are tested: standalone VR (Meta Quest) and mobile phone VR (DESTEK V3 VR with a Samsung Galaxy S8 smartphone). The study includes 30 participants and considers various factors such as hair length, body weight, and environmental conditions. For single-user verification, the system achieves an average accuracy of 98.87% using a Convolutional AutoEncoder (CAE) and Convolutional Neural Network (CNN) model, significantly outperforming the use of CNN alone. In a multi-user scenario, the system maintains high performance, with a slight drop in accuracy as the number of registered users increases. The long-term study over 15 months demonstrates the system's robustness to practical variations, achieving an average accuracy of 98.22% using CAE-CNN compared to 68.87% with CNN alone. Tracking two participants over 8 months on two VR devices further confirms the system's effectiveness in providing daily VR authentication services, with only minor performance fluctuations due to varying participant conditions and environmental factors.

Photoplethysmogram: Seok et al. [47] present a novel approach to biometric authentication in the context of head-mounted displays for VR and metaverse applications. Instead of traditional input devices, the study explores the use of wrist-worn photoplethysmogram (PPG) sensors for non-intrusive and continuous authentication. The key innovation is the application of a one-dimensional Siamese network to identify individuals based on unique PPG characteristics. To enhance accuracy and reduce noise, a multicycle averaging method is employed. The authors evaluate the effectiveness of their approach by varying the number of cycles and demonstrate strong results, with an accuracy of 97.23%. The research highlights the potential of PPG as a biometric identifier and underscores the importance of continuous efforts in cybersecurity to ensure the safety of VR and metaverse applications beyond user authentication.

4.2.3. Multi-Factor Methods

Multi-factor methods use combined technologies to achieve a higher level of accuracy, authentication security and effectiveness of the AR and VR systems. Most of the papers use a combination of two technologies (mainly knowledge-based and biometric-based). For example, Nahar et al. [12] propose a token-based (one-time password) method combined with a biometric method (iris authentication process). Zhu et al. [14] combine different knowledge-based and biometric methods (eye blinking rhythms representing a password and pupil size variation). Similarly, Mathis, Khamis and Fawaz [52] also combine knowledge-based and biometric methods in RubikBiom authenticating users by password check on a 3D cube combined with hand movement biometric data. All the reviewed multi-factor combinations of methods are described in the next paragraphs.

In [50,53], the mixed methods include formation of graphical/motion passwords combined with biometric data. In a rather similar way, paper [54] elaborates the creation of doodles serving as passwords.

Y. Lu et al. [53] present a scheme combining the drawing of a 3D trajectory in an eyes-free interaction, measuring movement as a distance vector from the controller to user hand (dominant hand controller). The system has a registration and an authentication module. At the registration phase, users draw a trajectory representation of a password ten times. Feature vectors are formulated based on trajectory and motion. These are used to train the system and serve as input for prototype formation as a template. At the login (authentication) phase, the users are asked to draw the trajectory in a similar manner to the registration phase, and the system compares it to the template. The system is evaluated as a pilot with the participation of 10 users.

The same authors in another paper [50] present a multi-factor user authentication scheme combining knowledge-based and special metrics methods, with users shaping passwords in the air, in a VR environment. A total of 100 users participate, creating two accounts each. The users register to the accounts by writing in the air a password five times for each account (enrollment phase data), and they also provide a password for authentication (authentication phase data). Seven additional participants have the role

of impostors, making spoofing attacks. A group of 22 participants from the first sample of 100 are requested to enter the passwords in their account periodically in a duration of four weeks, making 10 sessions (for evaluating long-term stability of the used algorithm).

The matching procedure calculates the distance between the authentication phase password and the saved passwords, using velocity, acceleration and coordinates. The system also includes a hand geometry component (biometric data) capturing information for the length of each bone (except the wrist) and for the hand width. During authentication, participants should use the same hand for writing the password, as hand geometry is examined together with password features. Error rate scores for the combined method is below 2%.

Alsulaiman and Saddik [49] describe the development and evaluation of a user authentication system with a 3D password. The concept is that the user navigates in a virtual environment, interacting with several objects, creating a 3D password with these interactions. This application combines knowledge-based methods (recall of the objects to interact and their order), recognition and biometric methods (movement of the user that interacts with the objects or a fingerprint), letting the user select the method(s) to apply (for example, the user may not want to release biometric information, such as an iris scan, but use only information which the user is comfortable with).

At the enrollment stage, the user selects what type(s) of authentication methods will be used for the creation of the password and creates a password. At the authentication phase, the user must reproduce the password, replicating all information (recall- or knowledge-based) as well as biometric elements. For example, the user may choose to formulate the 3D password by (a) opening the door to a virtual room, (b) typing some alphanumeric characters on the computer keyboard in the room, e.g., "A" "B" "C", (c) providing a fingerprint and (d) lifting a virtual object of the virtual room.

The authors indicate that the design provides a considerably wide password space, larger than other password methods. For example, a number of 5 actions, interactions and inputs can create 265 passwords, and 10 action interactions and inputs have a password space of 2130. This enhances the security against attacks. Its application is suggested for critical servers, nuclear and military facilities (such organizations need the maximum level of security), airplanes/jetfighters.

The experimental result of the use with almost 30 users shows that most of them used textual passwords, and less than 5% used graphical passwords. However, the majority of the users agreed that 3D passwords have potential and acceptability.

Wazir et al. [54] develop a user authentication scheme for AR environments as a combination of knowledge-based and gesture methods. Their system elaborates real-time size and coordinate matching of doodles created by the users and serving as passwords. Creation of the doodles is performed by the users by touching a smartphone screen in the AR environment and moving it in the AR space drawing a doodle shape. This is used as a password. The user draws four doodles for registration (enrollment) and a test doodle for authentication. Saved information includes the space coordinates of the doodle as a dynamic array to be used for comparison–authentication purposes.

At the authentication phase, the users are asked to draw the doodle in the AR space, and matching with the saved prototypes is performed using size, placement, or content. If the compared doodles match by at least 80% in size, authentication moves to the next step, controlling for differences in 3D coordinates and calculating a sum of differences. If differences are within a predefined threshold, the user is authenticated. The scheme is evaluated using 20 participants with regard to ease of use, interactivity, usability, satisfaction, effectiveness, usefulness, utility and relevance. The authors report that the results indicate that the use of this AR technique is more satisfying for users than that of traditional methods, and it provides higher security levels.

Funk et al. [51] present LookUnlock, a method for user identification for HMDs, elaborating the use of passwords comprising spatial and virtual targets. The method is based on the tracking of head movement and spatial mapping and performs the authentication pro-

cess without an additional device. The application formulates passwords by using objects from the virtual and the physical world and their combination. It is, therefore, a combination of a knowledge-based method with special information. Spatial passwords are formed by data from a sequence of spatial targets. Virtual passwords are also crated representing random positions in the virtual environment. Hybrid passwords are a combination of spatial and virtual ones, allowing the user the definition of any combination of physical and virtual objects—positions. The scheme is tested for shoulder surfing by outstanders. Evaluation of the system is performed with 15 participants, and each password type has 135 attack attempts. From the three types, least security against hacking is associated with spatial passwords (5.9% successful hack attempts), then hybrid passwords (3.7% successful hack attempts), and best security performance is associated with virtual passwords with no successful hack attempts, showing high level of resistance to shoulder-surfing attacks.

Gaebel et al. [8] presente a system called "Looks Good To Me" (LGTM), a user authentication protocol for augmented reality environments. LGTM uses data from the AR headsets and combines facial recognition with wireless localization of the user. The system model refers to a point-to-point connection between two users equipped with AR HMDs who can be identified/authenticated from each other by a facial recognition model performed by the headset. The user may share digital content of messaging. The model considers an attacker that may attempt to impersonate using publicly available information, intervene with malicious or sensitive data, or even prevent communication of the two users. The model protocol uses wireless localization of users and an additional security measure to prevent attacks. This is attempted by connecting a wireless signal to a physical location as a result of computation of the signal's point of origin.

Abdelrahman et al. [11] study a cue-based password authentication scheme for VR environments (CueVR). The concept is based on a PIN which the user should know in order to authenticate and enter with a laser-pointer on a virtual pad. In addition, the authentication is based on cues presented to the user on the virtual PIN-Pad, a feature that makes it resistant to observations by a bystander who may observe user's input, but has no access to the generated cues needed for successful PIN entry. Cues are of Up, Down, Center, Left, and Right, with center marked with a circle on the digit and the rest with arrows. The cues are assigned to digits of each color (there are two colors) in a random way, a technique that makes sure that each cue-color combination is unique. The system is evaluated with the participation of 20 users, creating 480 entries. Three input methods are applied: Laserpointer, two-handed Trackpad and two-handed Motion Controller. Laserpointer is the least secure input method, but the most preferred by the users.

Yang et al. [55] address the need for secure authentication in the metaverse, where users interact through avatars. The proposed two-factor authentication framework combines biometric-based authentication (iris biometrics) and chameleon signatures to ensure the consistency and traceability of virtual and physical identities of the avatars. The proposed framework introduces decentralized authentication protocols and leverages blockchain technology and iris recognition, achieving both real-time authentication and virtual–physical tracking in the metaverse.

5. Discussion

The aim of this paper was to provide a comprehensive and systematic literature review of the related research published in the last fifteen years on user authentication within the fields of virtual reality, augmented reality, and mixed reality. A total of 36 papers were identified and reviewed (RQ1), all of which focus on immersive technologies for user authentication in immersive applications. In line with previous literature reviews [7,17] on immersive technology in user authentication, the present analysis identified three types of authentication methods that have applications to AR and VR. The identified authentication methods were classified as knowledge-based, biometric-based, and multi-factor methods. Almost half of the reviewed papers (19 out of 36) focused on biometric methods, indicating recent trends in user authentication. One out of three studies (11 out of 36) used multi-

factor methods, which involved various combinations of knowledge-based, biometric, and token-based methods, while one out of six studies (6 out of 36) focused solely on knowledge-based authentication methods. This answers the second research question (RQ2) regarding the authentication schemes investigated in the recent literature. For the remaining research questions (RQ3–RQ5), their answers are summarized in the following paragraphs organized according to the classified authentication method.

Biometric-based user authentication employs a wide range of measurements to ensure secure identification, and it is a promising technology. However, it also raises concerns about the potential risk of sensitive user information being leaked. These methods make use of physical characteristics of the user, such as brain signal [36,46], photoplethysmogram [47], breathing patterns [37,44], ultrasonic-based mapping [45,48] and facial recognition [31,32], as well as movement detection, including head movement [41,42], eye gaze [38,40,43] and ball throwing activities [33–35,39], and finally haptic authentication [30]. An interesting approach of John et al. [38,40] is the usage of iris defocusing, in an attempt to prevent iris information from being transferred and risk of an attack, at the cost of lower information and authentication success.

The devices used for biometric authentication include head-mounted displays (HMDs), which are often equipped with accelerometers, gyroscopes, and magnetometers, as well as high- and low-resolution cameras. Some examples of such devices include the HoloLens, Oculus Go, HTC VIVE, HTC VIVE Cosmos, and HTC VIVE Pro headset and controller, as well as Pupil Labs Pro glasses. Other devices used for biometric authentication include electroencephalography (EEG), photoplethysmography (PPG) and Doppler radar motion-sensing transceivers, as well as haptic devices. Algorithms and computational methods used for biometric authentication include k-Nearest Neighbors, Random Forest, Support Vector Machine (SVM), and Bag of Symbolic-Fourier-Approximation Symbols (BOSS), as well as Principal Components Analysis (PCA), Gaussian Blur, Gaussian distribution functions, and descriptive statistical calculations.

Knowledge-based methods include complex, graphical passwords and PINs, such as versions of the Rubik cube [13,15,52]. A novel knowledge-based approach uses avatars with a bond to users who authenticate by providing avatar information [26]. Equipment used in this group of user authentication methods includes HMD, virtual panels, hand controllers and pointing devices.

Multi-factor methods use both of the above techniques to ensure maximum security for user authentication. The combinations found in the literature include graphical or other passwords combined with positioning, distance and movement data [50,51,53], 3D passwords with behavioral data [49], doodles with space coordinates [54], facial characteristics with physical location [8], iris biometrics [55] and password recall with cues [11].

Most of the proposed solutions were evaluated with user studies for various aspects of the systems, such as usability, effectiveness, security, error rate, attack success rate. Almost half of the studies reported evaluations regarding prevention of shoulder surfing attacks.

After studying the relevant literature, the overall conclusion is that state-of-the-art methods utilizing immersive technologies for user authentication employ multiple techniques to enhance security and user experience. These multi-factor methods typically incorporate a biometric component, which provides users with a seamless, trusted, and secure means of identity verification. However, certain biometric methods remain vulnerable to nefarious attacks that capture and replicate physical biometric information, such as fingerprints, iris and retina scans, or facial recognition. This highlights the need for future research opportunities in user authentication in AR and VR that rely on behavioral data captured by immersive applications and appropriate sensors rather than physical information. While some research papers in the literature review presented in this paper have explored this dimension of behavioral authentication, further research could be developed to incorporate behavioral authentication as a part of a multi-factor authentication scheme. In the future, researchers could further explore behavioral data, such as tapping on a touch screen, typing speed, typing errors, talking, walking, body movements, and other

similar metrics. This type of information is challenging to replicate, and the uniqueness of behavioral data for each individual provides a promising avenue for future research in user identification.

Study Limitations

The limitations of this systematic review are mainly related to the maturity of the publications and the search engine utilized for retrieving publications. Our search was only based on the scientific literature indexing system called Scopus because it contains the most important digital libraries, such as Elsevier, Springer, ACM, IEEE, and MDPI. Because our research focused on the scientific literature, we did not consider the gray literature as well as real implementations, which can be inferred from the holistic consideration of the purpose of the study. Finally, as a limitation, it should be noted that user authentication methods based on immersive technologies that find application in VR, AR, and MR were not easy to separate from general authentication technologies in this application domain, and this resulted in a sufficient number of publications being excluded when accessing full-text articles.

Author Contributions: Conceptualization, I.A., G.D. and K.R.; methodology, I.A., G.D. and K.R.; validation, I.A., G.D., G.P. and K.R.; formal analysis, I.A., G.D., G.P. and K.R.; investigation, I.A.; data curation, I.A. and G.D.; writing—original draft preparation, I.A.; writing—review and editing, G.D., G.P. and K.R.; visualization, I.A. and G.D.; supervision, K.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This work was carried out in the context of the Master program "Immersive Technologies—Innovation in Education, Training and Game Design", Department of Computer Science, International Hellenic University, Kavala, Greece.

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

References

1. Pavithra, A.; Kowsalya, J.; Keerthi Priya, S.; Jayasree, G.; Kiruba Nandhini, T. An Emerging Immersive Technology-A Survey. *Int. J. Innov. Res. Growth* **2020**, *6*, 119–130.
2. Li, J.; Barmaki, R. Trends in Virtual and Augmented Reality Research: A Review of Latest Eye Tracking Research Papers and Beyond. *Prepr. Math. Comput. Sci.* **2019**, 2019090019. [CrossRef]
3. Rebbani, Z.; Azougagh, D.; Bahatti, L.; Bouattane, O. Definitions and Applications of Augmented/Virtual Reality: A Survey. *Int. J. Emerg. Trends Eng. Res.* **2021**, *9*, 279–285. [CrossRef]
4. LaValle, S.M. *Virtual Reality*; Cambridge University Press: Cambridge, UK, 2019.
5. Bonasio, A. Immersive Experiences in Education: New Places and Spaces for Learning. [White Paper]. 2019. Available online: https://edudownloads.azureedge.net/msdownloads/MicrosoftEducation_Immersive_Experiences_Education_2019.pdf accessed on 1 August 2023).
6. Rosenblum, L. Virtual and Augmented Reality 2020. *IEEE Comput. Graph. Appl.* **2000**, *20*, 38–39. [CrossRef]
7. 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 (ARES'22), Vienna, Austria, 23–26 August 2022. [CrossRef]
8. 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; pp. 57–67. [CrossRef]
9. Cao, Q.; Xu, F.; Li, H. User Authentication by Gait Data from Smartphone Sensors Using Hybrid Deep Learning Network. *Mathematics* **2022**, *10*, 2283. [CrossRef]
10. Avola, D.; Bigdello, M.J.; Cinque, L.; Fagioli, A.; Marini, M.R. R-SigNet: Reduced space writer-independent feature learning for offline writer-dependent signature verification. *Pattern Recognit. Lett.* **2021**, *150*, 189–196. [CrossRef]

11. 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, Rome, Italy, 6–10 June 2022; pp. 1–9. [CrossRef]
12. Nahar, M.N.; Alsadoon, A.; Prasad, P.W.C.; Giweli, N.; Alsadoon, O.H. An enhanced one-time password with biometric authentication for mixed reality surgical Tele-presence. *Multimed. Tools Appl.* **2021**, *80*, 10075–10100. [CrossRef]
13. 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]
14. Zhu, H.; Jin, W.; Xiao, M.; Murali, S.; Li, M. BlinKey: A Two-Factor User Authentication Method for Virtual Reality Devices. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2020**, *4*, 1–29. [CrossRef]
15. 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, 25–30 April 2020; pp. 1–9. [CrossRef]
16. 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]
17. Jones, J.M.; Duezguen, R.; Mayer, P.; Volkamer, M.; Das, S. A Literature Review on Virtual Reality Authentication. In Proceedings of the Human Aspects of Information Security and Assurance; Furnell, S., Clarke, N., Eds.; Springer International Publishing: Cham, Switzerland, 2021; Volume 613, pp. 189–198. [CrossRef]
18. 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. [CrossRef]
19. 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, 24–26 January 2023; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2023; pp. 1–7. [CrossRef]
20. 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, 23–26 May 2022; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2022; pp. 267–284. [CrossRef]
21. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Keele University: Newcastle, UK, 2007.
22. Fink, A. *Conducting Research Literature Reviews: From the Internet to Paper*, 2nd ed.; Sage Publications: Thousand Oaks, CA, USA, 2005.
23. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *BMJ* **2009**, *339*, b2535. [CrossRef] [PubMed]
24. Boland, A.; Dickson, R.; Cherry, G. *Doing a Systematic Review: A Student's Guide*; SAGE Publications Ltd.: London, UK, 2017.
25. 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, 7–9 February 2018; pp. 1–8. [CrossRef]
26. Micallef, N.; Just, M. Using avatars for improved authentication with challenge questions. In Proceedings of the SECURWARE 2011, Nice/Saint Laurent du Var, France, 21–27 August 2011; pp. 121–124.
27. 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; pp. 277–285. [CrossRef]
28. Kumar, A.; Lee, L.H.; Chauhan, J.; Su, X.; Hoque, M.A.; Pirttikangas, S.; Tarkoma, S.; Hui, P. PassWalk: Spatial Authentication Leveraging Lateral Shift and Gaze30th ACM International Conference on Multimedia, Lisboa, Portugal, 10–14 October 2022; Association for Computing Machinery, Inc.: New York, NY, USA, 2022; pp. 952–960. [CrossRef]
29. Wang, J.; Gao, B.; Tu, H.; Liang, H.N.; Liu, Z.; Luo, W.; Weng, J. Secure and Memorable Authentication Using Dynamic Combinations of 3D Objects in Virtual Reality. *Int. J. Hum.-Interact.* **2023**, 1–19. [CrossRef]
30. Orozco, M.; Graydon, M.; Shirmohammadi, S.; El Saddik, A. Experiments in haptic-based authentication of humans. *Multimed. Tools Appl.* **2008**, *37*, 73–92. [CrossRef]
31. Zhang, Z.; Zhang, M.; Chang, Y.; Esche, S.; Chassapis, C. A Virtual laboratory system with biometric authentication and remote proctoring based on facial recognition. *Comput. Educ. J.* **2016**, *16*, 74–84.
32. Zhou, Z.; Mingshao, Z.; Yizhe, C.; Esche, S.; Chassapis, C. A virtual laboratory combined with biometric authentication and 3D reconstruction. In Proceedings of the ASME 2016 International Mechanical Engineering Congress and Exposition, Phoenix, AZ, USA, 11–17 November 2016; Volume 5.
33. 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; pp. 253–2531. [CrossRef]
34. 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; pp. 9–97. [CrossRef]

35. 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.; Springer International Publishing: Cham, Switzerland, 2019; Volume 11295, pp. 55–67. [CrossRef]
36. 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; pp. 115–120. [CrossRef]
37. Islam, S.M.M.; Rahman, A.; Prasad, N.; Boric-Lubecke, O.; Lubecke, V.M. Identity Authentication System using a Support Vector Machine (SVM) on Radar Respiration Measurements. In Proceedings of the 2019 93rd ARFTG Microwave Measurement Conference (ARFTG), Boston, MA, USA, 7 June 2019; pp. 1–5. [CrossRef]
38. 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, 25–28 June 2019; pp. 1–5. [CrossRef]
39. 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, 22–26 March 2020; pp. 311–316. [CrossRef]
40. 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. Vis. Comput. Graph.* **2020**, *26*, 1880–1890. [CrossRef]
41. Sivasamy, M.; Sastry, V.; Gopalan, N. 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; pp. 518–523. [CrossRef]
42. 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, Hong Kong, China, 7 June 2021; pp. 41–52.
43. Lohr, D.; Komogortsev, O.V. Eye Know You Too: Toward Viable End-to-End Eye Movement Biometrics for User Authentication. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 3151–3164. [CrossRef]
44. Islam, S.M.M.; Boric-Lubecke, O.; Lubecke, V.M. Identity Authentication in Two-Subject Environments Using Microwave Doppler Radar and Machine Learning Classifiers. *IEEE Trans. Microw. Theory Tech.* **2022**, *70*, 5063–5076. [CrossRef]
45. Chang, Z.; Wang, L.; Li, B.; Liu, W. MetaEar: Imperceptible Acoustic Side Channel Continuous Authentication Based on ERTF. *Electronics* **2022**, *11*, 3401. [CrossRef]
46. Jang, H.; Park, S.; Woo, J.; Ha, J.; Kim, L. Authentication System Based on Event-related Potentials Using AR Glasses. In Proceedings of the 2023 11th International Winter Conference on Brain-Computer Interface (BCI), Gangwon, Republic of Korea, 20–22 February 2023; pp. 1–4. [CrossRef]
47. Seok, C.L.; Song, Y.D.; An, B.S.; Lee, E.C. Photoplethysmogram Biometric Authentication Using a 1D Siamese Network. *Sensors* **2023**, *23*, 4634. [CrossRef]
48. Wang, R.; Huang, L.; Wang, C. Low-effort VR Headset User Authentication Using Head-reverberated Sounds with Replay Resistance. In Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 22–25 May 2023; pp. 3450–3465. [CrossRef]
49. Alsulaiman, F.; El Saddik, A. Three-Dimensional Password for More Secure Authentication. *IEEE Trans. Instrum. Meas.* **2008**, *57*, 1929–1938. [CrossRef]
50. 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, Australia, 20–23 February 2018; pp. 255–262. [CrossRef]
51. 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, Scotland, UK, 4–9 May 2019; pp. 1–6. [CrossRef]
52. 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, 25–30 April 2020; pp. 1–10. [CrossRef]
53. 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, 22–26 March 2020; pp. 714–715. [CrossRef]
54. 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]
55. Yang, K.; Zhang, Z.; Youliang, T.; Ma, J. A Secure Authentication Framework to Guarantee the Traceability of Avatars in Metaverse. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 3817–3832. [CrossRef]