systems

MDPI

Article

Continuous Behavioral Biometric Authentication for Secure Metaverse Workspaces in Digital Environments

Giluk Kang, Jihoon Park and Young-Gab Kim *

Department of Computer and Information Security, and Convergence Engineering for Intelligent Drone, Sejong University, Seoul 05006, Republic of Korea; giluk1027@sju.ac.kr (G.K.); syr03099@sju.ac.kr (J.P.)
* Correspondence: alwaysgabi@sejong.ac.kr

Abstract

As many companies adopted hybrid work arrangements during and after the COVID-19 outbreak, interest in Metaverse applications for virtual offices grew considerably. Along with this growing interest, the risk of data breaches has also increased, as virtual offices often handle confidential documents for businesses. For this reason, existing studies have explored Metaverse user authentication methods; however, their methods suffer from several limitations, such as the need for additional sensors and one-time authentication. Therefore, this paper proposes a novel behavioral authentication framework for secure Metaverse workspaces. The proposed framework adopts keyboard typing behavior that is common in the office and does not cause fatigue to users as an authentication factor to afford active and continuous user authentication. Based on our evaluation, the user identification accuracy achieved an average of approximately 95% among 11 of 15 participants, with the highest-performing user reaching an accuracy of 99.77%. In addition, the proposed framework achieved an average false acceptance rate of 0.41% and a false rejection rate of 4.02%. It was also evaluated with existing studies using requirements for user authentication in the Metaverse to demonstrate its strengths. Therefore, this framework can fully ensure a secure Metaverse office by preventing unauthenticated users.

Keywords: user authentication; behavioral biometric; Metaverse; remote work

check for updates

Academic Editor: Anas M Alsobeh

Received: 6 June 2025
Revised: 12 July 2025
Accepted: 13 July 2025
Published: 15 July 2025

Citation: Kang, G.; Park, J.; Kim, Y.-G. Continuous Behavioral Biometric Authentication for Secure Metaverse Workspaces in Digital Environments. *Systems* **2025**, *13*, 588. https://doi.org/10.3390/systems13070588

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

In recent years, office workers have exhibited increased resistance to in-person office work and demanded remote work after experiencing it during the COVID-19 pandemic. According to the 2022 Work Trend Index report [1], most employees now prefer off-site work. In addition, the coworking market is expanding with the emerging "work near home" concept [2]. In response to this demand and growth, numerous companies are transitioning to hybrid work arrangements [3], which combine in-office and remote work. Many companies have expressed interest in virtual office applications and are increasingly introducing them to hybrid work environments. Aligned with this growing interest, big tech companies have released virtual office applications and related immersive devices, e.g., head-mounted displays (HMD). For instance, Meta launched Meta Horizon Workrooms, Microsoft released Microsoft Mesh, and Apple has introduced its latest product, i.e., Apple Vision Pro. With the growing adoption of hybrid work and the increase in international enterprises, similar applications and devices are expected to be released steadily in the future.

Generally, the Metaverse office provides virtual working spaces to employees to enable flexible work and collaborative meetings in order to achieve the company's goals without restrictions in terms of time and location. To facilitate their work, it also contains confidential documents, such as financial or customer information, marketing reports, business strategy documents, and intellectual property [4]. However, attackers may attempt to leak these documents because they are related to the company's financial gains [5]. To mitigate such data breaches, commercial applications implemented a user authentication method prior to accessing virtual offices; however, the authentication method utilizes password authentication, which is vulnerable to shoulder surfing attacks as users are wearing immersive devices, such as the HMD. Several Metaverse applications offer two-factor authentication, but it is still inadequate because it relies on possession-based user authentication, e.g., smartphone ownership. The most common method for user authentication in applications is one-time authentication, which does not verify users continuously after completing the first authentication process. Hence, if an authenticated employee leaves their device unattended in the coworking space for even a short period, a competitor's employee could potentially access the device and confidential documents.

For this reason, many studies have investigated user authentication methods for the Metaverse. For example, to prevent shoulder-surfing attacks, authentication methods that utilize graphical passwords [6,7] have been proposed; however, such methods are not suitable for the Metaverse because one-time authentication methods can lead to decreased usability and increased cognitive load because long and complex interactions with virtual objects are required to remember credentials and input passwords. Moreover, physiological biometric authentication [8–14] has been designed recently to address the limitations of knowledge-based authentication. Biometric authentication methods can ensure continuous user authentication; however, additional and expensive Internet of Things (IoT) sensors are required to realize high identification accuracy, and privacy issues related to the collection of sensitive data must be considered [15]. Many behavior-based user authentication methods [16–23] have also been designed; however, most of these methods are not suitable for static office environments because they focus on dynamic tasks. Methods that utilize general tasks, such as walking [16], gaze [17], and expression [23], have also been investigated, but they are ineffective for continuous user authentication because they induce movements that can cause user fatigue. To address the limitations of existing studies, this study proposes continuous behavioral biometric authentication for secure Metaverse offices. The proposed framework authenticates users based on virtual hand movements and dwell time during typing tasks in the office. Unlike existing studies, the proposed framework does not require additional IoT sensors or memorization of complex interactions with virtual objects. It also enables active authentication by adopting a common and less fatiguing typing task. The primary contributions of this study are summarized as follows.

- To address illegal access by unauthenticated users in the Metaverse office, an active and continuous user authentication framework that uses virtual hand movements and dwell time is proposed.
- Based on a systematic literature review, we analyze prior studies on user identification or authentication for the Metaverse. In addition, the requirements for authentication are defined.
- To validate the feasibility of the proposed framework, the framework was implemented as a prototype. The performance of the framework was validated by several evaluation metrics using various feature combinations and compared with existing studies using the defined requirements to demonstrate its strengths.

The remainder of this paper is organized as follows. Section 2 analyzes existing studies on user authentication and identification in the Metaverse. Section 3 introduces the

proposed framework and the major requirements for user authentication in the Metaverse. Then, Section 4 presents the implemented framework and the dataset creation process in detail. In Section 5, we evaluate the performance of the proposed framework and compare it with existing methods. Section 6 presents a general discussion of the proposed framework and future work. Finally, the paper is concluded in Section 7.

2. Literature Review

A wide range of user authentication methods have been studied to ensure a secure Metaverse. This section reviews three categories of prior user authentication methods in the Metaverse (i.e., knowledge-based, physiological biometric, and behavioral biometric authentication). Many existing works for authenticating users by keyboard typing [24–27], similar to this study, have been proposed in other domains; however, they are not covered in this section because the primary goal of our study is to propose a novel user authentication that focuses on the Metaverse.

2.1. Literature Review Process

Prior to discussing the related work, we describe the literature review process. First, we defined the following search terms: "Authentication" AND ("Metaverse" OR "Immersive" OR "Virtual Reality" OR "Augmented Reality"). In this process, five well-known publishers (i.e., IEEE, ACM, Elsevier, Springer, and MDPI) were selected. In addition, we set the following criteria: publication date (2019–2024), several paper types (i.e., conference, journal, magazine, and early access), and articles on user authentication in the Metaverse or immersive devices. Our search was conducted in the 3rd and 4th weeks of August 2024. The results without the set criteria presented 413 papers from IEEE, 1652 papers from ACM, 3401 papers from Elsevier, 16,517 papers from Springer, and 6258 papers from MDPI. As MDPI and Springer do not support parentheses, these publishers were searched by each keyword (e.g., "Authentication" AND "Immersive"). Thus, the presented results are the sum of the individual searches. For publishers that returned greater than 3000 results, we searched for our terms in the title, abstract, or author-defined keywords. The results presented 24 papers from Elsevier, 94 papers from MDPI, and 71 papers from Springer. We then applied our criteria to the results. Finally, 52 papers were selected. Among these studies, significant studies are discussed in this section. The articles were classified into three main types (i.e., knowledge-based authentication, physiological biometric authentication, and behavioral biometric authentication), as shown in Figure 1.

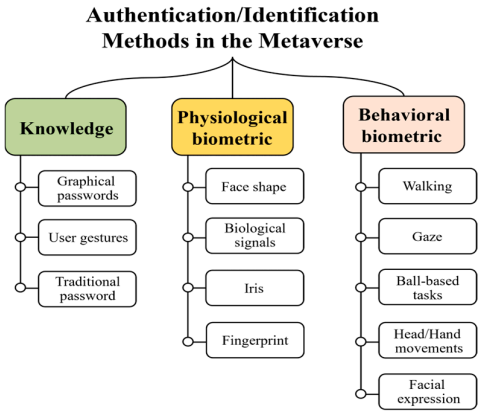


Figure 1. Taxonomy for prior studies on user authentication and identification in the Metaverse.

2.2. Knowledge-Based Authentication

Many approaches to user authentication have been proposed in recent years for various domains (e.g., smart home and IoT). Among these authentication approaches,

knowledge-based authentication is widely adopted in confidential or commercial systems due to its user-friendliness and ease of implementation. It continues to be utilized as a form of graphical password or user gesture in the Metaverse and with immersive devices (e.g., HMD and smart glasses). These forms ensure immersive experiences, which are important in the virtual environment because they are based on interaction with virtual objects. Most existing studies focused on the graphical password, as this password is less complex and more memorable for users than gestures. In these studies, user authentication is performed through various interactions, such as pointing at voxels, selecting images, or choosing a combination of objects and colors. As a representative study, Bu et al. [28] investigated a novel password-based authentication method utilizing an interactive sphere in which the password can be selected using controllers with trackpads. Abdelrahman et al. [29] also proposed a fast authentication method utilizing the ten-digit keypad. Their method allows the use of either one or two controllers, and the password is entered by pressing buttons on trackpads (i.e., up, down, left, right, and center) that appear next to the keypad. In their experiment, the authentication process took approximately 4–5 s when users selected four-digit passwords, which is faster than the authentication time shown in prior studies. Turkmen et al. [6] designed a voxel-based 3D authentication using users' gaze. In this system, users first choose images before entering the virtual environment, and then voxelated images created by those choices are shown. Users direct their gaze to a specific voxel and select it utilizing their controllers, therefore performing the authentication process. Wazir et al. [7] proposed a doodle-based user authentication system as an improved method based on graphical passwords. Their proposed system compares the differences among all coordinates and sizes in registered doodles and drawn doodles currently, then determines users' validity when the doodles' similarity is more than 80%.

Knowledge-based authentication based on users' gestures was also proposed in several studies. In these studies, users perform predefined gestures corresponding to ten digits for authentication. For example, Rupp et al. [30] defined gestures, which include social interactions with the designated virtual agent. To authenticate in their proposal, users approach the agent within three meters and then perform interactive gestures (e.g., handshake, high five, and open hand) or personal gestures, such as a wave and a finger gun. On the other hand, a time-based authentication method using a traditional password (i.e., not using graphical passwords or gestures) is proposed in [31], differing from previous studies. This method first verifies the user's registered password and then requires the user to enter a one-time password (OTP), which is generated based on a timestamp on the user's screen when the password is valid. According to their experiment, physical and video-based inference attacks were impossible.

2.3. Physiological Biometric Authentication

Physiological biometrics have been utilized more than behavioral biometrics due to their fast recognition, high uniqueness, and usability [32]. However, they have not yet been used in commercial HMDs because the required sensors incur high costs and suffer from low accuracy. Moreover, privacy concerns have been raised due to the collection and use of sensitive data. Despite these challenges, physiological biometrics still provide many benefits, such as being nonintrusive, offering high uniqueness, and having good resistance to spoofing; thus, the application of physiological biometrics has been explored extensively in the immersive device. In particular, many studies have investigated physiological biometrics, such as the shapes of face parts (i.e., the ear, face, and skull), bioacoustic signals in the neck, vibration in the head, brain signals, cardiovascular signals, iris, and hand tremor. For example, Zhong et al. [8] proposed an ear recognition method based on regular

audio. This method collects high-quality ear canal responses for user enrollment in a controlled environment, and data augmentation techniques are employed to enable user identification in all audio samples. Moreover, in [9], a multimodal biometric authentication method that uses face recognition and signatures was proposed. This method performs user authentication by recognizing in-air dynamic and static signatures, as well as the face, using a laptop's camera. The method collects face and static signature images, along with the positional data of the signature while the user's index fingertip is creating the signature. Li et al. [10] designed the VibHead authentication scheme, which uses vibration signals. The VibHead scheme authenticates the user using a deep learning model (i.e., a convolutional neural network) after emitting short vibration signals generated by a vibration motor. In their experiments, high accuracy was demonstrated compared with traditional machine learning (ML) models, e.g., the random forest model. In addition, an authentication method that utilizes brain signals has also been proposed [11]. This method uses brain signals (i.e., electroencephalography) while the user watches a two-minute video, collecting data in virtual and real-world environments. The results demonstrated that the difference in signals between the two environments was not significant.

Moreover, Seok et al. [12] presented a user authentication method based on a photoplethysmogram obtained using a wrist-wearable device, such as a smartwatch. Boutros et al. [13] explored the usability of traditional iris recognition in HMDs. They focused on an iris segmentation and synthetic image generation technique for HMDs with low processing requirements, utilizing eye images captured within the devices. The suitability of this method was demonstrated by benchmarking several feature extractions. In addition, a cryptographic scheme has been proposed to realize mutual authentication between the user and the Metaverse using hand tremors collected by the Leap Motion device [14].

2.4. Behavioral Biometric Authentication

Recently, behavioral biometric authentication has been recognized as the most suitable approach in Metaverse. This approach, often called task-driven biometric authentication, is naturally performed based on users' behavioral patterns during interactions with virtual objects. In addition, unlike traditional methods, it does not need to collect private data and remember complex graphical passwords. With these advantages, many studies have investigated task-driven authentication, especially focusing on the following various behaviors: walking, facial expression, gaze, ball-based tasks, head moving, and hand movement. Table 1 summarizes the strengths and weaknesses of significant studies and the proposed framework. A detailed description of these studies is as follows:

Table 1. Summary of significant behavioral biometric authentication methods.

References	Strength	Weakness
Shen et al. [16]	High recognition accuracy (i.e., approximately 98%), and additional biometric sensors are not required.	Users wearing immersive devices can experience physical limitations (e.g., lightheadedness) when walking and then refuse to perform this behavior.
LaRubbio et al. [17]	Investigated gaze-based user authentication during random dot viewing, 360-degree image viewing, and nuclear training simulations.	Consistent data collection can be difficult, as user focus may decrease because the method requires extended gaze collection.

Table 1. *Cont.*

References	Strength	Weakness
Miller et al. [18]	This system continuously authenticates users as they interact in the virtual environment, allowing them to continue activities.	Trajectory data are utilized during ball-throwing, which may limit applicability in various domains.
Mai et al. [19]	They explored the potential of head-based movement as a method for user authentication.	Head movement may be uncomfortable for some users and cause fatigue over long sessions.
Lu et al. [20]	The users' passcodes and unique handwriting styles are adopted for multi-factor authentication.	Their method requires additional sensors to capture users' handwriting patterns.
Gopal et al. [21]	This approach verifies the secret code and user's hand movements during code entry, preventing attackers from impersonating users even if the password is obtained.	Not suitable for use in the Metaverse office due to one-time authentication.
Suzuki et al. [22]	PinchKey allows for authentication utilizing small finger movements without larger movements.	Pinch gestures are difficult to apply for continuous authentication because they are only used in limited situations.
Jitpanyoyos et al. [23]	Their scheme resists shoulder surfing by authenticating users based on facial expressions obscured by the HMD.	Continuous authentication is impossible because the user must have a smiling expression to be authenticated.
Our framework	This framework achieves active and continuous user authentication by adopting the most common office task across many domains.	The framework needs validation on large-scale datasets and evaluation using diverse metrics.

Shen et al. [16] developed the GaitLock system for gait recognition via smart glasses. The GaitLock authenticates the user's unique gait patterns when the user walks in an indoor or outdoor space for 5–10 min. It guarantees higher usability because only the on-board inertial measurement unit (IMU) sensor adapted to most commercial HMDs is utilized without additional sensors for authenticating the user. In [17], gaze-based continuous authentication was proposed. The authors collected gaze patterns from three scenarios (i.e., random dot viewing, image viewing, and the nuclear training simulation) and compared their accuracy. The result showed that the image viewing achieved the highest authentication success rate at 72%. Miller et al. [18] explored the continuous user authentication method by the ball-throwing task in the virtual environment. In their method, trajectory data is collected during the ball-throwing and then compared with the previous trajectories in the user library to detect whether the user is an authenticated user or not. Additionally, Mai et al. [19] investigated a behavior-based user authentication approach using head movement. This approach authenticates the user by the HMD's position, rotation angle, speed, and angular velocity when the user tilts the head to control

speed and direction while reaching a target indicated by a red arrow. Similar to previous studies, the authentication method using hand movement was also proposed in [20]. In their method, the user is authenticated by hand motion when handwriting a passcode in the air. Gopal et al. [21] proposed behavioral biometric authentication leveraging unique hand movements. This movement to authenticate the user includes acceleration and angular velocity collected by an IMU sensor worn on the wrist during typing. Suzuki et al. [22] introduced the PinchKey, which authenticates users using only small hand movements of two fingers (i.e., thumb and index finger) rather than larger gestures like throwing a ball, as in earlier studies. Meanwhile, the user authentication method utilizing facial expression was proposed in [23]. This method prompts users to smile and then authenticates them by collecting facial data. It was demonstrated in two proposed scenarios: sharing the HMD with family members or unspecified public users.

3. Continuous Behavioral Biometric Authentication for Secure Metaverse Workspaces

This study aims to propose a novel framework by ML for authenticating users in the Metaverse office continuously to prevent data leakage by unauthenticated users. The proposed framework guarantees an immersive experience, which is important, as it adopts the most common task (i.e., typing) in the virtual office. Furthermore, it does not require remembering complex passwords and is resistant to shoulder-surfing attacks due to keyboard input patterns being difficult to imitate. This section describes the proposed framework in detail. Requirements for user authentication on Metaverse are also presented based on prior work.

3.1. Requirements for User Authentication in the Metaverse

Unlike traditional domains (e.g., finance, healthcare, and e-commerce), user authentication methods on Metaverse should be designed to satisfy several requirements that are considered Metaverse's characteristics, such as maintaining a long session and needing immersive devices. For instance, they should be resistant to shoulder-surfing attacks, as wearing an HMD blocks the user's view of the actual space. This subsection defines the requirements considering prior work. Figure 2 presents five major requirements for user authentication in the Metaverse. These requirements are described as follows:



Figure 2. Requirements for user authentication in the Metaverse.

1. **Continuity.** In general, users perform various activities while maintaining long sessions in the Metaverse; thus, they should be verified continuously by the authentication process during active sessions. This process is referred to as continuous user authentication, which is essential because an attacker can intercept sessions authenticated through one-time authentication and access sensitive data without sufficient credentials.
2. **Universality.** The Metaverse is being used increasingly across a wide range of fields, so its user authentication methods should be designed for broad applicability. In other words, focusing on specific domains or environments is inappropriate. Thus, common or implicit tasks in various environments should be adopted in authentication processes. Complex tasks that may induce user fatigue are also inappropriate

because repeated authentication processes can be demanded to satisfy the continuity requirement. The adoption of implicit and common tasks is generally accepted as active authentication, which is performed without the user's awareness.

3. **Non-additional sensor.** Immersive devices allow social activities in the Metaverse using various mounted sensors to offer more realistic experiences. However, they are very heavy, which leads to user discomfort during extended use due to these sensors. Given the current weight, adopting additional sensors poses a considerable challenge because an increase in weight may further increase user discomfort during prolonged use. Thus, authentication methods should operate using sensors already built into immersive devices without requiring additional sensors.
4. **Resistance to shoulder-surfing**. As mentioned earlier, immersive devices are widely used in the Metaverse. To enhance the realism of virtual spaces, they provide more immersive experiences by obstructing the user's field of view and then showing only virtual environments via the display. However, this blocking makes it difficult to feel whether an attacker in a real space is spying on users while they perform confidential tasks. Even if the pass-through function is adopted in confidential behaviors or input processes, users should still continuously check whether there is an attacker behind, because the function is only offered in the gaze direction. Accordingly, methods for authenticating users on the Metaverse should resist the shoulder-surfing attack.
5. **High acceptability.** Acceptability is closely related to privacy and refers to the extent to which users commonly exhibit reluctance to provide authentication factors. According to the previous study [32], biometric factors have lower acceptance than the knowledge factor, with the exception of a few factors, e.g., fingerprints. In addition, privacy concerns caused by collecting physiological biometrics have been raised. In the Metaverse, this low acceptance may become more pronounced when adopting active and continuous authentication, which collects biometric data repeatedly and implicitly. The concerns also remain, as sharing sensitive data with third-party servers can be required due to the low performance of immersive devices. Thus, user authentication methods should adopt factors that have relatively proper acceptability and those that do not involve sensitive data.

3.2. Assumption

The proposed continuous user authentication framework assumes four key assumptions. This subsection discusses these assumptions prior to describing the proposed framework in detail. The first assumption concerns the devices used to realize authentication. In the proposed framework, an HMD that supports hand tracking is needed as an immersive device. In addition, all users do paperwork in the virtual space using a Bluetooth-enabled keyboard in the real-world environment. Second, the users' chairs and keyboards in the physical space are fixed at a set position. In the proposed framework, this immobility avoids changes in users' virtual hand positions by moving the keyboards and chairs on different days or sessions. The third assumption is that the proposed framework operates after users complete an initial password-based authentication process. Therefore, the proposed framework functions as a second factor in a multi-factor authentication process. The initial password-based authentication is required prior to operating the proposed framework. If the prediction accuracy regarding the specific user drops below the threshold defined by the administrator, the user is required to re-authenticate through the additional factors. Finally, in the framework, secure communication between components without network attacks is ensured. Although mitigating network attacks is essential, this issue is not addressed in this paper because it is beyond the scope of this study.

3.3. Overview

This study aims to investigate a continuous user authentication framework in the Metaverse office. Figure 3 presents the proposed framework as an overview. The proposed framework consists of two major phases. The first phase involves training an ML classifier to generate individual user profiles after collecting training data from users entering sentences in the Metaverse office. The second phase involves predicting a user using the trained ML classifier based on behavioral motion data, which is collected when a user enters the same text during a business process.

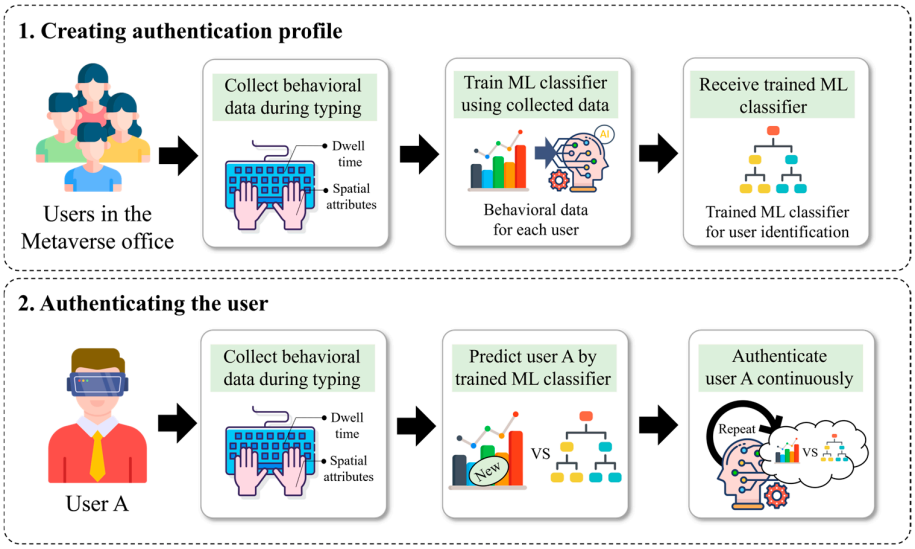


Figure 3. Overview of the proposed framework.

The framework focuses on authenticating users through hand movements during a common task; thus, the task is first discussed. Generally, office workers working in the Metaverse office environment participate in meetings and perform paperwork [33,34]. Meetings can be used as a task for voice-based user authentication; however, they require expensive and additional sensors, and meetings do not occur as frequently as paperwork. Accordingly, the framework adopts keyboard typing as a common task while the user is wearing the HMD. The proposed framework is configured by four components, i.e., the Metaverse user, the data collection module, the Metaverse office, and the ML classifier, each of which is described in detail in the following.

1. **Metaverse user.** Metaverse users are workers in a specific company that permits remote work. In the Metaverse office, this work involves handling documents or joining meetings without time and space constraints. In particular, the user can work with the keyboard and immersive device at home or in a coworking space without going to the physical company office. While performing document tasks, the user is verified continuously by determining whether preregistered typing patterns are similar to the current user's typing patterns using virtual hand movement data collected by the data collection module.
2. **Data collection module.** To support the authentication process, the data collection module continuously collects virtual hand-related data while users are performing document work. The data is behavioral patterns regarding input and hand movement. Specifically, the user's spatial data of virtual right and left hands, input values, and dwell times during keyboard typing are collected. The module preprocesses the collected hand data and then transmits the processed data to the ML classifier to request continuous user authentication. In the Metaverse office, the module operates alongside the ML classifier for each active user session.

3. **Machine learning classifier.** The ML classifier is a significant component of the proposed framework. While a specific user session is active, the ML classifier continuously validates the user, who was previously verified via the initial authentication process, using the data processed by the data collection module (i.e., hand movements). The classifier also manages each user's authentication profile. When a new user is registered, the ML classifier creates the user's profile. Otherwise, it deletes or updates user profiles when users want to reregister their profiles or resign from the company.
4. **Metaverse office.** The Metaverse office is a virtual workspace that facilitates remote work by enabling employees to collaborate or perform business tasks free from space and time constraints. The Metaverse office involves many business and confidential documents; thus, if the ML classifier detects a potential unauthenticated user during an active session, the office restricts access to the user temporarily and prompts additional authentication. As the central component of the proposed framework, the Metaverse office serves as the environment where all other components function to enable continuous user authentication.

3.4. Sequences

The proposed framework comprises 10 sequences based on the previously described components and assumptions. Figure 4 illustrates the framework's detailed sequences. First, new user A, who is hired by the company, accesses the Metaverse office work remotely. By entering the registered user ID and password in the company, user A is first authenticated.

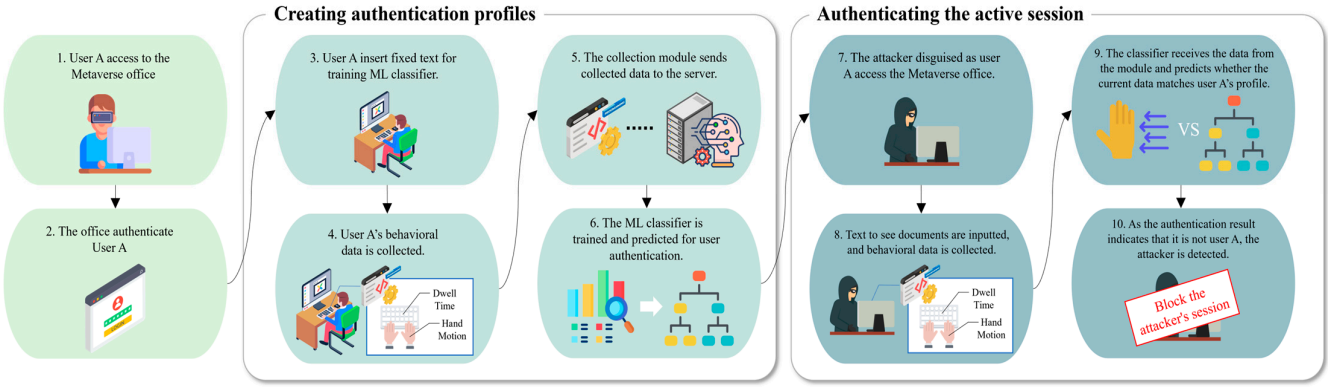


Figure 4. Detailed sequence of the proposed framework.

If the initial authentication process is successful, the user types the floating fixed text throughout two enrollment sessions to register the authentication profile as the Metaverse office is accessed for the first time. When the user inputs the text, the data collection module collects user A's virtual hand movements and dwell time. After the user completes two typing sessions, the module sends the collected data to the ML classifier. The ML classifier creates an authentication profile to verify user A by training on the collected data. Then, the user performs work in the Metaverse office after creating the profile. While the user performs their work, the data collection module continues to collect the user's virtual hand movement and dwell time data, which are sent to the ML classifier. The ML classifier continuously evaluates whether the current typing patterns are similar to user A's established profile to realize active and continuous user authentication in the Metaverse office.

Consider the following scenario. An attacker steals user A's ID and password and attempts to access the Metaverse office to obtain confidential documents. The attacker

successfully accesses the Metaverse office and attempts to retrieve and view the documents. Here, the data collection module sends the attacker's virtual hand movements and requests that the ML classifier verify that the current user is user A. If the prediction accuracy repeatedly falls below the threshold set by the administrator during the evaluation process, the classifier informs the Metaverse office to block the attacker. Depending on the different typing patterns, the Metaverse office will block the attacker and then request an additional user authentication process. Therefore, the proposed framework can detect an attacker disguised as an authenticated user using keyboard typing patterns.

4. Implementing Continuous User Authentication Framework

To demonstrate the feasibility of the proposed framework, this section shows a prototype of the implemented framework and describes the data collection process for the experiment.

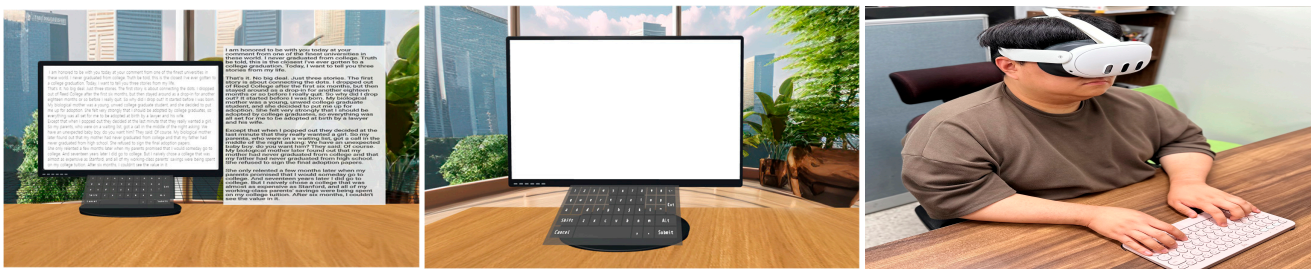
4.1. Implementation

Prior to discussing the implemented prototype of the proposed framework, we first describe the implementation environment. Table 2 presents the specifications of the environment in which the framework was implemented. The Metaverse office was developed using A-Frame, which is an open-source framework for building virtual reality experiences on the web [35]. In addition, the floating keyboard and hand tracking are realized using JavaScript in the virtual office [36,37]. The hand tracking is based on the WebXR hand input module (level 1) [38]. To facilitate paperwork in the virtual office, the Meta Quest 3 headset and Logitech K380 keyboard were adopted as immersive and input devices, respectively.

Table 2. Specifications of the implemental environment.

Type	Specification
Processor	AMD Ryzen 5 5600G with Radeon Graphics
Memory	8 GB
Development stack	Python 3.12, Nodejs, JavaScript, HTML
A-Frame	Ver. 1.5.0
Machine learning model	Random Forest
Bluetooth Keyboard	Logitech K380
Head-mounted display	Meta Quest 3

Furthermore, a random forest model was used as the ML classifier. The continuous user authentication framework in the Metaverse office was developed as a prototype to validate its feasibility in the implementation environment. To facilitate this implementation, three components (i.e., the ML classifier, the Metaverse office, and the data collection module) were integrated into a single system. Figure 5 shows the implemented Metaverse office.



(**a**) (**b**) (**c**)

Figure 5. Implemented Metaverse office. (**a**) Metaverse office for creating authentication profiles. (**b**) Metaverse office for business. (**c**) A scene of the user performing work.

When Metaverse users register at the office, they should enter the floating text to create their authentication profile, as shown in Figure 5a. In this evaluation, the floating text used part of the text of Steve Jobs' speech at Stanford University. After creating the profile, the users can perform paperwork in the Metaverse office, as shown in Figure 5b. Figure 5c presents the user performing paperwork in the office using the Meta Quest 3 headset and Logitech K380 keyboard. According to the third assumption, we set the threshold regarding prediction accuracy as 90%. If the specific user's prediction accuracy drops below 90%, access to the office is blocked temporarily until the user completes the additional authentication process; however, the additional authentication process was not implemented in this evaluation. In addition, the initial authentication process to access the Metaverse office was also not implemented in the current study.

4.2. Participants and Procedure

The proposed framework utilizes virtual hand movements and dwell time at the physical keyboard to authenticate users in the Metaverse office for each keystroke. To the best of our knowledge, a public dataset related to the data utilized in the proposed framework does not currently exist, and most previous studies have focused on keystroke dynamics or hand tracking [39,40]. In other words, a public dataset that captures virtual hand movements in the Metaverse and keystroke dynamics during input processes is not currently available. Therefore, we created a task-driven behavioral dataset to demonstrate and evaluate the proposed framework by recruiting participants. It was deemed as an exemption from an ethical review by the Institutional Review Board (IRB) of Sejong University under exemption number SUIRB-HR-E-2024-014, as the data collected in this study do not include private data. Overall, 15 participants (5 females and 10 males) aged 24 to 36 years (mean age = 28.5) were recruited from Sejong University (Seoul, Republic of Korea) and social networking services to participate in the experiment. Prior to conducting the experiment, we described the proposed framework and the data collection process in detail. Then, all participants provided informed consent for the experiment. The participants' data were anonymized as User1 to User15, and the data were collected over a 2-day period. Most participants did not have previous experience with immersive devices, especially HMDs.

The experimental dataset was collected following the procedure outlined in the following. The participants wore the HMD and sat in a fixed chair, as shown in Figure 5c. After accessing the implemented Metaverse office via the web browser, the participant was first asked to move and input freely into the office for 10 min to become familiar with the virtual environment. Following this practice session, the participant typed the floating text in the virtual office using the connected keyboard, as shown in Figure 5a. While entering the floating text, the position of the participant's virtual hands in the office and their dwell time were collected for each letter. After completing the text input task, the participant was permitted a break time of approximately 10–20 min. All participants completed the procedure twice on the first day to create a training dataset. On the second day, the procedure was again performed by 11 participants to generate a test dataset because several participants felt it was difficult.

5. Evaluation

This section first describes the data preprocessing and presents a performance analysis of the proposed framework. In addition, the framework is compared with prior studies based on the user authentication requirements in the Metaverse.

5.1. Data Preprocessing

The behavioral data in the implemented Metaverse office were collected from 15 participants. In particular, the data were collected over two days. On the first day, the data were gathered from all 15 participants, and on the second day, data were collected from a subset of 11 participants. In addition, on the first day, the data were collected across two sessions, and on the second day, the data were collected in a single session. The collected data include five skeleton joints, i.e., the wrist, thumb, index finger, middle finger, ring finger, and little finger, following the WebXR standard. Excluding the wrist joint, all joints were further classified into five points, i.e., the metacarpal, proximal phalanx, intermediate phalanx, distal phalanx, and tip. In addition, each joint is characterized by spatial parameters, including position, direction, normal, and quaternion, represented as three-dimensional or four-dimensional arrays. All users' virtual hands (i.e., the left and right hands of all participants) were collected. The user ID, dwell time, and pressed keys were also included in the data. Thus, the data collected for each participant included a total of 203 features. During data preprocessing, the data collected from one hand (either right or left) for a single character were first excluded based on the identical dwell time. The first processed data divided by joint points were combined into a single row for each input. Here, the position, direction, and normal of each joint were decomposed into x, y, and z features, and each joint's quaternion was represented with w, x, y, and z features. As a result, the final preprocessed data included a total of 652 features. For the preliminary study, we also transformed the first preprocessed data to relative coordinates. Here, the data were adjusted based on the relative distance from the initial letter "I" in the text of Steve Jobs' speech. In particular, the relative quaternions were determined by calculating the inverse of the reference quaternion and multiplying it by the current quaternion. Then, the position, direction, normal, and quaternion of each joint were decomposed into their respective features, as in the previous preprocessing phase, and the final data included a total of 652 features.

5.2. Performance Analysis

We explored whether specific users could be identified and utilized reliably as an authentication factor based on the preprocessed data. The data collected on the first day were combined into a training dataset, and the data collected on the second day were used for testing. The experimental methodology was divided into four separate studies, and the results of each study are discussed in the following.

5.2.1. Study 1: Relative Coordinates

In a pilot study, we initially explored whether absolute or relative coordinates facilitate accurate user identification more effectively. The relative coordinates are related to our second data preprocessing, which calculates differences between current virtual hands during typing from virtual hands when the initial character "I" In contrast, the absolute coordinates mean only applying our first data preprocessing. Note that the preliminary study leveraged all collected data, including position, direction, normal, quaternion, dwell time, and pressed key. Table 3 presents the identification accuracy for the 11 users. As indicated by research findings, the classification accuracy for most users (except User7 and User14) was higher with the relative coordinates than with the absolute coordinates. In other words, most users demonstrated improved accuracy, particularly those whose accuracy was close to 0% when using absolute coordinates. The results of this initial study demonstrated that the relative coordinates are more suitable as authentication factors than the absolute coordinates.

Table 3. Specifications of the implementation environment.

Coordinates	Specification (%)										
	User1	**User4**	**User5**	**User6**	**User7**	**User8**	**User9**	**User12**	**User13**	**User14**	**User15**
Relative	94.05	93.91	92.98	90.25	93.07	99.08	99.17	95.31	99.77	95.96	91.46
Absolute	0.05	19.98	4.43	26.9	99.23	79.02	0	62.6	0	100	82.79

5.2.2. Study 2: Each Spatial Attribute

Based on the results of the initial study, we investigated which spatial attributes (i.e., the position, direction, normal, and quaternion attributes) have high user identification accuracy. Here, four feature sets were defined, i.e., quaternion only, position only, direction only, and normal only, and the dataset was classified according to the feature sets. Figure 6 shows the results of the second study. First, in the feature set using only the quaternion, the overall identification accuracy decreased for all users compared with all spatial attributes, as shown in Figure 6a. Notably, User1, User6, User7, and User15 demonstrated a steep decrease in accuracy of approximately 20%. Moreover, in the set using only the position, all users demonstrated reduced accuracy. In contrast, the feature sets using only the normal or the direction exhibited improved accuracy for some users, e.g., User5, compared with all of the spatial parameters. However, the identification accuracy for some other users was still reduced, as shown in Figure 6c,d. In summary, the results suggest that a combined feature set is more effective for the user authentication factor than individual spatial attributes.

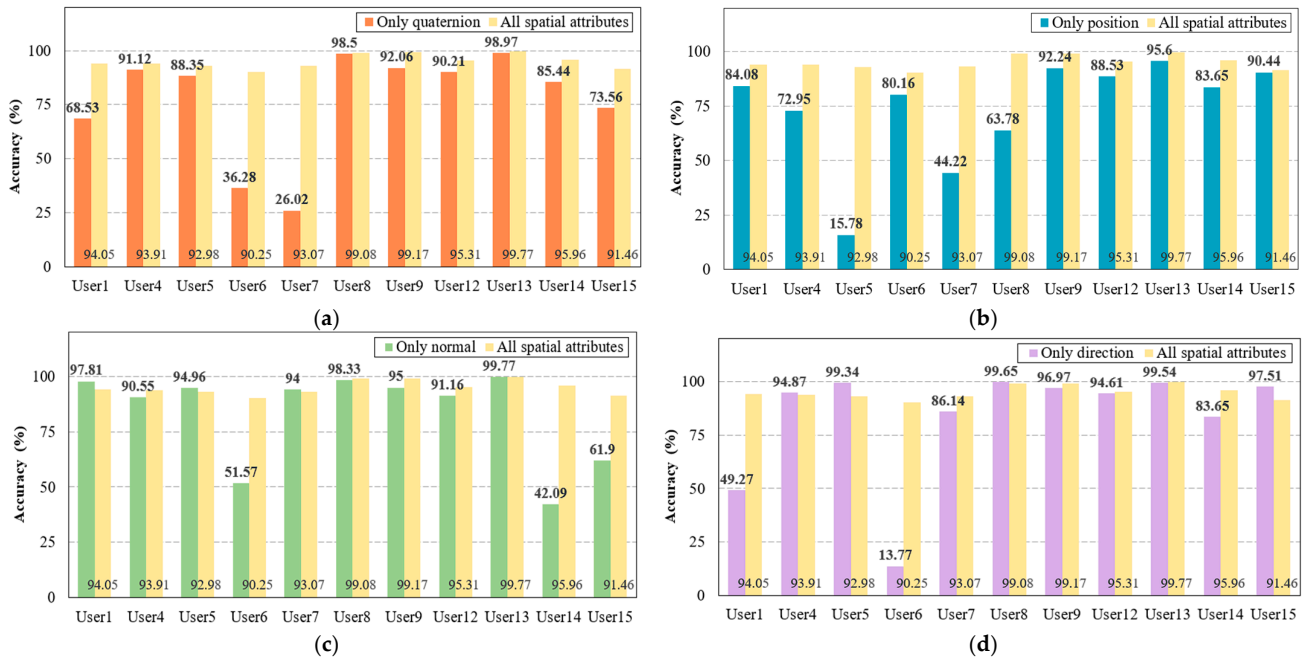


Figure 6. Comparison of user identification accuracy between all spatial attributes and individual attributes. (**a**) Accuracy of the only-quaternion compared with all spatial attributes. (**b**) Accuracy of the only-position compared with all spatial attributes. (**c**) Accuracy of the only normal compared with all spatial attributes. (**d**) Accuracy of the only direction compared with all spatial attributes.

Furthermore, the second experimental study compared the identification accuracy among feature sets with and without the quaternion, as in the previous results. This experiment attempted to determine the extent to which rotation impacts user identification accuracy in the proposed framework. The results indicate that there was no significant difference in the accuracy between combining all spatial attributes or normal position and direction, as shown in Figure 7. However, while User6's identification accuracy exceeded

approximately 90% of all spatial attributes, the user's accuracy decreased to 87% in the feature set without quaternions. The proposed framework forces a reauthentication process when the accuracy falls below 90%; thus, the results suggest that using all spatial attribute combinations is appropriate. Based on these findings, the final analysis examines the user identification accuracy for the top features with high weights to optimize the complexity of the ML classifier, as the framework uses all features.

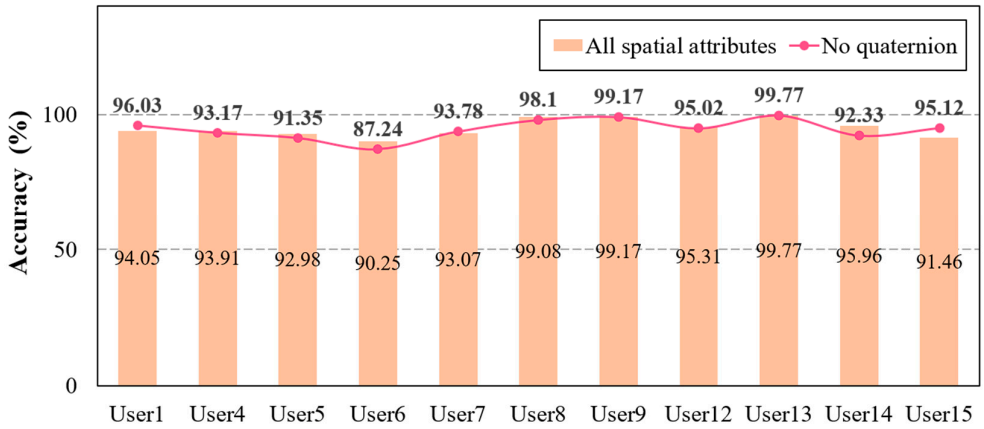


Figure 7. Comparison of accuracy among all spatial data and the combination of three data without quaternion.

5.2.3. Study 3: Significant Features

The findings of the second study confirmed that a feature set combining various spatial attributes is more effective for user identification than using individual attributes. It was also demonstrated that the proposed framework cannot adopt the feature set without the quaternion because its results include users with an accuracy of less than 90%. Driven by the previous findings, the final study was conducted to investigate the user identification accuracy of the significant features to optimize the ML classifier's complexity due to the use of all spatial attributes. Here, we first extracted and analyzed the top 10 features from all spatial attributes. Figure 8 illustrates the weights of the 10 major features.

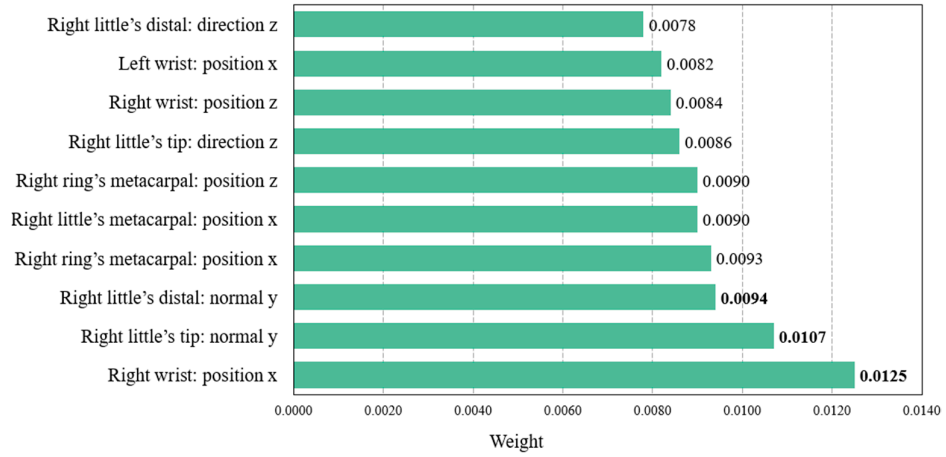


Figure 8. Major 10 features with weight in spatial attributes.

To summarize the results seen in Figure 8, it indicates that the wrist, little finger, and metacarpal point on the right hand—appearing more than three times in the significant features—have a great influence. Based on the findings, this study configured the wrist, little finger, and metacarpal of the right hand as each feature set, as well as a combined feature set encompassing all three (i.e., wrist, little finger, and metacarpal). The identifica-

tion accuracy for each configured set was then compared to the accuracy using all spatial attributes, as shown in Figure 9.

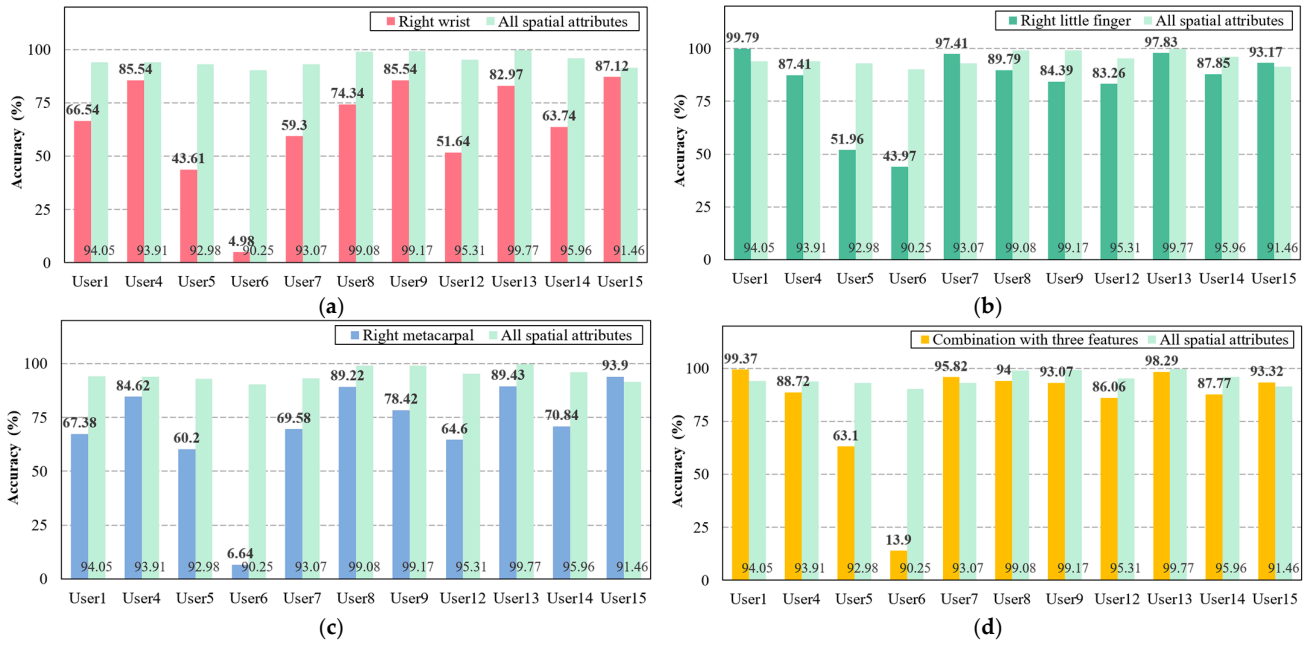


Figure 9. Comparison of user identification accuracy between all spatial attributes and each major feature or combination of three major features. (**a**) Accuracy of the right hand's wrist compared with all spatial attributes. (**b**) Accuracy of the right hand's little finger compared with all spatial attributes. (**c**) Accuracy of the right hand's metacarpal joints compared with all spatial attributes. (**d**) Accuracy of the combined three features compared with all spatial attributes.

The results show that all configured feature sets are difficult to use in our framework compared to the feature set using all spatial data. Specifically, in the right hand's wrist, the accuracy for all users was notably lower than in all spatial attributes. This trend was also consistent across other feature sets, with few exceptions among certain users. In particular, among many users, the identification accuracy of User6 decreased sharply, similar to Study 2. Consequently, this study analyzes significant features to optimize the classifier's complexity due to numerous features, but it determined that the feature set, including all features, remained the most suitable for the proposed framework.

5.2.4. Study 4: False Acceptance Rate (FAR) and False Rejection Rate (FRR)

In this final study, we analyzed the false acceptance rate (FAR) and false rejection rate (FRR) of the proposed framework. As FAR and FRR are indicators for evaluating authentication performance based on the trained model, the dataset collected on the first day (i.e., the training dataset) was excluded from the error rate calculation. In other words, error rates were calculated based only on the test dataset from 11 participants collected on the second day. Table 4 shows the findings of calculating FAR and FRR per user and their averages.

Table 4. Performance of FAR and FRR for each user.

Metric	Rates (%)											
	User1	**User4**	**User5**	**User6**	**User7**	**User8**	**User9**	**User12**	**User13**	**User14**	**User15**	**Average**
FAR	0.84	0.16	0.25	0.13	0.61	0.07	0.33	0.97	0.24	0.47	0.42	**0.41**
FRR	1.58	5.67	5.97	9.31	6.78	0.41	0.41	3.42	0.23	1.92	8.54	**4.02**

As shown in Table 4, the average FAR across all users was 0.41%, while the FRR was 4.02%. These results indicate that the proposed framework clearly identifies all users from others and maintains a low rate of false rejections. In particular, the proposed framework achieved a FAR of less than 1% for all users, which demonstrates that it is difficult for malicious attackers to successfully impersonate registered users. The average FRR for all users is also 4.02%, which means that intended users were rarely rejected, indicating that the framework consistently authenticated most users. Ultimately, the findings indicate that the proposed framework can be fully utilized as a continuous user authentication method in the Metaverse office.

5.3. Comparison with Prior Work

As discussed in Section 2, we analyzed previous studies on user authentication in the Metaverse. In this subsection, we compare the reviewed studies regarding task-driven user authentication in the Metaverse with the proposed framework. Specifically, we evaluate prior studies and the proposed framework depending on whether the defined authentication requirements were satisfied. Table 5 presents that the proposed framework and the prior studies satisfy specific requirements.

Table 5. Comparative evaluation of significant prior studies and our framework based on requirement satisfaction.

References	Requirements for User Authentication in the Metaverse				
	Continuity	**Universality**	**Non-Additional Sensor**	**Resistance to Shoulder Surfing**	**High Acceptability**
Shen et al. [16]	○	-	●	●	●
LaRubbio et al. [17]	○	●	-	●	-
Miller et al. [18]	○	-	●	●	●
Mai et al. [19]	○	●	●	○	●
Lu et al. [20]	●	○	-	○	○
Gopal et al. [21]	○	○	-	○	●
Suzuki et al. [22]	●	○	●	○	●
Jitpanyoyos et al. [23]	-	-	-	●	-
Our framework	●	●	●	●	●

Note that the symbols in the requirements denote the following: (●) is a study that fully satisfies the requirement, (○) is a study that partially satisfies the requirement, (-) is a study that does not satisfy the requirement.

As mentioned previously, "continuity," commonly referred to as continuous user authentication, is the first requirement. Continuity is essential in the Metaverse, where user sessions are longer than those in other systems. We found that continuity is fully addressed in [20,21] along with the proposed framework. In particular, continuous authentication was achieved in the framework when performing typing tasks in the office. By contrast, studies that utilized gait [16], gaze [17], ball tasks [18], and head movement [19] partially satisfied the continuity requirement, which was large because repetitive interactions can cause user fatigue despite the simplicity of tasks. Moreover, a study [22] adopted the simple task but depended on one-time passwords. Facial expression [23] is a one-time password and causes fatigue to users, as it is not realistically possible for users to maintain specific facial expressions.

"Universality" is the second requirement and is related to active authentication. Unfortunately, most studies have not fully met this requirement compared to other requirements. In other words, they adopted either domain-specific or infrequent tasks during user authen-

tication processes. For example, as mentioned previously, the gait task [16] is not typically performed in the Metaverse. Performing this task repeatedly for user authentication may also lead to discomfort due to the weight of the devices. A previous study [18] employed a dynamic ball game task; thus, their method is not suitable for domains that require static environments, such as professional office environments. In other words, the ball-based task is only used in the game domain. Their method may also induce fatigue if the users are required to repeat the task frequently to realize continuous authentication. Moreover, facial expression [23] is an infrequent task and not common. Other studies [20–22] partially satisfied this requirement; however, some limitations should be considered, particularly regarding non-implicit authentication factors. They are not implicit because the adopted tasks are not performed frequently; nevertheless, these tasks are common across various domains. In contrast, the proposed framework satisfies this requirement by adopting the common typing task, which is utilized in various domains, as the authentication task.

The third requirement is "non-additional sensors." Currently, HMDs are relatively heavy, which can impact user comfort. Thus, attaching additional IoT sensors to the HMD to realize continuous authentication is inappropriate. Nevertheless, several previous studies [17,20,21,23] required ancillary sensors to capture behavioral data during the adopted tasks. In particular, HMDs equipped with these sensors were employed in two existing studies [17,23] However, to the best of our knowledge, such sensors are not yet widely available outside high-end models. Other studies [20,21] require special wrist devices (e.g., smart gloves with Leap motion). Unlike these studies, numerous previous studies [16,18,19,22] and the proposed framework fully satisfied this requirement. The framework only requires a physical keyboard to perform the task, and the keyboard is a commonly adopted piece of equipment for the Metaverse office. In other words, additional sensors are not required to perform hand tracking, which is a common function in contemporary HMDs. The next requirement is "resistance to shoulder-surfing," which was partially satisfied by all studies. Immersive devices are widely utilized in the Metaverse; thus, this requirement appears to be largely satisfied. Specifically, several existing studies [16–18,22] and the proposed framework fully satisfiy this requirement. These methods rely on behavior-based user authentication, where imitation based on shoulder-surfing is difficult due to the inclusion of the user's physical characteristics and habitual behaviors. In contrast, several other studies [19–22] only partially addressed this requirement because they employed simple tasks that have the potential for imitation, even though behavior-based user authentication was adopted.

Finally, the "high acceptability" requirement is closely related to privacy, and this requirement is generally not satisfied in physiological biometric authentication due to the collection of sensitive data. In contrast, behavior-based user authentication primarily focuses on actions, which effectively satisfies this requirement in most cases. Thus, all previous studies [16,18,19,21,22] and the proposed framework fully satisfied this requirement, except for three excluded specific cases [17,20,23]. The excluded studies did not fully satisfy this requirement because they employ private data that users may find sensitive, such as eye gaze [17], signature [20], and facial expression [23]. In particular, users can refuse to utilize their gaze for authentication because the gaze reflects the user's preferences. In summary, we found that the proposed framework satisfied all requirements, especially "universality," which was not satisfied by most previous studies. In addition, most existing studies caused inconvenience in active and continuous authentication because they cannot be used in various domains or do not adopt general tasks. On the other hand, this study indicates that the proposed framework overcomes these limitations effectively.

6. Discussion

The proposed continuous user authentication framework was described in Section 3, and Section 4 presented a prototype implementation of the framework. Then, the framework was evaluated and compared with existing methods reported in the literature. In the following section, we discuss the proposed framework in general, including its assumptions, potential limitations, and corresponding future work.

6.1. Assumptions for the Proposed Framework

Prior to presenting the proposed framework, several assumptions were defined, which are briefly discussed in this subsection. As outlined in the first assumption, the framework requires an HMD that supports hand tracking and a Bluetooth-capable physical keyboard. Due to the increasing interest in the Metaverse, many HMDs have been released; however, hand tracking is not supported by some low-cost or older devices. In addition, the need for the physical keyboard was due to the limitations of immersive technology. Working with documents using a floating keyboard in virtual space is challenging with respect to speed and input compared with using a physical keyboard. Thus, many released applications for the Metaverse office support the use of physical keyboards. Driven by these limitations, this study currently defines supporting hand tracking by the HMD and the need for a physical keyboard as an assumption. However, we expect that these issues will be addressed and improved in the near future. Most recently released HMDs support hand tracking, and leading technology companies are researching methods to enable floating keyboards in virtual spaces to achieve input speeds that are comparable to those of physical keyboards [41].

In addition, we assumed that the keyboard and chair would remain in fixed positions while the user performs tasks. Hand tracking relies on positional data gathered from multiple cameras located at the front of the HMD, which means that the tracked hand position may vary with shifts in the position of the cameras. To mitigate this, we fixed the positions of the keyboard and chair to minimize the changes in the virtual hand positioning caused by these external factors (i.e., adjustments to the chair and keyboard). Fixing the HMD itself could have yielded more precise results; however, this approach, unlike the previous adjustments, would likely introduce significant discomfort for the users and was therefore excluded. Nevertheless, fixing the chair and keyboard may still cause some discomfort and, therefore, require further improvement. In the future, we plan to explore whether authentication is feasible using behavioral data collected in a free environment without these stabilizations.

6.2. Participants in the User Study

To demonstrate the feasibility of our framework, this study recruited participants for the user study and collected spatial data from virtual hands during a typing task, as the participants performed a business document-related task. This subsection discusses the participants in detail. Firstly, all participants, except three, had no experience with the HMD or the Metaverse. This lack of experience was expected to affect user identification accuracy; however, the result demonstrated a high accuracy rate of over 90% for all users. This result is likely attributed to the practice session conducted before the data collection process.

Meanwhile, most participants were non-native English speakers, and several participants faced challenges due to limited proficiency in English typing in the virtual office. As a result, four participants were excluded from the data collection process on the second day. In this regard, further study is required to investigate the influence of various factors, such as stress and fatigue. It is also necessary to analyze how these factors may impact the accuracy of the proposed framework based on the findings.

In the user study, a small group of 15 participants was recruited, and the data were collected over two days to validate the proposed framework. However, to fully show the framework's robustness and reliability, the proposed framework should be validated by a large-scale dataset from many users of text typing based on different languages. In particular, this dataset should also be collected over several days. For this reason, our future work plans to demonstrate the scalability of the proposed framework by generating a larger dataset over several days and recruiting more participants from diverse languages. The dataset will be shared in anonymized or synthetic datasets after IRB review to support further development in the authentication research field.

6.3. Evaluation of the Proposed Framework

This study conducted four experiments to evaluate the performance of the proposed framework. These experiments focused on verifying the accuracy of user identification and extracting the optimized feature sets. The feasibility of the proposed framework was also proved by achieving acceptable FAR and FRR. However, this study only uses a traditional ML model, i.e., random forest, without considering other ML models or deep learning models. The adopted model has many advantages for user authentication, but various experiments are needed to analyze which model is most suitable for optimizing the framework. In addition, the user study did not perform a security analysis of presentation attacks by setting up hypothetical attackers. This analysis is important to validate the proposed framework thoroughly. Therefore, future research will be conducted to compare the accuracy of security analysis with that of different models.

Although this dissertation analyzed the accuracy of user identification, it did not compare quantitatively with prior studies because the proposed framework is the first study to collect the dataset related to hand movements and dwell time using a physical keyboard in the Metaverse office. Thus, in this study, the framework was evaluated via identification accuracy and showed high accuracy; however, its evaluation should be performed using more diverse metrics (e.g., precision, recall, and F1-score) to clearly prove the framework's reliability. For this reason, a comprehensive evaluation of the proposed framework will be conducted based on various metrics in future work. The equal error rate (EER) will also be calculated using a large-scale dataset, since only user-wise FAR and FRR were presented in this study. This is because EER becomes more meaningful in large-scale datasets to demonstrate the strength of the framework. In other words, we plan to clearly prove the adversarial robustness of the proposed framework in a larger dataset as further work. As previously mentioned in Section 6.2, this large-scale dataset will also be published after IRB approval to support further development in the authentication research field as a form of a synthetic or anonymized dataset.

Nevertheless, this paper conducted a qualitative comparison of the user authentication requirements for the Metaverse, as a simple accuracy comparison is meaningless. The findings of the user study indicate that the proposed framework can also be used as an active and continuous user authentication method for the Metaverse office because it shows high accuracy and resolves the limitations of prior methods.

7. Conclusions

Driven by the demand for remote and hybrid work, large technology companies have released Metaverse applications for virtual offices. However, these applications frequently involve access to numerous confidential documents related to corporate goals to support efficient and flexible work, which can potentially be leaked by attackers. To mitigate this data leakage, various user authentication methods have been developed; however, these methods involve some limitations, such as remembering complex interactions with virtual

objects, requiring additional sensors, and performing dynamic tasks. Therefore, this study has proposed a continuous user authentication framework in the Metaverse office. The proposed framework performs user authentication using virtual hand movement and dwell time data while typing text. By adopting tasks commonly performed in the Metaverse office, the proposed framework realizes active and continuous user authentication. The proposed framework was evaluated experimentally, and the results demonstrated high accuracy in user identification. Thus, the proposed framework ensures a secure Metaverse office by preventing unauthenticated users from accessing and leaking confidential documents.

Author Contributions: The authors contributed to this paper as follows: G.K.: Writing—original draft, Writing—review and editing, Methodology, and Conceptualization; J.P.: Investigation, Formal analysis, and Writing—review and editing; Y.-G.K.: Project administration, Supervision, and Funding acquisition. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. RS-2024-00335672).

Data Availability Statement: Behavioral data were collected from 15 participants in this study. During the consent process, all participants were explicitly informed that their data would not be shared; thus, the collected data are not disclosed. However, in our future work, we plan to publish a synthetic or anonymized dataset with IRB approval to support further development in the authentication research field.

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

Abbreviations

The following abbreviations are used in this manuscript:

HMD	Head-mounted displays
IoT	Internet of things
OTP	One-time password
ML	Machine learning
IMU	Inertial measurement unit
IRB	Institutional review board
FAR	False acceptance rate
FRR	False rejection rate
ERR	Equal error rate

References

1. Great Expectations: Making Hybrid Work. Available online: https://www.microsoft.com/en-us/worklab/work-trend-index/great-expectations-making-hybrid-work-work (accessed on 2 June 2025).
2. Mahindru, R.; Bapat, G.; Bhoyar, P.; Abishek, G.D.; Kumar, A.; Vaz, S. Redefining Workspaces: Young Entrepreneurs Thriving in the Metaverse's Remote Realm. *Eng. Proc.* **2024**, *59*, 209. [CrossRef]
3. Dale, G.; Wilson, H.; Tucker, M. What is healthy hybrid work? Exploring employee perceptions on well-being and hybrid work arrangements. *Int. J. Workplace Health Manag.* **2024**, *17*, 335–352. [CrossRef]
4. Dwivedi, Y.K.; Hughes, L.; Baabdullah, A.M.; Ribeiro-Navarrete, S.; Giannakis, M.; Al-Debei, M.M.; Dennehy, D.; Metri, B.; Buhalis, D.; Cheung, C.M.K.; et al. Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *Int. J. Inf. Manag.* **2022**, *66*, 102542. [CrossRef]
5. Kang, G.; Koo, J.; Kim, Y.-G. Security and privacy requirements for the metaverse: A metaverse applications perspective. *IEEE Commun. Mag.* **2024**, *62*, 148–154. [CrossRef]
6. Turkmen, R.; Nwagu, C.; Rawat, P.; Riddle, P.; Sunday, K.; Machuca, M.B. Put your glasses on: A voxel-based 3D authentication system in VR using eye-gaze. In Proceedings of the 2023 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Shanghai, China, 25–29 March 2023.
7. Wazir, W.; Khattak, H.A.; Almogren, A.; Khan, M.A.; Din, I.U. Doodle-based authentication technique using augmented reality. *IEEE Access* **2020**, *8*, 4022–4034. [CrossRef]

8. Zhong, H.; Huang, C.; Zhang, X. Metaverse CAN: Embracing Continuous, Active, and Non-intrusive Biometric Authentication. *IEEE Netw.* **2023**, *37*, 67–73. [CrossRef]
9. 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 the 2019 IEEE International Conference on Embedded and Ubiquitous Computing (EUC), New York, NY, USA, 1–3 August 2019.
10. Salturk, S.; Kahraman, N. Deep learning-powered multimodal biometric authentication: Integrating dynamic signatures and facial data for enhanced online security. *Neural Comput. Appl.* **2024**, *36*, 1131–11322. [CrossRef]
11. Li, F.; Zhao, J.; Yang, H.; Yu, D.; Zhou, Y.; Shen, Y. Vibhead: An authentication scheme for smart headsets through vibration. *ACM Trans. Sens. Netw.* **2024**, *20*, 91. [CrossRef]
12. 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] [PubMed]
13. Boutros, F.; Damer, N.; Raja, K.; Ramachandra, R.; Kirchbuchner, F.; Kuijper, A. Iris and periocular biometrics for head mounted displays: Segmentation, recognition, and synthetic data generation. *Image Vis. Comput.* **2020**, *104*, 104007. [CrossRef]
14. Gupta, B.B.; Gaurav, A.; Arya, V. Fuzzy logic and biometric-based lightweight cryptographic authentication for metaverse security. *Appl. Soft Comput.* **2024**, *164*, 111973. [CrossRef]
15. Wang, M.; Qin, Y.; Liu, J.; Li, W. Identifying personal physiological data risks to the Internet of Everything: The case of facial data breach risks. *Humanit. Soc. Sci. Commun.* **2023**, *10*, 216. [CrossRef] [PubMed]
16. Shen, Y.; Wen, H.; Luo, C.; Xu, W.; Zhang, T.; Hu, W.; Rus, D. GaitLock: Protect virtual and augmented reality headsets using gait. *IEEE Trans. Dependable Secure Comput.* **2018**, *16*, 484–497. [CrossRef]
17. LaRubbio, K.; Wright, J.; David-John, B.; Enqvist, A.; Jain, E. Who do you look like?-Gaze-based authentication for workers in VR. In Proceedings of the 2022 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Christchurch, New Zealand, 12–16 March 2022.
18. Miller, R.; Ajit, A.; Banerjee, N.K.; 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.
19. Mai, Z.; He, Y.; Feng, J.; Tu, H.; Weng, J. Behavioral authentication with head-tilt based locomotion for metaverse. In Proceedings of the 2023 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Shanghai, China, 25–29 March 2023.
20. Lu, D.; Deng, Y.; Huang, D. Global feature analysis and comparative evaluation of freestyle in-air-handwriting passcode for user authentication. In Proceedings of the 37th Annual Computer Security Applications Conference (ACSAC), Online, 6–10 December 2021.
21. Gopal, S.R.K.; Gyreyiri, P.; Shukla, D. HM-Auth: Redefining User Authentication in Immersive Virtual World Through Hand Movement Signatures. In Proceedings of the 18th IEEE International Conference on Automatic Face and Gesture Recognition (FG), Istanbul, Turkiye, 27–31 May 2024.
22. Suzuki, M.; Iijima, R.; Nomoto, K.; Ohki, T.; Mori, T. PinchKey: A Natural and User-Friendly Approach to VR User Authentication. In Proceedings of the 2023 European Symposium on Usable Security (EuroUSEC), Copenhagen, Denmark, 16–17 October 2023.
23. Jitpanyoyos, T.; Sato, Y.; Maeda, S.; Nishigaki, M.; Ohki, T. ExpressionAuth: Utilizing Avatar Expression Blendshapes for Behavioral Biometrics in VR. In Proceedings of the 2024 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Orlando, FL, USA, 16–21 March 2024.
24. Lu, X.; Zhang, S.; Hui, P.; Lio, P. Continuous authentication by free-text keystroke based on CNN and RNN. *Comput. Secur.* **2020**, *96*, 101861. [CrossRef]
25. Darabseh, A.; Pal, D. Performance analysis of keystroke dynamics using classification algorithms. In Proceedings of the 2020 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA, 9–12 March 2020.
26. Tsai, C.-J.; Huang, P.-H. Keyword-based approach for recognizing fraudulent messages by keystroke dynamics. *Pattern Recognit.* **2020**, *98*, 107067. [CrossRef]
27. Rahman, A.; Chowdhury, M.E.H.; Khandakar, A.; Kiranyaz, S.; Zaman, K.S.; Reaz, M.B.I.; Islam, M.T.; Ezeddin, M.; Kadir, M.A. Multimodal EEG and keystroke dynamics based biometric system using machine learning algorithms. *IEEE Access* **2021**, *9*, 94625–94643. [CrossRef]
28. Bu, Z.; Zheng, H.; Xin, W.; Zhang, Y.; Liu, Z.; Luo, W.; Gao, B. Secure authentication with 3d manipulation in dynamic layout for virtual reality. In Proceedings of the 2023 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Shanghai, China, 25–29 March 2023.
29. 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 (AVI), Frascati, Rome, Italy, 6–10 June 2022.

30. Rupp, D.; Grießer, P.; Bonsch, A.; Kuhlen, T.W. Authentication in Immersive Virtual Environments through Gesture-Based Interaction with a Virtual Agent. In Proceedings of the 2024 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Orlando, FL, USA, 16–21 March 2024.
31. Li, P.; Pan, L.; Chen, F.; Hoang, T.; Wang, R. TOTPAuth: A Time-based One Time Password Authentication Proof-of-Concept against Metaverse User Identity Theft. In Proceedings of the 2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom), Kyoto, Japan, 26–28 June 2023.
32. Alrawili, R.; AlQahtani, A.A.S.; Khan, M.K. Comprehensive survey: Biometric user authentication application, evaluation, and discussion. *Comput. Electr. Eng.* **2024**, *119*, 109485. [CrossRef]
33. Chen, Z. Metaverse office: Exploring future teleworking model. *Kybernetes* **2024**, *53*, 2029–2045. [CrossRef]
34. Park, H.; Ahn, D.; Lee, J. Towards a metaverse workspace: Opportunities, challenges, and design implications. In Proceedings of the ACM CHI Conference on Human Factors in Computing Systems (CHI), Hamburg, Germany, 23–28 April 2023.
35. A-FRAME. Available online: https://aframe.io (accessed on 2 June 2025).
36. Aframe-Keyboard. Available online: https://github.com/WandererOU/aframe-keyboard (accessed on 2 June 2025).
37. Aframe-Hand-Tracking-Controls-Extras. Available online: https://github.com/gftruj/aframe-hand-tracking-controls-extras (accessed on 2 June 2025).
38. WebXR Hand Input Module—Level 1. Available online: https://immersive-web.github.io/webxr-hand-input/#skeleton-joints-section (accessed on 2 June 2025).
39. Murphy, C.; Huang, J.; Hou, D.; Schuckers, S. Shared dataset on natural human-computer interaction to support continuous authentication research. In Proceedings of 2017 IEEE International Conference on Biometrics (IJCB), Denver, CO, USA, 1–4 October 2017.
40. Liebers, J.; Brockel, S.; Gruenefeld, U.; Schneegass, S. Identifying users by their hand tracking data in augmented and virtual reality. *Int. J. Hum.-Comput. Interact.* **2022**, *40*, 409–424. [CrossRef]
41. Meta Develops Virtual Keyboard for Meta Quest. Available online: https://gadgetadvisor.com/gadgets/ar-vr/meta-develops-virtual-keyboard-for-meta-quest (accessed on 2 June 2025).

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