Usable Authentication in Virtual Reality: Exploring the Usability of PINs and Gestures

HTMA Riyadh[1,2], Divyanshu Bhardwaj[1,2], Adrian Dabrowski[1], and Katharina Krombholz[1]

[1] CISPA Helmholtz Center for Information Security, Germany
{htma.riyadh, divyanshu.bhardwaj, adrian.dabrowski, krombholz}@cispa.de
[2] Saarland University, Germany

Abstract. Virtual Reality (VR) is becoming increasingly popular with its ability to offer new forms of interaction, user interface, and immersion not only for recreation but also for work, therapy, arts, or education. These new spaces need to be safeguarded by authentication similar to conventional IT systems. However, porting conventional interfaces to VR has often been found to be less than optimal as it fails to fully embrace the technology's potential and potentially disrupt the immersive experience. This paper evaluates and compares the usability of two major authentication methods for VR: 2D Personal Identification Number (PIN) and gesture-based authentication - with 40 participants. While prior research has shown promising results in authentication security, there is a lack of studies specifically on usability in VR. Our findings indicate that the type of authentication and the user's experience level affect usability, with gesture-based authentication having a higher usability score than a PIN and having faster authentication times. Hereby, users with less VR experience profited the most from a natural interaction mode for VR. The results suggest that developers should rather choose a native interaction mode in VR than try to port a familiar conventional interaction such as number pads for PINs.

Keywords: Virtual Reality · Usability · Authentication · PINs · Gestures.

1 Introduction

Virtual Reality (VR) is an immersive technology that allows users to engage with computer-generated graphics in a virtual environment. In the wake of the COVID-19 pandemic, VR has become increasingly popular among researchers and consumers [2, 5, 37], resulting in a surge in revenue [42]. Although several authentication solutions have been offered for VR, usability studies related to VR authentication have not been given adequate consideration.

VR presents innovative methods of interacting with technology but questions the effectiveness and usability of traditional authentication techniques in this new realm. When using VR, users must authenticate themselves to access their confidential data. As such, it is crucial to safeguard users' data, ensuring their security and establishing trustworthiness through a seamless and user-friendly [35] authentication process in virtual reality. Presently, different authentication methods are being proposed, such as knowledge-based authentications like PIN [15], Pattern Lock [15], 3D Password [3], 3D Pattern [48], or biometric-based authentication [26, 34, 44]. Although these methods offer robust security, they often sacrifice usability.

To address the need for better authentication in VR, we conducted a between-subjects design user study with N=40 participants. Our research was guided by two key questions:

1. Does the authentication type impact the authentication usability in Virtual Reality?
2. Does the authentication usability vary based on the user's experience with Virtual Reality?

To address these inquiries, we explored two authentication methods: a 2D PIN and a gesture-based authentication. PIN is a well-established traditional authentication process that users frequently use daily. We used the classic 4-digit numerical PIN pad. In contrast, gesture-based authentication is a knowledge-based authentication process relatively new to most users. We utilized four single-hand alphabetic mid-air gestures in a 3D space. The gestures simulated drawing on a 2D touch surface.

Our study revealed that participants with prior experience generally performed better in PIN-based authentication, while no significant differences were observed in gesture-based authentication. These results suggest that experience may have less impact on performance when the design of the VR system follows natural interaction patterns. Interestingly, despite the widespread use of PINs in daily activities and authentication methods, our findings indicate that their performance decreases when used in VR. This could be attributed to the differences in input modalities, as gestures were found to be a more natural and intuitive means of interaction, leading to a better performance and usability.

Our research provides valuable insights into the naturalness of input modalities in VR, which can aid developers in implementing more effective authentication methods that are both user-friendly and secure. Additionally, our usability study enhances our comprehension of user interaction, which we hope can prove beneficial in the design of VR applications moving forward.

The rest of this paper is structured as follows: In Section 2, we provide some background knowledge to help our readers understand the work-related topics, terms, and technologies. After that, Section 3 dives deep into the previous work on VR authentication and usability. Section 4 outlines our study design, methodology, and a brief discussion about user study. Sections 5 and 6 characterize our results, followed by the discussion. Section 7 contains the conclusion and future work.

2 Background

This section provides the prerequisite context and information for readers to engage with the paper.

2.1 Virtual Reality

Virtual Reality (VR) is an advanced computer graphic-generated human-computer interface that simulates a realistic environment. In VR, users have the ability to immerse themselves in experiences that can either replicate real-world scenarios or transport them to entirely different environments. VR evolved from the early stages of computer graphics, which began in the mid-1960s to the early 1970s. At that time, it was referred to as Artificial Reality. The term 'Virtual Reality' [30] was first coined by Jaron Lanier, the founder of VPL Research. Nowadays, VR uses a mixture of different senses like light, touch, sound, and tactile feedback to generate more natural experiences. Head-Mounted Display (HMD) is used in standard VR systems as a display device. Augmented Reality smart glasses augment the virtual world to the real world and allow users to interact in real-time [40]. Figure 1 demonstrates two popular forms of VR display devices.

VR is based on two core ideas: immersiveness and interactivity. VR is fully immersive because it is built in such a way that it keeps the user away from other environmental distractions by blocking surroundings selectively. One of the primary objectives of VR is to immerse users in a virtual environment in a way that makes them feel as if they are present in the real world. Achieving this requires taking into account factors such as human psychology, anatomy, user perspective, and environmental awareness [18]. The applications of VR are vast, from medical research and training simulations to online gaming, virtual shopping, and even conferences and meetings. Due to its widespread usage, the VR market has grown significantly [42], with its current size estimated at 28.42 billion USD in 2022, up from 21.83 billion USD in the previous year. As VR technology continues to evolve, it is becoming more accessible to people from all walks of life.

(a) Head Mounted Display (HMD) (b) Augmented Reality Glass

Fig. 1: VR Display Device

2.2 Authentication

Authentication is the process of recognizing a user's identity. It ensures the prevention of unauthorized access to sensitive data. User identification usually can be done by sending a secret code/password to the system [10]. This secret passcode can consist of four factors: (1) Something you know e.g., password, pattern, etc. (2) Something you are e.g., biometric features, fingerprint, etc. (3) Something you own e.g., ID card (4) Something you do e.g., typing pattern, pupil movement. Accessing the storage, intercepting the communication channel, or disclosing information can compromise the security of a secret password [23]. Therefore, authentication is crucial for data protection from the end-user perspective. Various mechanisms, such as numeric PINs, fingerprints, biometric features, and pattern locks, can authenticate the true user. The usability of authentication hinges on finding the right balance between security and user experience. Complex authentication procedures may discourage users or result in insecure practices, such as overly simplistic passwords.

2.3 Usability

Usability is one of the fundamental properties of a system or a process that defines how easily, effectively, efficiently, and safely a task can be performed. It is a measure of user satisfaction in a specific context. Usability vastly depends on human behavior and psychology. The quality of a product, software, device, or service is sometimes measured by its usability study. The 1996 System Usability Scale (SUS) [9] by Brooke is frequently used to evaluate the usability of a system. Later, Peres et al. validated that SUS can be used to compare two more systems [36].

There exists a reciprocal relationship between usability and security [49]. When security is prioritized, usability may suffer. An illustration of this is the common requirement for 11-character passwords containing at least one uppercase, one lowercase, one number, or one special character. These complex passwords can be difficult for users to recall, reducing usability and prompting evasive behavior – which in turn lowers security. Therefore, usability is an integral consideration throughout the design process.

3 Related Work

3.1 Interaction in VR

Different input modalities are used to interact with the virtual environment in VR, such as controller tapping, gaze input, head pose, or body gestures. People are habituated to using a physical keyboard, mouse, device, or hard surface as an input medium. In a virtual environment, for example, typing on a virtual keyboard or deforming an object (e.g., Rubik's Cube) lacks haptic feedback. The missing feedback degrades the usability of the virtual input systems [14].

UI designers try to work around this limitation. For example, tapping can mimic real-world interaction, and pointing-based interaction (e.g., a laser beam) in VR enjoys popularity. A study by Hale et al. [16] discourages using pointers as an input method because it does not follow the natural interaction of real life. They also emphasize the precision problem on small screens. However, Ballagas et al. [6] showed that on large public displays, pointer-based interaction is useful and, indeed increases usability. In our study, we adopted the previous studies and combined both pointers and tapping as interaction concepts in the development. See Table 5 in the Appendix for our adaptation decision.

3.2 Authentication in VR

At the time of writing, available devices such as HTC Vive[3], or Oculus Quest[4] provide high-end usability and portability [12,39]. These devices are wireless and self-contained with an in-built display screen. But in some cases, they lack seamless interaction. For example, the authentication process sometimes requires a second device or the removal of the headset. While VR does offer some options for seamless and continuous authentication [33, 38, 43], the usability of the authentication process has often been overlooked in favor of prioritizing security and overall VR experience.

From the users' perspective, seamless authentication is necessary. Taking off the VR set to provide a secret code breaks the immersion and the experience. Researchers have proposed various solutions for VR authentication. These solutions can be categorized into the following groups:

Traditional Authentication Methods: These are predominantly based on the "something you know" principle. Established authentication methods such as Personal Identification Numbers (PINs), patterns, or passwords are widely used and accepted. They are time efficient and well integrated in 2D devices like mobile phones [46]. Initial research claimed that 2D devices' authentication methods are not well suited in virtual reality [3], as they are vulnerable to observation attacks [19, 31, 46]. To bolster the security of PINs, Krombholz et al. [21] proposed incorporating a pressure-sensitive layer into screens that would provide an additional pressure dimension when entering PINs, mostly invisible to shoulder surfers. They evaluated these *force-PINs* in touch screen devices and showed that it could increase the entropy of PINs without sacrificing usability. Furthermore, Lu et al. [27] proposed 3D passwords as an alternative, assuming they would be more secure due to the added dimension, thereby preventing shoulder surfing attacks. However, recent works show that PINs can be used for authentication in VR [32, 48]. A comparative study by George et al. [15] found that PINs are suitable in the VR space due to their fast input speed. This is because PINs can be easily input in VR by tapping or pointing; while drawing a pattern on a 2D or 3D surface can be challenging as it relies on motor skills [15]. After considering

[3] https://www.vive.com/
[4] https://www.meta.com/quest/

all the options, we decided to use PINs as the baseline of a traditional method of authentication for our study.

Behavioural Biometric Authentication: Behavioral biometric authentication leverages the human behavior patterns such as body movements [25], head movements [43], or gestures [22, 38]. Behavioral biometrics has recently become increasingly popular due to its ability to block guessing and shoulder-surfing attacks [27]. This authentication method can be categorized into gesture, gaze, and rhythm-based authentication. However, one major drawback of behavioral biometrics is its observability, making it unsuitable for most public settings. Furthermore, the HMD obstructs the participant's vision. In 2009, Hansen et al. [17] reviewed gaze-based studies from the past 30 years and proposed that gaze features have unique characteristics that could be utilized for authentication. Eye movements, blinking, velocity, and other behaviors are distinctive [11, 28, 41, 49] and can be used successfully to authenticate users. However, these biometric features demand a high cognitive load and are less user-friendly. Consequently, Mustafa et al. [34] suggested using behavioral biometric features in conjunction with other security measures as an added layer of security in VR applications that require rigorous protection. They also highlighted the potential challenges of relying solely on behavioral biometrics in a large-scale setting.

Knowledge-Based Biometric Authentication: Knowledge-based biometric authentication is a hybrid authentication method that leverages the strengths of both knowledge-based and biometric authentication methods. It offers a higher level of security and accuracy by validating the user's identity through a combination of something they know (knowledge-based authentication) and something they are (biometric authentication). The knowledge-based component involves the user providing information only they should know, while the biometric component uses physiological or behavioral characteristics to identify the user. While knowledge-based authentication methods are robust against traditional attacks, researchers have found novel attacks that exploit human traces on smartphone touchscreens, such as smudge [4], thermal [1], and microbiological attacks [20]. In light of this, Mathis et al. [32] suggested including hand movement patterns during PIN entry as an additional layer of protection.

3.3 Usability issues in VR authentication

One of the critical components of immersive technologies is their ability to integrate into our lives seamlessly. To achieve this, continuous authentication can be a viable solution for VR usage [43]. As VR headsets cover the user's eyes, they become less aware of their surroundings, hindering their 'body and environment awareness' and skills [18]. Therefore, an implicit and smooth authentication process is essential for VR. Research conducted by Zhu et al. [49] found that if security measures are too stringent, usability tends to suffer. Overly complex passwords may increase security (in the short run) but lower usability and user-friendliness, prompting possible evasive user behavior (e.g., writing them down).

Table 1: Pros and Cons of authentication in VR by their category.

Traditional Authentication	
Pros:	**Cons:**
- Well established	-Not hands free
- Easy to transfer	-Interruption in interaction

Behavioural Biometric Authentication	
Pros:	**Cons:**
-Implicit interaction	-Low stability
-Continuous auth.	-Depends on cognitive mode
-Not observable	-Expose user in public space

Knowledge-Based Biometric Authentication	
Pros:	**Cons:**
-Added extra layer of security	-Memorability
-Implicit interaction	
-Protection in public space	

There is always a trade-off between security and usability. Keeping a balance between them is a tedious task in the design process for an authentication mechanism. The main goal is to maintain an ecosystem where users are protected without feeling burdened.

4 Study Design and Implementation

Our study employed a between-subjects design, consisting of two groups that were further divided based on their VR experience. Using two distinct methods, we obtained user authentication data and followed up with questions regarding their usability, based on the System Usability Scale (SUS) [9]. One group was given a four-digit PIN, while the other used gesture-based authentication. A total of 40 (mean age=29.02, SD=6.78, 67.5% male) people participated in our study. The overview of our study design and population is shown in Figure 2.

Participants were recruited through social media advertising and posters in public spaces, such as bus stops and cafeterias. The recruited individuals represented diverse study programs and had backgrounds in both technical and non-technical fields. Participants received no financial compensation, and the study was entirely voluntary.

Based on our experiment design, we determined that a between-subject study would be the most appropriate choice for our sample category. This was done to eliminate any potential learning and ordering effects for participants. Login time and SUS score usability metrics were measured throughout the user study. VR authentication application was developed using C# in Unity 3D, and Oculus Integration 46.0 SDK (OVR) was used for the interaction framework and

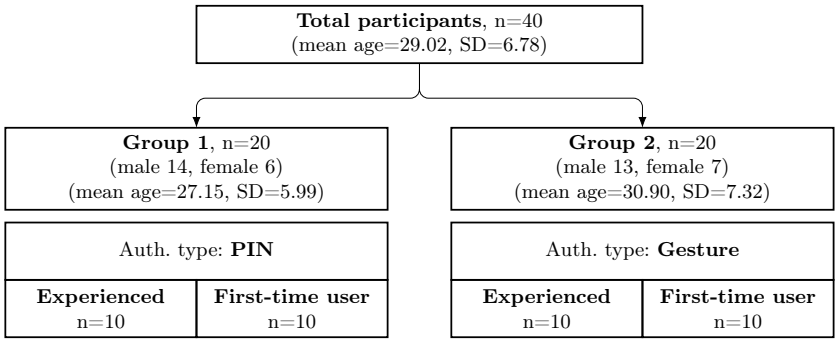


Fig. 2: Participant distribution for data collection.

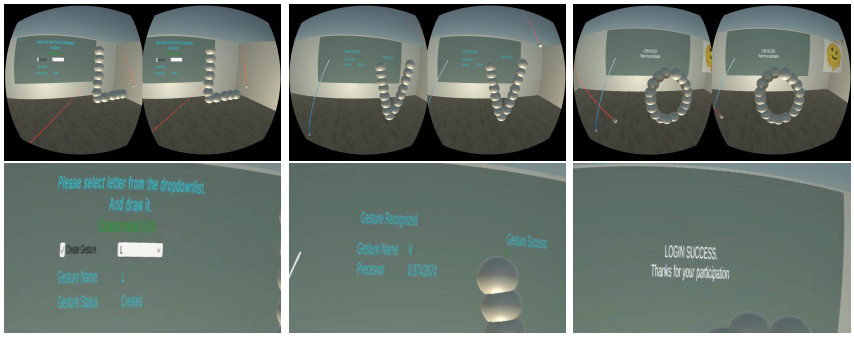
displayed in Oculus Quest 2 HMD. Figure 3 shows the layout of the interface. Table 5, in the Appendix, summarizes our decision to select PIN authentication.

4.1 Methodology

The PINs had a four-digit length, and handwriting gestures comprised four symbols. Both were generated at random to ensure uniqueness among participants. We employed the login time calculation proposed by George et al. [15], which begins at the start of the virtual interface interaction and ends upon password entry via pointing and pressing the enter button. Wrist movements and relative wrist coordinates were used to identify gestures, with any four letters from the English alphabet (capitalized or lowercase) accepted for recognition. Stroke order and direction were disregarded to eliminate the need for users to remember during training/sample collection. This approach was inspired by the Point Cloud Recognizer [45] and adapted to accommodate 3D gesture recognition, utilizing the controller gyroscope and inbuilt HMD's camera to track hand and wrist positions and coordinates during movement.

(a) Registration (b) Authentication (c) Login Success

Fig. 3: UI for 4-digit PIN



(a) Registration (b) Authentication (c) Login Success

Fig. 4: Different phases of gesture recognition authentication (full view and closeup)

4.2 Recruitment

We conducted the study with 40 university graduate students from various departments. Our recruitment strategy was informed by VR market analysis, which suggested that individuals between 16 and 34 are more likely to use VR [24]. Therefore, we focused on selecting participants falling within this demographic. Our selection process took into account prior experience with VR. Experienced users had used VR systems at least five times before, whereas first-time users had never interacted with VR before. There were no in-betweens. All participants possessed normal vision and were right-handed. They did not receive any financial compensation.

4.3 Data Collection

We divided our participants into two authentication groups. Figure 2 shows the participants' distribution for the data collection process.

Prior to commencing the study, we presented our research protocol and informed participants about our data collection methods. We proceeded to request their consent, giving them the opportunity to decline if they were not comfortable with the process. Following this, we provided a brief training session and introduced them to the VR setup and the input modality. We provided a tutorial to build familiarity with the authentication method (either PIN or gesture). Participants were then asked to enter their respective authentication type (PIN or gesture). During the trial run, most participants entered their authentication type once.

Participants were assigned a four-digit PIN or a four-letter gesture for the main experiment. Gestures incurred the additional step of registering them first (training the system). Subsequently, participants would authenticate themselves with those credentials once. The login time was measured from the beginning of the interaction until the authentication succeeds, i.e., if the user needed to

re-enter because of a failed authentication, the total time across all the attempts was considered. Visual feedback in text form informs about the success or failure of the authentication.

In a post-study questionnaire, we collected users' usability evaluation of our authentication systems through a System Usability Scale (SUS) questionnaire [9]. SUS is a quantitative method to evaluate the usability of a system and provides a higher-level overview of the product from the user's perspective. SUS is also frequently used as a usability comparison tool between two systems [36].

4.4 Pilot Testing

Two participants who wore glasses encountered difficulties with our HMD. Specifically, one expressed that they could only see a blur while experimenting. As such, we limited recruiting to participants without corrective glasses. Additionally, our pilot study revealed that four participants favored a lighter-colored pointer. Thus, we changed the pointer color to a light blue when pointing to a button and a dim white when pointing somewhere else.

4.5 Data Analysis

Section 5.1 delves into the impact of authentication type on usability. We analyzed SUS scores for both PIN and gesture for all 40 participants without considering experience. To compare the difference between independent sample SUS scores for the two authentication types, we conducted the Wilcoxon Rank Sum Test [47].

Subsequently, in Section 5.2, we analyzed the impact of authentication type on login time. We conducted a statistical analysis to assess the performance of both methods. Since our data did not follow a normal distribution, we used the Independent-Samples Mann-Whitney U test [29], which is a non-parametric statistical analysis.

We furthered our analysis by factoring in experience to examine the impact of authentication types on both usability and login times. We repeated the tests mentioned above within each group for first-time and experienced participants for both PIN and gesture authentication types.

4.6 Ethical Considerations

No real credentials were used in the study. Our study was designed to minimize the need for personally identifiable information. We took steps to anonymize all data before processing it. Every participant was required to fill out a consent form and was free to ask questions and withdraw from the study at any time, both during and after participation. We made it clear that their decision to participate was entirely voluntary and that their privacy was paramount to us.

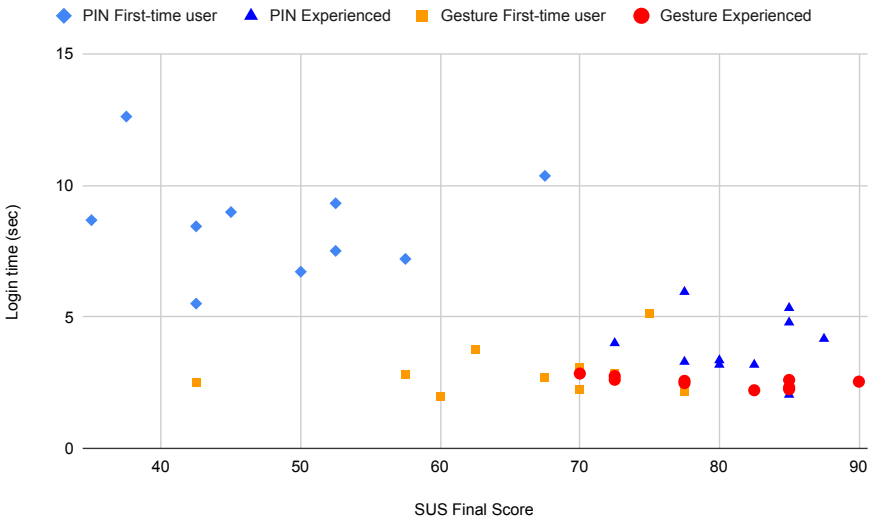


Fig. 5: Login times compared to SUS scores and participant groups

5 Results

Our findings show that experienced users rate the usability of PIN and gesture-based authentication equally and perform similarly on both, although PIN may take them more time to log in. However, first-time users, especially when using PINs, tend to perform significantly worse both in terms of usability and login time. Conversely, gesture-based authentication is generally faster and more readily embraced by those new to virtual reality. Figure 5 gives a broad overview of our results. The following sub-sections provide a detailed analysis of our findings.

5.1 Authentication Type and Usability

Wilcoxon Rank Sum Test shows that authentication type has a significant (Z=-2.320, p=0.02, rejection level=0.05) effect on system usability with a medium (r=0.37) effect size. On a five-point (1=strongly disagree, 5=strongly agree) System Usability Scale, participants show more preferences for gesture-based authentication. Table 2 presents the summary of the SUS score of each authentication method. Overall, our findings show that gestures have a higher acceptability than PINs. Thus, according to the classification from Bangor et al. [7], gesture authentication scores as 'Acceptable' while PIN scores only 'High Marginal' in acceptability.

5.2 Authentication Type and Login Time

Independent-Samples Mann-Whitney U Test shows that login time (mean=4.486, SD=2.706, median=3.195, n=40) statistically differs ($p=.001 < .05$) based on

Authent-ication Type	Experience	Count	Mean	Min	Max	Grade Scale	Acceptability [7]
PIN	Experienced	10	81.25	72.5	87.5	B	Acceptable
	First-time user	10	48.25	35	67.5	F	Not Acceptable
	Overall	20	64.75	35	87.5	D	Marginal (High)
Gesture	Experienced	10	79.75	70	90	C	Acceptable
	First-time user	10	65.50	42.5	77.5	D	Marginal (High)
	Overall	20	72.63	42.5	90	C	Acceptable

Table 2: SUS Score Summary

the authentication type. Login time depends on the authentication type. Our statistical test indicates a significant difference (U=30, Z=-4.599, p=.001) to gesture (mean rank=12.0, median=2.599, n=20) and PIN (mean rank=29.0, median=5.74, n=20). Gestures as an authentication method require less time to log in compared to PIN. This notable speed difference shows that users are able to log in at a faster pace when using gestures rather than a PIN. Table 3 summarizes the login time for each authentication method.

Authentication Type	Experience	Count	Mean	SD	Min	Max
PIN	Experienced	10	3.94 s	1.17	2.06 s	5.96 s
	First-time user	10	8.54 s	2.0	5.51 s	12.61 s
	Overall	20	6.24 s	2.85	2.06 s	12.61 s
Gesture	Experienced	10	2.53 s	0.21	2.22 s	2.85 s
	First-time user	10	2.94 s	0.93	2.00 s	5.14 s
	Overall	20	2.73 s	0.69	2.00 s	5.14 s

Table 3: Login time summary

5.3 PIN: Experienced vs. First-time User

We also examined whether VR experience has an impact on usability. We found that participants with prior VR experience scored significantly (Z=-3.79, p=.001) higher on the SUS scale than first-time participants with a large effect size. Our results show that experienced participants are more confident using the PIN authentication and provide a high average score of 4.8/5 by answering question 9 (*[Q9] "I felt very confident using the system"*), whereas first-time

users rate it as 2.5/5. From question 10 (*[Q10] "I needed to learn a lot of things before I could get going with this system"*), we can infer that first-time users may need some time to learn how to use the VR system. This may lead to a lack of confidence in using the PIN to log in to the system, affecting the time taken to log in. Based on the Independent-Samples Mann-Whitney U Test, we found that participants with VR experience take significantly less time (p=.001, Z=-3.704) to log in than those with no prior VR experience. Figure 6 compares the average SUS score for each question when using PIN for authentication while taking experience into account.

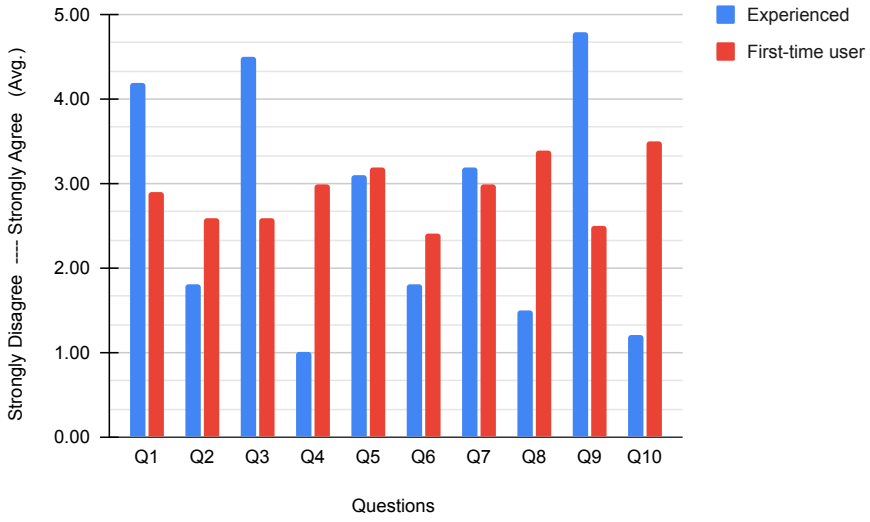


Fig. 6: Average SUS score of the individual questions for PIN

5.4 Gesture: Experienced vs. First-time User

The Independent-Samples Mann-Whitney U Test demonstrates no significant difference (U=37, Z=.983, p=.353) in login time between experienced users (median=2.57, n=10) and first-time users (median=2.28, n=10). However, the same statistical test for usability shows that experienced users score significantly higher than first-time users (U=10, Z=-3.042, p=.002). It is worth noting that while the SUS score indicates experience has an impact on using gesture authentication, login time suggests otherwise. One possible explanation for this discrepancy is that PIN entry requires a specific motor task confined to a fixed surface area, whereas gesture authentication allows for more natural, free movement. Participants with no VR experience report feeling more confident using

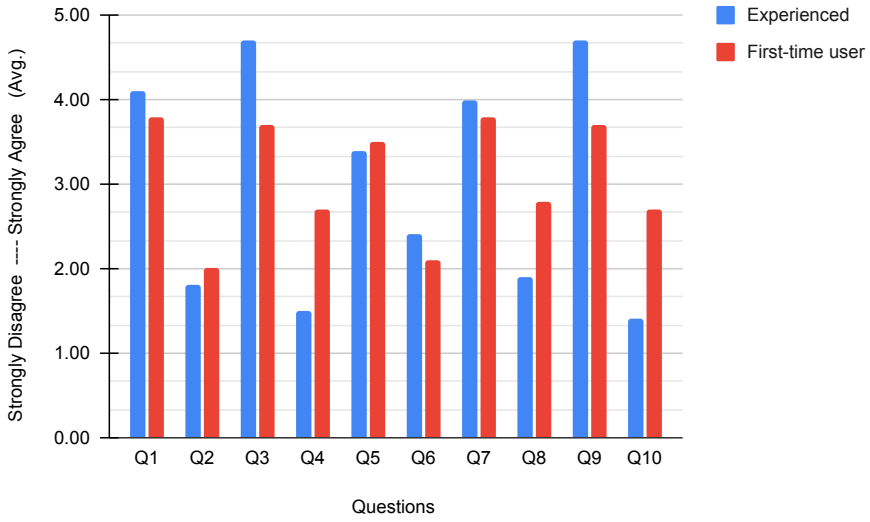


Fig. 7: Average SUS score of the individual questions for Gesture

gesture authentication than PIN (Q9, score 3.7 vs. 2.5). Figure 7 compares the average SUS score for each question, when using gesture for authentication while taking experience into account.

6 Discussion

A developer can follow two major schools of thought when porting a process from conventional GUI to VR.

For one, focus on familiarity with the conventional 2D user interface and try to mimic that as closely as possible. The idea is to increase usability by tapping into what users already learned and know from the 2D world and thus reduce adaption costs.

The other school of thought is to increase usability by natively integrating it into the new medium at the expense of familiarity. The benefit here is the seamless and coherent integration into the advanced interaction capabilities and the internal working logic of the virtual world.

Our results clearly suggest that familiarity gains from the 2D world weigh much less than one might expect. Native VR methods that take advantage of the new UI style should be preferred. In our study, gesture-based handwriting authentication provided security levels similar to the 2D PIN while delivering the most benefits to first-time users and significantly improving the performance of experienced users.

6.1 Impact of Authentication Type on Usability in VR

Our findings indicate that authentication type influences usability. Participants found gesture authentication to be *acceptable*, while PIN was only rated as *marginally acceptable* [7]. Though PIN is established and one of the faster (1.5 seconds) [46] authentication methods in a mobile device, in our study, PIN authentication took 6.24 seconds on average, while gesture authentication took only 2.74 seconds. This login time difference affected the usability score, implying that if the established PIN is transferred to the VR space, there is a significant performance drop, reducing the usability.

The data demonstrates that conventional authentication methods, such as the PIN, may be less effective in the immersive VR world, where users prefer more natural interactions. Our study participants showed that they favored gesture-based authentication, emphasizing the importance of modifying authentication methods to cater to the particular requirements of VR and improve overall usability.

6.2 Impact of Experience on Usability in VR

Our findings also indicate that experience has an impact on the overall usability of the authentication system. For both the PIN and the gesture authentication method, experienced participants provided a higher usability score than first-time participants.

Familiarity and learning curves play a significant role in technology adoption, particularly in immersive environments like VR. The greater ease experienced by first-time participants with gestures suggests that incorporating natural and intuitive interactions has a shorter learning curve for newcomers, thereby facilitating a smoother transition into VR. This implies that VR applications aimed at a diverse user base, including beginners, may benefit from prioritizing user-friendly, gesture-based interactions. Additionally, adaptive VR interfaces that adjust authentication and interaction methods based on the user's experience level can enhance overall usability.

6.3 Limitations

By recruiting student participants from mostly technology-related fields, our sample only partially represents the general population. On the other hand, our recruitment selected participants that align with the market analysis of VR users [24], i.e., technology-affine aged between 16 and 35. Furthermore, we conduct our research in a lab setting that ensures a controlled environment, though expanding to diverse settings can enhance the generalizability of our results. We believe that our research provides a strong foundation for understanding the usability of PIN and gesture authentication in VR, and our findings hold valuable implications for improving the usability design of authentication methods.

7 Conclusion and Future Work

This paper assesses the usability of two distinct authentication methods in virtual reality - one utilizing a familiar number pad for PINs and the other a handwriting gesture. Based on factors such as login time and SUS score, it then pinpoints the factors that influence the usability of those VR authentication methods. The data shows that the type of authentication interaction and the user's proficiency in virtual reality significantly impact the authentication process's usability. In particular, the naturalness of interaction, such as with gesture-based authentication, is crucial for usability.

The research has shown promising directions regarding the usability of authentication in virtual reality. Moving forward, we aim to broaden our investigation to include more authentication methods and interaction styles. Furthermore, we intend to conduct our study in both laboratory and natural settings. Additionally, future work should examine how factors such as design, behavior, and context influence authentication usability.

References

1. Abdelrahman, Y., Khamis, M., Schneegass, S., Alt, F.: Stay cool! understanding thermal attacks on mobile-based user authentication. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. pp. 3751–3763 (2017)
2. Alsop, T.: VR device shipments by vendor worldwide 2017-2019 (Feb 2022), https://www.statista.com/statistics/671403/global-virtual-reality-device-shipments-by-vendor/
3. Alsulaiman, F.A., El Saddik, A.: A novel 3D graphical password schema. In: 2006 IEEE Symposium on Virtual Environments, Human-Computer Interfaces and Measurement Systems. pp. 125–128. IEEE (2006)
4. Aviv, A.J., Gibson, K., Mossop, E., Blaze, M., Smith, J.M.: Smudge attacks on smartphone touch screens. In: 4th USENIX Workshop on Offensive Technologies (WOOT 10) (2010)
5. Ball, C., Huang, K.T., Francis, J.: Virtual reality adoption during the covid-19 pandemic: A uses and gratifications perspective. Telematics and Informatics **65**, 101728 (2021)
6. Ballagas, R., Rohs, M., Sheridan, J.G.: Sweep and point and shoot: phonecam-based interactions for large public displays. In: CHI'05 extended abstracts on Human factors in computing systems. pp. 1200–1203 (2005)
7. Bangor, A., Kortum, P., Miller, J.: Determining what individual sus scores mean: Adding an adjective rating scale. Journal of usability studies **4**(3), 114–123 (2009)
8. Bi, X., Li, Y., Zhai, S.: Ffitts law: modeling finger touch with fitts' law pp. 1363–1372 (2013)
9. Brooke, J., et al.: Sus-a quick and dirty usability scale. Usability evaluation in industry **189**(194), 4–7 (1996)
10. Burrows, M., Abadi, M., Needham, R.: A logic of authentication. ACM Transactions on Computer Systems (TOCS) **8**(1), 18–36 (1990)
11. Cantoni, V., Galdi, C., Nappi, M., Porta, M., Riccio, D.: Gant: Gaze analysis technique for human identification. Pattern Recognition **48**(4), 1027–1038 (2015)

12. Craddock, I.M.: Immersive virtual reality, google expeditions, and english language learning. Library Technology Reports **54**(4), 7–9 (2018)
13. Doronichev, A.: Daydream labs: exploring and sharing VR's possibilities. Retrieved April **10**, 2020 (2016)
14. Earnshaw, R.A.: Virtual reality systems. Academic press (2014)
15. George, C., Khamis, M., von Zezschwitz, E., Burger, M., Schmidt, H., Alt, F., Hussmann, H.: Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality (2017)
16. Hale, K.S., Stanney, K.M.: Handbook of virtual environments: Design, implementation, and applications. CRC Press (2014)
17. Hansen, D.W., Ji, Q.: In the eye of the beholder: A survey of models for eyes and gaze. IEEE transactions on pattern analysis and machine intelligence **32**(3), 478–500 (2009)
18. Jacob, R.J., Girouard, A., Hirshfield, L.M., Horn, M.S., Shaer, O., Solovey, E.T., Zigelbaum, J.: Reality-based interaction: a framework for post-wimp interfaces pp. 201–210 (2008)
19. Khamis, M., Alt, F., Hassib, M., von Zezschwitz, E., Hasholzner, R., Bulling, A.: Gazetouchpass: Multimodal authentication using gaze and touch on mobile devices. In: Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems. pp. 2156–2164 (2016)
20. Krombholz, K., Dabrowski, A., Weippl, E.: Poster: The petri dish attack-guessing secrets based on bacterial growth (2018)
21. Krombholz, K., Hupperich, T., Holz, T.: Use the force: Evaluating {Force-Sensitive} authentication for mobile devices. In: Twelfth symposium on usable privacy and security (SOUPS 2016). pp. 207–219 (2016)
22. 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: 25th International Conference, MMM 2019, Thessaloniki, Greece, January 8–11, 2019, Proceedings, Part I 25. pp. 55–67. Springer (2019)
23. Lamport, L.: Password authentication with insecure communication. Communications of the ACM **24**(11), 770–772 (1981)
24. Laricchia, F.: UK: VR headset owners by age 2023 (Aug 2023), https://www.statista.com/statistics/1362661/share-of-vr-headset-owners-by-age-uk/
25. Liebers, J., Abdelaziz, M., Mecke, L., Saad, A., Auda, J., Gruenefeld, U., Alt, F., Schneegass, S.: Understanding user identification in virtual reality through behavioral biometrics and the effect of body normalization. In: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. pp. 1–11 (2021)
26. Lin, F., Cho, K.W., Song, C., Xu, W., Jin, Z.: Brain password: A secure and truly cancelable brain biometrics for smart headwear. In: Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services. pp. 296–309 (2018)
27. Lu, D., Lee, T., Das, S., Hong, J.I.: Examining visual-spatial paths for mobile authentication. In: WAY@ SOUPS (2016)
28. Luo, S., Nguyen, A., Song, C., Lin, F., Xu, W., Yan, Z.: Oculock: Exploring human visual system for authentication in virtual reality head-mounted display. In: 2020 Network and Distributed System Security Symposium (NDSS) (2020)
29. MacFarland, T.W., Yates, J.M., MacFarland, T.W., Yates, J.M.: Mann–whitney u test. Introduction to nonparametric statistics for the biological sciences using R pp. 103–132 (2016)
30. Machover, C., Tice, S.E.: Virtual reality. IEEE Computer Graphics and Applications **14**(1), 15–16 (1994)

31. Maguire, J., Renaud, K.: You only live twice or" the years we wasted caring about shoulder-surfing". arXiv preprint arXiv:1508.05626 (2015)
32. Mathis, F., Fawaz, H.I., Khamis, M.: Knowledge-driven biometric authentication in virtual reality. In: Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems. pp. 1–10 (2020)
33. Miller, R., Ajit, A., Banerjee, N.K., Banerjee, S.: Realtime behavior-based continual authentication of users in virtual reality environments. In: 2019 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR). pp. 253–2531. IEEE (2019)
34. Mustafa, T., Matovu, R., Serwadda, A., Muirhead, N.: Unsure how to authenticate on your VR headset? come on, use your head! In: Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics. pp. 23–30 (2018)
35. Partala, T.: Psychological needs and virtual worlds: Case second life. International Journal of Human-Computer Studies **69**(12), 787–800 (2011)
36. Peres, S.C., Pham, T., Phillips, R.: Validation of the system usability scale (sus) sus in the wild. In: Proceedings of the human factors and ergonomics society annual meeting. vol. 57, pp. 192–196. SAGE Publications Sage CA: Los Angeles, CA (2013)
37. Petrock, V.: Us virtual and augmented reality users 2020 (Apr 2020), https://www.insiderintelligence.com/content/us-virtual-and-augmented-reality-users-2020
38. Pfeuffer, K., Geiger, M.J., Prange, S., Mecke, L., Buschek, D., Alt, F.: Behavioural biometrics in VR: Identifying people from body motion and relations in virtual reality. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. pp. 1–12 (2019)
39. Phelan, D.: Google daydream VR review: Comfy, capable and affordable but not enough content yet (Nov 2016), https://www.independent.co.uk/tech/google-daydream-view-vr-review-virtual-reality-pixel-xl-headset-is-it-worth-it-a7444226.html
40. Rauschnabel, P.A., Brem, A., Ro, Y.: Augmented reality smart glasses: definition, conceptual insights, and managerial importance. Unpublished Working Paper, The University of Michigan-Dearborn, College of Business (2015)
41. Rigas, I., Economou, G., Fotopoulos, S.: Biometric identification based on the eye movements and graph matching techniques. Pattern Recognition Letters **33**(6), 786–792 (2012)
42. Sergei Vardomatski: Council post: Augmented and virtual reality after covid-19 (2021), [Online; accessed 4-November-2022]
43. Sivasamy, M., Sastry, V., Gopalan, N.: VRCAuth: continuous authentication of users in virtual reality environment using head-movement. In: 2020 5th International Conference on Communication and Electronics Systems (ICCES). pp. 518–523. IEEE (2020)
44. Sluganovic, I., Roeschlin, M., Rasmussen, K.B., Martinovic, I.: Using reflexive eye movements for fast challenge-response authentication. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. pp. 1056–1067 (2016)
45. Vatavu, R.D., Anthony, L., Wobbrock, J.O.: Gestures as point clouds: a $ p recognizer for user interface prototypes. In: Proceedings of the 14th ACM international conference on Multimodal interaction. pp. 273–280 (2012)
46. Von Zezschwitz, E., Dunphy, P., De Luca, A.: Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices. In: Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services. pp. 261–270 (2013)

47. Wilcoxon, F.: Individual comparisons by ranking methods. In: Breakthroughs in Statistics: Methodology and Distribution, pp. 196–202. Springer (1992)
48. Yu, Z., Liang, H.N., Fleming, C., Man, K.L.: An exploration of usable authentication mechanisms for virtual reality systems. In: 2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS). pp. 458–460. IEEE (2016)
49. Zhu, H., Jin, W., Xiao, M., Murali, S., Li, M.: Blinkey: A two-factor user authentication method for virtual reality devices. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies **4**(4), 1–29 (2020)

A System Usability Scale

	Strongly disagree				**Strongly agree**
1. I think that I would like to use this (PIN/Gesture-based) authentication system frequently in VR	1	2	3	4	5
2. I found the system unnecessarily complex	1	2	3	4	5
3. I thought (PIN/Gesture-based) authentication system was easy to use in VR	1	2	3	4	5
4. I think that I would need the support of a technical person to be able to use this system	1	2	3	4	5
5. I found the various functions in this system were well integrated	1	2	3	4	5
6. I thought there was too much inconsistency in this system	1	2	3	4	5
7. I would imagine that most people would learn to use this (PIN/Gesture-based) authentication system very quickly	1	2	3	4	5
8. I found the system very cumbersome to use	1	2	3	4	5
9. I felt very confident using (PIN/Gesture-based) authentication system in VR	1	2	3	4	5
10. I needed to learn a lot of things before I could get going with this system	1	2	3	4	5

Table 4: Adapted System Usability Scale

Input Modalities	
Pointer	Ray cast on the input surface, Controller tapping for selection, Both hand interaction [13, 15]
Pointer on click	Two button presses are required for complete selection. Relatively slow, and not usable.
Tap (touch)	Adopt from the touch screen physical devices, Virtual typing is required. Left visual clues, vulnerable for observation attack [15]. Conflict with "Area Awareness and Skill", and "Body Awareness and Skill" as the user's eyes are covered with VR headset [18]. Not suitable for public place authentication. Screen/input surface size matters, suitable for (relatively) small surface [8].
Input Surface	
Large	Not suitable for our study, Touch is not suitable, Pointer requires a noticeable motor (wrist, hand, head) movements
Medium	For Pointing modalities, medium type surface is the best suitable [15]
Small	Adopt form the personal device such as smartphones. Suitable for touch interaction, Pointer interaction is harder because of the motor movements
Password Type	
PIN	Established and widely used, faster, usable and secure [15]
Pattern	Relatively slower, error-prone, sensitive motor task required
Other decisions	
Username	Not required,
Joystick selection	Required longer time, not suitable with Fitt's law [8]

Table 5: Decision table for PIN authentication type.