cLock: Single-Handed Two-Factor Authentication in VR Using Wrist Rotation and Multi-Finger Tapping

ANONYMOUS AUTHOR(S)*

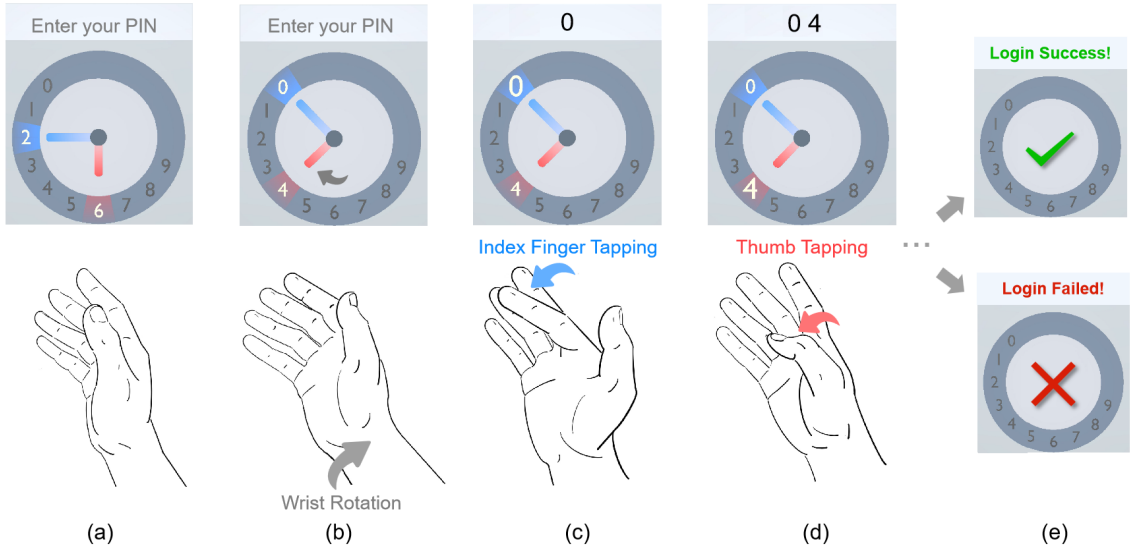

Fig. 1. A storyboard depicting a user employing cLock to input a PIN code. The nickname "cLock" originates from "circular lock", with its interface also resembling a clock's appearance. (a) Upon the emergence of the PIN input interface, the user elevates their hand to a comfortable position. (b) Subsequently, the user rotates the wrist to direct any cursor to the desired digit key (in this case, digits "0" and "4"). (c) To enter the digit "0", the user taps the index finger which controls the elongated blue cursor. (d) Then, to enter the digit '4', the user taps the thumb which activates the shorter red cursor. (e) The user repeats the above actions until the PIN entry concludes. The system then assesses the success or failure of the login, factoring in both the entered PIN and the distinct behavioral biometrics linked to hand movements.

In this paper, we proposed cLock, a single-handed two-factor authentication technique in VR, which allowed the users to rotate the wrist and tap different fingers to enter the PIN from a circular virtual numpad. cLock featured a multi-cursor design, which facilitated the input performance and reduced fatigue. We first examined the participants' input performance with different UI designs, and optimized key density, the number of cursors, and cursor interval. A usability study found that cLock achieved competitive authentication speed and accuracy compared with laser and touch authentication, effectively minimizes palm movement distance, and showed significant advantages in terms of privacy. In designing the authentication algorithm for cLock, we integrated behavioral biometrics with PIN entry to bolster security. Our approach leveraged the spatiotemporal features of both finger and palm movements during interaction. Simulation based on real data showed that even with collided PINs, cLock could achieve a False Acceptance Rate (FAR) of 2.4% and a False Rejection Rate (FRR) of 2.6%. A final 11-day study verified the learnability and long-term stability of cLock.

Manuscript submitted to ACM

CCS Concepts: • **Human-centered computing** → **Interaction techniques**; **Virtual reality**; • **Security and privacy** → **Multi-factor authentication**.

Additional Key Words and Phrases: behavioral biometrics, wrist rotation, finger tap, multiple cursors

ACM Reference Format:

Anonymous Author(s). 2018. cLock: Single-Handed Two-Factor Authentication in VR Using Wrist Rotation and Multi-Finger Tapping. In *IMWUT: Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*. ACM, New York, NY, USA, 27 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

As Virtual Reality (VR) technology spreads across various fields, including gaming, education, and design, the demand for secure, intuitive, and privacy-focused authentication in VR settings intensifies. This need is particularly pressing as VR devices are increasingly shared among users, such as family members in homes, colleagues in workspaces, or students in classrooms [4]. Consequently, there's a growing imperative for robust security protocols to ensure safe device logins, application access, and the safeguarding of sensitive operations, like transactions [13, 33, 66].

Current VR authentication solutions exhibit certain limitations. The most widely used authentication methods currently are knowledge-based, such as entering PINs or graphical patterns used by devices like Meta Quest[1]. However, these methods fall short in security, particularly when facing issues like multiple users with conflicting PINs or the risk of PIN leakage. Moreover, explicit input methods that involve mid-air touch or using controller lasers for keyboard selections are vulnerable to "shoulder surfing" attacks [9, 12] and may lead to user fatigue. Otherwise, devices like Microsoft Hololens[2] have adopted biometric technologies, such as iris scanning. However, biometric data is closely linked with inherent privacy issues and is particularly vulnerable to data breaches [19, 41]. The irreversible nature of biometric data heightens the risk; once compromised, it leads to persistent security problems.

To address shoulder-surfing and privacy concerns, methods based on behavioral biometrics have been proposed. These methods utilize various sensors to collect user behavior data, such as gaze behavior [38], hand gestures [67], full-body movements [36, 50], and interactions with interface elements [49, 57], and apply machine learning for authentication. However, these methods generally have much lower accuracy compared to traditional biometrics like fingerprints or iris scans, with error rates of between 1% and 10%, thus lacking sufficient security for widespread commercial use. Recently, two-factor authentication approaches have emerged, combining behavioral biometrics with knowledge-based methods to enhance security. For instance, Blinkey [80] uses eye blink rhythms, and RubikBiom [45] employs hand movement patterns during PIN entry. Nevertheless, these require additional devices like eye trackers or hand-held controllers and involve uncommon interactions that may result in a steep learning curve. To our knowledge, there isn't yet an intuitive, easy-to-use bare-hand two-factor authentication method.

In this paper, we present cLock, a two-factor authentication system based on single-hand interaction. cLock provides an intuitive approach to PIN entry in VR, as illustrated in Figure **??**. With cLock, wrist rotations guide cursor movement while finger taps facilitate the selection. By adopting a multi-cursor approach, in which both the index finger and thumb independently control distinct cursors, we optimize input efficiency while minimizing fatigue. Concurrently, cLock excavates the underutilized kinematic features of the palm and fingers as the secondary biometrics factor for authentication. This method combines the inherent simplicity, memorability, and convenience of PIN codes with the added strength of behavioral biometrics, ensuring heightened security and usability.

[1]https://www.meta.com/help/quest/articles/getting-started/getting-started-with-quest-2/unlock-pattern-quest/
[2]https://learn.microsoft.com/en-us/hololens/hololens-identity

In Study 1, we explored three design factors of cLock, including the number of cursors, key density, and cursor interval. Based on both user performance metrics (speed and accuracy) and subjective feedback, our study identified an optimal design (2 cursors, medium key density, and medium cursor interval) that balances user comfort with efficiency. We also implemented a series of enhancements to both UI and interaction design according to subjective feedback.

In Study 2, we further assessed cLock's usability in both seated and standing postures. cLock was benchmarked against prevalent input techniques for authentication: PIN and pattern, with touch-based and laser-pointing-based interactions. In metrics of speed and input accuracy, cLock stands on par with these baselines. In addition, cLock substantially decreases palm movement distance, aiding in fatigue reduction. Subjective feedback indicates that cLock is user-friendly and easy to learn, while also offering better privacy protection and higher social acceptance.

During user authentication, cLock employs a two-factor methodology, validating both the input PIN and the behavioral biometrics. We extract the kinematic features of finger bending angles, palm orientation, and relative palm position. Subsequently, Random Forests are deployed to classify users with precision, and we integrate a voting mechanism to enhance security by accurately identifying and rejecting impostors.

In study 3, we assessed the algorithm's authentication performance. With 6 repetitive trials during registration, cLock can achieve a False Rejection Rate (FRR) of 2.6% and a False Acceptance Rate (FAR) of 2.4%. This demonstrates cLock's proficiency in differentiating legitimate users from impostors, even when the same PIN is entered.

Finally, in Study 4, we assessed cLock's long-term usability and security over 11 days with 12 participants. Within 2-3 minutes of daily use, participants elevated their input speeds and diminished their error rates in just 11 days. By implementing a cumulative learning strategy, the False Rejection Rate (FRR) dropped to 0% by the eleventh day. This proves that cLock's authentication performance can remain stable over long-term use.

The contributions of this paper are three-folded:

- We are the first to propose combining wrist rotation and finger tapping for input in VR. Specifically, we examined the effects of cursor number, key density, and cursor interval on user behavior when adopting our proposed interaction. The design implications extend beyond authentication, applicable to a variety of input interactions.
- We present cLock, a two-factor authentication technique based on wrist rotation and finger tap to enter PIN. We exploited motion features including finger bending angle, palm posture, and relative palm position. We use random forests and voting mechanisms to ensure high authentication performance.
- In terms of authentication performance, we have validated that cLock could achieve an FRR of 2.6% and FAR of 2.4% even when imposters steal the correct PIN, which became stable within 11 days in long-term evaluation. In terms of usability, cLock showed significant advantages in terms of privacy, and exhibited learnability in continued use.

2 RELATED WORKS

2.1 VR Authentication Techniques Leveraging Behavioral Biometrics

In VR environment, users interact with their surrounding environment as well as digital objects and entities, often involving sensitive information[10]. Therefore, powerful and adaptable authentication techniques are needed. Research in the field of VR focuses on developing new, usable, and effective user authentication techniques. Typically, such techniques can be based on knowledge [27, 28, 33, 46, 79] and biometric features[3, 21].

Particularly, behavioral biometrics are gaining attention in research. These biometrics utilize unique individual behavioral traits such as movement, coordination, and body kinetics. They are considered effective for identity authentication due to their ubiquity, distinctiveness, consistency, and accessibility [24, 36, 57].

Prolific studies have focused on diverse behavior features for authentication like head movements [38, 54, 57, 59, 61, 65, 71], blink patterns [61, 80], eye movements [38–40, 54, 57], dental occlusion variances [81], footstep dynamics [31], and spontaneous body gestures [48, 53]. Given the hand's intricate capabilities, its movements in VR [2, 32, 36, 37, 49, 52, 57] have been spotlighted, with studies underscoring their user recognition potential[21]. Notably, several research endeavors have harnessed hand movements for VR-based authentication during naturalistic tasks, such as throwing a virtual ball [2, 32, 36, 49, 52] or virtual archery [36].

Recent VR research focusing on hand-based interactions primarily emphasizes behavior recognition through trajectories, orientations, and positions of both Head-Mounted Displays (HMDs) and controllers. While some studies have exclusively explored controller trajectories [32, 36, 45], it's more common to combine features from both the headset and the controller [2, 45, 48, 49, 52, 54, 57]. However, intricate hand features, such as wrist rotations and finger postures, remain relatively under-researched. The sole previous study that employed the hand tracking data from contemporary HMDs in conjunction with Augmented and Virtual Reality interactions for user identification [37] did not attain satisfactory authentication accuracy, exhibiting a fluctuation range between 30% and 95%. To the best of our knowledge, our research is pioneering in achieving high authentication security using VR hand-tracking data.

Behavioral biometrics often serve as a supplemental layer in two-factor authentication systems. For instance, unique blinking patterns and specific pupil size variations [80] and hand movement features during engagements with knowledge-based authentication systems [45] can all act as secondary authentication factors. Our approach notably avoids complex learning phases and the requirement for additional instruments. The one-handed interaction technique we introduce is not only simpler and more user-friendly but also requires minimal effort. Additionally, it provides enhanced security and authentication performance.

2.2 Interaction Techniques Leveraging Wrist Movements

The dexterity of the human wrist enabled precise actions, igniting substantial research interest across various applications that harness wrist movements. Investigations span a spectrum of wrist interaction techniques, such as scrolling through wrist deflection [11], the innovative use of wrist actions to enhance the safety of baby strollers on stairs [44], and the adoption of arm and wrist rotation gestures as keyboard shortcuts [5]. Wrist movements can be easily detectable by wrist-worn or handheld devices, unlocking significant potential for enabling single-handed operations. For instance, they enable managing a phone with one hand by using tilting as an input method.[73]. Research has been made towards wristband watches [15, 17, 68, 77], promoting single-handed input via wrist tilt and rotation.

[60] The versatility of wrist mobility has catalyzed research exploring the comfort, flexibility, and precision of wrist movements across different postures. These studies have incorporated devices ranging from handheld phones [60, 70] to smartwatches [68, 77], rings [18], and wristbands [62]. Further examinations have delved into wrist interactions in mid-air, focusing on the impact of varied rotation axis positions [63] and assessing motor control capabilities [74]. Rahman et al. [60] observed that among various wrist rotation types, pronation proved most accurate, with pronation/supination constrained to 12 levels within a 180° arc. Grandjean et al. [16] reported pronation and supination angles at 65° and 60°, respectively. There have been investigations into discernible angles and orientations during wrist rotation [60, 70]. However, many of these studies were either tethered to handheld devices, omitting finger movements, or restricted to a

single cursor, rendering them non-transferrable to our designed paradigm. Our research delves into the comfort range, speed, and precision of wrist movements under the influence of multi-finger actions, addressing this research void.

2.3 Circular Interface Design

The quest for efficient and intuitive text input methods has led researchers to investigate innovative keyboard layouts [34, 55]. Numerous circular keyboard designs have emerged, each tailored for specific contexts, underscoring their benefits. The inception of circular input interface can be traced back to pen-based computing, as seen in Cirrin [42] and its subsequent iterations [7]. T-cube introduces a word-level pen-based alphabet, enabling concise text input via single-stroke gestures [69]. Devices such as touchwheels [58] offer users tactile and intuitive interaction mechanisms. The circular layout has become a preferred choice for text input on wearables with circular designs, like smartwatches [14, 26, 75]. Shoemaker et al. [64] devised a circular keyboard optimized for large wall displays. Additionally, multi-cursor technology finds its place in circular interfaces, as demonstrated by COMPASS [75], which strategically places multiple cursors on a circular keyboard, adapting in real-time to reduce rotational distances during typing.

In VR, devices featuring circular motion naturally benefit from circular interfaces. This includes controllers with joysticks operating within a circular activity zone, touchpads with a circular layout, and the plethora of sensors embedded within VR equipment. While designs such as PizzaText [78], Hipad [25], and Ringtext [72] have advanced the field, VR's multi-sensory capabilities remain insufficiently exploited. Our research bridges this gap by utilizing hand tracking technology to obtain data during freehand interaction actions.

3 CLOCK: INTERACTION DESIGN AND IMPLEMENTATION

We developed the cLock virtual numpad with Unity (refer to Figure 1) and deployed it on the Meta Quest Pro headset, which provides hand-tracking capabilities using built-in cameras. In practice, cLock can also be adapted to other devices that support real-time hand tracking, such as Meta Quest 2 and Pico 4.

3.1 Interaction Design

Our design aims for minimal, comfortable hand movements in VR PIN entry. It focuses on wrist rotation and finger taps to minimize shoulder, arm, and forearm movements. The virtual interface, as shown in Figure 1, features a circular layout aligning with wrist motions. The digits 0-9 are evenly placed around the circle for easy identification. Cursors, like clock hands, originate from the center, each with a unique color for clarity. Users simply rotate their wrist to position the cursors and tap a finger to select digits during PIN entry.

To address the challenges of wrist rotation being slow and tiring, we adopted a multi-cursor approach [29, 75] where each cursor moves simultaneously at a fixed interval and is controlled by a different finger. A finger tap inputs the digit selected by its corresponding cursor. In Section 4, we conducted a comparative study on various cursor numbers, digit key densities, and intervals to identify the optimal design.

Figure 1 presents a storyboard illustrating the step-by-step process of PIN entry using cLock. The interaction is as follows:

(1) After the PIN input interface appears, the system turns on real-time hand tracking, and the user raises his hand to a comfortable position that can be effectively tracked.
(2) The user rotates the wrist and points any cursor to the target digit key.
(3) The user taps the corresponding finger to enter the pointed digit.

(4) The user repeats the above actions until the PIN input is completed, and the system determines whether the authentication is successful or failed.

3.2 Mapping of Wrist Rotation to Cursor Movement

To enable users to control the cursors' positions in real-time by rotating their wrists, we leveraged the real-time tracking of hand skeletal points provided by the Oculus Integration SDK [8] to compute the wrist rotation angle. The mapping of the wrist rotation angle (roll angle) to cursors rotation angle is set as $1:1$.

Our design ensures that the direction of finger movement matches the cursor's pointing direction, enhancing user comfort and the ease of remembering cursor-finger associations. For example, in Figure 1(c)(d), the index finger moves top-left, and the thumb bottom-left, aligning with the blue (index finger) and red (thumb) cursors' directions, respectively. This alignment is intuitive and user-friendly.

3.3 Finger Tap Detection

We consider the angle between the vector from the wrist to the proximal phalange bone (finger root) and the vector from the finger root to the fingertip as the bending angle for each finger.

In our pilot study, participants tapped their fingers naturally. We found that the bending angle of all fingers usually exceeded 10 degrees when tapping. Fingers typically reached their maximum bend in about 0.1 seconds and returned to the starting position in roughly 0.5 seconds. Consequently, we set the criteria for cursor control: a finger bend of over 10 degrees in the past 0.1 seconds indicates an input. To avoid repeat inputs, we implemented a 0.75-second pause after each cursor trigger.

4 STUDY 1: COMPARISON OF DIFFERENT UI DESIGNS

We conducted a user experiment to explore the placement strategy of digit keys and cursors on our circular interface. The goal of this study was to determine the optimal number of cursors, key density, and interval between cursors based on user performance and subjective feedback during input tasks.

4.1 Participants and Apparatus

We recruited 24 participants from the campus (15 females, 9 males) with ages ranging from 20 to 30 (M = 24.3, SD = 3.1). All participants were right-handed. We asked participants to report their experiences with VR usage using a 5-point Likert scale, where 1 indicates a strong unfamiliarity and little usage, and 5 signifies a high level of familiarity and frequent usage. The mean reported VR usage experience was 2.2 (SD = 1.0). Each participant was paid $15.

We used a Meta Quest Pro headset as the apparatus. The headset had a refresh rate of 72Hz and a resolution of 1800 $\times$ 1920 per eye, with 106° horizontal $\times$ 96° vertical claimed field of view. In experiments, we used hand tracking v2.0 with high tracking frequency offered by the Oculus Integration SDK [8]. The experimental platform was developed in C# using Unity 3D 2021.3.12f1c2. The coordinate data of hand skeleton was recorded in every frame.

4.2 Experiment Design

To simulate actual PIN entry, we asked participants to enter multiple pre-designed 6-digit codes, asking them to enter them as quickly and accurately as possible. We employed a within-subjects design with three factors:

- **Number of cursors**: As shown in Figure 2(a), this refers to the actual number of cursor (and thus fingers) used. Our pilot study indicated that tapping with the index, thumb, and middle fingers was most natural for participants, especially the index finger, followed by the thumb. The ring and pinky fingers were deemed less intuitive. Based on these findings, we experimented with **one cursor** (index finger only), **two cursors** (index finger and thumb), and **three cursors** (index, thumb, and middle finger). These cursors were color-coded as blue for the thumb, red for the index finger, and yellow for the middle finger.
- **Key Density**: As shown in Figure 2(b), we evaluated three levels of key density: **high** (with each digit key having an angular width of 15 degrees), **medium** (22.5 degrees), and **low** (30 degrees).
- **Cursor Interval**: As shown in Figure 2(c), three intervals between cursors were examined: **small** (2 keys between the cursors), **medium** (3 keys), and **large** (4 keys).

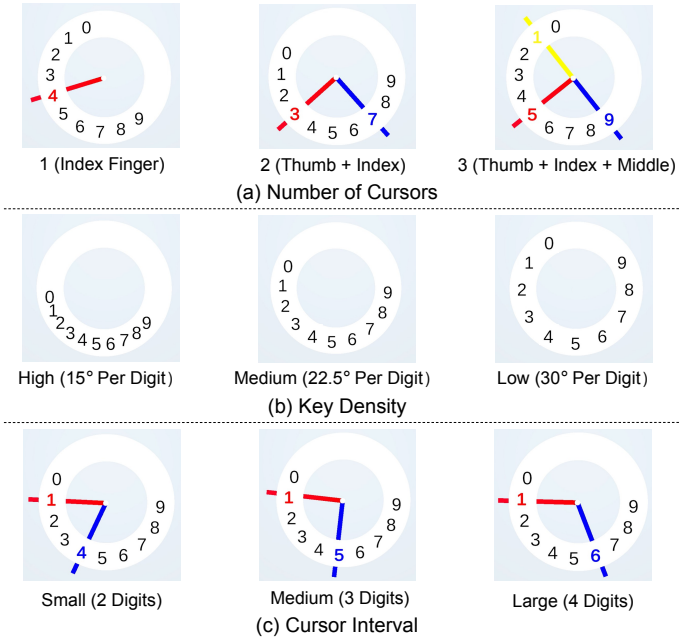

Fig. 2. Our experimental platforms under different factors. (a) the number of cursors, (b) key density, and (c) cursor interval.

As depicted in Figure 2, Study 1 utilizes a simple prototype of circular interface. Above it, we also placed a instruction panel to inform participants of the 6-digit code they need to enter and what they have already entered. By rendering small balls of corresponding colors on the fingertips, we prompted the user about the correspondence between the finger and the cursor.

Our pilot study found the user's right hand rotation ranges from about -80 degrees (supination) to 140 degrees (pronation), with a median of 30 degrees. We arranged the digit keys on the circular interface to match this median, balancing wrist pronation and supination. To keep wrist rotations comfortable, we avoided low key density under a single cursor (requiring too much rotation) and, with three cursors, excluded high key density (due to high error rates in pilot study) and large cursor intervals (as cursors were too spread out). This led to testing 15 different factor combinations, as shown in Table 1.

Table 1. The 15 combinations of different factors in Study 1. "Choose" means that we tested this combination.

Number of Cursors	Key Density	Cursor Interval	Choose
1	High	/	
	Medium	/	✓
	Low	/	✓
2	High	Small	✓
		Medium	✓
		Large	✓
	Medium	Small	✓
		Medium	✓
		Large	✓
	Low	Small	✓
		Medium	✓
		Large	✓
3	High	Small	
		Medium	
		Large	
	Medium	Small	✓
		Medium	✓
		Large	
	Low	Small	✓
		Medium	✓
		Large	

4.3 Procedure

Before the experiment, participants had a 10-minute session to familiarize themselves with the equipment and interface. In the study, they sat in an armless chair and completed 15 task sessions, each involving a different factor combination from Table 1, in a randomized order. Each session had 10 trials, with each trial requiring the entry of a unique 6-digit number. Participants were instructed to memorize and input these numbers quickly and accurately, moving to the next digit after an error. Breaks between sessions were provided for rest. The experiment lasted about 45 minutes, after which participants filled out a questionnaire about their cursor, key density, and cursor interval preferences, and participated in brief interviews for further insights.

4.4 Results

In total, We collected data from 24 participants × 15 conditions × 10 repetitions = 3, 600 trials from all participants. We did not remove any outliers. We used RM-ANOVA for all statistical tests. When our data violated the assumption of sphericity, we reported results with a Greenhouse-Geisser correction. We performed post-hoc pairwise comparisons using Bonferroni-corrected paired t-tests.

4.4.1 Input Time. The input time refers to the average duration required for users to input each digit. Figure 3 illustrates the input time across varying configurations. A notable effect of the Number of Cursors on input time ($F_{2,46} = 21.1, p < .001$) was observed. Post-hoc comparison shows that the input time with three cursors ($M = 1.53, SE = 0.04$) was significantly longer than with one cursor ($M = 1.35, SE = 0.04$) ($p < .001$). And two cursors ($M = 1.34, SE = 0.04$) ($p < .001$). We speculate that with three cursors, users might require additional time to determine which cursor to

employ for the next digit selection due to more options. Yet, no significant difference existed between the input times of one and two cursors.

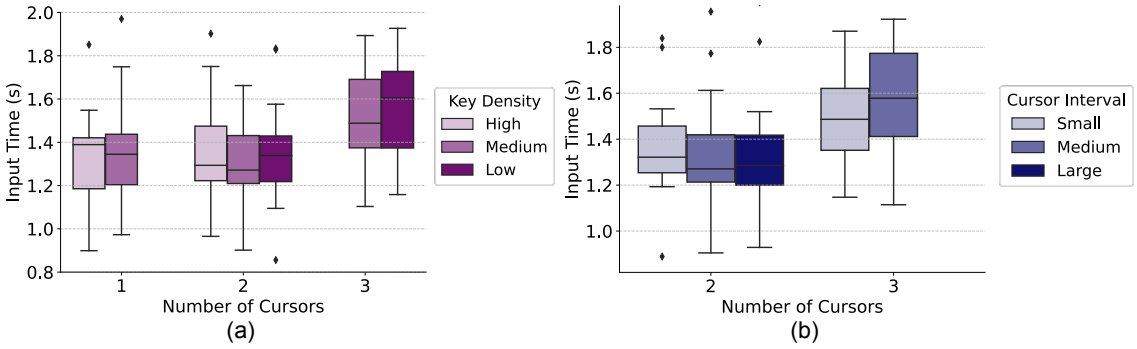

Fig. 3. Box plots grouped by the Number of Cursors showing Main effects of (a) Key Density and (b) Cursor Interval on the input time.

In terms of Key Density, as shown in Figure 3(a), only with three cursors did Key Density have a significant bearing on input time ($F_{1,23} = 4.9, p < .05$), with the input duration at low density ($M = 1.56, SE = 0.04$) being markedly longer than at medium density ($M = 1.51, SE = 0.04$) ($p < .05$). We speculate that a sparser key arrangement leads users to select cursors more carefully for the next key, aiming to minimize wrist rotation. This careful selection likely results in increased time spent on the task.

In terms of Cursor Interval, as shown in Figure 3(b), only at three cursors does the Cursor Interval significantly influence the input time ($F_{1,23} = 12.4, p < .005$); the input duration for a small interval ($M = 1.49, SE = 0.04$) is appreciably shorter than that for a medium interval ($M = 1.58, SE = 0.04$) ($p < .005$). With three cursors, sparse-placed cursors frequently exceeds the digit area's boundaries, compromising its efficacy. For one and two cursors, Key Density or Cursor Interval doesn't markedly influence the input time.

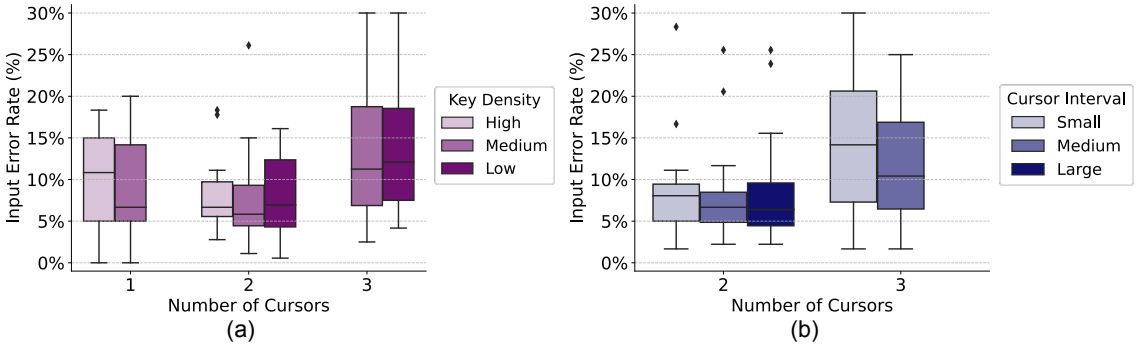

Fig. 4. Box plots grouped by the Number of Cursors showing Main effects of (a) Key Density and (b) Cursor Interval on the input error rate.

4.4.2 Input Errors. The input error rate refers to the proportion of user-input digits that deviate from the designated task digits. Figure 4 illustrates the input error rate across varying configurations. Although the input error rate did

not significantly differ across the Numbers of Cursors ($F_{1.4,31.8} = 3.4, p = 0.06$), Figure 4 suggests the lowest error rate with two cursors ($M = 9.9\%, SE = 2.0\%$) and the highest with three ($M = 14.5\%, SE = 2.3\%$). Moreover, Key Density and Cursor Interval didn't have a marked impact on the input error rate.

Three cursors caused prolonged input times and elevated error rates. We hypothesize that this stem from challenges users face while manipulating cursors with three fingers simultaneously. It becomes particularly arduous for users to maintain a clear mental mapping of the fingers-to-cursors relationship, leading to increased errors and cognitive load. The slightly heightened error rate with a single cursor ($M = 12.7\%, SE = 2.6\%$), in comparison to two cursors ($M = 9.9\%, SE = 2.0\%$) might be attributed to the increased wrist rotations, which in turn raises the potential for tapping on the wrong key due to fatigue.

4.4.3 Wrist Rotation Angle. The rotation angle refers the average angle of wrist rotation observed between successive digit inputs. Figure 5 illustrates the wrist rotation angle across varying configurations. Firstly, a notable effect of the Number of Cursors on the rotation angle ($F_{1.3,29.3} = 284.1, p < .001$) was observed. The rotation angle for a single cursor ($M = 61.4, SE = 0.9$), of two cursors ($M = 35.5, SE = 0.5$), and of three cursors ($M = 27.3, SE = 2.0$) descended in sequence. This proves that the multi-cursor design can indeed reduce the user's wrist rotation.

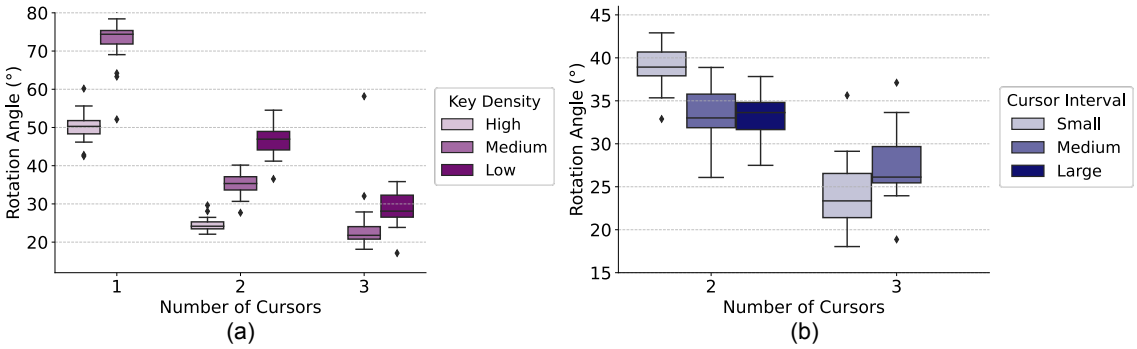

Fig. 5. Box plots grouped by the Number of Cursors showing Main effects of (a) Key Density and (b) Cursor Interval on the wrist rotation angle.

Secondly, as shown in Figure 5(a), Key Density exerted a significant influence on the rotation angle regardless of whether the number of cursors was 1 ($F_{1,23} = 544.8, p < .001$), 2 ($F_{2,46} = 684.5, p < .001$), or 3 ($F_{1,23} = 37.5, p < .001$). Interestingly, when the Number of Cursors is 1 or 2, although the Key Density significantly affects the wrist rotation amplitude, it does not significantly affect the input speed. We speculate that this may be because the user's wrist rotation speed increases as the rotation distance increases.

Lastly, as shown in Figure 5(b), a pronounced effect of Cursor Interval on the rotation angle is observed when the number of cursors is set to 2 ($F_{2,46} = 117.2, p < .001$) and 3 ($F_{1,23} = 12.5, p < .005$). The results show that compared with small interval, medium cursor interval will reduce the need for rotation when using two cursors, but it will lead to high wrist rotation load when using three cursors. This confirms our inference in Section 4.4.1 about the impaired cursor utility for three cursors with sparse spacing.

4.4.4 User Preference. Overall, participants found the designed interface intuitive and straightforward. With some practice, they perceived wrist rotation and finger tapping as user-friendly input methods. Figure 6 showcases participants'

preferences regarding the most comfortable settings. A significant 79.2% of participants favored two cursors, 75% deemed the medium key density optimal, and 65% preferred a medium cursor interval.

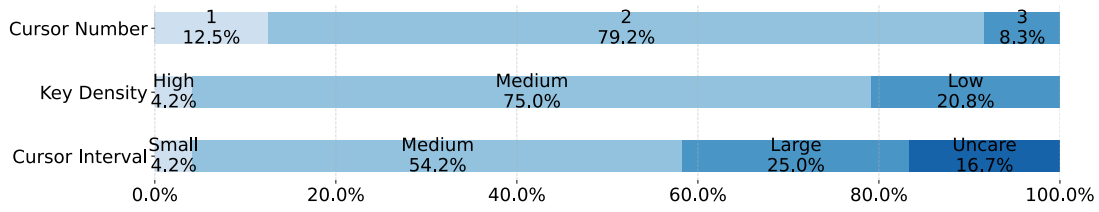

Fig. 6. User Preferences for Number of Cursors, Key Density, and Cursor Interval.

In terms of Number of Cursors, a majority of participants found using two cursors to be the optimal balance of comfort and convenience. 12 out of 24 participants felt that while the index finger was naturally more adept than the thumb, relying solely on it led to excessive wrist rotation, resulting in fatigue. In addition, 18 out of 24 participants found using three cursors less appealing, mainly because of the difficulty in remembering cursor-to-finger associations and the ensuing confusion.

In relation to Key Density, 19 out of 24 participants indicated that a higher key density increased the risk of unintended clicks. Even minor wrist movements could lead the cursor astray. Similarly, 9 out of 24 participants expressed reservations about larger numerical angles, associating them with heightened wrist rotation and consequent fatigue.

In terms of Cursor Interval, the majority of participants felt it had a negligible effect on their user experience. Five participants didn't even discern differences in cursor intervals. Among those who recognized its potential impact, 11 users reasoned that a smaller cursor interval might require more wrist rotation, making medium to larger cursor intervals more favorable.

4.5 Discussion and Design Decisions

The experimental results show that a two-cursor design, compared to a single cursor, doesn't complicate interaction but reduces wrist rotation, decreasing user fatigue and errors. Users found using two cursors with the index finger and thumb to be intuitive and simple. However, more cursors don't improve the experience; using three cursors notably increases input time and errors.

In subjective ratings, two cursors, medium key density, and a medium cursor interval won the preference of most participants. Given that those configurations also demonstrated superior (or at least comparable) results in the quantitative analysis, we consequently adopted this configuration for our interface's final design.

Based on user feedback, we adjusted the placement of digit keys on the circular interface. Participants opined that a clockwise wrist rotation (supination) is more effortless than a counterclockwise one (pronation) (P1, P2, P11, P16, P23). They also expressed a preference for adjusting the number placements on the interface in a clockwise direction to minimize the need for pronation. Consequently, in our finalized interface, as shown in Figure 7, we have realigned the digit placement with an 18.75° clockwise rotation from the center. This specific rotation angle also positions digit "6" precisely at the bottom center, enhancing the interface's aesthetic appeal.

In Figure 7(b), we enhanced the interface's visual elements to enrich the user experience. To resolve frequent mix-ups between the thumb and index finger, cursors of varying lengths were introduced: a longer cursor for the index finger

and a shorter one for the thumb, reflecting their natural lengths. Additionally, we implemented a gradient color scheme for digit keys to address accidental selection of adjacent digits. This scheme highlights both the selected key and its neighbor when the cursor is not perfectly aligned, signaling a potential mis-tap risk. Precise alignment results in only the selected key being highlighted.

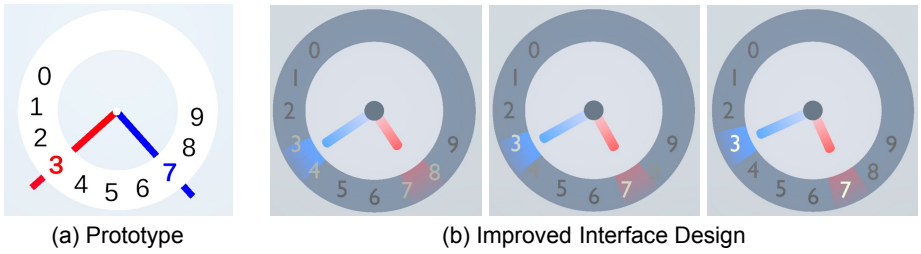

Fig. 7. (a) the circular interface utilized in Study 1. (b) improved interface design based on user feedback and input error analysis. Key modifications include: (1) Rotating the digit key placement clockwise by 18.75° to enhance comfort; (2) Adopting one long and one short cursor to correspond to the index finger and thumb, respectively, minimizing cursor confusion; and (3) Introducing gradient coloring for the selected key during cursor movement, assisting users in aligning the cursor with the key. As the cursors gradually move from the numbers "4" and "8" to pointing at the numbers "3" and "7", "3" and "7" are gradually highlighted.

5 STUDY 2: USABILITY EVALUATION

In this section, we evaluated the usability of cLock in real authentication tasks, comparing it with widely used authentication input methods.

5.1 Participants and Apparatus

We recruited 20 participants (10 male, 10 female, age = 23.6, SD = 2.3) from the campus. None of them have participated in previous studies and all are right-handed. The mean reported VR usage experience was 2.0 (SD = 0.8). Each participant was compensated $10.

5.2 Experiment Design

In our study, we employed a within-subject design focusing on two aspects: authentication methods and user posture. We compared cLock, our proposed method, with four common techniques shown in Figure 8: a standard numeric keypad and a nine-dot pattern, using mid-air finger touch and laser-pointing with pinch confirmation, named Touch PIN, Laser PIN, Touch Pattern, and Laser Pattern. We also replicated real-world VR authentication scenarios by evaluating both seated (without armrests) and standing postures.

Our study's testing for each technique involved two stages: registration and login. Participants were asked to complete tasks quickly and accurately. During registration, they set and confirmed a 6-digit code (or a dot sequence for the nine-dot pattern) for memorization. If the entries didn't match, registration restarted. In the login phase, participants logged in three times with their codes, able to see their inputs. They were encouraged to proceed after errors but focus on accuracy in subsequent tries. All entries and completion times were recorded for analysis.

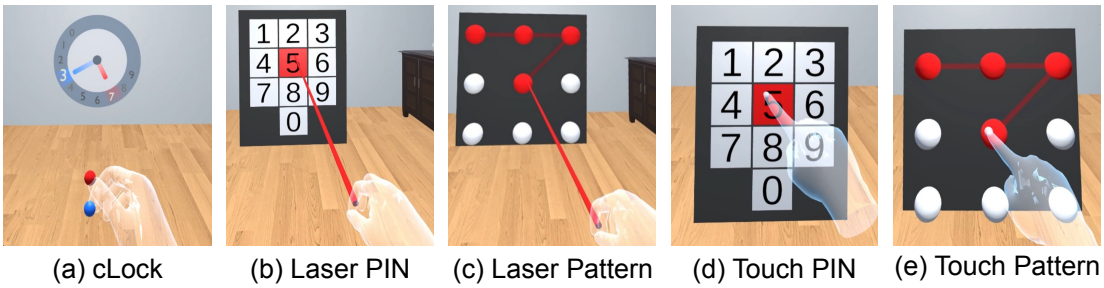

Fig. 8. User interface of the five authentication techniques.

5.3 Procedure

Participants began with a 10-minute session to familiarize themselves with the equipment and five authentication methods. They then engaged in two sessions, one standing and one seated, each including five blocks for different input techniques. Each block involved registration and login phases, with 5-second arm rests after each login repetition and longer breaks between blocks. The sequence of sessions and blocks was randomized to avoid biases. Afterward, participants completed questionnaires and took part in brief interviews for additional feedback. The entire study took about 45 minutes.

5.4 Results

In total, We collected data from 20 participants × 2 scenarios × 5 techniques = 200 registrations and 20 participants × 2 scenarios × 5 techniques × 3 repetitions = 600 logins. We used RM-ANOVA for statistical tests, and Friedman test for non-parametric tests.

5.4.1 Interaction Time. We assessed the registration time, which is the total duration of the registration phase, and the login time, measured from when the login interface appears to when the user completes their input.

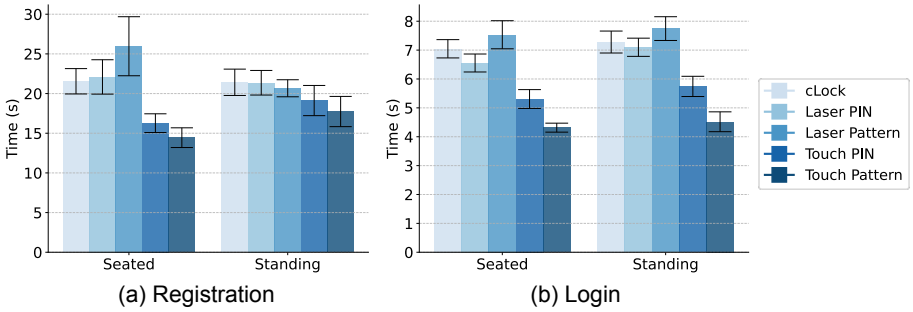

Fig. 9. (a) Average registration time for different techniques. (b) Average login time for different techniques. The error bar shows standard error.

Figure 9(a) and (b) reveal significant differences in registration ($F_{4,76} = 4.5$, $p < .005$) and login times ($F_{4,76} = 23.6$, $p < .001$) across techniques. For login, cLock ($M = 21.5s, SE = 1.1s$) was slower than Touch Pattern ($M = 16.1s, SE = 1.0s$) ($p < .05$), but comparable to the other three methods. For registration, cLock ($M = 7.2s, SE = 0.30s$) lagged behind

Touch Pattern ($M = 4.4s, SE = 0.22s$) ($p < .001$) and Touch PIN ($M = 5.5s, SE = 0.30s$) ($p < .01$), but matched Laser Pattern and Laser PIN. Posture showed no significant impact.

The results show cLock is slower than touch-based methods but comparable to laser-based ones. This initial slower speed may stem from users adapting to cLock's unique interaction, with potential for increased efficiency over time. Touch-based methods are more familiar due to widespread use in devices like smartphones. Notably, experienced cLock users, including the authors of this paper, can enter a 6-digit PIN in about 5 seconds. Thus, we believe cLock's interaction time is competitive with existing VR authentication techniques.

5.4.2 Input Accuracy. Input accuracy, the ratio of incorrect to total clicks, was measured for each technique. As shown in Figure 10, the success rates for cLock, Laser PIN, Laser Pattern, Touch PIN, and Touch Pattern were 93.2% ($SE = 0.02$), 95.7% ($SE = 0.01$), 98.3% ($SE = 0.01$), 94.7% ($SE = 0.02$), and 96.5% ($SE = 0.02$) respectively. No significant differences in accuracy were found across techniques or postures, suggesting cLock's comparability with other methods. The slightly lower accuracy of cLock is also likely due to user unfamiliarity.

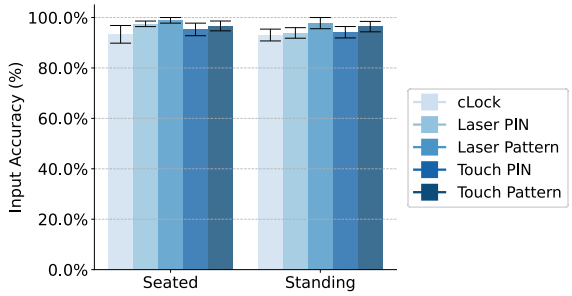

Fig. 10. Average input accuracy for different techniques. The error bar shows standard error.

5.4.3 Palm Movement Distance. Palm movement distance is the total distance traveled by the palm while entering a 6-digit code. Figure 11 shows significant differences in this distance across methods ($F_{4,76} = 31.7$, $p < .001$), with cLock's distance notably less than other techniques. This reduction is due to the fact that cLock is based on wrist rotation and finger tapping, which does not require large movements of the palm and arm. This not only lessens user fatigue but also makes PIN entry more discreet and less observable. cLock's minimal arm movement also benefits users with upper limb mobility challenges.

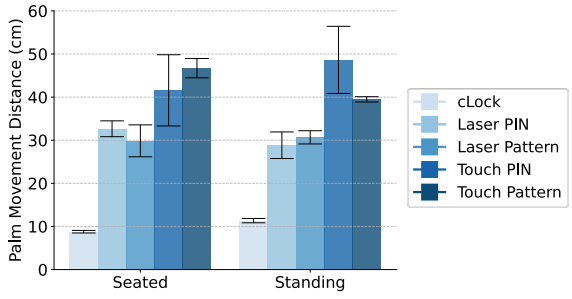

Fig. 11. Average palm movement distance during 6-digit code input for different techniques. The error bar shows standard error.

5.4.4 Subjective Ratings. We gathered participants' subjective evaluations of the techniques through a 7-point Likert-scale questionnaire (7: extremely positive, 1: extremely negative). We adopt the five dimensions of **Privacy**, **Social Acceptance**, **Effortless**, **Easy to Learn**, and **Overall Satisfaction**.

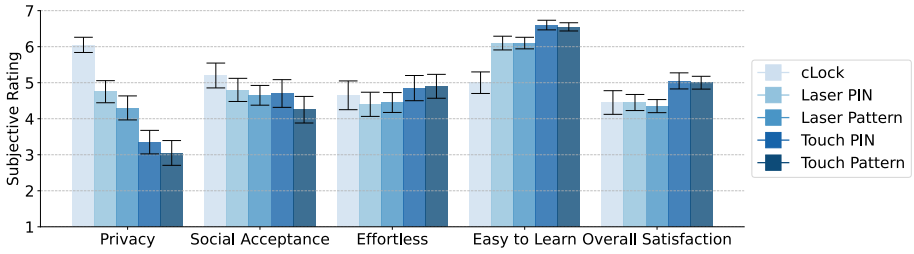

Fig. 12. Subjective ratings of different techniques (7: most positive, 1: most negative). The error bar shows one standard error.

Figure 12 shows average ratings for different techniques. A significant difference in "Privacy" ($\chi^2(4) = 54.052, p < .001$) was noted, with participants viewing cLock as superior in privacy protection. Nine out of twenty participants highlighted cLock's minimal motion requirement, making it less noticeable and more comfortable, especially in public settings. P2, P9 and P17 deemed it the most secure. Conversely, twelve participants found touch-based methods to involve more motion and be less secure.

While cLock was rated relatively lower in ease of learning ($\chi^2(4) = 47.352, p < .001$), it received overall positive feedback, averaging 5 out of 7 points. Participants noted its usability improved with practice, as P12 mentioned. P10 and P11 found it highly efficient once learned, while P17 appreciated its novelty and flexibility. P19 even described it as enjoyable, interesting, and very "cool" to use.

However, cLock faced some criticism. P8 mentioned that it required constant focus during usage to avoid mis-selections, leading to fatigue. P7 highlighted accidental touches due to the thumb's limited flexibility. P5 observed that thumb taps could inadvertently flex the index finger, causing misidentification. Furthermore, P10 found wrist movement control challenging.

6 TWO-FACTOR AUTHENTICATION ALGORITHM

6.1 Algorithm Design

Like traditional authentication methods [76, 80], cLock involves registration and login phases. In registration, users enter a chosen PIN multiple times, capturing both the PIN (knowledge-based) and the associated hand motion pattern (biometric feature). For login, users enter their PIN, and cLock's dual-layered authentication checks the PIN's correctness and the hand movement's biometric pattern. Figure 13 provides an overview of cLock's authentication algorithm.

During user registration, the system follows these steps:

(1) It collects the user's chosen PIN and spatiotemporal sequences of hand movements during repeated PIN inputs.
(2) In the preprocessing stage, sequences are segmented to extract Tap and Rotation Features.
(3) These features undergo data augmentation, and Tap and Rotation Classifiers are trained to identify registered users. These classifiers are updated with each new registration.

For user login, the process involves:

(1) Verifying if the entered PIN matches the user's declared identity.

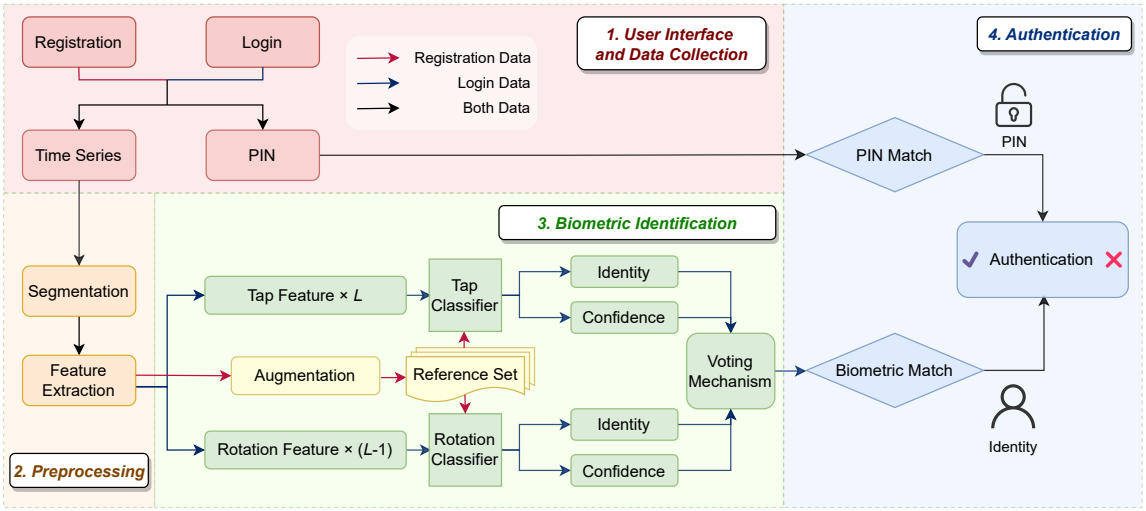

Fig. 13. Authentication algorithm design of cLock.

(2) Repeating the data collection, segmentation, and feature extraction steps from the registration phase.
(3) Utilizing the trained Tap and Rotation Classifiers to ascertain the identity of all segments and assign confidence scores.
(4) Implementing a voting mechanism that consolidates all classification results to confirm the match between user identity and behavioral biometrics.
(5) Granting access only if both the entered PIN and the biometric data match the claimed identity; otherwise, access is denied.

Since the verification of PIN codes is straightforward and self-explanatory, we'll focus instead on the more intricate authentication algorithm based on behavioral biometrics in the subsequent sections.

6.2 Segmentation of Time Series Data

For a PIN code of length L, users with cLock will tap L times and rotate their wrists $L-1$ times. We recognize finger taps and wrist rotations have distinct motion characteristics. Thus, we split the time series into Tap and Rotation Segments. Based on Study 1, a Tap Segment is defined as 50 frames (about 0.7 seconds) centered on a tap. The $L-1$ Rotation Segments are identified between these taps.

6.3 Feature Extraction

For both Tap and Rotation Segments, features were extracted from raw hand skeleton data via real-time tracking. Local coordinates relative to the Head-Mounted Display (HMD) were calculated by subtracting global coordinates from the HMD's. This normalization minimizes the effect of user positioning [36].

In Study 1 and 2, we observed variations in hand movements among participants using cLock, including finger curvature, palm postures due to elbow elevation and forearm rotation angles, and palm position relative to the head. Based on these observations and prior researches on hand-tracking for identity recognition [37, 57], we identified the following features characterizing hand movements during PIN input:

- **F0: Finger Bending Angles.** As depicted in Figure 14, each finger encompasses four skeletal points. Taking the index finger as a reference, the points are denoted as index proximal phalange (I_1), index intermediate phalange (I_2), index distal phalange (I_3), and the tip of the index finger (I_t). Including the wrist position (W), the bending of the index finger can be described by three angles: $\angle WI_1I_2$, $\angle I_1I_2I_3$, and $\angle I_2I_3I_t$. Consequently, F0 encompasses a set of 15 dimensions across all five fingers.
- **F1: Palm Posture.** We utilize the Forward and Upwards vectors of the palm, highlighted in Figure 14, to delineate the palm's orientation. Represented by the vectors (x, y, z), F1 spans a total of six dimensions.
- **F2: Palm Position.** The position of the palm is described using the wrist's coordinates relative to the HMD. Given that this position can be denoted by the coordinates (x, y, z), F2 comprises three dimensions.

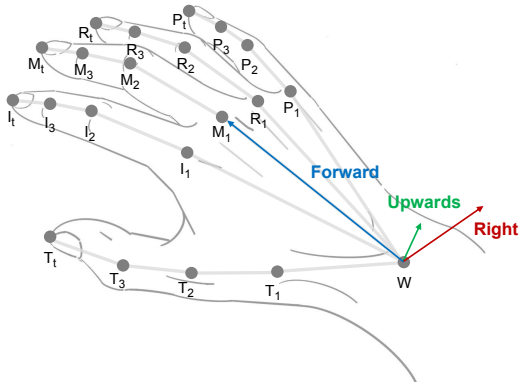

Fig. 14. Illustration of the right hand's skeletal point positions and palm posture vectors.

For each Tap Segment, the Tap Feature is derived by sampling every 5th frame from 50, using 11-frame hand tracking data. The same sampling applies to Rotation Segments for the Rotation Feature. Then, we calculate features F0, F1, and F2 for these subsequences. Supplementally, we compute each feature's first-order (rate of change) and second-order (acceleration) temporal differences. For expanded features, we derive mean, median, minimum, maximum, and standard deviation, resulting in final feature sets [57]. Thus, the total dimensionality for each tap and rotation feature is $(15 + 6 + 3) \times 3 \times 5 = 360$ dimensions.

To enhance our training dataset, we applied data augmentation techniques [35, 76]. This involved adding Gaussian noise to the raw data, with a mean of 0 and a standard deviation equal to one-third of the user data's standard deviation. We used an augmentation ratio of 20. Additionally, each feature in the training set was normalized to have a mean of 0 and a standard deviation of 1. For the test set, normalization was based on the mean and standard deviation from the training set.

6.4 Model Selection

Upon extraction of hand movement features, we utilized classification techniques to recognize user identity. We evaluated five leading classification methods [36, 54, 71]: Random Forests (RF), Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Multilayer Perceptron (MLP), and Stochastic Gradient Descent (SGD). A rigorous assessment

based on data collected in Study 1 was conducted to identify the optimal method. Using the scikit-learn Machine Learning library in Python, we trained classifiers and adopted default hyperparameter values.

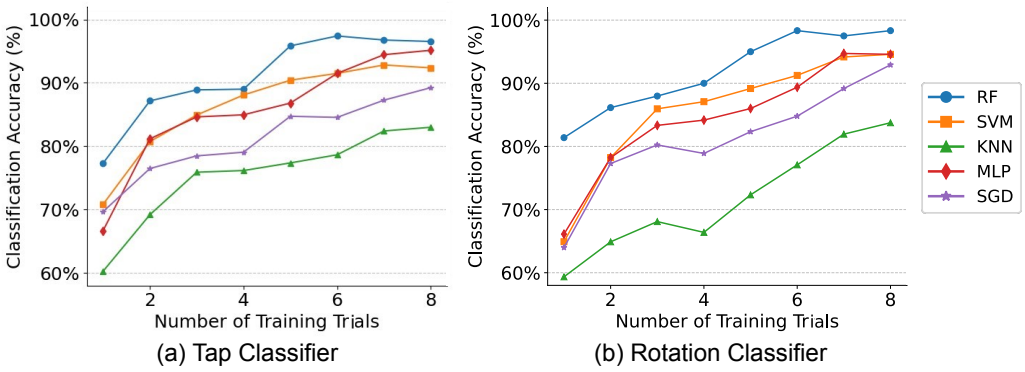

Fig. 15. Classification accuracy of user identity across different methods as the number of training trials T varies. (a) for Tap Classifier. (b) for Rotation Classifier.

Based on the 24 participants in Study 1, we used 10 input trials using two cursors, medium key density, and cursor interval, for a total of 240 test samples. To assess classifier performance with different training sizes, we split the first T trials for training and the remaining $10 - T$ trials for testing, and compare the accuracy under different T. We trained separate Tap and Rotation Classifiers using the respective features. Classification accuracy is shown in Figure 15. Across training sizes, the Random Forest algorithm consistently excelled in both classifiers. With 6 training trials, tap classification accuracy reached 97.4% and rotation 98.3%, making Random Forest our chosen algorithm.

6.5 Voting Mechanism for Rejecting Imposters

In user authentication, behavioral biometric systems must accurately identify registered users and reject impostors, even with password access. We incorporated a voting mechanism to bolster identity classification and detect unregistered impostors. For a PIN of length L entered during login, L tap and $L - 1$ rotation segments are generated. After feature extraction, each segment is classified for identity and confidence score, yielding predictions for $2L - 1$ segments in total. We then aggregate these predictions to determine the most frequent predicted identity. We calculate:

- **Elected Identity** (I_{elect}): The identity with the highest occurrence.
- **Elected Confidence Score** (CS_{elect}): The average confidence scores of the I_{elect}.

In scenarios where multiple identities share the highest frequency, the identity with the highest CS_{elect} is selected. To counteract potential unregistered impostors, we've established an **Confidence Score Threshold** ($Threshold_{CS}$). Using I_{claim} to represent the identity claimed by the user when logging in, behavioral biometric is accepted only when:

$$\begin{cases} CS_{elect} > Threshold_{CS} \\ I_{elect} = I_{claim} \end{cases} \tag{1}$$

We conducted a simulation experiment to evaluate the impact of $Threshold_{CS}$. Following the approach in Section 6.4, we used data from 24 participants in Study 1. Each iteration treated one participant as an impostor and the other 23

as registered users, leading to 24-fold validation. For the 10 trials per participant, the first 6 served as the training set and the remaining 4 for testing.

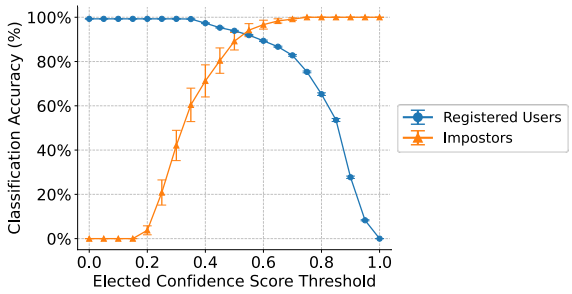

Fig. 16. Classification accuracy for registered users and impostors when Confidence Score Threshold ($Threshold_{CS}$) changes. The error bar denotes a standard error.

Figure 16 shows how classification accuracy for both registered users and impostors changes with different threshold settings. As the threshold rises from 0 to 1, the chance of wrongly accepting an impostor decreases to 0, while the chance of wrongly rejecting a registered user increases to 1. A threshold between 0.4 and 0.6 is recommended for maintaining high accuracy for both groups. In our two-factor system, which requires the correct PIN and biometric verification, we set $Threshold_{CS}$ at 0.4 to minimize incorrect denials to legitimate users.

7 STUDY 3: AUTHENTICATION PERFORMANCE EVALUATION

Password leakage poses a significant challenge for code-based authentication methods. It's crucial for a two-factor system to accurately identify when an imposter uses a legitimate user's password. This study tests cLock's effectiveness in recognizing the correct user in a PIN leakage scenario. Our simulations use real user data, and the algorithmic framework and parameters align with those previously described.

7.1 Participants

We enlisted 17 participants (10 males, 7 females; average age = 22.7, SD = 2.4) from our campus. None had participated in our previous studies, and all were right-handed. The average self-reported VR usage experience was 2.3 (SD = 1.0). We employed the refined final version of the cLock design for data collection. Each participant was compensated $10.

7.2 Experiment Design

We created ten unique six-digit PINs, distinct from those in Study 1, with each digit appearing equally. After practicing, participants were tasked with inputting this set of PINs in ten consecutive rounds with breaks in between, taking 30-40 minutes in total.

To evaluate our algorithm against PIN leakages, we used 17-fold cross-validation. In each round, 10 of 17 users were assigned the PINs as rightful owners. The remaining seven acted as impostors. Legitimate inputs were from users entering their own PINs, whereas inputs from registered users entering another's password, as well as impostor inputs, were categorized as illegitimate.

7.3 Results

To evaluate the authentication performance of cLock, we utilized two widely-adopted metrics [51, 76, 80]:

- **False Rejection Rate (FRR)**: The percentage of legitimate samples erroneously rejected.
- **False Acceptance Rate (FAR)**: The percentage of illegitimate samples incorrectly accepted.

To evaluate how different registration counts affect performance, we varied the number of training trials, with each trail involving a complete 6-digit PIN entry: we used the first T trials out of 10 as the training set, and the remaining $10 - T$ trials served as the test set. Figure 17(a) displays the False Rejection Rate (FRR) and False Acceptance Rate (FAR) for various T values. FRR dropped markedly from 20.8% (SE=2.5%) at $T = 2$ to 4.0% (SE=0.8%) at $T = 4$, then gradually to 0.97% (SE=0.7%) at $T = 8$. Meanwhile, FAR remained low, slightly decreasing from 3.1% (SE=0.2%) to 2.5% (SE=0.2%) as T increased. These results highlight cLock's accuracy in authenticating legitimate inputs and rejecting unauthorized ones. Based on the above findings, we advise that during actual user registration, 5 to 6 repetitions are sufficient to achieve satisfactory identification accuracy while avoiding user fatigue. Specifically, with 6 repetitions, we observed a FRR of 2.6% (SE=0.9%) and a FAR of 2.4% (SE=0.2%).

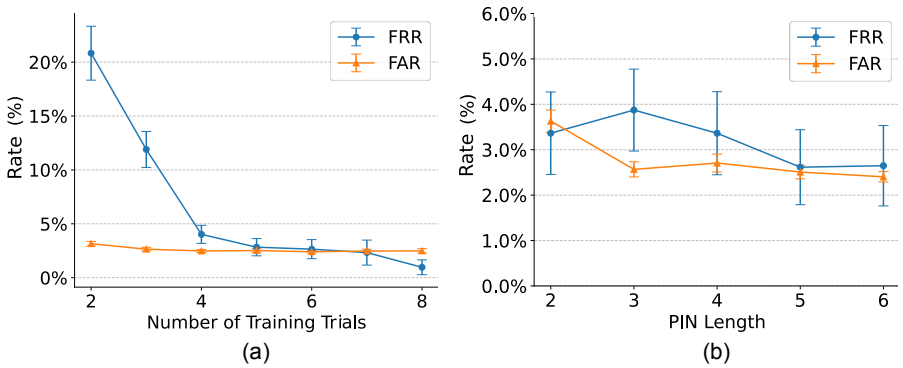

Fig. 17. False Rejection Rate (FRR) and False Acceptance Rate (FAR) of cLock across different (a) number of training trials and (b) PIN length. The error bar shows the standard error.

To explore the impact of varying PIN lengths (L), while keeping registration repetitions (training trials) at 6, we simulated scenarios with shorter PINs. We considered the first L digits from each user's input as the actual PIN. Figure 17(b) shows that as L increases from 2 to 6, the False Rejection Rate (FRR) slightly decreases from 3.4% (SE=0.9%) to 2.6% (SE=0.9%), and the False Acceptance Rate (FAR) subtly reduces from 3.6% (SE=0.2%) to 2.4% (SE=0.1%). The shorter PIN length did not significantly raise the error rate, maintaining a low and secure performance. This showcases cLock's robustness and reliability across varying PIN lengths.

8 STUDY 4: LONG-TERM EVALUATION

Our above studies have strongly validated cLock's usability and security. However, a key challenge for behavioral biometric authentication is the long-term consistency and uniqueness of user behaviors. We also aimed to evaluate users' adaptation and proficiency over time. Following existing research [30, 52, 76], we conducted an 11-day study with 12 participants to assess cLock's learnability and the ongoing effectiveness of its authentication. This long-term evaluation is crucial for gauging its practicality and reliability in real-world scenarios.

8.1 Participants

We recruited 12 right-handed participants (8 male, 4 female, age = 23.4, SD=2.2) from the campus. None of them have participated in previous studies. The mean reported VR usage experience was 3.1 (SD = 1.7). Each participant was compensated $20.

8.2 Experiment Design

Our 11-day user study began with an introductory session on Day 0, where participants familiarized themselves with cLock and created a unique 6-digit PIN, avoiding overly simple or predictable choices. They completed registration by entering their PIN ten times. Subsequent sessions on days 2, 4, 6, 8, and 10 involved a single task: entering their PIN ten times. We chose ten repetitions, considering that people unlock their smartphones dozens of times daily [22]. As VR becomes more prevalent, users are likely to frequently unlock their devices throughout the day, similar to smartphone usage. At each session's start, participants recalled their PIN to test memorability, then completed the entry task. Given that Study 3 already confirmed cLock's effectiveness against impostors, we didn't include impostor setups in this study to lessen the burden on long-term participants.

8.3 Results

8.3.1 Learnability of cLock. Over 11 days, all 12 participants consistently recalled their PINs, proving its memorability. We examined cLock's long-term learnability by analyzing performance metrics when inputting each digit. Figure 18(a)(b) shows a decline in average input time and error rate. RM-ANOVA revealed a significant learning effect on input time of ($F_{2.3,25.3} = 6.0$, $p < .01$), dropping from 0.98s (SE=0.03) to 0.88s (SE=0.04). Error rate decreased from 3.9% (SE=1.3%) to 1.7% (SE=0.5%) ($p = 0.12$), suggesting improved user proficiency. This demonstrates that users can greatly enhance their proficiency with just a few minutes of daily use over several days, showcasing the ease of learning cLock.

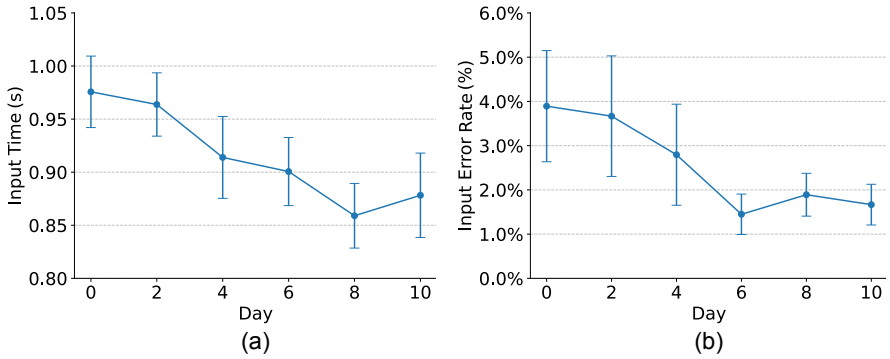

Fig. 18. (a) Average user input time over 11 days. (b) Average user input error over 11 days. The error bar represents standard error.

8.3.2 Long-term Authentication Performance. For long-term usage of cLock, we used a cumulative learning strategy [6, 56] for model adaptation to temporal changes in user behaviors. Initially, we trained the classifier with Day 0 registration data. Subsequent login data (starting Day 2) served both for evaluation and as additional training material, continually fine-tuning the classifier. Given the significant impact of sample quantity on model fine-tuning and

performance, we controlled the number of daily login attempts used as fine-tuning samples. This method allows us to better understand the influence of increased login frequency on the system's performance.

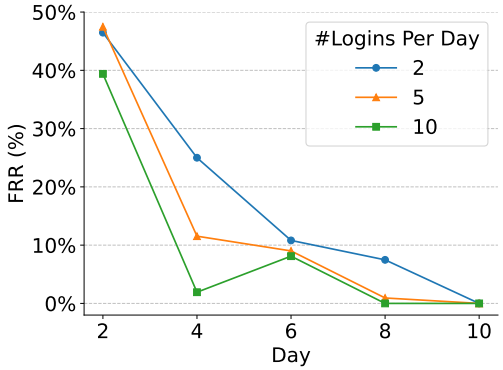

Fig. 19. False Rejection Rate (FRR) trends across 2, 5, and 10 logins per day over 11 days.

As this study do not set impostor attempts and only involved legitimate PIN entries, our focus was exclusively on the False Rejection Rate (FRR), to examine if legitimate users' biometric verification remains stable and accurate over long-term use. As depicted in Figure 19, initially, the model incorrectly rejected 40-50% of valid logins on Day 2. However, with increased usage, the FRR rapidly declines. The more daily user login attempts we utilized for fine-tuning the model, the quicker the FRR reduces. By Day 10, FRR dropped to zero, regardless of daily login frequency (2, 5, or 10 times).

We speculate that the initial high FRR stem from users' adaptation to cLock during initial use, leading to significant changes in their behavioral characteristics, such as posture, input speed, and muscle tension [52]. These behavioral changes could hinder user identity confirmation, causing more rejections. Nevertheless, our cumulative learning strategy swiftly adapts to these behavioral modifications. The strategy enables the model to effectively learn and identify unique and stable user features. Experimental evidence indicates that minimal daily logins, as few as two times per day, substantially improve model performance, achieving an accuracy of 100% by Day 10. We anticipate that with the continuous accumulation of user data, the FRR will maintain a very low level, thereby ensuring high usability.

9 DISCUSSION

9.1 Feasibility of cLock

9.1.1 Usability. cLock introduces an innovative and user-friendly method for PIN entry in VR, utilizing wrist rotations for navigating multiple cursors and finger taps for selection. Study 1's results indicate that this multi-cursor design doesn't complicate interactions; rather, it effectively reduces wrist rotation, thereby lowering user fatigue and input errors. Users particularly found the use of the index finger and thumb for controlling two cursors to be the most natural, easy to learn, and use. Additionally, Study 1 meticulously assessed the effects of key density and cursor interval, discovering optimal performance with medium key density and interval. We believe this novel interaction technique is not only highly effective for PIN input but can also be adapted for various other input tasks.

In Study 2, we compared cLock with four common authentication input methods, further validating its usability. cLock matched these methods in speed and accuracy but reduced palm movement distance. Users also favored cLock

for its privacy and social acceptability. Study 4 demonstrated cLock's learnability, with users showing significant improvements in efficiency and accuracy after 11 days. By minimizing palm spatial movement and lessening arm movement reliance, cLock is highly accessible, especially beneficial for users with upper limb movement disorders. Differing from methods that rely on mid-air touching or pointing, when paired with a wearable hand gesture tracker, cLock can be used with arms relaxed at the sides, further decreasing fatigue and increasing concealment.

We believe that cLock achieves a better balance between security and usability compared to current methods. Unlike behavioral biometric authentication methods that require users to perform unusual and potentially difficult operations [23, 43, 45, 80], cLock offers an intuitive interaction with a straightforward PIN-entry task. Contemporary knowledge-based methods employ intricate randomization mechanisms to counter shoulder-surfing attacks [1, 9, 20, 47], often resulting in substantial physical and cognitive demands on the user. In contrast, by incorporating behavioral biometrics, cLock eliminates the need for randomizing digit key placement, thereby greatly simplifying the user experience.

9.1.2 Security. cLock combines PIN with behavioral biometrics from hand tracking to achieve commendable security. Study 3 shows that cLock successfully rejects 97.6% of imposters and accepts 97.4% of genuine users, even if the PIN is exposed. While most behavioral biometric methods focus on classifying multiple users rather than simple accept-reject tasks, making direct accuracy comparisons challenging, cLock outperforms many methods with identity classification accuracies ranging from 90% to 95% (e.g., 93.03% for 33 users [2], 92.86% for 14 users [32], 90.0% for 16 users [36], 91.0% for 41 users [49]). Study 3 also explored the effects of registration times and PIN length. To avoid user fatigue, we recommend 5-6 repetitions during registration for good identification accuracy. Despite shorter PINs still being secure, we suggest using a PIN of at least 4-6 digits for optimal security.

Additionally, while not formally tested, we argue that the behavioral biometrics used in cLock are exceptionally difficult to observe and imitate. Its unique interaction design records a comprehensive range of hand movement metrics, like finger angles, hand postures, positions, and hand dimensions. Even if adversaries can detect and replicate general gestures, accurately mimicking detailed aspects such as the amplitude, velocity, and acceleration of a finger's motion during interactions remains a significant challenge.

Study 4's results emphasize that, with prolonged use of cLock, our cumulative learning strategy enables the adaptation of models to evolve user behaviors. This approach helps the model effectively recognize unique and stable user features, achieving near-zero False Rejection Rate (FRR) in just a few days. In the rare instances where legitimate inputs are not recognized, users can use alternative authentication methods, such as a mobile verification code. Concurrently, their hand movements contribute to fine-tuning the model, enhancing the user experience for subsequent logins.

9.2 Design Implications

When designing and testing the input interface and interaction for combined wrist rotation and finger taps, we came up with the following design implications:

- Utilizing both the index finger and thumb to control cursors offers the most comfortable and efficient approach, while involving more fingers tends to increase user strain.
- The comfortable range of wrist rotation lies between approximately 65° of pronation (inward rotation) to 45° of supination (outward rotation). Moreover, a majority of users found pronation to be more naturally comfortable than supination.

- Given the limited precision of wrist rotation [60], keys should not be positioned too closely, as this may result in unintended selections. Conversely, excessively large spacings can lead to wrist fatigue. A separation of about 20-25° between keys is recommended.
- Users find it most intuitive and comfortable when the direction of the cursor aligns with the actual finger direction during a finger tap.
- Both visual and auditory feedback enhance user input speed and accuracy.

10 LIMITATIONS AND FUTURE WORKS

Our study was conducted exclusively with the Quest Pro VR headset due to experimental constraints. While centered on VR headsets, cLock's application is potentially extendable to any head-mounted device equipped with hand-tracking capabilities, such as AR and MR systems. Future research will explore more devices with varied hand-tracking capabilities. Moreover, our participant group was limited and not comprehensive, consisting solely of right-handed individuals aged between 20 to 30 years. The behavioral patterns and user experiences of left-handed or older users may differ, meriting additional investigation. Further, larger-scale and longer-term experiments are necessary to assess how an increasing user base affects authentication performance.

Studies 2 and 3 focused on evaluating cLock's usability for PIN entry and the effectiveness of its authentication algorithm, respectively. Due to constraints in article length, a comprehensive analysis of the system's usability in actual authentication scenarios, especially in comparison with other behavioral biometric-based or two-factor methods, has been reserved for future research. Additionally, our usability tests were limited to sitting and standing postures. Expanding these evaluations to include more common positions, such as lying down or resting an arm on a desk, is crucial in subsequent studies.

While cLock is presently used for digit-PIN entry, its capability for text input is a notable potential we aim to explore. Moreover, cLock's unique design, which captures biometric features from user behavior during input, suggests the potential for implicit authentication. This means authentication could feasibly occur as users input their username with cLock. The security implications of this method could be a primary subject of future research.

11 CONCLUSION

In this paper, we present cLock, a novel two-factor authentication mechanism tailored for Virtual Reality (VR) environments. cLock employs a single-hand interaction by integrating wrist rotation with finger taps for PIN entry, concurrently utilizing the spatio-temporal dynamics of hand movements as a secondary authentication layer. This method bolsters security, safeguards user privacy, and ensures an intuitive and ergonomic authentication experience. In Study 1, we delve into human ability of combining wrist rotation and multi-finger tapping as an input mechanism, optimizing cLock's design in the process. Through rigorous evaluations, we ascertain cLock's effective usability (Study 2), robust security (Study 3), and enduring stability (Study 4), marking it as an advancement for secure and user-centric authentication in VR contexts. Additionally, we delineate design implications based on our findings.

REFERENCES

[1] Yomna Abdelrahman, Florian Mathis, Pascal Knierim, Axel Kettler, Florian Alt, and Mohamed Khamis. 2022. Cuevr: Studying the usability of cue-based authentication for virtual reality. In *Proceedings of the 2022 International Conference on Advanced Visual Interfaces*. 1–9.

[2] Ashwin Ajit, Natasha Kholgade Banerjee, and Sean Banerjee. 2019. Combining pairwise feature matches from device trajectories for biometric authentication in virtual reality environments. In *2019 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR)*. IEEE Computer Society, 9–97.

[3] Ioanna Anastasaki, George Drosatos, George Pavlidis, and Konstantinos Rantos. 2023. User Authentication Mechanisms Based on Immersive Technologies: A Systematic Review. *Information* 14, 10 (2023), 538.

[4] Muhammad Mujtaba Asad, Aisha Naz, Prathamesh Churi, and Mohammad Mehdi Tahanzadeh. 2021. Virtual reality as pedagogical tool to enhance experiential learning: a systematic literature review. *Education Research International* 2021 (2021), 1–17.

[5] Daniel Buschek, Bianka Roppelt, and Florian Alt. 2018. Extending keyboard shortcuts with arm and wrist rotation gestures. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–12.

[6] Francisco M Castro, Manuel J Marín-Jiménez, Nicolás Guil, Cordelia Schmid, and Karteek Alahari. 2018. End-to-end incremental learning. In *Proceedings of the European conference on computer vision (ECCV)*. 233–248.

[7] Jared Cechanowicz, Steven Dawson, Matt Victor, and Sriram Subramanian. 2006. Stylus based text input using expanding CIRRIN. In *Proceedings of the working conference on Advanced visual interfaces*. 163–166.

[8] Meta company. 2023. Set Up Hand Tracking | Oculus Developers — developer.oculus.com. https://developer.oculus.com/documentation/unity/unity-handtracking/. [Accessed 09-09-2023].

[9] Reyhan Düzgün, Peter Mayer, and Melanie Volkamer. 2022. Shoulder-Surfing Resistant Authentication for Augmented Reality. In *Nordic Human-Computer Interaction Conference*. 1–13.

[10] Reyhan Düzgün, Naheem Noah, Peter Mayer, Sanchari Das, and Melanie Volkamer. 2022. Sok: A systematic literature review of knowledge-based authentication on augmented reality head-mounted displays. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*. 1–12.

[11] Jacqui Fashimpaur, Amy Karlson, Tanya R Jonker, Hrvoje Benko, and Aakar Gupta. 2023. Investigating Wrist Deflection Scrolling Techniques for Extended Reality. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–16.

[12] Ceenu George, Mohamed Khamis, Emanuel von Zezschwitz, Marinus Burger, Henri Schmidt, Florian Alt, and Heinrich Hussmann. 2017. Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality. NDSS.

[13] Alberto Giaretta. 2022. Security and Privacy in Virtual Reality–A Literature Survey. *arXiv preprint arXiv:2205.00208* (2022).

[14] Jun Gong, Zheer Xu, Qifan Guo, Teddy Seyed, Xiang'Anthony' Chen, Xiaojun Bi, and Xing-Dong Yang. 2018. Wristext: One-handed text entry on smartwatch using wrist gestures. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–14.

[15] Jun Gong, Xing-Dong Yang, and Pourang Irani. 2016. Wristwhirl: One-handed continuous smartwatch input using wrist gestures. In *Proceedings of the 29th Annual Symposium on User Interface Software and Technology*. 861–872.

[16] Etienne Grandjean. 1980. Fitting the task to the man: an ergonomic approach. *(No Title)* (1980).

[17] Anhong Guo and Tim Paek. 2016. Exploring tilt for no-touch, wrist-only interactions on smartwatches. In *Proceedings of the 18th international conference on human-computer interaction with mobile devices and services*. 17–28.

[18] Aakar Gupta, Cheng Ji, Hui-Shyong Yeo, Aaron Quigley, and Daniel Vogel. 2019. Rotoswype: Word-gesture typing using a ring. In *Proceedings of the 2019 CHI conference on human factors in computing systems*. 1–12.

[19] Sunil Swamilingappa Harakannanavar, Prashanth Chikkanayakanahalli Renukamurthy, and Kori Basava Raja. 2019. Comprehensive study of biometric authentication systems, challenges and future trends. *International Journal of Advanced Networking and Applications* 10, 4 (2019), 3958–3968.

[20] Mudarabilli Harshini, Padigala Lakshman Sai, Singam Chennamma, Alavalapati Goutham Reddy, Hyun Sung Kim, et al. 2021. Easy-Auth: Graphical Password Authentication using a Randomization Method. In *2021 IEEE Latin-American Conference on Communications (LATINCOM)*. IEEE, 1–6.

[21] Chandra Hermawan Heruatmadja, Achmad Nizar Hidayanto, Harjanto Prabowo, et al. 2023. Biometric as Secure Authentication for Virtual Reality Environment: A Systematic Literature Review. In *2023 International Conference for Advancement in Technology (ICONAT)*. IEEE, 1–7.

[22] Daniel Hintze, Rainhard D Findling, Sebastian Scholz, and René Mayrhofer. 2014. Mobile device usage characteristics: The effect of context and form factor on locked and unlocked usage. In *Proceedings of the 12th international conference on advances in mobile computing and multimedia*. 105–114.

[23] Julie Iskander, Ahmed Abobakr, Mohamed Attia, Khaled Saleh, Darius Nahavandi, Mohammed Hossny, and Saeid Nahavandi. 2019. A k-nn classification based vr user verification using eye movement and ocular biomechanics. In *2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)*. IEEE, 1844–1848.

[24] A.K. Jain, A. Ross, and S. Prabhakar. 2004. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology* 14, 1 (Jan 2004), 4–20. https://doi.org/10.1109/tcsvt.2003.818349

[25] Haiyan Jiang and Dongdong Weng. 2020. HiPad: Text entry for head-mounted displays using circular touchpad. In *2020 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*. IEEE, 692–703.

[26] Keiko Katsuragawa, James R Wallace, and Edward Lank. 2016. Gestural text input using a smartwatch. In *Proceedings of the International Working Conference on Advanced Visual Interfaces*. 220–223.

[27] Mohamed Khamis, Mariam Hassib, Emanuel von Zezschwitz, Andreas Bulling, and Florian Alt. 2017. GazeTouchPIN: Protecting Sensitive Data on Mobile Devices Using Secure Multimodal Authentication. In *Proceedings of the 19th ACM International Conference on Multimodal Interaction* (Glasgow, UK) *(ICMI '17)*. Association for Computing Machinery, New York, NY, USA, 446–450. https://doi.org/10.1145/3136755.3136809

[28] Mohamed Khamis, Ludwig Trotter, Ville Mäkelä, Emanuel von Zezschwitz, Jens Le, Andreas Bulling, and Florian Alt. 2018. Cueauth: Comparing touch, mid-air gestures, and gaze for cue-based authentication on situated displays. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 4 (2018), 1–22.

[29] Masatomo Kobayashi and Takeo Igarashi. 2008. Ninja cursors: using multiple cursors to assist target acquisition on large screens. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 949–958.

[30] Katharina Krombholz, Thomas Hupperich, and Thorsten Holz. 2016. Use the Force: Evaluating {Force-Sensitive} Authentication for Mobile Devices. In *Twelfth symposium on usable privacy and security (SOUPS 2016)*. 207–219.

[31] Abhishek Kumar, Lik-Hang Lee, Jagmohan Chauhan, Xiang Su, Mohammad A Hoque, Susanna Pirttikangas, Sasu Tarkoma, and Pan Hui. 2022. PassWalk: Spatial Authentication Leveraging Lateral Shift and Gaze on Mobile Headsets. In *Proceedings of the 30th ACM International Conference on Multimedia*. 952–960.

[32] Alexander Kupin, Benjamin Moeller, Yijun Jiang, Natasha Kholgade Banerjee, and Sean Banerjee. 2019. 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*. Springer, 55–67.

[33] Pınar Kürtünlüoğlu, Beste Akdik, and Enis Karaarslan. 2022. Security of virtual reality authentication methods in metaverse: An overview. *arXiv preprint arXiv:2209.06447* (2022).

[34] Frank Chun Yat Li, Richard T Guy, Koji Yatani, and Khai N Truong. 2011. The 1line keyboard: a QWERTY layout in a single line. In *Proceedings of the 24th annual ACM symposium on User interface software and technology*. 461–470.

[35] Yantao Li, Hailong Hu, and Gang Zhou. 2018. Using data augmentation in continuous authentication on smartphones. *IEEE Internet of Things Journal* 6, 1 (2018), 628–640.

[36] Jonathan Liebers, Mark Abdelaziz, Lukas Mecke, Alia Saad, Jonas Auda, Uwe Gruenefeld, Florian Alt, and Stefan Schneegass. 2021. 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*. 1–11.

[37] Jonathan Liebers, Sascha Brockel, Uwe Gruenefeld, and Stefan Schneegass. 2022. Identifying Users by Their Hand Tracking Data in Augmented and Virtual Reality. *International Journal of Human–Computer Interaction* (2022), 1–16.

[38] Jonathan Liebers, Patrick Horn, Christian Burschik, Uwe Gruenefeld, and Stefan Schneegass. 2021. Using Gaze Behavior and Head Orientation for Implicit Identification in Virtual Reality. In *Proceedings of the 27th ACM Symposium on Virtual Reality Software and Technology*. https://doi.org/10.1145/3489849.3489880

[39] Dillon Lohr, Samuel-Hunter Berndt, and Oleg Komogortsev. 2018. An implementation of eye movement-driven biometrics in virtual reality. In *Proceedings of the 2018 ACM Symposium on Eye Tracking Research amp; Applications*. https://doi.org/10.1145/3204493.3208333

[40] Dillon J Lohr, Samantha Aziz, and Oleg Komogortsev. 2020. Eye Movement Biometrics Using a New Dataset Collected in Virtual Reality. In *ACM Symposium on Eye Tracking Research and Applications*. https://doi.org/10.1145/3379157.3391420

[41] Davide Maltoni, Dario Maio, Anil K Jain, Salil Prabhakar, et al. 2009. *Handbook of fingerprint recognition*. Vol. 2. Springer.

[42] Jennifer Mankoff and Gregory D Abowd. 1998. Cirrin: A word-level unistroke keyboard for pen input. In *Proceedings of the 11th annual ACM symposium on User interface software and technology*. 213–214.

[43] Karola Marky, Martin Schmitz, Verena Zimmermann, Martin Herbers, Kai Kunze, and Max Mühlhäuser. 2020. 3d-auth: Two-factor authentication with personalized 3d-printed items. In *Proceedings of the 2020 chi conference on human factors in computing systems*. 1–12.

[44] Ririka Masuda, Kai Sasaki, Masakazu Hirokawa, Taku Hachisu, and Kenji Suzuki. 2022. Posture Control of the Passenger Based on Caregiver's Wrist Motion for a Step-Climbing Stroller. *IEEE Robotics and Automation Letters* 7, 2 (2022), 3016–3021.

[45] Florian Mathis, Hassan Ismail Fawaz, and Mohamed Khamis. 2020. Knowledge-driven biometric authentication in virtual reality. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–10.

[46] Florian Mathis, Kami Vaniea, and Mohamed Khamis. 2021. Replicueauth: Validating the use of a lab-based virtual reality setup for evaluating authentication systems. In *Proceedings of the 2021 chi conference on human factors in computing systems*. 1–18.

[47] Florian Mathis, John Williamson, Kami Vaniea, and Mohamed Khamis. 2020. Rubikauth: Fast and secure authentication in virtual reality. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–9.

[48] Mark Roman Miller, Fernanda Herrera, Hanseul Jun, James A Landay, and Jeremy N Bailenson. 2020. Personal identifiability of user tracking data during observation of 360-degree VR video. *Scientific Reports* 10, 1 (2020), 17404.

[49] Robert Miller, Natasha Kholgade Banerjee, and Sean Banerjee. 2020. Within-system and cross-system behavior-based biometric authentication in virtual reality. In *2020 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*. IEEE, 311–316.

[50] Robert Miller, Natasha Kholgade Banerjee, and Sean Banerjee. 2021. Using siamese neural networks to perform cross-system behavioral authentication in virtual reality. In *2021 IEEE Virtual Reality and 3D User Interfaces (VR)*. IEEE, 140–149.

[51] Robert Miller, Natasha Kholgade Banerjee, and Sean Banerjee. 2022. Combining real-world constraints on user behavior with deep neural networks for virtual reality (vr) biometrics. In *2022 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*. IEEE, 409–418.

[52] Robert Miller, Natasha Kholgade Banerjee, and Sean Banerjee. 2022. Temporal effects in motion behavior for virtual reality (VR) biometrics. In *2022 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*. IEEE, 563–572.

[53] Tahrima Mustafa, Richard Matovu, Abdul Serwadda, and Nicholas Muirhead. 2018. 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*. https://doi.org/10.1145/3180445.3180450

[54] Ilesanmi Olade, Charles Fleming, and Hai-Ning Liang. 2020. BioMove: Biometric User Identification from Human Kinesiological Movements for Virtual Reality Systems. *Sensors* (May 2020), 2944. https://doi.org/10.3390/s20102944

[55] Stephen Oney, Chris Harrison, Amy Ogan, and Jason Wiese. 2013. ZoomBoard: a diminutive qwerty soft keyboard using iterative zooming for ultra-small devices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2799–2802.

[56] German I Parisi, Ronald Kemker, Jose L Part, Christopher Kanan, and Stefan Wermter. 2019. Continual lifelong learning with neural networks: A review. *Neural networks* 113 (2019), 54–71.

[57] Ken Pfeuffer, Matthias J Geiger, Sarah Prange, Lukas Mecke, Daniel Buschek, and Florian Alt. 2019. 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*. 1–12.

[58] Morten Proschowsky, Nette Schultz, and Niels Ebbe Jacobsen. 2006. An intuitive text input method for touch wheels. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*. 467–470.

[59] Luis Quintero, Panagiotis Papapetrou, Jaakko Hollmén, and Uno Fors. 2021. Effective Classification of Head Motion Trajectories in Virtual Reality using Time-Series Methods. In *2021 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR)*. IEEE, 38–46.

[60] Mahfuz Rahman, Sean Gustafson, Pourang Irani, and Sriram Subramanian. 2009. Tilt techniques: investigating the dexterity of wrist-based input. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/1518701.1518997

[61] Cynthia E. Rogers, Alexander W. Witt, Alexander D. Solomon, and Krishna K. Venkatasubramanian. 2015. An approach for user identification for head-mounted displays. In *Proceedings of the 2015 ACM International Symposium on Wearable Computers - ISWC '15*. https://doi.org/10.1145/2802083.2808391

[62] Farshid Salemi Parizi, Wolf Kienzle, Eric Whitmire, Aakar Gupta, and Hrvoje Benko. 2021. RotoWrist: Continuous Infrared Wrist Angle Tracking Using a Wristband. In *Proceedings of the 27th ACM Symposium on Virtual Reality Software and Technology* (Osaka, Japan) *(VRST '21)*. Association for Computing Machinery, New York, NY, USA, Article 26, 11 pages. https://doi.org/10.1145/3489849.3489886

[63] Dominik Schön, Thomas Kosch, Florian Müller, Martin Schmitz, Sebastian Günther, Lukas Bommhardt, and Max Mühlhäuser. 2023. Tailor Twist: Assessing Rotational Mid-Air Interactions for Augmented Reality. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–14.

[64] Garth Shoemaker, Leah Findlater, Jessica Q Dawson, and Kellogg S Booth. 2009. Mid-air text input techniques for very large wall displays.. In *Graphics Interface*. 231–238.

[65] Manimaran Sivasamy, V.N. Sastry, and N.P. Gopalan. 2020. VRCAuth: Continuous Authentication of Users in Virtual Reality Environment Using Head-Movement. In *2020 5th International Conference on Communication and Electronics Systems (ICCES)*. https://doi.org/10.1109/icces48766.2020.9137914

[66] Sophie Stephenson, Bijeeta Pal, Stephen Fan, Earlence Fernandes, Yuhang Zhao, and Rahul Chatterjee. 2022. Sok: Authentication in augmented and virtual reality. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 267–284.

[67] Mei Suzuki, Ryo Iijima, Kazuki Nomoto, Tetsushi Ohki, and Tatsuya Mori. 2023. PinchKey: A Natural and User-Friendly Approach to VR User Authentication. In *Proceedings of the 2023 European Symposium on Usable Security*. 192–204.

[68] Hsin-Ruey Tsai, Po-Chang Chen, Liwei Chan, and Yi-Ping Hung. 2018. One-Handed Input Through Rotational Motion for Smartwatches. *International Journal of Human–Computer Interaction* 34, 11 (2018), 971–986.

[69] Dan Venolia and Forrest Neiberg. 1994. T-Cube: A fast, self-disclosing pen-based alphabet. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. 265–270.

[70] William S Walmsley, W Xavier Snelgrove, and Khai N Truong. 2014. Disambiguation of imprecise input with one-dimensional rotational text entry. *ACM Transactions on Computer-Human Interaction (TOCHI)* 21, 1 (2014), 1–40.

[71] Xue Wang and Yang Zhang. 2021. Nod to auth: Fluent ar/vr authentication with user head-neck modeling. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–7.

[72] Wenge Xu, Hai-Ning Liang, Yuxuan Zhao, Tianyu Zhang, Difeng Yu, and Diego Monteiro. 2019. Ringtext: Dwell-free and hands-free text entry for mobile head-mounted displays using head motions. *IEEE transactions on visualization and computer graphics* 25, 5 (2019), 1991–2001.

[73] Hui-Shyong Yeo, Xiao-Shen Phang, Steven J Castellucci, Per Ola Kristensson, and Aaron Quigley. 2017. Investigating tilt-based gesture keyboard entry for single-handed text entry on large devices. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 4194–4202.

[74] Xin Yi, Xueyang Wang, Jiaqi Li, and Hewu Li. 2023. Examining the Fine Motor Control Ability of Linear Hand Movement in Virtual Reality. In *2023 IEEE Conference Virtual Reality and 3D User Interfaces (VR)*. IEEE, 427–437.

[75] Xin Yi, Chun Yu, Weijie Xu, Xiaojun Bi, and Yuanchun Shi. 2017. COMPASS: Rotational keyboard on non-touch smartwatches. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 705–715.

[76] Xin Yi, Shuning Zhang, Ziqi Pan, Louisa Shi, Fengyan Han, Yan Kong, Hewu Li, and Yuanchun Shi. 2023. Squeez'In: Private Authentication on Smartphones based on Squeezing Gestures. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–15.

[77] Eunhye Youn, Sangyoon Lee, Sunbum Kim, Youngbo Aram Shim, Liwei Chan, and Geehyuk Lee. 2021. Wristdial: An eyes-free integer-value input method by quantizing the wrist rotation. *International Journal of Human–Computer Interaction* 37, 17 (2021), 1607–1624.

[78] Difeng Yu, Kaixuan Fan, Heng Zhang, Diego Monteiro, Wenge Xu, and Hai-Ning Liang. 2018. PizzaText: Text entry for virtual reality systems using dual thumbsticks. *IEEE transactions on visualization and computer graphics* 24, 11 (2018), 2927–2935.

[79] Zhen Yu, Hai-Ning Liang, Charles Fleming, and Ka Lok Man. 2016. An exploration of usable authentication mechanisms for virtual reality systems. In *2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*. https://doi.org/10.1109/apccas.2016.7804002

[80] Huadi Zhu, Wenqiang Jin, Mingyan Xiao, Srinivasan Murali, and Ming Li. 2020. Blinkey: A two-factor user authentication method for virtual reality devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4, 4 (2020), 1–29.

[81] Yongpan Zou, Meng Zhao, Zimu Zhou, Jiawei Lin, Mo Li, and Kaishun Wu. 2018. BiLock: User authentication via dental occlusion biometrics. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 3 (2018), 1–20.