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

Xueyang Wang
Institute for Network Sciences and Cyberspace, Tsinghua University
Zhongguancun Laboratory

Xin Yi*
Institute for Network Sciences and Cyberspace, Tsinghua University
Zhongguancun Laboratory

Jiaqi Li
Department of Computer Seience and Technology, Tsinghua University

Shuning Zhang
Institute for Network Sciences and Cyberspace, Tsinghua University

BoYu Gao
College of Cyber Security/Guangdong Institute of Smart Education, Jinan University

Hewu Li
Institute for Network Sciences and Cyberspace, Tsinghua University
Zhongguancun Laboratory

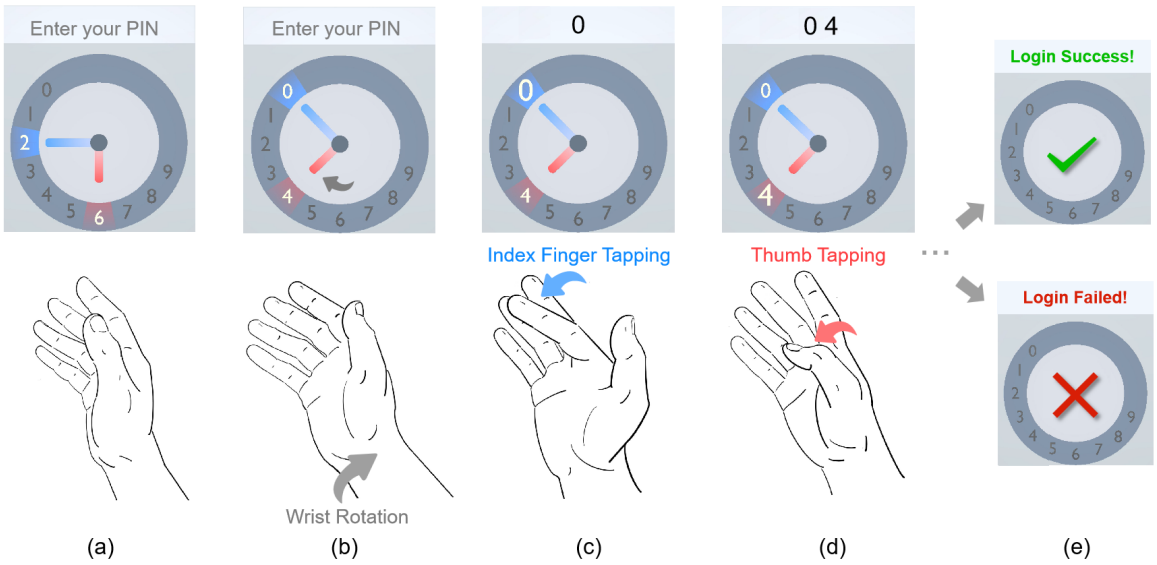


Figure 1: A storyboard depicting a user employing cLock to input the first two digits (“0” and “4”) of their PIN code. The nickname “cLock” originates from “circular lock,” with its interface resembling a clock’s appearance. (a) Upon the emergence of the PIN input interface, the user elevates their hand to a comfortable position. (b) The interface displays two cursors: an elongated blue cursor controlled by the index finger and a shorter red cursor controlled by the thumb, both rotating simultaneously with wrist movement. (c) For entering the digit “0”, the user rotates their wrist until either cursor aligns with “0”, then taps the corresponding finger (in this case, the index finger controlling the blue cursor). (d) Similarly, the user opts to use the thumb-controlled cursor to enter “4”. (e) After PIN entry completion, the system evaluates authentication success based on both PIN correctness and the unique behavioral biometrics of the user’s movements.

ABSTRACT

As Virtual Reality (VR) devices become increasingly shared among users, there is a pressing need for authentication methods that balance security, usability, and privacy while accommodating VR’s unique interaction constraints. This paper presents cLock, a novel single-handed two-factor authentication technique in VR that allows users to enter PINs with multiple cursors on a virtual circular numpad through wrist rotation and finger tapping. We first optimized the UI design of cLock by comparing participants’ input performance with different UI parameters. We then extracted spatiotemporal behavioral features of both fingers and palm during PIN entry, which facilitated cLock’s authentication algorithm. In the usability evaluation with four input postures, cLock achieved significantly faster authentication speed than laser and touch-based baselines, without sacrificing accuracy. Meanwhile, it was most preferred by participants in terms of privacy, social acceptance and physical effort. A following evaluation of security demonstrated that cLock achieved a deciphering rate of only 1/8 of the baselines against shoulder-surfing within 1m. Even in scenarios of password leakage, cLock could still achieve an FAR of 2.3% and FRR of 3.2% with 20 registered users. A final 11-day study verified the longitudinal stability of cLock.

*Corresponding author. e-mail: yixin@tsinghua.edu.cn

Index Terms: Two-factor Authentication, Behavioral Biometrics, Gesture Input, Multiple Cursors, Virtual Reality.

2025 IEEE International Symposium on Mixed and Augmented Reality (ISMAR) | 979-8-3315-8761-1/25/$31.00 ©2025 IEEE | DOI: 10.1109/ISMAR67309.2025.00064

2473-0726/25/$31.00 ©2025 IEEE
DOI 10.1109/ISMAR67309.2025.00064

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 (e.g., transactions) [26, 14, 53].

Current VR authentication solutions exhibit certain limitations. The most widely used approaches are knowledge-based [11, 53, 41], such as entering PINs or graphical patterns used by products like Meta Quest. 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 [10, 13] and may lead to user fatigue. Otherwise, devices like Microsoft Hololens and Apple Vision Pro 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 [18, 31]. Once compromised, the irreversible nature of biometric data 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 [29], hand gestures [54], full-body movements [37, 27], and interactions with interface elements [36, 44], 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. Recent advancements in two-factor authentication (2FA) have combined behavioral biometrics with knowledge-based methods to enhance security [69, 34, 62]. However, existing methods often employ uncommon interactions like eye blink rhythms [69], head movements [62], and head-eye coordination [68], which can be cumbersome and difficult to learn and remember, or they rely on hand-held controllers [34]. To our knowledge, there are currently no 2FA methods that use simple, widely accepted bare-hand interactions.

In this paper, we present cLock, a single-handed 2FA system for VR environments. As illustrated in Figure 1, cLock enables PIN entry using wrist rotations to guide cursor movement and finger taps for selection. By employing a two-cursor approach controlled by the index finger and thumb, cLock optimizes input efficiency while minimizing fatigue, simultaneously leveraging hand movement kinematics as a secondary biometric factor.

Through systematic user studies, we identified optimal UI parameters and developed a comprehensive feature extraction framework capturing finger joint angles, palm orientation vectors, and spatial positions. Using Random Forest classification with voting mechanisms, cLock achieves comparable security to 6-digit PIN systems while using only a 3-digit PIN, demonstrating effective security-usability balance.

Comprehensive evaluation against commercial authentication methods reveals cLock's multi-dimensional advantages: faster login speed (3.7s vs. 4.4-7.6s for baselines), robust performance across different postures, and enhanced user acceptance for privacy and social contexts. Security assessment demonstrates strong resilience against shoulder-surfing attacks (1.6%-3.3% vs. 20%-60% compromise rates for baselines) and robust protection even when credentials are fully compromised (97.7% attack rejection). Longitudinal evaluation (11 days) confirms system stability and adaptation over extended usage periods.

The contributions of this paper are three-fold:

- We introduce cLock, a novel 2FA technique combining wrist rotation and finger tapping for VR authentication, with UI design iteratively optimized through systematic user studies.
- We incorporate comprehensive hand motion features into 2FA, demonstrating effective user recognition through Random Forest classification and adaptive strategies.
- We validate cLock through multi-dimensional evaluation: usability testing across various postures, security assessment against shoulder-surfing and credential compromise, and longitudinal study confirming system stability.

2 Related Works

2.1 VR Authentication Techniques Leveraging Behavioral Biometrics

VR environments often involve sensitive information during user interactions [11], necessitating robust authentication techniques. Recent comprehensive surveys [41] have systematically categorized existing XR authentication approaches, with current research primarily focusing on knowledge-based methods [58, 26] and traditional biometric features [3, 19].

Behavioral biometrics leverage unique individual traits and are gaining prominence due to their ubiquity, distinctiveness, and accessibility [44]. Researchers have explored diverse features including head movements [52, 46, 59], blink patterns [69], eye movements [30, 29, 42], dental occlusion [72], footsteps [24], auditory-pupillary response [70], and spontaneous gestures [39, 35].

Hand movements in VR [44, 36, 27, 28, 38] have attracted particular attention due to their intricate capabilities and recognition potential [19]. Researchers have employed hand movements for authentication during naturalistic tasks like throwing virtual balls [36, 27, 38] or archery [27].

Current research primarily focuses on behavioral recognition through trajectories and positions of HMDs and controllers. Some studies explore controller trajectories exclusively [27, 25, 34], while most combine features from both headset and controller [1, 34, 42, 36, 38, 44]. However, intricate hand features like wrist rotations and finger postures remain under-researched. The only previous study using hand tracking data from modern HMDs for user identification [28] achieved inconsistent authentication accuracy (30%-95%). To our knowledge, our research is the first to achieve high authentication security using VR hand-tracking data.

Behavioral biometrics often serve as a secondary factor in two-factor authentication, such as blinking patterns [69], head movements [62], and hand movements during knowledge-based authentication [34]. Our approach offers a simpler one-handed interaction technique that requires minimal effort and no additional instruments while providing enhanced authentication performance.

2.2 Interaction Based on Wrist Movements

The human wrist's dexterity has inspired extensive research across various applications. Studies have explored diverse interaction techniques, including scrolling via wrist deflection [12], enhancing stroller safety [33], and using wrist rotations as keyboard shortcuts [6]. These movements, easily detectable by wearable or handheld devices, enable efficient single-handed operations, from phone management through tilting [61] to wristband watches that facilitate input via wrist rotation [55, 66].

Research has examined wrist mobility across various contexts, studying comfort, flexibility, and precision with different devices—from handheld phones [57, 47] to smartwatches [66, 55], rings [17], and wristbands [49]. Mid-air wrist interactions have been investigated with attention to rotation axis positions [50] and motor control capabilities [63].

Prior studies have provided valuable insights into wrist movement properties. Rahman et al. [47] identified pronation as the

most accurate rotation type, noting that pronation/supination could be limited to 12 discernible levels within a 180° arc. Grandjean et al. [16] reported natural pronation and supination angles of 65° and 60°, respectively. However, most existing research has been limited to handheld devices, single cursors, or excluded finger movements entirely. Our work addresses this gap by comprehensively exploring the comfort range, speed, and precision of wrist movements combined with multi-finger actions in VR environments.

2.3 Circular Input Interface Design

The pursuit of efficient and intuitive text input methods has driven research into innovative keyboard layouts, with circular designs emerging as beneficial solutions for various contexts. These interfaces originated from pen-based computing with Cirrin [32] and evolved through iterations [8] that enhanced functionality and user experience. T-cube introduced a word-level pen-based alphabet enabling concise text input via single-stroke gestures [56], while touchwheels [45] offered tactile and intuitive interactions.

Circular layouts have particularly flourished on devices with natural rotational affordances. They gained popularity for text input on circular wearables like smartwatches [15, 64] and have been adapted for large wall displays [51]. The introduction of multi-cursor technology, exemplified by COMPASS [64], further enhanced these interfaces by significantly reducing rotational distances during typing tasks.

In VR environments, circular interfaces naturally complement devices with circular motion capabilities, including controllers with joysticks, circular touchpads, and embedded sensors. The rapMenu [40] uses palm orientation to quickly indicate a set of menu items and pinch gestures to select a particular item from that set. Innovative designs like PizzaText [67], Hipad [21], and Ringtext [60] have also advanced the field. Our research leverages hand tracking technology to capture rich behavioral data during freehand interactions, thereby expanding the capabilities and applications of circular interfaces in immersive VR environments.

3 Interaction Design of cLock

We developed cLock's virtual numpad using Unity and deployed it on the Meta Quest Pro headset, leveraging its built-in hand-tracking cameras. The system is adaptable to other devices supporting real-time hand tracking, such as Meta Quest 3, Pico 4, Microsoft Hololens, and Apple Vision Pro.

3.1 Interaction Design

cLock minimizes hand movements for VR PIN entry by focusing on wrist rotation and finger taps, reducing shoulder, arm, and forearm fatigue. The interface (Figure 1) features a circular layout with digits 0-9 evenly distributed. Colored cursors resembling clock hands originate from the center, allowing users to position them through wrist rotation and select digits via finger taps.

To mitigate slow and tiring wrist movements, we implemented a multi-cursor approach [64, 22] where each cursor moves simultaneously at fixed intervals, controlled by different fingers. Section 4 details our comparative study to optimize cursor numbers, key densities, and intervals.

3.2 Wrist Rotation to Cursor Movement Mapping

The system leverages the Oculus Integration SDK's [9] real-time hand skeletal tracking to compute wrist rotation angles, implementing a direct 1:1 mapping between wrist movements and cursor rotation. Through pilot studies, we identified the comfortable rotation range for users' right hand: approximately -80 degrees in supination (outward rotation) to 140 degrees in pronation (inward rotation), with a median resting position at 30 degrees.

We aligned the circular interface's digit keys with this median position to optimize ergonomic comfort, ensuring balanced effort distribution between pronation and supination movements. The interface further enhances usability by maintaining natural alignment between finger movement trajectories and cursor directions, facilitating intuitive cursor-finger associations. During authentication, the system registers input by selecting the digit key nearest to the active cursor when a finger tap is detected.

3.3 Finger Tap Detection

We define finger bending angles as the angle between wrist-to-finger root and finger root-to-fingertip vectors. Based on our pilot study, we set tap detection criteria as a finger bend exceeding 10 degrees within 0.1 seconds. This threshold mitigates the Heisenberg effect [5], preventing unintended inputs. To avoid repeat inputs, we implemented a 0.75-second pause after each cursor trigger.

4 Preliminary Study: Optimizing cLock's UI

We conducted a preliminary user study to determine the optimal digit key and cursor placements for our circular interface, based on user performance and feedback during input tasks.

4.1 Experiment Design

To simulate actual PIN entry, participants entered multiple predesigned 6-digit codes as quickly and accurately as possible. We employed a within-subjects design with three factors (Figure 2): (1) **Number of Cursors**: As shown in Figure 2(a), we experimented with *one cursor* (index finger only), *two cursors* (index finger and thumb), and *three cursors* (index, thumb, and middle finger) based on pilot study findings. (2) **Key Density**: As shown in Figure 2(b), we evaluated three levels: *high* (15 degrees angular width per key), *medium* (22.5 degrees), and *low* (30 degrees). (3) **Cursor Interval**: As shown in Figure 2(c), we examined three intervals between cursors: *small* (2 keys), *medium* (3 keys), and *large* (4 keys).

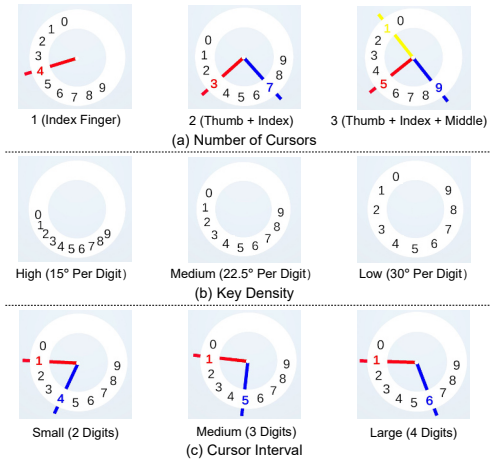


Figure 2: Our experimental platforms under different factors.

To ensure comfortable wrist rotations, we excluded certain combinations: low key density with a single cursor (excessive rotation) and, for three cursors, high key density (high error rates in pilot study) and large cursor intervals (overly spread cursors).

4.2 Participants and Procedure

Twenty-four participants (15 female, 9 male) aged 20-30 (M = 24.3, SD = 3.1) were recruited from campus, with average VR experience of 2.2 years (SD = 1.0). Each received $15 compensation. All participants provided written informed consent, and all studies were approved by the university's ethics committee.

The experiment began with a 5-minute familiarization period followed by the main study, conducted with participants seated in an armless chair. Participants completed 15 randomized task sessions, each implementing a unique combination of interface factors and comprising 10 trials of different 6-digit sequences. The interface displayed both target digits and real-time user input, providing immediate visual feedback. Participants prioritized both speed and accuracy, continuing to the next digit after any entry errors. Structured rest intervals between sessions minimized fatigue effects. The 45-minute protocol concluded with comprehensive evaluation through quantitative preference questionnaires and semi-structured interviews to gather detailed insights into user experience.

4.3 Results

In total, We collected data from 24 participants $\times$ 15 conditions $\times$ 10 repetitions $= 3,600$ trials from all participants. For analysis, no outliers were removed, and repeated measures within each condition for each participant were averaged.

Given the incomplete factorial design, linear mixed-effects models (LMMs) were employed using the SPSS MIXED procedure. Fixed effects included all three factors and their interactions, while participants were modeled as a random intercept to account for individual variability. Models were estimated using restricted maximum likelihood (REML), and denominator degrees of freedom were calculated using the Satterthwaite approximation. All dependent variables were confirmed to meet the assumption of normality.

4.3.1 Input Efficiency

Input time, defined as the average duration to input each digit, varied across configurations (Figure 3). **Number of Cursors** significantly affected input time ($F_{2,344} = 15.53, p < .001$). *Post-hoc* comparisons (Bonferroni-corrected) revealed that three-cursor input ($M = 1.53s, SE = 0.04$) was significantly slower than both one-cursor ($M = 1.35s, SE = 0.04$) and two-cursor ($M = 1.34s, SE = 0.04$) inputs (both $p < .001$), likely due to additional decision-making overhead during digit selection. No significant difference was found between one and two cursors ($p = 1.00$).

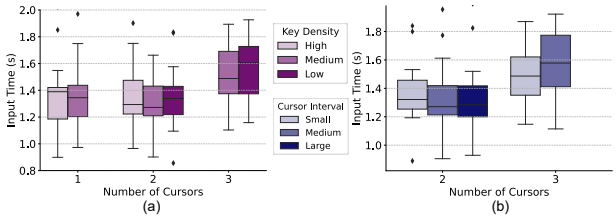


Figure 3: Box plots grouped by the Number of Cursors showing Main effects of (a) Key Density and (b) Cursor Interval on the input time.

No significant main effects were found for **Key Density** or **Cursor Interval**, and no significant interactions were observed between any of the three factors.

4.3.2 Input Errors

The input error rate, defined as the proportion of incorrectly entered digits, varied across interface configurations (Figure 4). **Number of Cursors** had a significant main effect on error rate ($F_{2,344} = 4.54, p < .05$). *Post hoc* comparisons (Bonferroni-corrected) indicated that the error rate in the three-cursor condition ($M = 12.5\%, SE = 2.3\%$) was significantly higher than in the two-cursor condition ($M = 6.9\%, SE = 2.0\%$; $p < .01$).

Neither **Key Density** nor **Cursor Interval** had a significant effect on error rate, and no significant interaction effects were observed among the three factors.

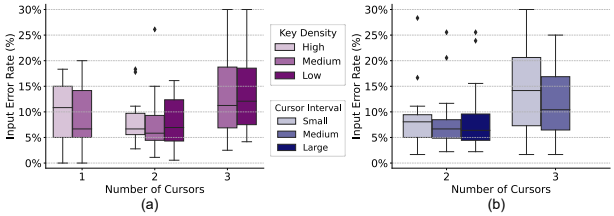


Figure 4: Box plots grouped by the Number of Cursors showing Main effects of (a) Key Density and (b) Cursor Interval on the input errors.

4.3.3 User Preference

Qualitative feedback indicated clear preferences across interface parameters (Figure 5). The dual-cursor configuration was preferred (79.2%), as it balanced input efficiency with comfort. While participants noted the index finger's superior dexterity compared to the thumb, they reported that using a single cursor led to excessive wrist rotation and fatigue. Three cursors were deemed less favorable due to increased cognitive load in cursor-finger mapping.

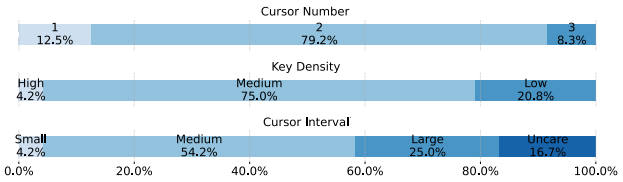


Figure 5: User Preferences for three factors.

Medium key density emerged as optimal (75.0% preference), with participants reporting that higher density risked misclicks while lower density demanded fatiguing wrist movements. The medium cursor interval, while preferred (54.2%), showed less decisive consensus, with participants indicating it had minimal impact on overall user experience compared to the other two parameters.

4.4 Discussion and Design Decisions

Our experimental results demonstrate that a two-cursor design effectively reduces wrist rotation without complicating interaction, thereby decreasing user fatigue and errors compared to a single cursor. Participants found using the index finger and thumb intuitive and simple, while three cursors notably increased input time and errors without improving user experience.

Based on both user preferences and performance data, the interface with **two cursors, medium key density, and medium cursor interval** was selected as the final design. We also incorporated enhanced visual elements based on user feedback (Figure 6): (1) Realigned digit placement for optimal ergonomics; (2) Varied cursor lengths to match natural finger proportions and reduce confusion between cursors; and (3) A gradient color scheme for digit keys that highlights both the selected key and its neighbor when cursor alignment is imprecise, signaling potential mis-tap risks.

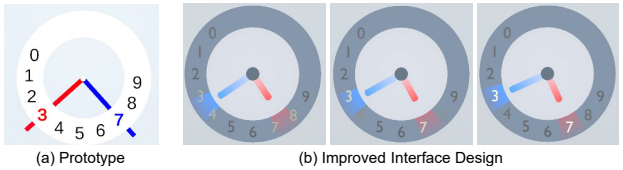


Figure 6: (a) the circular interface utilized in the preliminary study. (b) finalized interface of cLock.

5 Two-Factor Authentication Algorithm of cLock

5.1 Algorithm Design

cLock's authentication process, similar to traditional methods [69, 65], consists of registration and login phases. During registration, users enter a chosen PIN multiple times, capturing both the knowledge-based PIN and the associated hand motion pattern. At login, cLock employs dual-layered authentication, verifying both PIN correctness and the hand movement's biometric pattern. Figure 7 illustrates cLock's authentication algorithm.

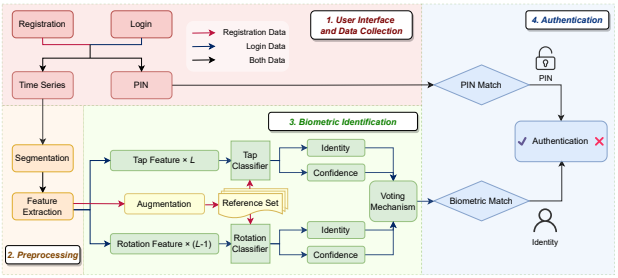


Figure 7: Authentication algorithm design of cLock.

5.2 Segmentation of Time Series Data

For a PIN of length L, cLock captures L finger taps and $L-1$ wrist rotations. Recognizing their distinct motion characteristics, we segment the time series into Tap and Rotation Segments. Based on statistics of preliminary study data, a Tap Segment comprises 50 frames (approximately 0.7 seconds) centered on each tap, while the $L-1$ Rotation Segments are identified in the intervals between taps.

We extracted features from raw hand skeleton data via real-time tracking for both segment types. Local coordinates relative to the Head-Mounted Display (HMD) were calculated by subtracting global coordinates from the HMD's, minimizing the effect of user positioning [27].

5.3 Feature Extraction

Based on observations from the preliminary study and prior research on hand-tracking for identity recognition [28, 44], we identified the following features characterizing hand movements during PIN input: (1) **F0: Finger Bending Angles.** Each finger comprises four skeletal points: proximal phalange (F_1), intermediate phalange (F_2), distal phalange (F_3), and fingertip (F_t). Including the wrist position (W), finger bending is described by three angles: $\angle WF_1F_2$, $\angle F_1F_2F_3$, and $\angle F_2F_3F_t$. F0 encompasses 15 dimensions across all five fingers. (2) **F1: Palm Posture.** We use the Forward and Upwards vectors of the palm to represent palm orientation, resulting in six dimensions (x,y,z) for each vector. (3) **F2: Palm Position.** The palm position is described using the wrist's coordinates relative to the HMD, comprising three dimensions (x,y,z).

For each segment, we sample every 5th frame from 50, using 11-frame hand tracking data. We calculate F0, F1, and F2 for these subsequences, along with their first-order and second-order temporal differences. We then derive statistical measures (mean, median, minimum, maximum, and standard deviation) for each feature [44], resulting in $(15+6+3)\times 3\times 5 = 360$ dimensions per tap and rotation feature.

5.4 User Identity Classifier Selection

Given that authentication scenarios inherently involve small-sample learning due to limited user registration data, and that high-parameter deep learning models are often unsuitable for such settings [2], we evaluated six classic machine learning algorithms commonly used in behavioral biometric classification [27, 42, 59]: Random Forests (RF), Naive Bayes (NB), Logistic Regression (LR), Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and Stochastic Gradient Descent (SGD). All classifiers used scikit-learn with default hyperparameters for reproducibility and fair comparison.

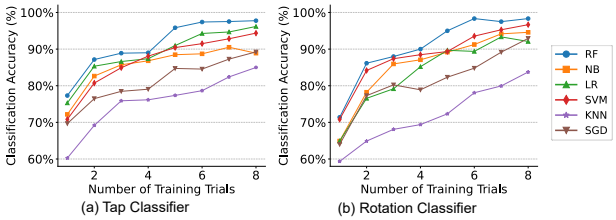


Figure 8: Classification accuracy of user identity across different methods as the number of training trials T varies. (a) for Tap Classifier. (b) for Rotation Classifier.

We used data from a preliminary study involving 24 participants, each completing 10 input trials using the optimal interface configuration. Each classifier was tasked with a 24-way classification problem to distinguish individual participants based on their unique behavioral patterns. Using a fixed train-test split (first 8 trials for potential training, last 2 for testing), we evaluated performance by incrementally increasing training trials (T) from 1 to 8 for separate Tap and Rotation Classifiers.

Figure 8 shows classification accuracy results. Random Forest consistently outperformed other methods across all training sizes for both classifiers, reaching 97.6% tap classification accuracy and 98.3% rotation accuracy at T=8. We selected **Random Forest** for our final model due to its superior performance with our complex, multi-dimensional feature space.

5.5 Voting Mechanism for Rejecting Imposters

To enhance security, we implemented a voting mechanism combining outputs from both tap and rotation classifiers. For a PIN of length L, our system generates L tap and $L-1$ rotation segments during login. After feature extraction, each segment is independently classified, producing identity predictions and confidence scores. These predictions are aggregated to determine: (1) **Elected Identity** (I_{elect}): The identity with the highest occurrence, and (2) **Elected Confidence Score** (CS_{elect}): The average confidence scores of the I_{elect}.

For tied frequencies, we select the identity with the highest CS_{elect}. To guard against imposters, we introduced a **Confidence Score Threshold** ($Threshold_{CS}$). Let I_{claim} represent the user-claimed identity during login. The system accepts the behavioral biometric only when:

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

We evaluated threshold impact through 24-fold validation using preliminary study data, treating each participant as an imposter once while considering others as registered users. Figure 9 shows how classification accuracy varies with different threshold settings. As the threshold increases from 0 to 1, false acceptance decreases to 0, while false rejection increases to 1. Balancing these factors, we set $Threshold_{CS}$ to 0.5, optimizing recognition precision while minimizing erroneous rejections.

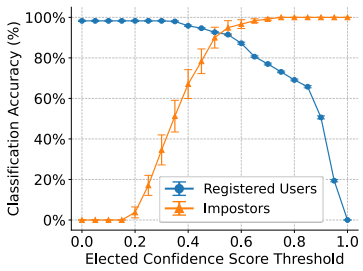
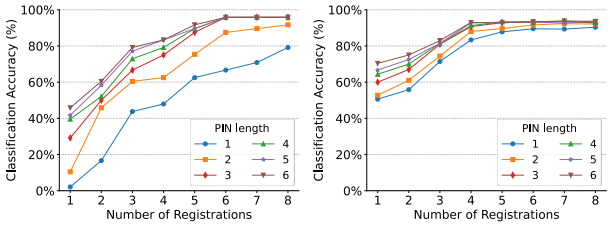


Figure 9: Classification accuracy for registered users and impostors when Confidence Score Threshold ($Threshold_{CS}$) changes. The error bar denotes a standard error.

5.6 Determining PIN Length and Number of Registrations

We systematically investigated the relationship between PIN length (L), registration attempts (T), and system performance. Following the methodology in Section 5.4, we evaluated classifier performance through incremental increases in T (1 to 8), analyzing authentication accuracy for varying PIN lengths using the initial L digits of each entry (Figure 10).



(a) Mean classification accuracy for registered users

(b) Mean classification accuracy for impostors

Figure 10: Mean classification accuracy trends across different numbers of registration attempts for registered users (a) and impostors (b), respectively, with various PIN lengths.

ANOVA analysis revealed optimal performance with a 3-digit PIN and six registration attempts, achieving 95.8% user identification accuracy and 93.1% impostor detection rate. Notably, neither extending PIN length to 6 digits nor increasing registration attempts to 10 yielded significant improvements.

This evidence guided cLock's final design: **a 3-digit PIN with six registrations**. While shorter than conventional PINs, this configuration leverages rich behavioral biometrics from three taps and two rotations to maintain security while optimizing efficiency. This approach aligns with emerging trends in 2FA, where systems like Blinkey [69], Squeez'In [65], and RubikBiom [34] employ similarly condensed credentials (3-4 items) while ensuring security through secondary biometric factors.

5.7 Adaptive Learning Strategy

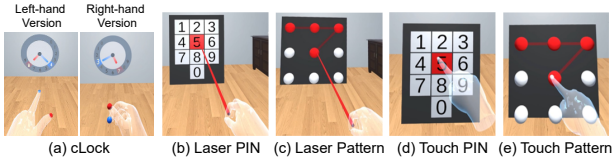
To accommodate natural variations in user behavior over time, cLock implements an adaptive learning strategy [43, 7]. The system periodically retrains its authentication model using newly collected behavioral data from legitimate login attempts, progressively refining each user's profile. These updates can be scheduled during device idle periods to minimize computational overhead. and user disruption.

6 Usability Evaluation

This section evaluates cLock's usability in real authentication tasks, comparing it with widely used authentication methods.

6.1 Experiment Design

We employed a within-subjects design to analyze usability differences across various authentication methods. Our proposed method, cLock (mirrored for left-handed users), was compared against four common barehanded authentication techniques (Figure 11): (1) **Laser PIN:** Standard numeric keypad using laser-pointing with pinch confirmation. (2) **Laser Pattern:** Nine-dot pattern using laser-pointing with pinch confirmation. (3) **Touch PIN:** Standard numeric keypad using mid-air finger touch. (4) **Touch Pattern:** Nine-dot pattern using mid-air finger touch.



(a) cLock (b) Laser PIN (c) Laser Pattern (d) Touch PIN (e) Touch Pattern

Figure 11: User interface of the five authentication techniques.

The experiment consisted of registration and authentication phases. During registration, seated participants established their credentials through a controlled procedure. Following optimal configuration (Section 5.6), cLock participants entered a 3-digit PIN six times, while baseline methods used a traditional single-factor approach requiring a 6-digit PIN with two confirmatory entries. This PIN length difference reflects each system's security paradigm: baseline methods rely on longer PINs for entropy against brute-force attacks, while cLock maintains equivalent security with shorter PINs through behavioral biometric validation. To ensure robustness, sequential or repetitive patterns were prohibited, with failed pattern matching requiring re-registration. Registration data trained the authentication models.

The authentication phase evaluated performance through three login attempts per participant with real-time feedback. To assess cLock's versatility, we examined performance across four scenarios: *Seated* (without armrests), *Standing*, *Reclining*, and *Walking*—reflecting common VR interaction contexts. Baseline methods were evaluated only in the seated position, identified by prior research as the optimal VR posture [71].

6.2 Participants and Apparatus

We recruited 20 new participants (13 male, 7 female; age: $M = 23.6$, $SD = 2.3$) from our campus, including both right-handed (12; 7 male, 5 female) and left-handed (8; 6 male, 2 female) individuals. Their average VR usage experience was 1.8 years ($SD = 0.7$), and each received $15 compensation.

The experimental setup utilized a Meta Quest Pro headset connected to an ASUS laptop (Windows 11, Intel i9-12900H CPU, 32.0 GB RAM, NVIDIA GeForce RTX 3080 Ti GPU), with all computations performed on the laptop and streamed to the VR headset. The system architecture included Unity-based virtual environment rendering and hand gesture detection, and Python-implemented motion feature preprocessing, model training, and inference.

6.3 Procedure

To mitigate learning bias, we began with a 10-minute training session. Participants then engaged in five randomized sessions: one for cLock (encompassing all four postures) and one for each baseline method. The cLock session was divided into four randomized blocks corresponding to four postures. Each session consisted of registration and login phases, conducted using the participant's dominant hand, with short breaks between sessions.

After completing all sessions, participants completed a 7-point Likert-scale questionnaire assessing six dimensions: *Privacy Protection*, *Social Acceptance*, *Physical Effortlessness*, *Mental Effort-*

lessness, *Ease of Learning*, and *Overall Satisfaction*. Brief follow-up interviews gathered qualitative feedback on each method's strengths and weaknesses, providing deeper insights into user experience. The entire study lasted approximately 60 minutes.

6.4 Results

To address the unbalanced experimental design (baseline methods tested only in seated posture while cLock evaluated across four postures), we employed a two-stage analysis approach. First, we compared cLock's seated performance with baseline methods for fair comparison. Second, we analyzed cLock's performance across different postures to evaluate its robustness. For analysis, no outliers were removed, and repeated measures within each condition for each participant were averaged. After confirming that all dependent variables met the assumption of normality, we conducted repeated-measures ANOVA (RM-ANOVA) for statistical tests and performed *post hoc* pairwise comparisons using Bonferroni-corrected paired *t*-tests. The Friedman test was used for analyzing non-parametric questionnaire data.

6.4.1 Authentication Method Comparison

Registration and Login Time: Figure 12(a) and (b) show significant differences in registration ($F_{4,76} = 4.2$, $p < .005$) and login time ($F_{4,76} = 22.7$, $p < .001$) across methods.

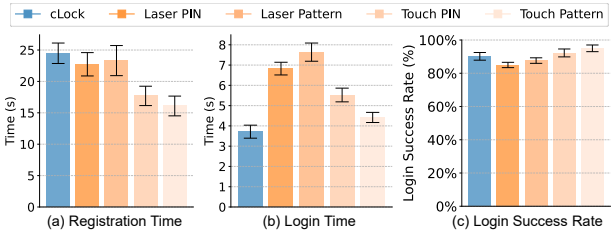


Figure 12: Average (a) registration time, (b) login time, and (c) login success rate for different authentication methods in seated posture. Error bars show standard error.

For registration time, cLock had the highest duration ($M = 24.5s, SE = 1.6$), significantly slower than *Touch Pattern* ($M = 16.1s, SE = 1.6$, $p < .05$), but comparable to the other three methods ($M = 17.7s - 23.3s, SE = 1.5 - 2.4$). This longer registration reflects the six-trial enrollment process required for robust behavioral biometric training (Section 5.6). Given registration's one-time nature, this minimally impacts overall user experience.

For login time, cLock ($M = 3.7s, SE = 0.32$) significantly outperformed three baseline methods: *Laser PIN* ($M = 6.8s, SE = 0.31$, $p < .001$), *Laser Pattern* ($M = 7.6s, SE = 0.45$, $p < .001$), and *Touch PIN* ($M = 5.5s, SE = 0.34$, $p < .05$), while achieving comparable speed to *Touch Pattern* ($M = 4.4s, SE = 0.25$, $p = .85$).

Authentication Success Rate: Figure 12(c) presents overall login success rates with significant differences across methods ($F_{4,76} = 6.2$, $p < .001$). Note that for cLock, login failures include both input errors and false rejections from biometric verification, while baseline methods' failures stem solely from input errors.

cLock achieved a success rate of $M = 90.2\%$ ($SE = 2.3\%$), which was significantly lower than *Touch Pattern* ($M = 95.0\%, SE = 2.0\%$, $p < .05$) but statistically comparable to *Laser PIN* ($M = 85.0\%, SE = 1.6\%$), *Laser Pattern* ($M = 87.6\%, SE = 1.7\%$), and *Touch PIN* ($M = 92.2\%, SE = 2.4\%$) (all $p > .05$).

6.4.2 cLock Posture Robustness Analysis

Login Time Across Postures: Figure 13(a) shows that postures significantly impacted cLock's login time ($F_{3,57} = 3.4$, $p < .05$). cLock performed consistently across static postures—*Seated* ($M = 3.7s, SE = 0.32$), *Standing* ($M = 3.9s, SE = 0.35$), and *Reclining* ($M = 4.2s, SE = 0.53$)—with no significant differences between them (all $p > .05$). Only *Walking* showed significantly increased duration ($M = 6.2s, SE = 0.75$) compared to *Seated* and *Standing* (both $p < .05$), likely due to motion-induced instability affecting precise hand movements.

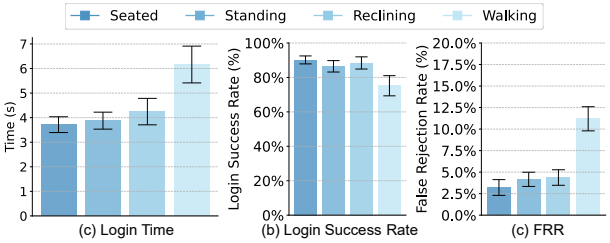


Figure 13: cLock posture robustness evaluation. cLock's (a) login time, (b) login success rate, and (c) False Rejection Rate (FRR) across four different postures. Error bars show standard error.

Authentication Success Across Postures: Figure 13(b) demonstrates that postures significantly affected cLock's login success rate ($F_{3,57} = 3.8$, $p < .05$). Static postures maintained high success rates: *Seated* ($M = 90.2\%, SE = 2.3\%$), *Standing* ($M = 84.4\%, SE = 3.5\%$), and *Reclining* ($M = 86.5\%, SE = 3.3\%$) showed no significant differences (all $p > .05$). However, *Walking* exhibited significantly lower success ($M = 75.2\%, SE = 5.9\%$) compared to *Seated* ($p < .05$) and *Reclining* ($p < .05$).

False Rejection Rate Analysis: To isolate biometric authentication performance, we analyzed the False Rejection Rate (FRR)—the rate at which valid login attempts are incorrectly rejected by the behavioral biometric system. Figure 13(c) reveals significant differences in FRR across postures ($F_{3,57} = 10.0$, $p < .001$). Static postures maintained low and comparable FRRs: *Seated* ($M = 3.2\%, SE = 0.9\%$), *Standing* ($M = 4.2\%, SE = 0.8\%$), and *Reclining* ($M = 4.4\%, SE = 0.9\%$) showed no significant differences (all $p > .05$). Only *Walking* exhibited significantly higher FRR ($M = 12.2\%, SE = 1.4\%$, $p < .001$ for all pairwise comparisons), indicating that motion-induced finger tremors introduce behavioral variability that challenges biometric recognition.

6.4.3 Subjective Ratings

As shown in Figure 14, cLock outperformed other methods in *Privacy Protection* ($Q(4) = 57.4, p < .001$). Its rating ($M = 6.1, SE = 0.23$) was comparable to *Laser PIN* ($M = 5.1, SE = 0.32$, $p = 0.1$) but significantly higher than other three methods ($p < .05$ to $p < .001$). 90% of participants deemed cLock safest, citing its minimal movements, complex gestures, and two-factor authentication. For *Social Acceptance* ($Q(4) = 17.1, p = .002$), cLock ($M = 5.8, SE = 0.21$) scored significantly higher than all other methods ($M = 4.4 - 4.6, SE = 0.22 - 0.27$, all $p < .05$), with 75% of participants preferring it due to shorter PINs and subtler movements, especially in public settings.

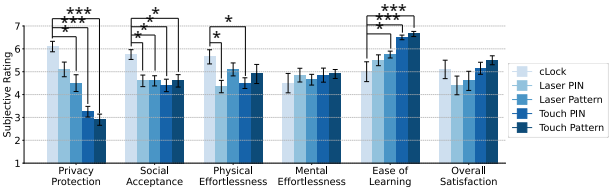


Figure 14: Subjective ratings of different techniques (1: extremely negative; 7: extremely positive). The error bar shows standard error. The significant differences (*, ***) were from *post-hoc* analysis.

In *Physical Effortlessness* ($Q(4) = 4.22, p < .05$), cLock ($M = 5.7, SE = 0.31$) matched pattern-based methods but surpassed PIN-based ones (both $p < .05$), with 55% of participants noting its minimal arm movements reduced fatigue. *Mental Effortlessness* showed no significant differences ($p = 0.6$), though cLock scored lowest ($M = 4.5, SE = 0.42$), with 25% of participants noting initial challenges with cursor alignment due to unfamiliarity.

Ease of Learning varied significantly ($Q(4) = 27.7, p < .001$), with cLock ($M = 5.0, SE = 0.43$) matching *Laser PIN* but scoring lower than other methods, reflecting its novel interaction paradigm. However, performance metrics suggest high usability once mastered, with 60% of users indicating cLock becomes easy to use after practice. *Overall Satisfaction* showed no significant differences ($Q(4) = 2.4, p = 0.06$) across methods, with cLock ($M = 5.1, SE = 0.40$) demonstrating marginally higher satisfaction than laser-based methods but slightly lower than touch-based approaches, potentially due to users' greater familiarity with touch interactions from everyday touchscreen devices.

7 Security Evaluation

We conducted a further investigation focused on the security of cLock, testing its resilience to attacks in practical usage scenarios.

7.1 Threat Models

To validate true two-factor authentication, we evaluate each authentication factor independently: knowledge factor security through shoulder-surfing resistance [48, 10], and biometric factor capability through credential-aware attack scenarios [69, 65].

Shoulder-Surfing Attack Model: In VR environments, virtual interface elements are invisible to external observers—attackers can only observe users' physical hand movements and gestures. Our threat model considers external observers who watch physical interactions during authentication, particularly relevant as VR/AR devices are increasingly used in public spaces [41].

Credential-Aware Attack Model: This examines worst-case scenarios where attackers possess complete knowledge of PINs and input gestures. Attackers attempt to replicate legitimate users' motions with known credentials, evaluating whether behavioral biometrics alone can reject unauthorized access when the knowledge factor is fully compromised.

7.2 Participants and Procedure

We recruited 20 new participants (9 males, 11 females; average age = 23.1 years, SD = 3.4 years) from our campus with average VR experience of 2.1 years (SD = 1.2 years). Each received $10 base compensation plus a performance bonus of up to $7 based on success in thwarting shoulder-surfing attempts.

After a 10-minute training session, randomly paired participants took turns registering their PINs privately, with this data training the authentication models. The experiment included three blocks simulating observation distances of **1m, 2m, and 4m**, representing realistic scenarios. Each block contained five randomized sessions (one per authentication method) to mitigate order effects. While one participant performed three login entries per method and distance in a seated position, their partner acted as an attacker observing the input process. Following each distance block, we conducted credential-aware attack phases where attackers attempted to mimic legitimate users' behavior with known PIN codes, simulating complete information leakage and testing the system's ability to reject unauthorized access based solely on behavioral biometrics. Participants switched roles after completing all blocks, with the entire procedure lasting approximately 80 minutes.

7.3 Results

7.3.1 Shoulder-Surfing Attacks

We assessed two key metrics: digit-wise guess accuracy (probability of correctly guessing individual digits) and entire entry guess accuracy (likelihood of guessing the complete PIN correctly). Figure 15 illustrates attackers' accuracy rates, demonstrating cLock's strong resistance to shoulder-surfing.

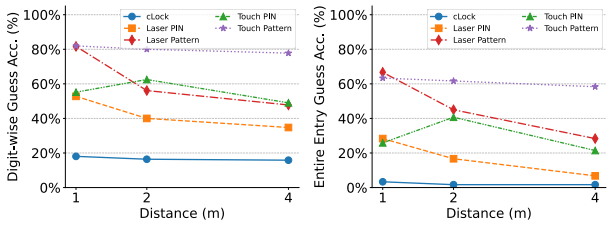


Figure 15: Digit-wise Guess Accuracy (left) and Entire Entry Guess Accuracy (right) for cLock and other comparison methods.

cLock's digit-wise guess accuracy remained consistently low across all distances (18.0%, 16.4%, and 15.8%), only slightly above the 10% random guess probability, indicating robust security even at close proximity. The entire entry guess accuracy was minimal at 1.6% for 2m and 4m distances, and only 3.3% at 1m.

In contrast, baseline methods showed significantly higher vulnerability, with accuracy increasing at closer distances. At one meter, pattern-based methods exceeded 80% digit-wise guess accuracy, while PIN-based methods approached 60%. For entire entry guesses at 1m, touch-based methods exhibited deciphering rates up to 60%, and pinch-based methods surpassed 20%. These results demonstrate that despite cLock's shorter three-digit PIN, inferring the code remains challenging, whereas even six-digit codes in baseline methods provide inadequate protection.

Participant feedback highlighted that cLock's lack of spatial references, variable gesture details, small motion amplitude, and dual-cursor design effectively mask visual cues that could facilitate input inference. Unlike traditional two-dimensional input interfaces, cLock's innovative design significantly enhances defense against shoulder-surfing attacks.

7.3.2 Credential-Aware Attacks

For fair evaluation in credential-aware attacks, we compared cLock with biometrically enhanced baseline methods by applying cLock's behavioral biometric features and algorithm to all methods. This enabled direct comparison between cLock's 3-digit PIN and the 6-digit PIN/pattern baselines. We calculated False Acceptance Rates (FAR, the rate of incorrectly accepted illegitimate samples) and False Rejection Rates as the number of registered users increased.

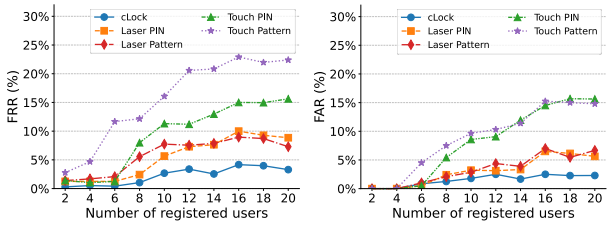


Figure 16: False Rejection Rate (left) and False Acceptance Rate (right) across biometrically enhanced authentication methods.

Figure 16 illustrates variations in FRR and FAR across authentication methods. cLock maintained a consistently low FRR of 3.2% even with 20 registered users, while baseline methods

showed marked increases (7.3% to 22.4%), which would significantly impair user experience through erroneous rejections. Similarly, cLock's FAR remained low at 2.3% with 20 registered users, while baseline methods showed higher rates (5.6% to 15.6%). This superior performance stems from cLock's utilization of rich temporal and spatial features from wrist rotations and finger taps that are more individually distinctive than the simpler hand movements used in baseline methods.

8 Validation of Longitudinal Stability

While our previous studies demonstrated cLock's fundamental usability and security, behavioral biometric authentication requires consistent user patterns over time. We conducted an 11-day longitudinal investigation following methodological approaches from prior research [65, 23, 38].

We recruited 15 new participants (10 male, 5 female; mean age = 23.5 years, SD = 2.2) who registered unique 3-digit PINs on Day 0 and completed experimental sessions on Days 0, 2, 4, 6, 8, and 10, each comprising 24 login attempts (10 legitimate, 14 impostor). After each session, the authentication model updated using newly collected legitimate data through our adaptive learning strategy.

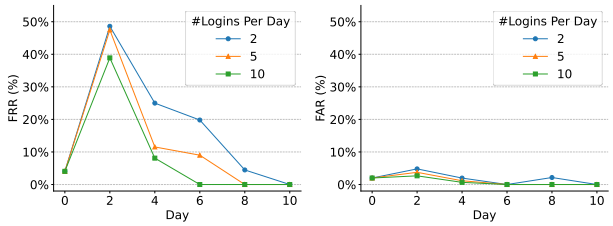


Figure 17: False Rejection Rate (FRR) and False Acceptance Rate (FAR) trends across 2, 5, and 10 logins per day over 11 days.

By controlling the number of daily login attempts used for model adaptation, we analyzed how authentication performance scaled with usage frequency. The False Rejection Rate (FRR) followed a characteristic pattern (Figure 17): initially rising to 40-50% on Day 2, then steadily declining as participants continued using the system. With ten daily logins, FRR reached zero by Day 6; even with minimal engagement (two attempts daily), it converged to zero by Day 10. This initial performance degradation reflects the adaptation period during which users' behavioral patterns stabilize [38].

The False Acceptance Rate (FAR) remained consistently low throughout the study, with only a brief elevation to 4.80% on Day 2 under the two-login condition before quickly decreasing. From Day 6 onward, conditions with 5-10 daily logins achieved zero false acceptances, which demonstrates the stable security of cLock.

9 Discussion

9.1 Usability of cLock

cLock introduces an ergonomic interaction paradigm that leverages the natural synergy between wrist rotation and finger tapping, with users highlighting its enhanced privacy protection and social acceptance. This approach neatly combines PIN entry with behavioral biometrics, simultaneously triggering two authentication factors while enhancing both user comfort and security.

While existing two-factor systems require deliberate security gestures such as specific blink patterns [69] or head movements [20], cLock achieves enhanced security through natural bare-hand movements with proven posture-resilient stability. Our system delivers faster authentication (3.7s versus 4.4-7.6s baseline, see Section 6.4.1) and comparable authentication success rates, though we acknowledge this advantage partly stems from shorter PIN length (3-digit vs. 6-digit for baselines). This demonstrates how a second security factor can be seamlessly integrated into natural interactions rather than imposed as additional tasks.

Despite the above advantages, cLock does present learning challenges. Users reported significantly lower ease-of-learning scores compared to all baseline methods and relatively poor subjective mental effort due to cursor mapping and alignment requirements. The novel interaction paradigm requires initial familiarization that traditional PIN/pattern methods do not, representing a trade-off between enhanced security and immediate usability.

9.2 Security of cLock

Unlike traditional VR interfaces that rely on visible spatial relationships between hand positions and UI elements, cLock's single-hand interaction inherently resists observation attacks. The combination of wrist rotation with dual-cursor input creates a spatially ambiguous interaction pattern, achieving remarkably low PIN deciphering rates (1.6-3.3% versus 20%-60% baseline, see Section 7.3.1) without requiring interface complexity (e.g., randomized input layouts).

cLock's hand interaction fully exploits the wrist, finger, and palm's movement capabilities, generating rich motion features that serve as distinctive and reliable behavioral biometrics. When we applied identical biometric algorithms to all methods, cLock's rich hand motion patterns provided superior biometric discriminability compared to simpler baseline interactions, maintaining significantly lower FAR and FRR (see Section 7.3.2). cLock's accuracy also exceeds many existing VR behavioral biometric systems that typically achieve 90%-95% classification accuracy [1, 25, 27, 36].

10 Limitations and Future Works

While our study demonstrates cLock's potential, key limitations remain. First, our two-factor authentication relies on temporally entangled data—behavioral biometrics are extracted during PIN entry rather than as independent verification. Future work could decouple these factors (e.g., requiring a separate biometric gesture post-PIN) for true independence. Second, our evaluation methodology favors cLock: it uses shorter PINs with richer motion data, while baselines weren't designed for biometric enhancement. Future studies should benchmark against behavioral-biometrics-native authentication methods rather than adapted traditional approaches.

The practical deployment of cLock faces real-world challenges not fully addressed in our controlled experiments. Future work must investigate: (1) performance across diverse user populations beyond our 20-30 age group, including users with motor impairments or varying hand sizes; (2) longitudinal adoption patterns and learning curves in everyday VR usage; (3) integration with existing VR platforms and applications; and (4) resilience against sophisticated attacks like replay attacks or adversarial mimicry. Additionally, theoretical analysis quantifying the security entropy contribution of behavioral biometrics would complement our empirical validation and guide optimization for commercial deployment.

11 Conclusion

This paper presents cLock, a novel two-factor authentication mechanism for VR environments. By combining wrist rotation and finger taps with spatio-temporal hand movement analysis, cLock achieves a unique balance between security and usability. Our studies demonstrate cLock's optimized UI design, robust performance across various postures, strong resistance to both shoulder-surfing and credential-aware attacks, and enduring stability for real-world deployment. These contributions advance the field of VR authentication and provide insights for designing secure and user-centric interaction techniques in immersive environments.

Acknowledgments

This work was supported by the Natural Science Foundation of China under Grant No. 62472243 and 62132010.

REFERENCES

[1] A. Ajit, N. K. Banerjee, and S. Banerjee. 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)*, pp. 9–97. IEEE Computer Society, 2019. 2, 9

[2] A. Alwosheel, S. van Cranenburgh, and C. G. Chorus. Is your dataset big enough? sample size requirements when using artificial neural networks for discrete choice analysis. *Journal of Choice Modelling*, 28:167–182, 2018. doi: 10.1016/j.jocm.2018.07.002 5

[3] I. Anastasaki, G. Drosatos, G. Pavlidis, and K. Rantos. User authentication mechanisms based on immersive technologies: A systematic review. *Information*, 14(10):538, 2023. 2

[4] M. M. Asad, A. Naz, P. Churi, and M. M. Tahanzadeh. Virtual reality as pedagogical tool to enhance experiential learning: a systematic literature review. *Education Research International*, 2021:1–17, 2021. 2

[5] D. Bowman, C. Wingrave, J. Campbell, and V. Ly. Using pinch gloves (tm) for both natural and abstract interaction techniques in virtual environments. 2001. 3

[6] D. Buschek, B. Roppelt, and F. Alt. Extending keyboard shortcuts with arm and wrist rotation gestures. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pp. 1–12, 2018. 2

[7] F. M. Castro, M. J. Marín-Jiménez, N. Guil, C. Schmid, and K. Alahari. End-to-end incremental learning. In *Proceedings of the European conference on computer vision (ECCV)*, pp. 233–248, 2018. 6

[8] J. Cechanowicz, S. Dawson, M. Victor, and S. Subramanian. Stylus based text input using expanding cirrin. In *Proceedings of the working conference on Advanced visual interfaces*, pp. 163–166, 2006. 3

[9] M. company. Set Up Hand Tracking — Oculus Developers — developer.oculus.com. `https://developer.oculus.com/documentation/unity/unity-handtracking/`, 2023. [Accessed 09-09-2023]. 3

[10] R. Düzgün, P. Mayer, and M. Volkamer. Shoulder-surfing resistant authentication for augmented reality. In *Nordic Human-Computer Interaction Conference*, pp. 1–13, 2022. 2, 8

[11] R. Düzgün, N. Noah, P. Mayer, S. Das, and M. Volkamer. 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*, pp. 1–12, 2022. 2

[12] J. Fashimpaur, A. Karlson, T. R. Jonker, H. Benko, and A. Gupta. Investigating wrist deflection scrolling techniques for extended reality. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pp. 1–16, 2023. 2

[13] C. George, M. Khamis, E. von Zezschwitz, M. Burger, H. Schmidt, F. Alt, and H. Hussmann. Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality. NDSS, 2017. 2

[14] A. Giaretta. Security and privacy in virtual reality–a literature survey. *arXiv preprint arXiv:2205.00208*, 2022. 2

[15] J. Gong, Z. Xu, Q. Guo, T. Seyed, X. Chen, X. Bi, and X.-D. Yang. Wristext: One-handed text entry on smartwatch using wrist gestures. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pp. 1–14, 2018. 3

[16] E. Grandjean. Fitting the task to the man: an ergonomic approach. *(No Title)*, 1980. 3

[17] A. Gupta, C. Ji, H.-S. Yeo, A. Quigley, and D. Vogel. Rotoswype: Word-gesture typing using a ring. In *Proceedings of the 2019 CHI conference on human factors in computing systems*, pp. 1–12, 2019. 2

[18] S. S. Harakannanavar, P. C. Renukamurthy, and K. B. Raja. Comprehensive study of biometric authentication systems, challenges and future trends. *International Journal of Advanced Networking and Applications*, 10(4):3958–3968, 2019. 2

[19] C. H. Heruatmadja, A. N. Hidayanto, H. Prabowo, et al. Biometric as secure authentication for virtual reality environment: A systematic literature review. In *2023 International Conference for Advancement in Technology (ICONAT)*, pp. 1–7. IEEE, 2023. 2

[20] J. Iskander, A. Abobakr, M. Attia, K. Saleh, D. Nahavandi, M. Hossny, and S. Nahavandi. 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)*, pp. 1844–1848. IEEE, 2019. 9

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

[22] M. Kobayashi and T. Igarashi. Ninja cursors: using multiple cursors to assist target acquisition on large screens. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 949–958, 2008. 3

[23] K. Krombholz, T. Hupperich, and T. Holz. Use the force: Evaluating {Force-Sensitive} authentication for mobile devices. In *Twelfth symposium on usable privacy and security (SOUPS 2016)*, pp. 207–219, 2016. 9

[24] A. Kumar, L.-H. Lee, J. Chauhan, X. Su, M. A. Hoque, S. Pirttikangas, S. Tarkoma, and P. Hui. Passwalk: Spatial authentication leveraging lateral shift and gaze on mobile headsets. In *Proceedings of the 30th ACM International Conference on Multimedia*, pp. 952–960, 2022. 2

[25] A. Kupin, B. Moeller, Y. Jiang, N. K. Banerjee, and S. Banerjee. Task-driven biometric authentication of users in virtual reality (vr) environments. In *MultiMedia Modeling: 25th International Conference, MMM 2019, Thessaloniki, Greece, January 8–11, 2019, Proceedings, Part I 25*, pp. 55–67. Springer, 2019. 2, 9

[26] P. Kürtünlüoğlu, B. Akdik, and E. Karaarslan. Security of virtual reality authentication methods in metaverse: An overview. *arXiv preprint arXiv:2209.06447*, 2022. 2

[27] J. Liebers, M. Abdelaziz, L. Mecke, A. Saad, J. Auda, U. Gruenefeld, F. Alt, and S. Schneegass. Understanding user identification in virtual reality through behavioral biometrics and the effect of body normalization. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pp. 1–11, 2021. 2, 5, 9

[28] J. Liebers, S. Brockel, U. Gruenefeld, and S. Schneegass. Identifying users by their hand tracking data in augmented and virtual reality. *International Journal of Human–Computer Interaction*, pp. 1–16, 2022. 2, 5

[29] J. Liebers, P. Horn, C. Burschik, U. Gruenefeld, and S. Schneegass. 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*, Dec 2021. doi: 10.1145/3489849.3489880 2

[30] D. J. Lohr, S. Aziz, and O. Komogortsev. Eye movement biometrics using a new dataset collected in virtual reality. In *ACM Symposium on Eye Tracking Research and Applications*, Jun 2020. doi: 10.1145/3379157.3391420 2

[31] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, et al. *Handbook of fingerprint recognition*, vol. 2. Springer, 2009. 2

[32] J. Mankoff and G. D. Abowd. Cirrin: A word-level unistroke keyboard for pen input. In *Proceedings of the 11th annual ACM symposium on User interface software and technology*, pp. 213–214, 1998. 3

[33] R. Masuda, K. Sasaki, M. Hirokawa, T. Hachisu, and K. Suzuki. Posture control of the passenger based on caregiver's wrist motion for a step-climbing stroller. *IEEE Robotics and Automation Letters*, 7(2):3016–3021, 2022. 2

[34] F. Mathis, H. I. Fawaz, and M. Khamis. Knowledge-driven biometric authentication in virtual reality. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1–10, 2020. 2, 6

[35] M. R. Miller, F. Herrera, H. Jun, J. A. Landay, and J. N. Bailenson. Personal identifiability of user tracking data during observation of 360-degree vr video. *Scientific Reports*, 10(1):17404, 2020. 2

[36] R. Miller, N. K. Banerjee, and S. Banerjee. 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)*, pp. 311–316. IEEE, 2020. 2, 9

[37] R. Miller, N. K. Banerjee, and S. Banerjee. Using siamese neural networks to perform cross-system behavioral authentication in virtual reality. In *2021 IEEE Virtual Reality and 3D User Interfaces (VR)*, pp. 140–149. IEEE, 2021. 2

[38] R. Miller, N. K. Banerjee, and S. Banerjee. Temporal effects in motion behavior for virtual reality (vr) biometrics. In *2022 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*, pp. 563–572. IEEE, 2022. 2, 9

[39] T. Mustafa, R. Matovu, A. Serwadda, and N. Muirhead. 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*, Mar 2018. doi: 10.1145/3180445.3180450 2

[40] T. Ni Ryan, P. McMahan, and D. A. Bowman. Tech-note: rapmenu: Remote menu selection using freehand gestural input. In *2008 IEEE Symposium on 3D User Interfaces*, pp. 55–58, 2008. doi: 10.1109/3DUI.2008.4476592 3

[41] N. Noah and S. Das. From pins to gestures: Analyzing knowledge-based authentication schemes for augmented and virtual reality. *IEEE Transactions on Visualization and Computer Graphics*, 31(5):3172–3182, 2025. doi: 10.1109/TVCG.2025.3549862 2, 8

[42] I. Olade, C. Fleming, and H.-N. Liang. Biomove: Biometric user identification from human kinesiological movements for virtual reality systems. *Sensors*, p. 2944, May 2020. doi: 10.3390/s20102944 2, 5

[43] G. I. Parisi, R. Kemker, J. L. Part, C. Kanan, and S. Wermter. Continual lifelong learning with neural networks: A review. *Neural networks*, 113:54–71, 2019. 6

[44] K. Pfeuffer, M. J. Geiger, S. Prange, L. Mecke, D. Buschek, and F. Alt. Behavioural biometrics in vr: Identifying people from body motion and relations in virtual reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pp. 1–12, 2019. 2, 5

[45] M. Proschowsky, N. Schultz, and N. E. Jacobsen. An intuitive text input method for touch wheels. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pp. 467–470, 2006. 3

[46] L. Quintero, P. Papapetrou, J. Hollmén, and U. Fors. 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)*, pp. 38–46. IEEE, 2021. 2

[47] M. Rahman, S. Gustafson, P. Irani, and S. Subramanian. Tilt techniques: investigating the dexterity of wrist-based input. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Apr 2009. doi: 10.1145/1518701.1518997 2

[48] V. Roth, K. Richter, and R. Freidinger. A pin-entry method resilient against shoulder surfing. In *Proceedings of the 11th ACM Conference on Computer and Communications Security*, CCS '04, p. 236–245. Association for Computing Machinery, New York, NY, USA, 2004. doi: 10.1145/1030083.1030116 8

[49] F. Salemi Parizi, W. Kienzle, E. Whitmire, A. Gupta, and H. Benko. Rotowrist: Continuous infrared wrist angle tracking using a wristband. In *Proceedings of the 27th ACM Symposium on Virtual Reality Software and Technology*, VRST '21. Association for Computing Machinery, New York, NY, USA, 2021. doi: 10.1145/3489849.3489886 2

[50] D. Schön, T. Kosch, F. Müller, M. Schmitz, S. Günther, L. Bommhardt, and M. Mühlhäuser. Tailor twist: Assessing rotational mid-air interactions for augmented reality. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pp. 1–14, 2023. 2

[51] G. Shoemaker, L. Findlater, J. Q. Dawson, and K. S. Booth. Mid-air text input techniques for very large wall displays. In *Graphics Interface*, pp. 231–238, 2009. 3

[52] M. Sivasamy, V. Sastry, and N. Gopalan. Vrcauth: Continuous authentication of users in virtual reality environment using head-movement. In *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, Jun 2020. doi: 10.1109/icces48766.2020.9137914 2

[53] S. Stephenson, B. Pal, S. Fan, E. Fernandes, Y. Zhao, and R. Chatterjee. Sok: Authentication in augmented and virtual reality. In *2022 IEEE Symposium on Security and Privacy (SP)*, pp. 267–284. IEEE, 2022. 2

[54] M. Suzuki, R. Iijima, K. Nomoto, T. Ohki, and T. Mori. Pinchkey: A natural and user-friendly approach to vr user authentication. In *Proceedings of the 2023 European Symposium on Usable Security*, pp. 192–204, 2023. 2

[55] H.-R. Tsai, P.-C. Chen, L. Chan, and Y.-P. Hung. One-handed input through rotational motion for smartwatches. *International Journal of Human–Computer Interaction*, 34(11):971–986, 2018. 2

[56] D. Venolia and F. Neiberg. T-cube: A fast, self-disclosing pen-based alphabet. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 265–270, 1994. 3

[57] W. S. Walmsley, W. X. Snelgrove, and K. N. Truong. Disambiguation of imprecise input with one-dimensional rotational text entry. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 21(1):1–40, 2014. 2

[58] T. Wan, L. Zhang, Y. Xu, Z. Guo, B. Gao, and H.-N. Liang. Analysis and design of efficient authentication techniques for password entry with the qwerty keyboard for vr environments. *IEEE Transactions on Visualization and Computer Graphics*, 2024. 2

[59] X. Wang and Y. Zhang. 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*, pp. 1–7, 2021. 2, 5

[60] W. Xu, H.-N. Liang, Y. Zhao, T. Zhang, D. Yu, and D. Monteiro. 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):1991–2001, 2019. 3

[61] H.-S. Yeo, X.-S. Phang, S. J. Castellucci, P. O. Kristensson, and A. Quigley. 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*, pp. 4194–4202, 2017. 2

[62] S. Yi, Z. Qin, E. Novak, Y. Yin, and Q. Li. Glassgesture: Exploring head gesture interface of smart glasses. In *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*, pp. 1–9. IEEE, 2016. 2

[63] X. Yi, X. Wang, J. Li, and H. Li. Examining the fine motor control ability of linear hand movement in virtual reality. In *2023 IEEE Conference Virtual Reality and 3D User Interfaces (VR)*, pp. 427–437. IEEE, 2023. 2

[64] X. Yi, C. Yu, W. Xu, X. Bi, and Y. Shi. Compass: Rotational keyboard on non-touch smartwatches. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pp. 705–715, 2017. 3

[65] X. Yi, S. Zhang, Z. Pan, L. Shi, F. Han, Y. Kong, H. Li, and Y. Shi. Squeez'in: Private authentication on smartphones based on squeezing gestures. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pp. 1–15, 2023. 5, 6, 8, 9

[66] E. Youn, S. Lee, S. Kim, Y. A. Shim, L. Chan, and G. Lee. Wristdial: An eyes-free integer-value input method by quantizing the wrist rotation. *International Journal of Human–Computer Interaction*, 37(17):1607–1624, 2021. 2

[67] D. Yu, K. Fan, H. Zhang, D. Monteiro, W. Xu, and H.-N. Liang. Pizzatext: Text entry for virtual reality systems using dual thumbsticks. *IEEE transactions on visualization and computer graphics*, 24(11):2927–2935, 2018. 3

[68] S. Zhao, J. Zhu, S. Zhang, X. Wang, H. Li, F. Yi, X. Yi, and H. Li. Coordauth: Hands-free two-factor authentication in virtual reality leveraging head-eye coordination. In *2025 IEEE Conference Virtual Reality and 3D User Interfaces (VR)*, pp. 738–748. IEEE, 2025. 2

[69] H. Zhu, W. Jin, M. Xiao, S. Murali, and M. Li. Blinkey: A two-factor user authentication method for virtual reality devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 4(4):1–29, 2020. 2, 5, 6, 8, 9

[70] H. Zhu, M. Xiao, D. Sherman, and M. Li. Soundlock: A novel user authentication scheme for vr devices using auditory-pupillary response. In *NDSS*, 2023. 2

[71] D. Zielasko and B. E. Riecke. To sit or not to sit in vr: Analyzing influences and (dis) advantages of posture and embodied interaction. *Computers*, 10(6):73, 2021. 6

[72] Y. Zou, M. Zhao, Z. Zhou, J. Lin, M. Li, and K. Wu. Bilock: User authentication via dental occlusion biometrics. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(3):1–20, 2018. 2