EyeGestureLogin: Spontaneous HandsFree GazeBased Lock Pattern Authentication for Public Displays

Omair Shahzad Bhatti
Interactive Machine Learning
German Research Center for Artificial Intelligence (DFKI)
Saarbrücken, Germany
omair_shahzad.bhatti@dfki.de

Abdulrahman Mohamed Selim
Interactive Machine Learning Department (IML)
German Research Center for Artificial Intelligence (DFKI)
Saarbrücken, Germany
abdulrahman.mohamed@dfki.de

László Kopácsi
Interactive Machine Learning
German Research Center for Artificial Intelligence (DFKI)
Saarbrücken, Germany
laszlo.kopacsi@dfki.de

Maximilian Biwersi
Interactive Machine Learning
German Research Center for Artificial Intelligence (DFKI)
Saarbrücken, Germany
mabi05@dfki.de

Michael Barz
Interactive Machine Learning
German Research Center for Artificial Intelligence (DFKI)
Saarbrücken, Germany
michael.barz@dfki.de

Daniel Sonntag
German Research Center for Artificial Intelligence (DFKI)
Saarbrücken, Germany
Applied Artificial Intelligence
Oldenburg University
Oldenburg, Germany
daniel.sonntag@dfki.de

Abstract

As public displays become more ubiquitous, common authentication methods face security (e.g., shoulder surfing) and sanitary risks. Gaze-based systems offer a promising alternative, but their adoption is often limited by required calibration and the Midas Touch problem. We present EyeGestureLogin, a touch-free, knowledge-based method that uses gaze to enter lock patterns on a familiar 3×3 layout. EyeGestureLogin supports spontaneous walk-up use by replacing explicit calibration with an implicit, single-point offset estimation, and mitigates the Midas Touch using a short dwell-time trigger for fully hands-free input. The interface captures patterns by processing AOI-based fixations; we additionally evaluate an offline saccade-based detector. In a controlled study ($n = 24$), we achieved 91.59% accuracy (91.88% offline) with a mean entry time of 4.36 s. These results suggest that EyeGestureLogin enables fast and accurate hands-free authentication for public displays, motivating further evaluation under real-world deployment conditions.

CCS Concepts

• **Human-centered computing** → **Human computer interaction (HCI)**; *User studies*; **Interaction design**; • **Security and privacy** → *Authentication.*

Keywords

Eye Tracking, Gaze-based Interaction, Authentication, Public Displays, Calibration-free Eye Tracking, Hands-free Authentication



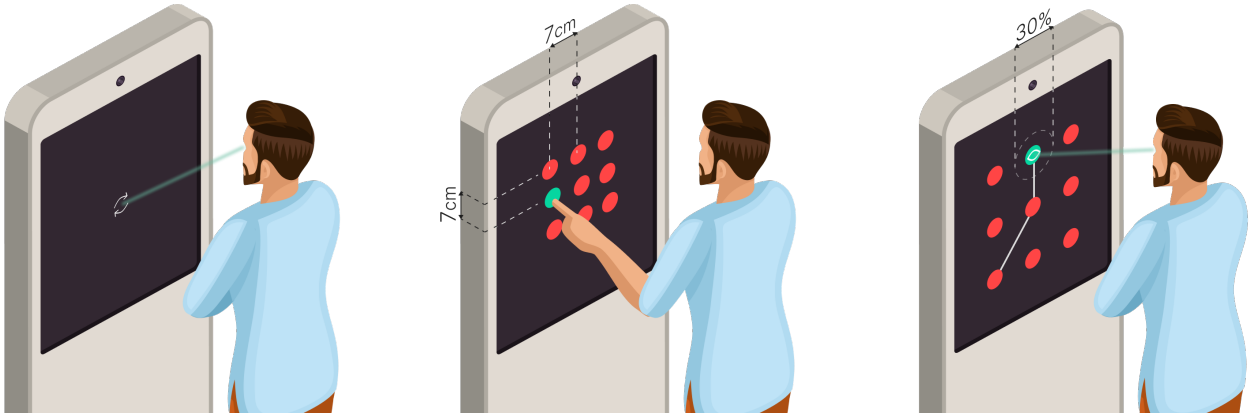
This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.
ETRA '26, Marrakesh, Morocco
© 2026 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-2519-7/26/06
https://doi.org/10.1145/3797246.3803033

ACM Reference Format:
Omair Shahzad Bhatti, Abdulrahman Mohamed Selim, László Kopácsi, Maximilian Biwersi, Michael Barz, and Daniel Sonntag. 2026. EyeGestureLogin: Spontaneous HandsFree GazeBased Lock Pattern Authentication for Public Displays. In *2026 Symposium on Eye Tracking Research and Applications (ETRA '26), June 01–04, 2026, Marrakesh, Morocco.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3797246.3803033

1 Introduction

Public displays have become commonplace in everyday life, ranging from interactive digital menus and information terminals to ATMs. Many of these systems require users to authenticate before accessing services or sensitive information. Common knowledge-based authentication methods (e.g., PINs, passwords, and lock patterns) typically rely on touch input on the display or on an external keyboard. In public settings, however, such methods can expose credentials to bystanders. For example, attackers may observe a user's input during authentication, i.e., shoulder surfing [Eiband et al. 2017]. More sophisticated attacks include hidden-camera observation of keypads or touchscreens [Ye et al. 2017], smudge attacks that infer input sequences from residues on touch surfaces [Aviv et al. 2010], and thermal attacks that exploit heat traces [Abdelrahman et al. 2017]. Further, public displays can also pose sanitary concerns due to high levels of surface contamination [Gerba et al. 2016].

These challenges have motivated alternative authentication mechanisms such as iris scans, fingerprints, and eye tracking. Eye tracking records eye movements and gaze behaviour over time [Carter and Luke 2020]. As an interaction modality, gaze leaves no visible touch traces on the screen and may reduce exposure to some observation-based attacks compared to touch [De Luca et al. 2007], although we do not empirically evaluate shoulder surfing resistance in this paper. In addition, gaze-based interaction is hands-free, which makes it a potentially more hygienic option for authentication on shared public displays.



(a) Initial start screen. (b) Baseline touch-based method. (c) EyeGestureLogin

Figure 1: Study setup of each method. Activation points are spaced 7 cm horizontally and vertically. For EyeGestureLogin, each node uses a circular detection radius equal to 15% of the display width (i.e., 30% diameter) to increase robustness under uncalibrated conditions.

Prior work has explored gaze-based authentication through PIN entry [Bhatti et al. 2021; Cymek et al. 2014; De Luca et al. 2007; Khamis et al. 2018; Peng et al. 2025], text entry [Kumar et al. 2007], pattern entry [De Luca et al. 2009], and biometric approaches that leverage eye-movement features [Jeon et al. 2025; Odya et al. 2023]. Despite this broad body of work, gaze-based authentication systems still face two fundamental challenges that limit their suitability for walk-up public displays. First, many systems require explicit eye-tracker calibration [Best and Duchowski 2016; Kumar et al. 2007], which is often perceived as time-consuming and tedious [Majaranta and Bulling 2014] and disrupts spontaneous interaction. Second, because users naturally explore a display visually, systems must distinguish intentional input from incidental gaze, an issue commonly referred to as the Midas Touch problem [Jacob 1991]. To mitigate unintended activation, several approaches introduce additional input modalities (e.g., pressing a key to trigger or confirm input) [Bhatti et al. 2021], which compromises fully hands-free interaction. These issues typically lead to a trade-off of at least one desirable property, such as speed, accuracy, calibration effort, or hands-free operation.

In this study, we present *EyeGestureLogin*, a touch-free, knowledge-based authentication system which uses gaze-based pattern entry on a familiar 3×3 layout. Our approach (1) supports spontaneous use by replacing explicit calibration with an implicit, single-point offset estimation, and (2) addresses the Midas Touch problem using a dwell-based trigger without requiring any additional modality. We evaluate *EyeGestureLogin* in a within-subject, repeated-measures user study against a traditional touch-based lock pattern (Figure 1). Our results show that *EyeGestureLogin* enables fast, accurate hands-free authentication while addressing key barriers to spontaneous gaze interaction on public displays.

2 Related Work

Gaze-based interaction offers a promising alternative for authentication on public displays, as it can reduce exposure to shoulder surfing, smudge attacks, and thermal attacks, while also eliminating physical contact with shared surfaces. Therefore, prior research has proposed authentication systems that integrate gaze-based interaction for use on public displays.

Calibration-based gaze authentication. Early gaze-based authentication systems typically relied on explicit eye-tracker calibration. Kumar et al. [2007] presented *EyePassword*, which supports password or PIN entry using a virtual keyboard or number pad. Characters are selected via dwell time, typically between 400 and 500 ms. While *EyePassword* achieved a low error rate (3%) comparable to a touch-based baseline (4%), it was substantially slower (9.2 s vs. 2.49 s on average) and required prior calibration. Calibration commonly involves fixating five or nine predefined points on the screen so the eye tracker can map eye features to screen coordinates. Although effective, this process is widely perceived as cumbersome and time-consuming, making it poorly suited to spontaneous, walk-up use at public displays [Khamis et al. 2015; Pfeuffer et al. 2013].

Smooth pursuit-based authentication. To avoid explicit calibration, several approaches rely on relative eye behaviour, most notably smooth pursuit, i.e. the eye movement that occurs while following a moving object [Holmqvist et al. 2011]. Rajanna et al. [2017] proposed an authentication method in which users follow three predefined moving shapes. While the method achieved high accuracy (96%), it required a minimum of 15 s for authentication and offered a smaller password space than a four-digit PIN. Liu et al. [2015] introduced a smartphone-based approach in which users follow digit trajectories to the screen edge; although faster (9.6 s), it achieved lower accuracy (77.1%) and further reduced the password space. Cymek et al. [2014] reported higher accuracy (91.55%) with pursuit-based PIN, but required a minimum entry time of 25 s.

Building on this line of work, Khamis et al. [2018] introduced *CueAuth*, where each digit is associated with a moving cue that users follow to select. In a 20-participant study, *CueAuth* achieved a success rate of 82%, but was significantly slower than touch input

Table 1: Comparison of gaze-based authentication approaches in terms of authentication method, exploited eye behaviour, reported accuracy (Acc), reported entry time (Time), hands-free operation, and support for spontaneous interaction (i.e., no explicit calibration).

Publication	Authentication	Eye Behaviour	Acc	Time [s]	Hands-free	Spontaneous
Kumar et al. [2007]	8-9 Chars QWERTY 8-9 Chars Alphabetic	Dwell	97%	9.2	✓	✗
De Luca et al. [2007]	4-digit (0-9) PIN	Relative Eye Movement	90.5%	54	✗	✓
De Luca et al. [2009]	Pattern	Relative Eye Movement	–	12.5	✗	✓
Rajanna et al. [2017]	3-shape PIN out of 12	Smooth Pursuit	96%	$\geq$ 15	✗	✓
Liu et al. [2015]	5-digit (1-4) PIN	Smooth Pursuit	77.1%	9.6	✗	✓
Cymek et al. [2014]	4-digit (0-9) PIN	Smooth Pursuit	91.55%	$\geq$ 25	✓	✓
Khamis et al. [2018]	4-digit (0-9) PIN	Smooth Pursuit	82%	26.35	✓	✓
Bhatti et al. [2021]	4-digit (0-9) PIN	Relative Eye Movement	95.88%	5.12	✗	✓

(26.35 s vs. 3.73 s). Overall, smooth-pursuit-based methods are robust and calibration-free, but lack the speed and can feel unnatural, as they require users to continuously track specific trajectories.

Relative eye movement-based. Another calibration-free direction is to infer input from relative eye movements such as saccades. De Luca et al. [2007] introduced *EyePIN*, which uses gaze gestures for PIN entry. Although the method achieved a relatively low error rate (9.5%), it required users to memorise gesture patterns and resulted in very long input times (54 s on average). The authors later presented *EyePassShapes* [De Luca et al. 2009], which combines gaze gestures with the touch-based *PassShapes* [Weiss and De Luca 2008]. While *EyePassShapes* substantially reduced input time (12.5 s), it remained slower than its touch-based counterpart (5.8 s). Both approaches required pressing and holding a key to delimit gaze input, which mitigates Midas Touch but prevents fully hands-free interaction. More recently, Bhatti et al. [2021] proposed *EyeLogin*, a calibration-free authentication method based on relative saccadic eye movements. Users initiate authentication by pressing the space bar while fixating the screen centre, which both addresses Midas Touch and enables estimation of a gaze offset to improve accuracy. *EyeLogin* achieved high accuracy (95.88%) and fast input times (5.12 s), but its reliance on an explicit key press means it is not fully hands-free.

In summary, prior gaze-based authentication systems typically compromise at least one key property: speed, accuracy, calibration effort, or fully hands-free operation (Table 1). Our work builds on these insights by combining implicit offset estimation with a lock-pattern interface to support fast, accurate, and entirely hands-free authentication suitable for spontaneous use on public displays.

3 Method

EyeGestureLogin employs a lock-pattern interface inspired by Android. The familiar 3×3 grid allows users to enter a pattern by sequentially fixating on grid points. Lock patterns provide comparatively large spatial margins between targets, which supports robust interaction when gaze input is not explicitly calibrated. While our authentication system detects fixations, users primarily progress through the pattern via saccades between points. The front end consists of two screens: a start screen (Figure 1a) and an authentication screen (Figure 1c). When a user approaches the display, the eye tracker detects the user's eyes and presents a central start target, visualised as a circle formed by two curved arrows (Figure 1a). When gaze enters the activation area, the target animates by spinning and shrinking, providing continuous feedback that the system is ready. After a dwell of 1.2 s, the authentication screen appears and the user can enter the pattern (Figure 1c).

Parameter selection. Unless otherwise noted, implementation parameters were fixed before the main study based on prior gaze-interaction work, system constraints, and a small formative pilot with two users. The pilot was used only to verify that the interaction flow was workable; parameters were not formally optimised or tuned per participant. In particular, the 1.2 s start dwell was chosen to balance accidental triggering against hands-free activation while leaving sufficient time for implicit offset estimation. The 100 ms minimum fixation duration was selected to support rapid node selection, whereas the 500 ms maximum fixation duration was introduced to allow the final node to be committed without requiring an explicit gaze exit. We did not perform a formal sensitivity analysis, so future work should examine how these thresholds affect the speed–accuracy trade-off under less controlled conditions.

Offset calculation. To improve the reliability of *EyeGestureLogin* without requiring explicit calibration, we incorporate an implicit offset estimation inspired by Bhatti et al. [2021]. The purpose of this step is to reduce the systematic mismatch between intended and detected gaze positions, thereby lowering the likelihood that gaze input is assigned to an incorrect Area-of-Interest (AOI), i.e., the grid points in *EyeGestureLogin*. Offset estimation is seamlessly integrated into the interaction and performed while the user fixates the central start target. When the eye tracker detects the user's eyes continuously for 300 ms, the start target appears. If gaze remains within the activation area, the target animation begins. To tolerate uncalibrated gaze input, we use a relatively large activation region

around the screen centre. The animation lasts 1.2 s, during which gaze samples are collected for offset estimation. Sample collection starts 500 ms after animation onset to allow gaze to stabilise on the target and continues for 700 ms. At 60 Hz, this yields approximately 42 samples; the 700 ms window was chosen to provide a sufficiently stable mean estimate while keeping the engagement phase short. If gaze leaves the activation area during sample collection, the animation is aborted, the target is reset, and offset estimation restarts. Offset estimation is also restarted if more than 20% of the collected samples contain invalid tracking data for at least one eye. This threshold was chosen to tolerate brief tracking losses while avoiding offset estimates based on poor-quality data. The offset is computed as the difference between the screen centre and the mean of the collected gaze points and is subsequently applied to all gaze input to approximate the intended gaze position.

I-AOI Fixation-based Detector. Lock-pattern grid points are treated as AOIs, and fixations are detected using the AOI-based (I-AOI) algorithm proposed by Salvucci and Goldberg [2000]. Because interaction is restricted to predefined targets, the algorithm discards gaze samples outside all AOIs and does not rely on dispersion-based measures. Gaze samples are accumulated while gaze remains within an AOI; if the dwell duration exceeds a minimum threshold, the segment is classified as a fixation, otherwise it is discarded. We use a minimum fixation duration of 100 ms. Each pattern node is represented by a circular AOI centred on the node location. To increase robustness under uncalibrated conditions, we enlarge the AOIs and use a radius equal to 15% of the display width (i.e., 30% diameter; see Figure 1c). Across the 3×3 grid, the union of all AOIs covers approximately 63% of the screen. Gaze samples are assigned using a nearest-centre rule: a sample is considered part of an AOI if it falls within that node's circular radius; if multiple AOIs satisfy this condition due to overlap, the sample is assigned to the closest node centre. Samples outside all AOIs are ignored.

During initial testing, we observed that the standard I-AOI behaviour can be unintuitive for final-node entry, as the last fixation is only emitted once the user's gaze leaves the AOI. Users often expect the final point to be registered while continuing to look at it. To address this, we introduce a maximum fixation duration threshold of 500 ms, allowing the final AOI to be registered without requiring an explicit gaze exit.During pattern entry, invalid or missing gaze samples are not mapped to any AOI. We did not implement additional recovery logic beyond ignoring invalid samples, which likely contributed to some recognition failures. In practice, this means that short tracking interruptions delay node confirmation rather than directly creating spurious nodes; if tracking loss persists, the current candidate fixation may fail to reach the minimum duration threshold and is therefore discarded.

Saccade-Based Relative Detector. In addition to absolute AOI-based decoding, we explore a saccade-based relative decoder that infers pattern nodes from the *direction* of eye movements rather than their absolute screen positions. This approach is motivated by the observation that saccade angles remain stable under systematic gaze offset [Bhatti et al. 2021], as both the origin and destination of a saccade are shifted equally. Fixations for this decoder are identified using the I-DT (Dispersion-Threshold) algorithm [Salvucci and Goldberg 2000]. To reduce noise in subsequent angle calculations, the gaze trajectory is smoothed using a Gaussian filter ($\sigma = 1.5$). The first fixation is anchored to the nearest AOI using absolute position, establishing a reference point for the pattern. For each subsequent fixation, a saccade vector is computed from the current AOI position to the fixation centroid, and its angle is compared against precomputed ideal transition angles between AOI pairs. Micro-saccades with very small magnitudes are discarded, as they typically represent corrective movements rather than intentional transitions. When multiple AOIs satisfy the angular criterion, the AOI closest to the fixation position is selected to resolve ambiguities. The candidate pattern is constructed from the resulting sequence of transitions, collapsing consecutive identical nodes. The primary advantage of this decoder is robustness to systematic gaze offset. Because decoding relies on relative movement direction rather than absolute position, calibration error affects both ends of a saccade equally and does not alter the transition angle.

4 Evaluation

To evaluate our approach, we conducted a controlled user study to compare *EyeGestureLogin* with a touch-based lock-pattern baseline. The study design follows [Bhatti et al. 2021]. During the study, *EyeGestureLogin* used the I-AOI fixation-based detector; the saccade-based relative detector was evaluated offline on the recorded gaze data. As a baseline, we implement a touch-based 3×3 lock-pattern system. The activation points in the baseline were spaced 7 cm horizontally and vertically on our display (see Figure 1b). Targets were enlarged to reduce acquisition time [Fitts 1954]. We did not show a visible trace while drawing the pattern. To reduce missed activations, we enlarged the touch activation radius of each point by 50%.

We recruited 24 participants (18 male, 6 female) (age: $M = 26.04$, range: 20-37). All reported normal or corrected-to-normal vision; 10 wore glasses and one wore contact lenses. Fourteen participants (58%) reported prior experience with eye trackers. The study used an HP Sprout (23-inch touchscreen, 1920×1080 resolution) with a Tobii Pro Nano eye tracker (60 Hz) mounted below the screen. Lighting was kept constant (shutters closed, ceiling lights on). The system was implemented in Python 3.8 using the Tobii Pro SDK. Participants held a wireless presenter only for study navigation (e.g., accept/reject/continue); it was not used to trigger gaze input.

Study. We used a within-subject repeated-measures design with two conditions: gaze (*EyeGestureLogin*) and touch (*baseline*). Condition order was counterbalanced. Dependent measures were detector accuracy (first attempt, excluding redo attempts), completion time, System Usability Scale (SUS) [Brooke 1996], and NASA TLX [Hart and Staveland 1988]. For each condition, participants completed 15 trials using the same set of pre-generated patterns; each condition began with three warm-up trials. In each trial, the target pattern was shown for 5 s (including start point and direction) and then entered using the respective modality. In the gaze condition, participants initiated input by dwelling on the central start target (which also performs implicit offset estimation) and then entered the pattern by sequentially fixating nodes. After each attempt, the system displayed the target pattern again and participants could accept the attempt or reject and redo it using a wireless presenter. Redo attempts were logged but excluded from the main analysis.

The display was placed on a height-adjustable standing desk and adjusted for each participant to ensure reliable eye-tracking. We logged interaction events and additionally recorded the raw gaze stream for offline decoding analysis. In total, we collected 720 primary attempts (24 participants × 15 patterns × 2 conditions).

4.1 Results

For the gaze-based condition, we report results for the online I-AOI fixation-based detector used during the study as well as for the saccade-based relative detector evaluated offline on the recorded gaze data. The touch-based lock-pattern method serves as a baseline. The main results are summarised in Table 2.

Accuracy. For *EyeGestureLogin*, we distinguish between the I-AOI fixation-based detector and the saccade-based relative detector. The touch-based baseline is included for comparison. The I-AOI fixation-based detector achieved a mean accuracy of 91.59% (SD = 10.44%). The saccade-based relative detector achieved a comparable mean accuracy of 91.88% (SD = 10.21%) when evaluated offline on the same recorded gaze data. The touch-based baseline achieved a higher mean accuracy of 97.7% (SD = 1.4%).

Task Completion Time. Task completion time was measured from the moment the start screen appeared until the final pattern input was registered. On average, participants completed authentication faster with touch input than with gaze input. *EyeGestureLogin* required 4.36 s on average, compared to 3.13 s for the touch-based baseline. The pure entry time without the start screen for *EyeGestureLogin* is 3.16 s vs 3.13 s for the touch-based method.

Usability & Workload. We assessed usability using SUS and perceived workload using NASA TLX. Mean scores and standard deviations are reported for both conditions. The touch-based baseline achieved a higher mean SUS score than *EyeGestureLogin*. *EyeGestureLogin* achieved a mean SUS score of 84.1, which corresponds to a high level of perceived usability [Bangor et al. 2009]. For perceived workload, *EyeGestureLogin* had a mean NASA TLX score of 14.46, compared to 10.43 for the baseline, suggesting that the baseline interaction is perceived as slightly less demanding than *EyeGestureLogin*.

Comparison to other gaze-based authentication systems. Table 3 reports a comparison between *EyeGestureLogin* and (1) the gaze-based authentication systems EyeLogin from Bhatti et al. [2021] and (2) their implementation of CueAuth* from Khamis et al. [2018]. EyeLogin achieved a mean accuracy of 95.88% (SD = 6.23%), while *EyeGestureLogin* achieved 91.88% (SD = 10.21%) and CueAuth* achieved 82.94% (SD = 11.58%). Mean entry time was 4.36 s (SD = 0.91 s) for *EyeGestureLogin*, 5.12 s (SD = 1.09 s) for EyeLogin, and 23.41 s (SD = 2.28 s) for CueAuth*. *EyeGestureLogin* achieved the highest mean SUS score (84.1, SD = 13.17), followed by EyeLogin (75.75, SD = 15.28) and CueAuth* (66.5, SD = 18.72).

5 Discussion

In this study, we presented and evaluated *EyeGestureLogin*, a gaze-based lock-pattern authentication method designed for spontaneous use on public displays. Our results indicate that *EyeGestureLogin* enables fast, accurate, and fully hands-free authentication without requiring explicit calibration. In the following, we discuss the implications of our findings, highlight design trade-offs, and outline practical considerations for deployment and future work.

Comparison to Touch-Based Authentication. The touch-based baseline outperformed *EyeGestureLogin* in terms of both accuracy and completion time, as expected. Our results are consistent with prior findings showing that direct touch input remains the most efficient and accurate modality for authentication under ideal conditions. However, the observed performance gap between gaze and touch was comparatively small. On average, gaze-based authentication was 1.23 s slower than touch, largely due to the 1.2 s start-screen delay (Figure 1a). Additional time could be reduced by adjusting the 500 ms end-limit for the final fixation. Considering that *EyeGestureLogin* eliminates physical contact and visible input traces, the observed performance represents a reasonable trade-off for public display scenarios, which require hygiene, privacy, security or hands-free interaction considerations.

Usage on Public Displays. Deploying *EyeGestureLogin* in public settings requires addressing two main considerations: enabling hands-free use without additional input modalities, and managing security and privacy risks. To mitigate Midas Touch, *EyeGestureLogin* uses a dwell-based trigger on the start screen, but walk-up public displays may still invite unintended activation (e.g., passers-by briefly fixating the central region or multiple people being present). A promising direction is to treat engagement as a multi-signal decision rather than relying on dwell alone, for instance, by conditioning activation on stable face/eye detection, viewing distance, and consistent head pose. Regarding security, *EyeGestureLogin* targets attacks that exploit visible input traces (e.g., shoulder surfing, smudge, thermal traces); gaze input has clear benefits because it leaves no residues and avoids overt touch trajectories. However, gaze-based authentication is not inherently observation-proof and depends on the attacker model: although it reduces leakage from finger traces, it may still reveal information via observable eye or head movements, particularly if recorded from favourable angles. Future work should therefore empirically evaluate resistance to observation attacks under controlled conditions, varying distance, angle, and camera quality.

I-AOI vs. Relative Gaze Detector. A key design decision for gaze-based authentication is whether patterns should be decoded from absolute gaze positions (AOI assignments) or from relative eye movements (saccade direction). We used the I-AOI fixation-based detector online, but evaluated the saccade-based relative detector offline on the recorded gaze data. Both detectors achieved almost identical accuracy, indicating that absolute and relative decoding provide similarly reliable pattern reconstruction under our conditions. The I-AOI approach is simple and directly maps between gaze and interface elements. Combined with enlarged AOIs and implicit offset estimation, it proves sufficiently robust for online use, but can still be affected by larger systematic offsets, user repositioning, and tracking noise near AOI borders. The relative decoder instead infers transitions mainly from movement direction, which is less affected by systematic offset after the initial AOI anchoring. Relative decoding may also offer speed advantages, as it does not inherently require precise endpoint assignment, and potentially

Table 2: Performance, Entry Time, and SUS results for EyeGestureLogin and touch-based baseline. Accuracy is the percentage of correctly detected authentication attempts. Entry time is in seconds. SUS scores range from 0 to 100.

Method	Detection Accuracy		Entry Time		SUS	
	Mean (%)	SD (%)	Mean (s)	SD (s)	Mean	SD
I-AOI Fixation-based Detector	91.59	10.44	4.36	0.91	84.1	13.17
Saccade-Based Relative Detector	**91.88**	**10.21**	-	-	-	-
Touch-based baseline	97.70	1.40	3.13	0.57	90.1	1.6

Table 3: Comparison of authentication performance and usability between EyeGestureLogin and gaze-based systems replicated from Bhatti et al. [Bhatti et al. 2021]. Values are reported as mean ± SD.

System	N	Accuracy [%]	Entry Time [s]	SUS	Midas Touch Mitigation
CueAuth* [Bhatti et al. 2021]	10	82.94 ± 11.58	23.41 ± 2.28	66.5 ± 18.72	**Yes**
EyeLogin [Bhatti et al. 2021]	10	**95.88 ± 6.23**	5.12 ± 1.09	75.75 ± 15.28	No
EyeGestureLogin	24	91.88 ± 10.21	**4.36 ± 0.91**	**84.1 ± 13.17**	**Yes**

less dwell-based confirmation, for each node. While we did not evaluate entry time for relative decoding online, these results motivate future evaluation of this approach in online setups.

Comparison to other gaze-based authentication systems. We compared *EyeGestureLogin* against related gaze-based authentication systems (Table 3). Overall, *EyeGestureLogin* achieves fast authentication times while also supporting hands-free use. However, cross-study comparisons should be interpreted cautiously because results can be influenced by differences in hardware, sampling rate, lighting, pattern sets, training, participant demographics, and interaction flow (e.g., engagement mechanisms). In particular, EyeGestureLogin was evaluated with 24 participants on a specific eye-tracker setup, whereas the replicated systems reported in [Bhatti et al. 2021] use only 10 participants and different study conditions. A potential next step is a direct within-study comparison against one or more representative calibration-free techniques (e.g., EyeLogin-style relative input, smooth pursuit-based selection) implemented on the same hardware and evaluated with identical tasks. This would allow clearer conclusions about which design choices (implicit offset, dwell engagement, AOI sizing, decoding strategy) contribute most strongly to speed, accuracy, and perceived usability.

Limitations. Our study has several limitations that should be considered when interpreting the results. First, participants were primarily students from a university environment, relatively young and highly technical. This demographic may not be representative of the broader public-display user population. Performance and usability perceptions may differ for older or less experienced users when interacting with new input modalities. Second, the study was conducted in a controlled indoor environment with stable lighting conditions and a fixed viewing distance. Real-world public displays are often used under varying conditions, including direct sunlight, which can negatively affect eye-tracking performance. The desk height was adjusted per participant to ensure that the eyes remained within the eye tracker's track box; this choice improved measurement reliability but likely overestimates real-world deployability on fixed public displays. In practice, variations in user height, posture, and stand-off distance may reduce trackability, offset-estimation quality, and recogniser accuracy. Third, we did not conduct a dedicated shoulder-surfing or observation-attack study. While EyeGestureLogin avoids touch residues and visible touch trajectories, we therefore do not claim resistance to all observation-based attacks.

Ethical Statement. Eye tracking is inherently privacy-sensitive, but its use in our system is explicit and visible to users as part of the interaction. Our system does not require a full calibration procedure, which limits the precision of gaze estimates and reduces the risk of fine-grained gaze analysis. However, even uncalibrated gaze data can reveal potentially sensitive information. Further, participants provided informed consent and were informed about what data were collected. We restricted logging to data required for analysis (interaction events and raw gaze streams), stored data securely, and removed direct identifiers from the dataset. Future deployments on public displays should make eye tracking clearly detectable and optional, minimise data retention, process gaze locally where possible, and avoid storing raw gaze streams unless strictly necessary.

6 Conclusion & Future Work

In this paper, we presented *EyeGestureLogin*, a gaze-based, hands-free, calibration-free lock-pattern authentication technique for public displays. Our evaluation shows that our proposed method achieves high accuracy and entry times close to a touch-based baseline, while enabling spontaneous, fully hands-free interaction without leaving a visible input trace. Future work should evaluate *EyeGestureLogin* in more realistic deployment settings (e.g., walk-up use, varying lighting, distance, and user posture) to assess robustness under everyday conditions. In addition, the saccade-based relative decoder should be integrated and tested online. This direction may also enable deployments with lower-cost sensing (e.g., RGB/IR cameras) where absolute gaze estimation is less reliable. Further studies should investigate larger password spaces (longer patterns or larger grids), long-term memorability, resistance to observation attacks, and performance for diverse users. Finally, the technique may also

transfer to other hands-free contexts, such as AR/VR in e.g. [Kopácsi et al. 2024], manufacturing settings, where touch input is limited, and calibration can be inconvenient or even worsened.

Acknowledgments

This work was funded by the Federal Ministry of Research, Technology and Space (BMFTR) under grant number 16IW23002 (No-IDLE) and grant number 16IW24006 (NoIDLEChatGPT), under grant number 16IW26002 (AMENABLE), the Lower Saxony Ministry of Science and Culture (MWK) in the zukunft.niedersachsen program, and the Endowed Chair of AAI at University of Oldenburg.

References

Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. Acm, Denver Colorado USA, 3751–3763. doi:10.1145/3025453.3025461

Adam J Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M Smith. 2010. Smudge Attacks on Smartphone Touch Screens. (2010), 11.

Aaron Bangor, Philip Kortum, and James Miller. 2009. Determining what individual SUS scores mean: adding an adjective rating scale. *J. Usability Studies* 4, 3 (May 2009), 114–123.

Darrell S. Best and Andrew T. Duchowski. 2016. A rotary dial for gaze-based PIN entry. In *Proceedings of the Ninth Biennial ACM Symposium on Eye Tracking Research & Applications*. Acm, Charleston South Carolina, 69–76. doi:10.1145/2857491.2857527

Omair Shahzad Bhatti, Michael Barz, and Daniel Sonntag. 2021. EyeLogin - Calibration-free Authentication Method for Public Displays Using Eye Gaze. In *ACM Symposium on Eye Tracking Research and Applications*. Acm, Virtual Event Germany, 1–7. doi:10.1145/3448018.3458001

John Brooke. 1996. SUS: A 'Quick and Dirty' Usability Scale. In *Usability Evaluation In Industry* (1st edition ed.). CRC Press, 6. doi:10.1201/9781498710411-35

Benjamin T. Carter and Steven G. Luke. 2020. Best practices in eye tracking research. *International Journal of Psychophysiology* 155 (Sep 2020), 49–62. doi:10.1016/j.ijpsycho.2020.05.010

Dietlind Helene Cymek, Antje Christine Venjakob, Stefan Ruff, Otto Hans-Martin Lutz, Simon Hofmann, and Matthias Roetting. 2014. Entering PIN codes by smooth pursuit eye movements. *Journal of Eye Movement Research* 7, 4 (May 2014). doi:10.16910/jemr.7.4.1

Alexander De Luca, Martin Denzel, and Heinrich Hussmann. 2009. Look into my eyes!: can you guess my password?. In *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*. ACM Press, Mountain View, California, 1. doi:10.1145/1572532.1572542

Alexander De Luca, Roman Weiss, and Heiko Drewes. 2007. Evaluation of eye-gaze interaction methods for security enhanced PIN-entry. In *Proceedings of the 2007 conference of the computer-human interaction special interest group (CHISIG) of Australia on Computer-human interaction: design: activities, artifacts and environments - OZCHI '07*. ACM Press, Adelaide, Australia, 199. doi:10.1145/1324892.1324932

Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. Acm, Denver Colorado USA, 4254–4265. doi:10.1145/3025453.3025636

Paul M. Fitts. 1954. The information capacity of the human motor system in controlling the amplitude of movement. *Journal of Experimental Psychology* 47, 6 (1954), 381–391. doi:10.1037/h0055392 Place: US Publisher: American Psychological Association.

Charles P. Gerba, Adam L. Wuollet, Peter Raisanen, and Gerardo U. Lopez. 2016. Bacterial contamination of computer touch screens. *American Journal of Infection Control* 44, 3 (March 2016), 358–360. doi:10.1016/j.ajic.2015.10.013

Sandra G. Hart and Lowell E. Staveland. 1988. Development of NASA-TLX (Task Load Index): Results of Empirical and Theoretical Research. In *Advances in Psychology*, Peter A. Hancock and Najmedin Meshkati (Eds.). Human Mental Workload, Vol. 52. North-Holland, 139–183. doi:10.1016/S0166-4115(08)62386-9

Kenneth Holmqvist, Marcus Nystrom, Richard Andersson, Richard Dewhurst, Halszka Jarodzka, Weijer, and Joost van de. 2011. *Eye Tracking: A comprehensive guide to methods and measures*. Oxford University Press, Oxford, New York.

Robert J. K. Jacob. 1991. The Use of Eye Movements in Human-Computer Interaction Techniques: What You Look at is What You Get. *ACM Trans. Inf. Syst.* 9, 2 (April 1991), 152–169. doi:10.1145/123078.128728 Place: New York, NY, USA Publisher: Association for Computing Machinery.

Junryeol Jeon, Yeo-Gyeong Noh, JooYeong Kim, and Jin-Hyuk Hong. 2025. Pre-AttentiveGaze: gaze-based authentication dataset with momentary visual interactions. *Scientific Data* 12, 1 (Feb. 2025), 263. doi:10.1038/s41597-025-04538-3 Publisher: Nature Publishing Group.

Mohamed Khamis, Andreas Bulling, and Florian Alt. 2015. Tackling Challenges of Interactive Public Displays Using Gaze. In *Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers (UbiComp/ISWC'15 Adjunct)*. Association for Computing Machinery, New York, NY, USA, 763–766. doi:10.1145/2800835.2807951 event-place: Osaka, Japan.

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 (Dec. 2018), 1–22. doi:10.1145/3287052

László Kopácsi, Tobias Sebastian Schneider, Chiara Karr, Michael Barz, and Daniel Sonntag. 2024. GazeLock: Gaze- and Lock Pattern-Based Authentication. In *Proceedings of the 30th ACM Symposium on Virtual Reality Software and Technology* (Trier, Germany) *(VRST '24)*. Association for Computing Machinery, New York, NY, USA, Article 94, 2 pages. doi:10.1145/3641825.3689520

Manu Kumar, Tal Garfinkel, Dan Boneh, and Terry Winograd. 2007. Reducing shoulder-surfing by using gaze-based password entry. In *Proceedings of the 3rd symposium on Usable privacy and security - SOUPS '07*. ACM Press, Pittsburgh, Pennsylvania, 13. doi:10.1145/1280680.1280683

Dachuan Liu, Bo Dong, Xing Gao, and Haining Wang. 2015. Exploiting Eye Tracking for Smartphone Authentication. In *Applied Cryptography and Network Security*, Tal Malkin, Vladimir Kolesnikov, Allison Bishop Lewko, and Michalis Polychronakis (Eds.). Springer International Publishing, Cham, 457–477.

Päivi Majaranta and Andreas Bulling. 2014. Eye Tracking and Eye-Based Human–Computer Interaction. In *Advances in Physiological Computing*, Stephen H. Fairclough and Kiel Gilleade (Eds.). Springer London, London, 39–65. doi:10.1007/978-1-4471-6392-3_3 Series Title: Human–Computer Interaction Series.

Piotr Odya, Franciszek Górski, and Andrzej Czyżewski. 2023. User Authentication by Eye Movement Features Employing SVM and XGBoost Classifiers. *IEEE Access* 11 (2023), 93341–93353. doi:10.1109/ACCESS.2023.3309000

Ruotian Peng, Yang Gao, and Zhanpeng Jin. 2025. Gazenum: unlock your phone with gaze tracking viewing numbers for authentication. *CCF Transactions on Pervasive Computing and Interaction* 7, 1 (March 2025), 1–14. doi:10.1007/s42486-024-00165-w

Ken Pfeuffer, Melodie Vidal, Jayson Turner, Andreas Bulling, and Hans Gellersen. 2013. Pursuit calibration: making gaze calibration less tedious and more flexible. In *Proceedings of the 26th annual ACM symposium on User interface software and technology*. Acm, St. Andrews Scotland, United Kingdom, 261–270. doi:10.1145/2501988.2501998

Vijay Rajanna, Seth Polsley, Paul Taele, and Tracy Hammond. 2017. A Gaze Gesture-Based User Authentication System to Counter Shoulder-Surfing Attacks. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '17)*. Association for Computing Machinery, New York, NY, USA, 1978–1986. doi:10.1145/3027063.3053070 event-place: Denver, Colorado, USA.

Dario D. Salvucci and Joseph H. Goldberg. 2000. Identifying fixations and saccades in eye-tracking protocols. In *Proceedings of the symposium on Eye tracking research & applications - ETRA '00*. ACM Press, Palm Beach Gardens, Florida, United States, 71–78. doi:10.1145/355017.355028

Roman Weiss and Alexander De Luca. 2008. PassShapes: Utilizing Stroke Based Authentication to Increase Password Memorability. In *Proceedings of the 5th Nordic Conference on Human-Computer Interaction: Building Bridges (NordiCHI '08)*. Association for Computing Machinery, New York, NY, USA, 383–392. doi:10.1145/1463160.1463202 event-place: Lund, Sweden.

Guixin Ye, Zhanyong Tang, Dingyi Fang, Xiaojiang Chen, Kwang In Kim, Ben Taylor, and Zheng Wang. 2017. Cracking Android Pattern Lock in Five Attempts. In *Proceedings 2017 Network and Distributed System Security Symposium*. Internet Society, San Diego, CA. doi:10.14722/ndss.2017.23130