# EyeLogin - Calibration-free Authentication Method for Public Displays Using Eye Gaze

Omair Shahzad Bhatti
omair_shahzad.bhatti@dfki.de
DFKI
Saarbrücken, Germany

Michael Barz
michael.barz@dfki.de
DFKI
Saarbrücken, Germany
Oldenburg University
Oldenburg, Germany

Daniel Sonntag
daniel.sonntag@dfki.de
DFKI
Saarbrücken, Germany
Oldenburg University
Oldenburg, Germany

## ABSTRACT

The usage of interactive public displays has increased including the number of sensitive applications and, hence, the demand for user authentication methods. In this context, gaze-based authentication was shown to be effective and more secure, but significantly slower than touch- or gesture-based methods. We implement a calibration-free and fast authentication method for situated displays based on saccadic eye movements. In a user study ($n = 10$), we compare our new method with *CueAuth* from Khamis et al. (IMWUT'18), an authentication method based on smooth pursuit eye movements. The results show a significant improvement in accuracy from 82.94% to 95.88%. At the same time, we found that the entry speed can be increased enormously with our method, on average, 18.28$s$ down to 5.12$s$, which is comparable to touch-based input.

## CCS CONCEPTS

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

## KEYWORDS

Eye Tracking; Gaze-based Interaction; Authentication; Public Displays; Calibration-free Eye Tracking

**ACM Reference Format:**
Omair Shahzad Bhatti, Michael Barz, and Daniel Sonntag. 2021. EyeLogin - Calibration-free Authentication Method for Public Displays Using Eye Gaze. In *ETRA '21: 2021 Symposium on Eye Tracking Research and Applications (ETRA '21 Short Papers), May 25–27, 2021, Virtual Event, Germany.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3448018.3458001

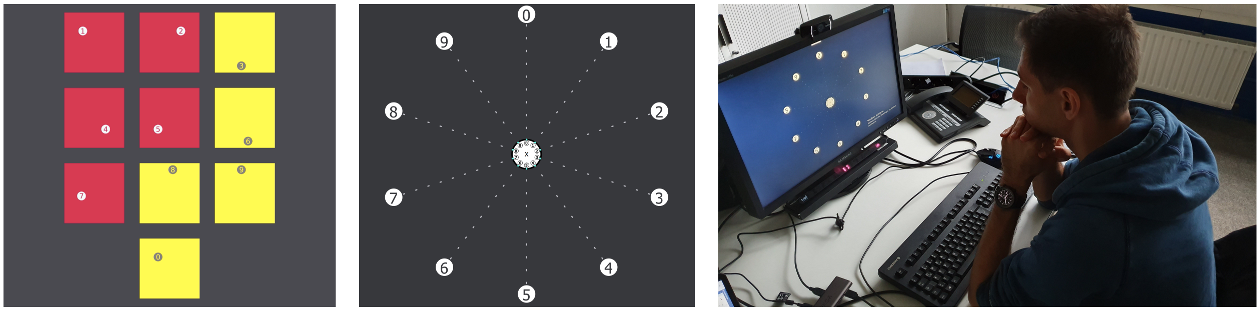
## 1 INTRODUCTION

An increasing amount of use cases require an authentication of users prior to interaction with a public display. Typical situations include making purchases, retrieving sensitive information, or for identification purposes. A common class of authentication methods are knowledge-based approaches, e.g., PIN, password or patterns are entered via touch-input on the public screen or via an external keyboard. However, these methods are prone residues- or observation-based attacks. Smudges [Aviv et al. 2010] or thermal residues [Abdelrahman et al. 2017] can be used to retrieve partial to full information of an entered PIN or password. Also, attackers might observe the input by shoulder surfing attacks [Brudy et al. 2014] or more sophisticated attacks involving a camera-based setup [Ye et al. 2017]. An alternative to knowledge-based approaches are biometric authentication methods such as fingerprint and iris scans. However, in this work we concentrate on knowledge-based and gaze-based authentication in the context of mobile gaze-based interaction [Barz et al. 2018] and pervasive attentive user interfaces [Bulling 2016]. Prior works propose authentication mechanisms based on different modalities to be more robust against attackers. For example, Kim et al. [2010] use the pressure-signal of touch-based input to overcome shoulder surfing. Other works introduce gaze-based methods that track the user's gaze with cameras or specialized eye tracking sensors. These methods were shown to be more secure than, e.g., touch-based input [De Luca et al. 2008; Khamis et al. 2018]. In addition, gaze-based input allows hands-free authentication and interaction which is more hygienic. This is an important factor, due to the high contamination of public displays [Gerba et al. 2016]. A major drawback of many gaze-based authentication methods is a mandatory calibration [Best and Duchowski 2016; Kumar et al. 2007]. These approaches are not suited for public displays, because calibration takes time and is perceived as cumbersome [Majaranta and Bulling 2014]. But interaction methods for public displays shall be designed for immediate usability [Khamis et al. 2015]. Calibration-free methods exist, but tend to be slow [Cymek et al. 2014; De Luca et al. 2007; Khamis et al. 2018; Rajanna et al. 2017] or suffer from low success rates [De Luca et al. 2009; Khamis et al. 2018].

In this work, we implement a novel gaze-based and calibration-free authentication method, *EyeLogin*, that addresses the limitations of prior approaches (see Figure 1b). Our system uses the direction of saccadic eye movements in a radial interaction design, similar to [Best and Duchowski 2016], that facilitates accurate and fast PIN entry. We use a low-cost remote eye tracking sensor that allows broad integration into public displays and spontaneous user interaction. Other than the approach described in [Best and Duchowski 2016], our method is calibration-free. In addition, we implement the

*ETRA '21 Short Papers, May 25–27, 2021, Virtual Event, Germany*

ACM ISBN 978-1-4503-8345-5/21/05…$15.00
https://doi.org/10.1145/3448018.3458001



**(a) Interface of *CueAuth*** **(b) Interface of *EyeLogin*** **(c) The setup of the study**

**Figure 1: We compare two gaze-based authentication methods. *CueAuth* (a) is based on a dial pad layout and smooth pursuit eye movements. *EyeLogin* (b) uses a radial digit pattern and saccadic eye movements for PIN entry. The setup of our study is shown in (c).**

state-of-the-art method *CueAuth*[1], that is described in [Khamis et al. 2018], as a baseline system. In a user study ($n$ = 10), we compare both authentication methods in terms of PIN entering accuracy, the PIN entry time, the usability and the perceived workload.

## 2 RELATED WORK

Prior gaze-based authentication methods can be classified into "dwell-based" and "gesture-based" methods. In dwell-based systems, the user makes selections by fixating elements for a pre-defined time threshold. Gesture-based systems use eye movement patterns that can be recognized automatically, e.g., combinations of fixations, saccades and smooth pursuit eye movements. Kumar et al. [2007] introduced "EyePassword," a dwell-based authentication method that displays a virtual keyboard or number pad for entering a password or a PIN. Their system achieves low error rates that are comparable to interaction with a physical keyboard, but the entry time is higher and the method requires prior calibration of the eye tracker. Best and Duchowski [2016] introduced a PIN entry method that relies on a spatial interaction design: they show digits in a circular design that imitates a rotary dial phone. A digit is entered by moving the gaze from the center of the screen to a digit-specific area and back. The average entry time is smaller than five seconds (M = 4.62). However, the system suffers from major drawbacks: it has a low accuracy (M=71.16%), does not support real-time authentication, and requires user calibration prior to each authentication. We adopt the circular design, because it enabled faster input times compared to the numpad design in [Best and Duchowski 2016]. However, our implementation is calibration-free and allows more accurate digit selection. Calibration-free eye tracking methods address the problem of time-consuming and tedious calibration procedures, which is important for spontaneous interaction with public displays [Khamis et al. 2015]. One approach to calibration-free gaze-based interaction is to use gaze gestures. De Luca et al. [2007] proposed *EyePIN* for gesture-based PIN entry via eye movements. The error rate is low (< 10%), but the patterns need to be memorized and, with 54$s$ the average input time is very high. The authors presented the extension *EyePassShapes* using shape-based gestures, similar to unlock patterns which are easier to remember [De Luca et al. 2009]. The entry time improved to 12.52$s$, but the error rate slightly increased. Another approach to facilitate calibration-free gaze input is based on smooth pursuit eye movements: eye movements are correlated with trajectories of elements in a dynamic user interface. Rajanna et al. [2017] proposed a system in which users have to follow three pre-defined moving shapes out of 36 to authenticate. They achieve a high accuracy of 96%, but the user can select from 12 shapes only which yields a smaller password space compared to a four-digit PIN. Each digit entry takes 5 seconds and a PIN entry takes at least 15 seconds. Liu et al. [2015] introduced a method for smartphones: the system uses the front-facing camera to track the eyes. Four randomly sorted objects, each assigned with a unique number between 1-4, are placed in the middle of the screen. To enter a PIN, the user follows the digit trajectory to each edge of the screen. The input time is low (9.6s), but also the accuracy (77.1%). With 1024 possibles PINs, the password space is 10x smaller compared to a four-digit PIN. Cymek et al. [2014] implemented another PIN entry method based on smooth pursuits. Each digit is shown as a button and follows a simple trajectory of three straight movements (combinations of up, down, left, right). They achieve a high detection rate of 91.55%, but the minimum entry time is high (25$s$). More recently, Khamis et al. [2018] introduced *CueAuth* which is based on a number pad layout. They implement a gaze-based version that, instead of moving buttons, includes a small moving circles in a button. The movements of the digits are either linear, circular, or zigzag. On average, the entry time is 26.35$s$ with minimal entry times around 18$s$. We implement *CueAuth* as a baseline system and compare the performance in terms of accuracy and entry time with our novel authentication method. Both interfaces are shown in Figure 1.

These gaze-based authentication methods were shown to be more secure than traditional PIN entry systems. However, all systems suffer from one or more disadvantages including low accuracy in recognizing the entered PIN, high entry times, or the need of prior calibration. We implement a novel calibration-free authentication system that addresses these flaws: our goal is to enable secure

[1] In *CueAuth* [Khamis et al. 2018], three authentication methods are described based on touch, gesture and gaze input, respectively. We refer to the gaze-based version unless stated otherwise.

and fast gaze-based authentication on public displays with high accuracy.

# 3 GAZE-BASED AUTHENTICATION

In the following, we describe the design and implementation of the gaze-based *CueAuth* method [Khamis et al. 2018] and our novel authentication method that is based on saccadic eye movements. We implement *CueAuth* as baseline system, because it is calibration-free, implements the same knowledge-based authentication method (four-digit PIN entry) and it is one of the most recent and comprehensive works that explores authentication on public displays.

## 3.1 CueAuth

We implement *CueAuth* as described in [Khamis et al. 2018]. The central concept of *CueAuth* is matching smooth pursuit eye movements of a user with the trajectory of moving digits (0-9) in the interface (see Figure 1a). The interface renders a virtual number pad. Each digit is presented in a small circle that moves with a predefined unique trajectory. The trajectories are either linear, circular or zigzag shaped as proposed in [Vidal et al. 2013]. To authenticate, the user needs to follow the movement of four digits in a row that form a PIN. For each iteration and match, the interface provides visual feedback in a separate text view by adding an asterisk symbol. Addressing the known limitations of *CueAuth*, we add a one second break after the trajectory-based animation ends to allow the user to re-focus and to provide feedback when the matching process begins and ends. The actual matching begins after the animations of the digits stop . We compare the trajectories of the interface controls with the relative eye movements of the same time-frame. We calculate the Pearson correlation for two axes (x and y) and average the correlation coefficients in the `Correlate` function. If the mean correlation $c \geq 0.8$, the digit is stored and the user receives immediate feedback of the match (asterisk). If more than one trajectory reaches the threshold detection threshold of 0.8, we choose the digit with the higher correlation. We call `Correlate` with two different time-windows: [2s-4s] and [1.5s-4s] that start $2s$ or $2.5s$ before the animation stops. The digit with the highest correlation coefficient is appended to the stored PIN.

## 3.2 EyeLogin

We propose a novel algorithm for calibration-free authentication which is based on saccadic eye movements. *EyeLogin* shows the digits 0 to 9 in a radial design (see 1b), similar to [Best and Duchowski 2016]. At the center, we present feedback on the progress (one asterisk per entered digit appears) and show miniaturized digits as direction cues for the user to prevent errors. A dashed line connects the inner and outer digits to guide the user's gaze. The user starts the authentication process by pressing the space bar while fixating the center area. This trigger is required to overcome Midas' touch problem inherent in gaze-based interaction and could be replaced by any trigger in the future, e.g., presence detection in combination with a long fixation or speech-based hotwords known from digital assistants. When the authentication process is started (trigger), the initial gaze position is stored as reference point *gaze_c* and provided as input to *EyeLogin* . The user enters a digit by fixating it and returning the focus to the center position. We leverage the quick saccadic eye movement between two fixations to determine the relative direction of the eye movement and to detect the digit of choice: we determine the farthest point *max_p* from the reference point *gaze_c* and calculate the direction vector *dir_n* with *gaze_c* as origin and *max_p* as destination point. The angle between the y-axis and the direction vector allows to infer the fixated digit : each digit is assigned to a certain angular sector. Upon detection, the system gives feedback by displaying an additional asterisk in the center area. Showing the feedback at the center region ensures that the user returns its focus to this point as expected by the algorithm. This process is repeated four times to complete the PIN entry. One limitation is, that users might turn their gaze to the next digit before returning to the center area. This would cause an erroneous input. However, this error type occurred rarely in our study.

# 4 EVALUATION

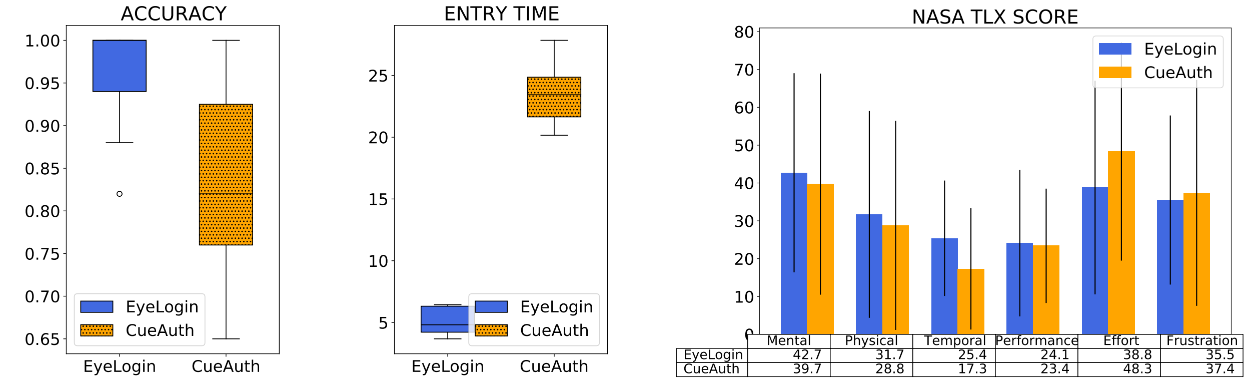
We conduct a user study (n=10) to compare our novel authentication method *EyeLogin* to the existing eye-tracking based method *CueAuth*. We investigate the effectiveness, efficiency, usability and perceived workload of both methods in a public display setting. We adopt the experimental design from Khamis et al. [2018] to ensure comparability with their results. Hence, we face the same problem that a consecutive PIN entry is no realistic scenario and might negatively impact our results. However, this should not cause problems due to our within-subjects design: the study is designed as a repeated measures experiment and is conducted with the independent variable *authentication method* as the within-subject factor. We recruited 10 students (two females and eight males) with normal or corrected to normal vision aged between 25 and 31. One participant with weak vision refrained from wearing eye correction, but did not report any problems. Two of the participants had prior experience with eye tracking.

## 4.1 Conditions & Metrics

We investigate the performance and usability of the authentication methods *EyeLogin* and *CueAuth*. For each method, we ask participants to enter 11 PINs in a training phase and 17 PINs in a main phase, totalling to 28 PINs per method and user. The instructor vocalizes the randomly selected four-digit PIN before the participant starts the authentication procedure by pressing the space-key. They receive automatic feedback about the progress as described above, but not whether a digit or the complete PIN was recognized correctly. To measure the performance of both methods, we use the following metrics: the PIN entry time, the accuracy in entering a PIN, the System Usability Scale (SUS) as usability measure, and the NASA TLX score as measure for the perceived workload. The PIN entry time is measured as the time between the recognition of the trigger (pressing the space bar) and the recognition of the fourth digit. The PIN accuracy is the average number of correct PIN entries (all digits are entered correctly). A false entry is counted in one or more digits are incorrect.

## 4.2 Procedure

After participants signed a informed consent form, the instructor explains the study. The instructor presents an authentication method (counterbalanced order) by demonstrating the interface and



**(a) Accuracy in PIN entry**

**(b) PIN Entry time [s]**

**(c) Perceived workload (NASA TLX scores)**

**Figure 2: Results from our user study ($n = 10$) including a box-plot for the accuracy of PIN entry (a) and for the PIN entry time (b), and a bar chart diagram visualizing the NASA TLX results: mean ± SD (c). All charts show the results for the main phase of *EyeLogin* (blue) and *CueAuth* (yellow, dotted).**

by explaining how a digit or password is entered. In the training phase (11 PINs), the participant can familiarise with each method by entering three simple PINs, followed by eight random PINs. If the instructor detects major problems, the user is corrected. In the main phase, the participant enters 17 PINs. Afterwards, the participant fills in a NASA TLX [Hart and Staveland 1988] form to asses the perceived workload. This procedure is repeated with the remaining authentication method. After all tasks are completed, the participant fills in a questionnaire including demographic questions and items of the System Usability Scale (SUS) [Brooke 1996] as well as open-ended questions for each authentication method. The order of the input methods is counterbalanced to avoid ordering effects.

## 4.3 Apparatus

A 27-inch widescreen monitor with a resolution of 1920x1080 pixels is used to display the authentication interfaces. We use the binocular Tobii 4C remote eye tracker [Tobii Gaming 2019] with a 60Hz sampling rate, which is attached below the screen (see Figure 1c). Prior to all sessions, the eye tracker is calibrated once by the study instructor: we use the same calibration for all participants. Participants are seated approximately 60cm in front of the display. A keyboard is provided to start the authentication trials. For analysis, we store the participant ID, the timestamped eye movements, and synchronized movements of all smooth pursuits stimuli (*CueAuth* only) for every PIN entry attempt. Further, we store the recognized PIN, the correct PIN, and the answers to the questionnaire and the NASA TLX items.

## 4.4 Hypotheses

We hypothesize that users are more accurate in entering PINs with *EyeLogin* compared to *CueAuth*, because directed saccadic movements are seemingly less error-prone than more complex smooth pursuits (H1). In addition, we expect that authentication is faster using our saccade-based method *EyeLogin* than using *CueAuth* which is bound to long animation times (H2). Further, we expect that the gains in effectiveness (accuracy) and efficiency (time) have no negative impact on the usability and the perceived workload (H3).

## 4.5 Results

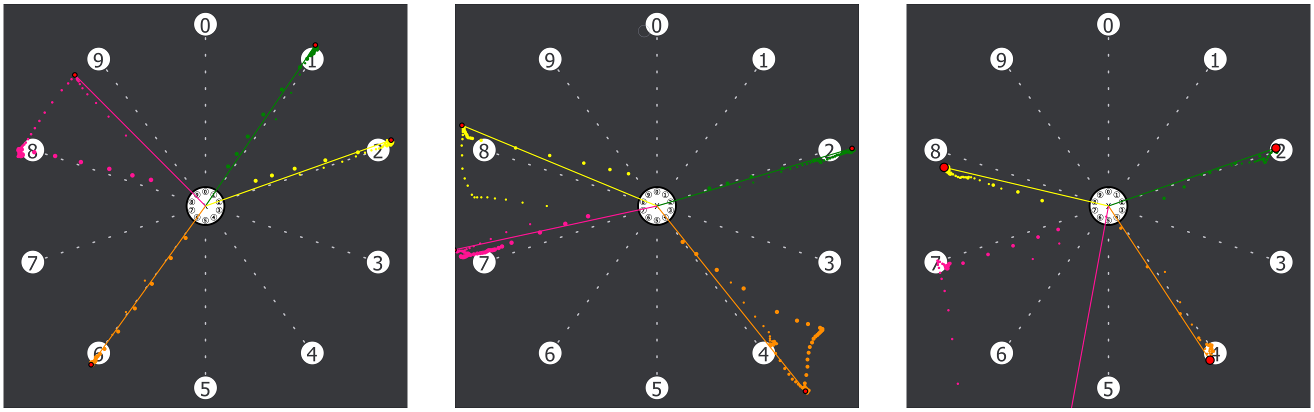
For both methods, we observe the accuracy, the entry time, the NASA TLX and the SUS score for entering PINs. We report the results of the main phase (17 PINs), because we found no significant differences to the results of the training phase. To test for statistical significance, we use the paired samples t-test[2]. The Shapiro-Wilk test is used to check whether the differences of the paired samples are from a normal distribution and, hence, no assumption of the dependent t-test is violated. We also checked whether the order of methods has an effect on our dependent variables, but found no significant differences using an independent t-test and the order as a between groups factor ($p > .05$).

*4.5.1 Accuracy.* Using our implementation of *CueAuth*, the users achieve a mean accuracy of 82.94% ($SD = 11.58$). This is close to the results from Khamis et al. [2018] which reported 82.72% ($SD = 38.53$). For our proposed method *EyeLogin*, we observe an accuracy of 95.88% ($SD = 6.23$), which is 12.94% better than the *CueAuth*-baseline (see Figure 2a). This difference is statistically significant with $t(9) = 3.18$, $p = .012$. In addition, our gaze-based method performs better than the best method of Khamis et al. [2018] that is based on touch interaction ($M = 93.38\%, SD = 26.05$).

*4.5.2 Entry Time.* On average, we measure entry times of 23.41$s$ ($SD = 2.28$) for *CueAuth*, which is similar to the result of 26.35$s$ reported in the literature [Khamis et al. 2018]. Their reported standard deviation of 22.09 is much higher compared to our implementation.

Using *EyeLogin*, we observe average pin entry times of 5.12$s$ ($SD = 1.09$). The time saving of 18.28$s$ compared to the baseline (see Figure 2b) is statistically significant ($t(9) = 24.063, p < .001$). The touch-based method in [Khamis et al. 2018] is reported to be the fastest and is, with an average of 3.73$s$ ($SD = 1.07s$) only slightly faster than our proposed gaze-based approach.

[2] We use the 2-tailed paired samples t-test in SPSS with an alpha-level of 5%



(a) Incorrect PIN (expected: 1628; detected: 1629)

(b) Correct PIN (expected: 2487)

(c) Incorrect PIN (expected: 2487; detected: 2485)

**Figure 3: Visualizations of the raw gaze signal of individual participants from our study including three trials using *EyeLogin*. Trials a) and c) result in a wrong PIN entry, b) shows the sequence of a successful trial. The colors indicate the input order (green, orange, yellow, pink), the dot size relates to the order of gaze samples (increasing radius corresponds to increasing timestamps) and the red dot marks the point $max_p$ from our algorithm.**

*4.5.3 Perceived Workload and Usability.* We use the NASA TLX questionnaire to evaluate the perceived workload as suggested in Khamis et al. [2018]. The mean scores for all dimensions of the test are reported in Figure 2c. None of the differences are significant as determined by a paired samples t-test per dimension ($df = 9; p > .05$). Also, we ask the participants to fill in a SUS questionnaire, which results in a subjective usability score, for both methods. We receive an average score of 66.5 ($SD = 18.72$) for *CueAuth* and 75.75 ($SD = 15.28$) for *EyeLogin* (higher is better). However, the difference of 9.25 points is not significant ($t(9) = -1.075, p = .31$).

*4.5.4 Qualitative Feedback.* We collect qualitative feedback via open-ended questions asking participants to note pros and cons for each method and to provide suggestions for improvements. Analysing the answers, we find that *EyeLogin* is perceived as fast (7/10) and easy to use (7/10). Three participants criticize that blinks are likely to cause errors during pin entry. For *CueAuth*, participants state as advantages that the layout is familiar (4/10) and easy to use (2/10). The participants perceive *CueAuth* as slow (7/10) and tiring (4/10). Two participants criticize that the system was not sensitive enough in recognizing their input.

## 5 DISCUSSION

The results of our evaluation show that our authentication method *EyeLogin* is significantly more accurate than the baseline system *CueAuth*. Users succeed in entering a PIN in 95.88% of all trials which is 12.94% better than the baseline and confirms H1. In addition, our gaze-based method achieved a similar accuracy to the touch-based version of *CueAuth* as reported in [Khamis et al. 2018]. Further, our method performs more accurately than the method by Best and Duchowski [2016] with 71.16% accuracy, which is also based on a circular design, but, nevertheless, requires user calibration. The PIN entry times for *EyeLogin* are tremendously lower than for *CueAuth* (significant). On average, users need 5.12$s$ to enter a four-digit PIN which is 18.28$s$ faster than measured for the baseline *CueAuth* (confirms H2). We measured similar PIN entry times using our implementation of *CueAuth* compared to the reported results by Khamis et al. [2018], and our result is close to the PIN entry times of their touch-based version (3.73$s$). We do not know whether *EyeLogin* achieves the same level of security than *CueAuth* (0.05% of attacks were successful, if the eyes and the display content have been visible). This evaluation is out of scope of this paper and will be the target of future work.

We used the SUS and the NASA TLX questionnaires for measuring the usability and the perceived workload of both authentication methods. The results do not reveal any significant differences for the two considered methods which suggests that we can confirm H3. Further, we observe a higher average SUS for *EyeLogin* (75.75) than for *CueAuth* (66.5). This might indicate that our authentication method has a better usability than the baseline system. For comparison, other works using the SUS questionnaire achieve, on average, a score of 69.5 ($n = 273$) [Bangor et al. 2009].

### 5.1 Limitations and Future Work

*EyeLogin* enables fast and reliable input for authentication on public displays on the same level of performance than more common touch-based methods. However, a few limitations remain including a required start trigger to overcome the Midas touch problem, some error types that cause avoidable authentication fails and potential vulnerabilities to camera-based attacks. We address each of these limitations and provide suggestions how they could be solved.

*5.1.1 Midas Touch Problem.* Our system requires users to press the space bar to capture the reference gaze position $gaze_c$ and start the authentication. Using an additional modality for disambiguating the gaze-based input [Oviatt et al. 2017; Qvarfordt and Pernilla 2017] is common practice. However, on public displays this trigger needs to be replaced by more suitable alternatives like touching a button. Other modalities include speech-based input: an instruction can be shown at the central area of the user interface asking the user to start the authentication by vocalizing a trigger word. A pure gaze-based method can be realized by using a dwell-time based trigger to start the authentication. The presence of a user can be detected by the presence or absence of gaze data from the eye tracking sensor.

5.1.2 *Error Types.* For *EyeLogin*, we observe two common error types that cause a wrong PIN entry. Figure 3a) shows the raw gaze signal of a user that moved its gaze to the wrong digit (9), subsequently corrects the gaze position (8) and returns to the center. However, *EyeLogin* detects 9 as input resulting in a wrong digit sequence. Figure 3b shows a similar case, but the correction (for 4 and 8) is done earlier and *EyeLogin* detects the correct sequence. Figure 3c shows a trial that failed due to a blink before fixating the last digit: 7. The blink resulted in a noisy gaze signal with distant samples, causing the algorithm to choose the wrong digit (5). A further limitation is, that users might turn their gaze to the next digit before returning to the center area, which is not supported.

5.1.3 *Camera-based Attacks. EyeLogin* is robust against traditional shoulder-surfing attacks, because an attacker must observe the display and the eyes of a user during PIN entry. More sophisticated attackers might attach a camera to the public display and infer the password from a video stream that captures the user's face and eye movements. We will use the collected video feeds and display contents from our study to evaluate the vulnerability of our PIN entry method similar to [Khamis et al. 2018]. We will also test a randomized arrangement of digits for *EyeLogin*, in case that our method suffers from an increased vulnerability. This was perceived as more secure by all our participants. Better security through randomly arranged digits probably needs to be traded off against usability and entry time.

## 6 CONCLUSION

In this paper, we presented a calibration-free and gaze-based authentication method for public displays. In a user study, we could show that our method *EyeLogin*, that leverages saccadic eye movements, performs significantly faster and significantly more accurate than *CueAuth*, a state-of-the-art gaze-based authentication system from the literature [Khamis et al. 2018]. With this work, we presented the first calibration-free authentication method using gaze that is as effective and efficient than less secure input modalities such as touch- and gesture-based input.

## ACKNOWLEDGMENTS

This work was funded by the German Federal Ministry of Education and Research (BMBF) under grant number 16SV7768 (Intera-kt) and 01JD1811C (GeAR).

## 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* (Denver, Colorado, USA) *(CHI '17)*. ACM, New York, NY, USA, 3751–3763. https://doi.org/10.1145/3025453.3025461

Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge Attacks on Smartphone Touch Screens. In *Proceedings of the 4th USENIX Conference on Offensive Technologies* (Washington, DC) *(WOOT'10)*. USENIX Association, Berkeley, CA, USA, 1–7. http://dl.acm.org/citation.cfm?id=1925004.1925009

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. http://dl.acm.org/citation.cfm?id=2835587.2835589

Michael Barz, Florian Daiber, Daniel Sonntag, and Andreas Bulling. 2018. Error-Aware Gaze-Based Interfaces for Robust Mobile Gaze Interaction. In *Proceedings of the 2018 ACM Symposium on Eye Tracking Research & Applications*. ACM, New York, NY, USA, 24:1–24:10. https://doi.org/10.1145/3204493.3204536

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* (Charleston, South Carolina) *(ETRA '16)*. ACM, New York, NY, USA, 69–76. https://doi.org/10.1145/2857491.2857527

John Brooke. 1996. SUS-A quick and dirty usability scale. (1996).

Frederik Brudy, David Ledo, Saul Greenberg, and Andreas Butz. 2014. Is Anyone Looking? Mitigating Shoulder Surfing on Public Displays Through Awareness and Protection. In *Proceedings of The International Symposium on Pervasive Displays* (Copenhagen, Denmark) *(PerDis '14)*. ACM, New York, NY, USA, Article 1, 6 pages. https://doi.org/10.1145/2611009.2611028

Andreas Bulling. 2016. Pervasive Attentive User Interfaces. *IEEE Computer* 49, 1 (jan 2016), 94–98. https://doi.org/10.1109/MC.2016.32

Dietlind Cymek, Antje Venjakob, Stefan Ruff, Otto Lutz, Simon Hofmann, and Matthias Roetting. 2014. Entering PIN Codes by Smooth Pursuit Eye Movements. *Journal of Eye Movement Research* 7 (08 2014), 1–11.

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* (Mountain View, California, USA) *(SOUPS '09)*. ACM, New York, NY, USA, Article 7, 12 pages. https://doi.org/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 19th Australasian Conference on Computer-Human Interaction: Entertaining User Interfaces* (Adelaide, Australia) *(OZCHI '07)*. ACM, New York, NY, USA, 199–202. https://doi.org/10.1145/1324892.1324932

Alexander De Luca, Roman Weiss, Heinrich Hussmann, and Xueli An. 2008. Eyepass - Eye-stroke Authentication for Public Terminals. In *CHI '08 Extended Abstracts on Human Factors in Computing Systems* (Florence, Italy) *(CHI EA '08)*. ACM, New York, NY, USA, 3003–3008. https://doi.org/10.1145/1358628.1358798

Charles Gerba, Adam Wuollet, Peter Raisanen, and Gerardo Lopez. 2016. Bacterial contamination of computer touch screens. *American Journal of Infection Control* 44 (03 2016), 358–360. https://doi.org/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 *Human Mental Workload*, Peter A. Hancock and Najmedin Meshkati (Eds.). Advances in Psychology, Vol. 52. North-Holland, 139 – 183. https://doi.org/10.1016/S0166-4115(08)62386-9

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* (Osaka, Japan) *(UbiComp/ISWC'15 Adjunct)*. ACM, New York, NY, USA, 763–766. https://doi.org/10.1145/2800835.2807951

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. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 4, Article 174 (Dec. 2018), 21 pages. https://doi.org/10.1145/3287052

David Kim, Paul Dunphy, Pam Briggs, Jonathan Hook, John W. Nicholson, James Nicholson, and Patrick Olivier. 2010. Multi-touch Authentication on Tabletops. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) *(CHI '10)*. ACM, New York, NY, USA, 1093–1102. https://doi.org/10.1145/1753326.1753489

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* (Pittsburgh, Pennsylvania, USA) *(SOUPS '07)*. ACM, New York, NY, USA, 13–19. https://doi.org/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*. Springer London, London, 39–65. https://doi.org/10.1007/978-1-4471-6392-3_3

Sharon. Oviatt, Björn Schuller, Philip R. Cohen, Daniel Sonntag, Gerasimos Potamianos, and Antonio Krüger (Eds.). 2017. *The Handbook of Multimodal-Multisensor Interfaces: Foundations, User Modeling, and Common Modality Combinations* (volume 1 ed.). Association for Computing Machinery and Morgan & Claypool, New York, NY, USA. 662 pages. https://doi.org/10.1145/3015783

Pernilla Qvarfordt and Pernilla. 2017. Gaze-informed multimodal interaction. In *The Handbook of Multimodal-Multisensor Interfaces: Foundations, User Modeling, and Common Modality Combinations* (volume 1 ed.). ACM, 365–402. https://doi.org/10.1145/3015783.3015794

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* (Denver, Colorado, USA) *(CHI EA '17)*. ACM, New York, NY, USA, 1978–1986. https://doi.org/10.1145/3027063.3053070

Tobii Gaming. 2019. *Tobii Eye Tracker 4C*. Tobii Gaming. https://gaming.tobii.com/tobii-eye-tracker-4c/

Mélodie Vidal, Andreas Bulling, and Hans Gellersen. 2013. Pursuits: Spontaneous Interaction with Displays Based on Smooth Pursuit Eye Movement and Moving Targets. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (Zurich, Switzerland) *(UbiComp '13)*. ACM, New York, NY, USA, 439–448. https://doi.org/10.1145/2493432.2493477

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 2017 (NDSS'17)*. Internet Society, 15.