Allowing for Secure and Accessible Authentication for Individuals with Disabilities of Dexterity

Abbie Price and Fernando Loizides

Cardiff University, Cardiff, UK - PriceA36,loizidesf@cardiff.ac.uk

Abstract. People living with disabilities of dexterity can be vulnerable to attackers when authenticating using physical input methods, such as when inputting PIN numbers using a keypad at an ATM(Cash Point), due to the extended time these interactions take because of the device's lack of accommodations and accessibility. This makes their input more observable to a potential attacker and thus compromises their security. In addition, when ease of use is severely compromised, this may cause a need to circumvent good security practices for practical usability which further makes these individuals vulnerable to potential attackers. While research in the field of accessible and secure authentication exists, limited work has focused on the unique needs of individuals who have limited to no hand or finger dexterity. This paper proposes an accessible framework for authentication (AAFIDD), that focuses on meeting the needs of this group. We implemented a prototype authentication model and present an initial user study with 7 participants that evaluated the efficacy of this prototype and the framework. Each participant was randomly assigned a PIN and asked to input it using a method reliant on hand-dexterity and then using the prototype gaze-based input. Users were timed and asked to evaluate their experience in terms of ease of use while a researcher attempted to perform an over-the-shoulder attack to evaluate the security. We found that the prototype input method was less likely to be interpreted by an observer than using a mouse to input, while users considered the prototype input method accessible and easy to use.

Keywords: Pupillary Biometrics · Dexterity Disability· Eye-tracking · Security · PIN

1 Introduction and Motivation

In modern society, technology has revolutionized the way people interact with digital systems. However, this digital revolution has also increased the risks of technologies being abused or exploited by criminals. The FBI reports an increase

in victim losses of over $3 billion [1] compared to the previous year [2], showing the significance of this risk. To combat this danger, scientists and security researchers place more and more emphasis on designing and implementing robust security systems to safeguard user privacy and data - however, this security often does not consider the needs of all individuals in its operation.

The Family Resources Survey [3] estimated that 14.6 million people in the UK are living with a disability of some kind. Of this population, the third most prevalent type of disability for state-pension-age adults and the fourth most prevalent for working-age adults was a disability of dexterity. For many of these individuals, this disability can add significant challenges to their ability to make use of technology which relies solely on finger and hand dexterity. Limitations in the usability of authentication technologies not only make it more prohibitive and time-consuming to perform authentication but also increase the likelihood that people who struggle with these operations may circumvent it in less secure manners when their needs are not met, as found by Lewis and Venkatasubramanian [15]. For example, password-sharing and shoulder-surfing attacks are greater security concerns for individuals for whom authentication is less accessible and more time-consuming. For PIN, password, one-time code and code-via-SMS methods of authentication, the security of individuals with Parkinson's and upper extremity disabilities is uniformly easier to circumvent through reduced search-space entropy or reliance on another individual [11].

An example of this model of authentication is in the use of ATMs, where the user has to insert their bank card and input their PIN on a keypad to verify their identity and access their funds. For individuals with disabilities of dexterity, this interaction can prove problematic in terms of accessibility and security. While ATM keypads have been commonly adapted in the UK to use braille for visually impaired users, there is no such adaptation for individuals with disabilities of dexterity who may struggle or be unable to use the keypad itself. This highlights the lack of provisions in terms of usability and security for individuals with disabilities of dexterity regarding authentication. In response to these lacking provisions, the primary objective of this work is to propose a new method of authentication that takes into consideration the distinct requirements of individuals with disabilities of dexterity in terms of usability and security. Additional objectives are to explore alternate input methods for individuals with disabilities of dexterity, test the accessibility and security of the proposed framework with

[1] Federal Bureau of Investigation Internet Crime Report for 2022 - https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf - accessed February 2024

[2] Federal Bureau of Investigation Internet Crime Report for 2021 - https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf - accessed February 2024

[3] Department for Work and Pensions Family Resources Survey: 2020 to 2021 - https://www.gov.uk/government/statistics/family-resources-survey-financial-year-2020-to-2021/family-resources-survey-financial-year-2020-to-2021disability-1 - accessed February 2024

users, and ultimately evaluate the appropriateness of the framework for use in this context.

We present a bespoke eye-tracking system and process to allow users with dexterity disabilities to control the entry of their pin code and investigate its efficacy and its vulnerability to over-the-shoulder attacks. Our fully working system and pilot testing give us positive results and a methodology that shows promise to be implemented to encourage accessibility in security design and enable people with dexterity issues to more securely enter their PIN.

2 Related Work

Accessibility is commonly considered to be a neglected need within the field of authentication [10]. While it is best practice to consider accessibility from the outset, solutions are still commonly designed without adequate consideration of the needs of disabled users [21]. However, with the advent of biometric data, there is cause for optimism for some disabled users; for example, a survey of dyslexic users highlighted limitations faced by this user base in creating and remembering passwords but found that biometric methods including face recognition enjoyed higher success metrics [13]. Legislation is also beginning to address the needs of accessibility. In 2006, the United Nations first enshrined in law the minimum standards required for accessibility [18]. The UK agreed to follow these legal guidelines in 2009. First established in 1999, the World Wide Web Consortium (W3C) has created the Web Content Accessibility Guidelines (WCAG) to promote accessibility within web content. Prior to the most recent revision, WCAG did not include many references to authentication but in 2023 WCAG 2.2 was introduced which addressed this need with a success criterion based on Accessible Authentication [4]. However, the criterion is based on avoiding the need for cognitive tests in authentication. This is useful for some disabled users, such as users with cognitive disabilities, but does not assist other forms of disability as greatly such as visual impairments and disabilities of dexterity. While the field is thought to still be in its infancy [21], there have been many innovations to assist with the authentication needs of users with visual impairments. One such example is BendyPass, a novel form of authentication involving the user remembering a series of bends to input on a given bend device [2]. However, this does have some limitations. The study found that there is lower memorability of bend passwords in comparison to traditional passwords, and the practicality relies on flexible phones being introduced in the future [8]. In the case of users with disabilities of dexterity, there are barriers to many of the stages of authentication. One study [17] interviewed eight users with upper extremity impairment (UEI) to discover the nature of these barriers and the workarounds used to bypass them. They suggested voice print or eye gaze approaches would be good opportunities for this user group. However, it called for more research with disabled users in both of these approaches. The researchers

[4] W3C Web Content Accessibility Guidelines 2.2 - https://w3c.github.io/wcag/guidelines/22 - accessed February 2024

discovered that the participants found assistive technology cumbersome and inconvenient to use. They found that security measures for reaching verification, such as pressing 'ctrl-alt-del', were difficult to use and workarounds were found such as using software to automate these button presses.

In particular, biometric-based credentials were found to have barriers. While participants enjoyed fingerprint and facial recognition for their relative speed and ease of use, it was not always possible to use this as fingerprints and faces can fail to register, which caused participants to avoid enabling authentication entirely. One common workaround for authentication used by people with disabilities when there are usability issues is password-sharing [22]. However, this is an imperfect workaround as the increase in usability comes with a reduction in the level of security. Some approaches have countered this by making password sharing almost impossible, such as with the use of image authentication [6]. While this approach could help reduce the cognitive load, which would help users with cognitive disabilities, it is unlikely to help users with disabilities of dexterity as they must still navigate to and select the chosen image. Users with disabilities of dexterity are also likely to be unable to use some approaches designed for individuals with other disabilities, such as BendyPass. Other innovations have been made in the field of accessible authentication for individuals with disabilities of dexterity. One alternate approach to authenticating the wearable Internet of Things (wIoT) devices often used by people with UEI was the use of an accelerometer and a gyroscope to be mounted on the wIoT device, which then analyses the heart to create ballistocardiograms which are fed into convolutional neural networks to authenticate the user. The downside of this approach is that the equal error rate (EER) increases in the time after training; over the course of two months, the EER increased from 4.02% to 10.02% [16]. Another approach which could be useful for people with UEI is breath authentication. One study [3] explored the use of breathing gestures in authentication. The users found that deep breathing was the best gesture to analyse for this purpose. However, this technique is recommended as a secondary modality in a multimodal system rather than a standalone approach. It is also vulnerable to replay attacks and voice conversion attacks. One advantage this study has over previously mentioned studies is that it does not require future technology or external devices, as it uses the microphone of the smartphone or laptop. It seems from this body of research that the most promising advances are in voice print and eye gaze technology. However, voice print recognition has several limitations such as being susceptible to background noise, being easy to spoof, and the issue that users with severe illness or throat problems can find this method difficult to use [7]. One of the earlier studies in eye gaze interaction [5] emphasised the usefulness of the technique in avoiding shoulder surfing attacks and evaluated three different eye gaze interaction methods for PIN entry; gaze gestures, dwell time method, where the dwell time of the eye on the number designates which button should be pressed, and the look and shoot method, which involves pressing a button while looking at the PIN. The look-and-shoot method may be discounted for the purpose of users with UEI, as many users would be unable to press the button.

The gaze gestures method is promising as it had the lowest error rate, but users found the method to be unintuitive as the gaze gesture alphabet needed to be learned before use. The study also required a "gesture button" to assist with the gestures, thereby making it less useful for users with UEI. Several multimodal approaches have been attempted with gaze-tracking software. One of these is a 2010 study [9] which focuses on eye gaze upon user-selected points on images. This is promising but does not address the need for eye gaze software to function with legacy passwords and PINs. Another study [20] explores augmenting eye gaze with facial gestures, where eye gaze is used to direct the cursor whereas facial gestures are used to perform actions. This shows a clear accessibility increase over the look-and-shoot method but is not primarily designed for authentication and may be unusable for users whose disabilities affect their ability to use facial recognition, such as the participants in the study previously discussed which interviewed users with UEI [17]. The work displayed at this conference in 2018 by Yigitbas et al [23] presented a model-driven UI development approach for cross-device UIs that included the use of Authentication via VisualPin, a method of gaze-based password input where the user gazes at predefined password symbols and found usability difficulties where testers were unsure of how long to look at a UI element, an issue we could then anticipate and counteract with an audible confirmation chime upon successful input. This paper also significantly differs from Yigitbas' approach to gaze-based authentication in that it does not make use of predefined password symbols. Finally, one study [1] discussed the combination of eye gaze with midair hand gestures. This method performed well in the metrics of input time, error rate, perceived workload, and resistance to observation attacks, but is impossible to use for most users with UEI. We have focused on unimodal eye gaze in this study. The advantage of this is that it can integrate with existing backends. An example of this is the gesture eye gaze methods EyePin and EyePassShapes developed to use at banking ATMs with the aid of an inbuilt camera [4]. However, as previously discussed, gaze gestures have an impact on memorability. One review of the topic praises unimodal methods as easy to use while hands-free [12]. This paper differs from similar work in this area by Manu Kumar [14] in that rather than using the gaze to input an alphanumeric password it uses only the PIN system, and also in that it makes use of a wearable technology - the Pupil Labs Core glasses - as opposed to the Tobii 1750 eye tracker that was used in that study. We also particularly focus on designing and evaluating how this technology may be of use to individuals with disabilities of dexterity.

3 System Description

We define a set of requirements for the system based on a combination of the functionality of eye-tracking and the process of inputting a pin on a standard ATM (Automated Teller Machine). These are also used to base success and inform Key performance indicators when testing. Our requirements (presented in a hierarchical MUST - SHOULD - COULD method) are based on a combination

of the literature and expert requirements from accessibility evaluator communications as an initial starting set.

Must

1. Be able to input their PIN using the solution.
2. Be able to connect to the eye-tracking hardware.
3. Be able to collect data from the hardware.
4. Support calibration of the eye-tracking system.
5. Securely store and process the PIN.

Should

1. Be able to input their PIN entirely hands-free.
2. Provide a reliable means of user authentication, minimizing false positives and negatives.
3. Be compatible with a variety of devices and platforms.

Could

1. Receive feedback to let them know about the status of the input method during operation.
2. Integrate with eye biometric data for enhanced security.
3. Support gaze gestures for common tasks (e.g, cancel, submit)

Based on the requirements we built our eye-tracking prototype testing system. We utilized a Pupil Labs w120 e200b binocular eye tracking headset fitted with nose support, two eye cameras, and a world camera connected to the system with USB 3.0. Data recording was achieved using the software Pupil Capture v3.5.1 and the plugins 'Fixation Detector', 'Network API', and 'Surface Tracker' for said software, all with their default settings. For surface detection, it makes use of the AprilTag [19]; specifically, the tag36h11 family of markers. These tags are to be placed in each corner of the display and we are aware of a limitation which is that the apparatus must be located in a well-lit environment for optimal results (See Figure 1).

The prototype relies on the use of the Pupil eye-tracking glasses (See Figure 2) to receive gaze fixation data. To do this, the glasses must be set up properly. This is best done in the Pupil Capture software, as it displays what the cameras currently can see, and involves physically adjusting the cameras using the sliding camera arm and ball joint to ensure a good image of the eyes is captured. The world camera can also be angled up and down to align with the user's field of vision.

We make use of the ZeroMQ messaging library to establish a connection to the glasses and subscribe to the 'surfaces' publisher to retrieve gaze data that is related to any surface currently visible with the world camera. The Pupil network API returns information in the 'Surface datum format', an example of which is in the figure below [5]. We are particularly interested in the "fixations_on_surfaces"

[5] Pupil Labs Core Developer Overview - https://docs.pupil-labs.com/developer/core/overview/surface-datum-format - accessed February 2024

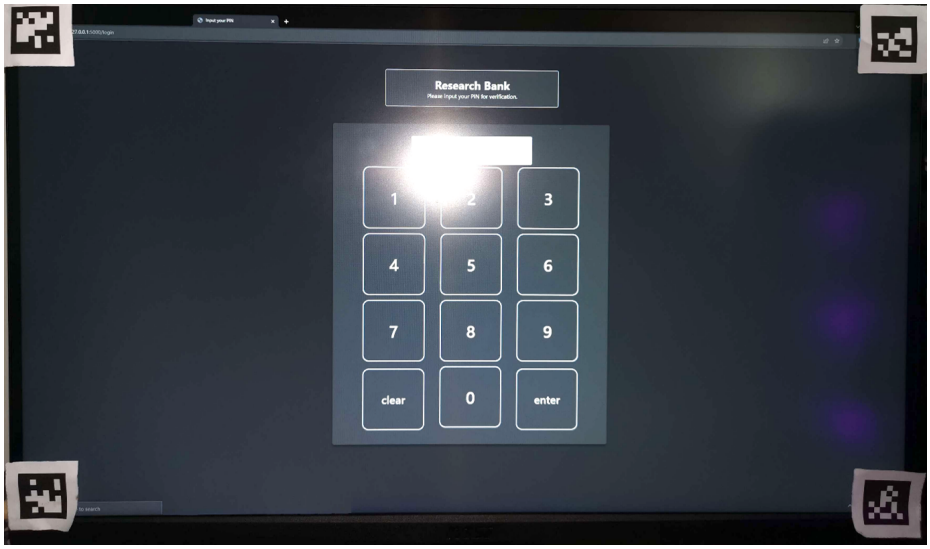

Fig. 1. Tag markers placed on the four corners for more accurate eye-tracking gaze data

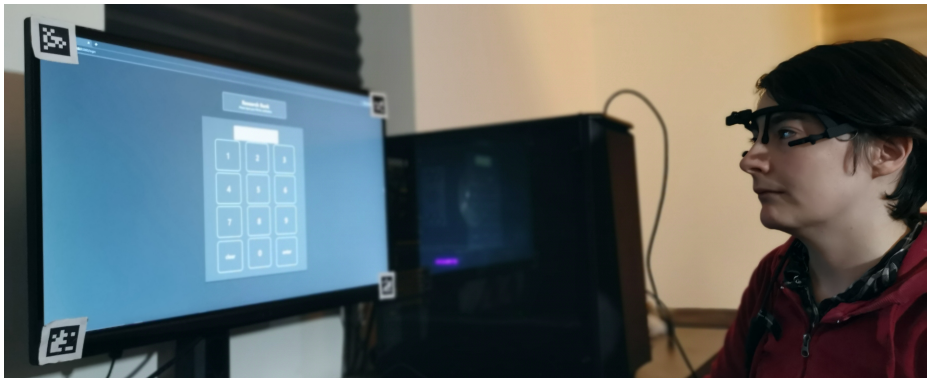

Fig. 2. A Pilot Tester Using the Pupil Glasses to Enter a Pin Code

data, which contains the "confidence" and "norm_pos" fields. The "confidence" data is a percentage rating on how confident Pupil Capture is with the position. For this prototype, we discounted any fixation with a confidence that was not 100% to maintain accuracy during input. The "norm_pos" data is an X,Y normalized position corresponding to where on the surface the user is currently looking. This is delivered as a percentage ranging from 0 to 1, with percentage (0,0) being the bottom left corner of the surface and percentage (1,1) being top right. These normalized coordinates must be processed by the software to approximate where on the screen the user's gaze is fixed. Our code [6] detects the screen size of the operating device and computes where on the screen the given normalized coordinates correspond. This code makes use of the ZeroMQ messaging library to establish a connection to the glasses and subscribes to the 'surfaces' publisher to retrieve gaze data that is related to any surface currently visible with the world camera. The prototype and all related tests were confirmed to work on a Microsoft Windows 10 computer running Build 19045 with the following hardware. Due to the use of the ctypes module, the prototype will not work on an Apple device as it will be unable to detect the screen size of the device. It requires Python version 3.7.9 or above. We utilized bcrypt to hash PINs prior to storing. The PIN was generated randomly with the Python random.randint function and then passed to bcrypt. bcrypt also generates a random salt with a work factor of 12 (212 iterations) with the gensalt function, then hashes the PIN. The prototype also utilises the bcrypt function checkpw to authenticate, by hashing the user input pin from the keypad with the salt stored in the hash and comparing the computed hash with the stored one. The Process diagram of the high-level functionality and interaction can be seen in Figure 3.

4 Initial Testing and Findings

For our initial pilot user tests, seven participants were recruited voluntarily. This project received a favorable ethical opinion from the - ANON - Research Ethics Committee per SREC reference COMSC/Ethics/2023/083. Participants attended a test session where they were asked to input a randomly generated PIN in two conditions – the traditional input condition using a mouse and keyboard and the alternate input condition using gaze tracking glasses. Prior to the beginning of the gaze prototype test, users had to wear the Pupil glasses, which required some time to adjust the camera positioning per individual. Participants were timed and notes about the experience were made to identify areas of difficulty or ease, and the researcher attempted to observe the participants' actions to try and discover what had been input. Participants were aware of their observation in this manner. At the end of each of these conditions they were directed to a web-based survey to answer questions evaluating the input method in terms of accessibility, ease of use, and adaptability through a Likert 1 – 5 rankings, with the opportunity present to expand on their ranking. All participant information was anonymized at the time of submission.

[6] can be shared on request

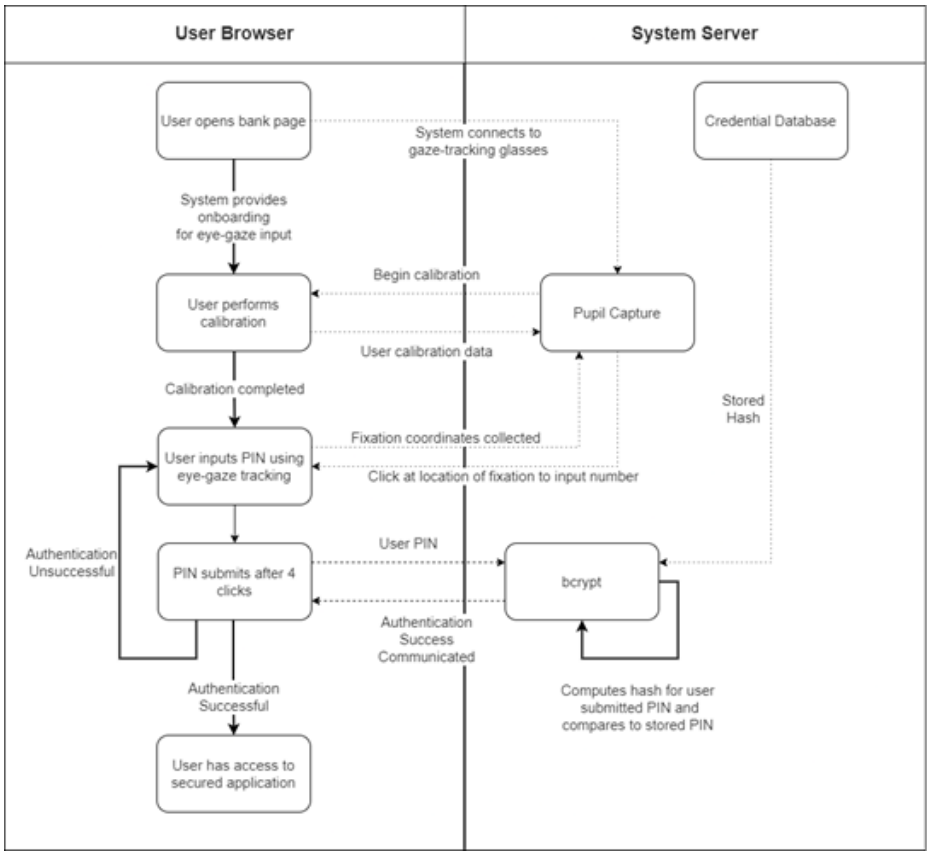

Fig. 3. Process Diagram of the Prototype

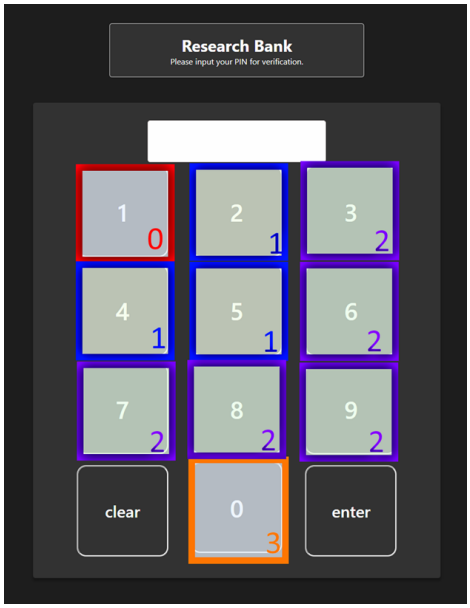

Fig. 4. PIN entry test

To evaluate the success of the over-the-shoulder attack performed by the researcher, a scoring system was created to compare the digits the researcher suspected were correct and the digits of the actual PIN (See Figure 4). Where an observed digit matched the similarly placed digit of the actual PIN, a score of 0 was given. Where the observed digit was incorrect, the guessed digit was given an incremental score based on its adjacency to the actual digit to indicate the reduction in search-space entropy were someone to attempt to brute force the PIN – for example, knowing that the digit is within the top left region (numbers 1,2,4,5) is a reduction of over 50% of candidates, and so a score of 1 for such a guess indicates that the guess is a significant reduction in security compared to a wholly unknown digit. As such, a lower 'PIN proximity score' (PPS) indicates a more successful attempt at the over-the-shoulder attack. There is some variability in this scoring system, as 3 points could only be awarded when a digit was in the top or bottom rows of the keypad. To accommodate this, we used a scaling system that calculated what percentage a score was out of the maximum available, where a lower percentage represented a more accurate attack attempt.

4.1 Condition 1: Traditional Input

In the traditional input condition, all participants used the mouse rather than the keyboard and reported that they very quickly understood how to input their PIN thanks to the recognizable input system of a keypad. All participants also

gave the highest score for how quickly they could input their PIN and how easy it was to do so with most stating this was related to their regular use of a mouse as an input device. Most participants reported that they understood how to input their PIN with this method quickly or very quickly. They stated that the operation was intuitive and that the explanation was effective. One participant gave a lower score for understanding, stating that the "explanation given was okay, but I didn't understand fully until calibrating". Most participants also reported that this input device was maximally comfortable for their use, although two participants gave slightly lower scores, with one finding the mouse too big for their hands and the other finding this input modality less comfortable than using a touchscreen. Participants also identified multiple limitations of this input method. Most participants considered the operation of the mouse; that it required a suitable flat surface, that its wire could get tangled, that it was slower than a touchscreen; while one participant considered that it was wholly limited by the ability to make use of the mouse. The participants took an average of 2.702 seconds to input their PIN, with the longest taking 5.043 seconds due to a need to repeat their input after an incorrect entry. The average PPS was 25.77% with scores ranging from 0%, where the researcher successfully completed the over-the-shoulder attack and could fully observe the user PIN, to 66.67%. The results from the first condition suggest that the design of the website was a suitable analog for an ATM machine, as no participants reported confusion on how to operate the site or input their PIN. The high scores given for speed and ease of inputting their PIN indicates that this group of participants found no difficulties in the operation of a mouse, which is an input method that relies on high hand and wrist dexterity. This is also supported by the time taken for users to input their PIN, with 4 participants taking under 2 seconds to input their pin, suggesting this is an efficient method of operation when undertaken by familiar and able individuals. The results from the over-the-shoulder attack suggests that this input method is quite susceptible to this attack. It was notably easier to identify the PINs of the users with longer input times compared to those without, with the longest three times at most being only one point away from the correct PIN. This suggests that an extended interaction time while inputting the PIN increases the vulnerability of the user to an over-the-shoulder attack when input with this method. Overall, these results indicate that the participants had no difficulties identifying what they were supposed to do to input their PIN and so the website served as an appropriate ATM analog. The results also suggest that the participants were comfortable inputting their PIN with this input modality, though its resilience to over-the-shoulder attacks is considerably lacking. Input in this manner appears to be comfortable, though the variability of hand size and mouse design gives a degree of variability to this comfort.

4.2 Condition 2 - Prototype Input

In the prototype input condition, most participants reported that they understood how to input their PIN with this method quickly or very quickly. They stated that the operation was intuitive and that the explanation was effective.

One participant gave a lower score for understanding, stating that the "explanation given was okay, but I didn't understand fully until calibrating". When asked how quickly they could input their PIN using this input method, participants gave an average score of 2.8, ranging from 2 to 4. When asked how easy it was to input their PIN, they gave an average score of 3.5, ranging from 2 to 5. The most common reason given for this was that it took a long time to input each digit. One participant also stated that it was unclear whether they were successfully inputting their PIN at first, though this changed when they heard the 'click' to confirm input. When asked how comfortable the input method was, participants gave an average score of 3.14, ranging from 2 to 5. Most participants stated that the headset was comfortable, but a major complaint was the time taken to input each digit. Other notable complaints were given by participant 5, who reported that the time taken to adjust the headset to track their eyes appropriately would be uncomfortable if they had to make use of the device multiple times a day, and participant 3 who experienced a particularly lengthy calibration period. Participants identified several limitations of this input method, mentioning the extended input time, sensitivity to head movement, the need for very precise camera placement, and the need for adequate lighting. Two participants also mentioned the limitations of the glasses themselves, stating that the perceived price of the glasses was a limitation and that they felt they would be unsafe wearing the glasses outside because of the mounted camera. The participants took an average of 52.336 seconds to input their PIN, ranging from 41.329 seconds to 71.460 seconds. The average PPS was 66.52%, with scores ranging from 50% to 88.89%. The individual results are presented in the figure below. The results from the second condition survey suggest that while the design of the website was a suitable analog for an ATM, participants reported confusion on how to operate the site. The lower scores given for speed and ease of inputting their PIN compared to the first condition indicate that this input method is more time-consuming than the operation of a mouse. This is also supported by the time taken for users to input their PIN, with one participant taking over a minute, which is a significant increase in authentication time. This may suggest that the prototype is not very competitive in terms of authentication efficiency compared to using a mouse for this group of participants. The results also suggest that the participants were much less comfortable inputting their PIN with this input modality than with the mouse due to the extended time it could take per digit. Participant 5 particularly identified issues during the setup of the eye-tracking glasses which were believed to be due to their hooded eyes. The results from the over-the-shoulder attack suggest that this input method is significantly less susceptible to this attack than in the first condition. It was notably harder to identify the PINs of the users due to the significantly reduced scope of visible movement, especially from behind. The primary indicator for movement became slight adjustments in head tilt and skew which were very subtle when evident. Significantly, no participant's PIN was successfully recovered, with the best score being 50% with participant 4. This suggests that this input method has significantly reduced vulnerability to over-the-shoulder attacks. Overall, these results

indicate that the participants had no difficulties identifying what they were supposed to do to input their PIN and so the website served as an appropriate ATM analog. However, the results also suggest that the participants were much less comfortable inputting their PIN with this input modality than with a mouse. The improvements to the PPS score between conditions suggest that the prototype is more resilient against over-the-shoulder attacks than mouse input. The necessity for a setup and calibration were also reported issues with this input method that were not necessary in the prior condition.

5 Conclusions and Future Work

This paper presents the initial stage of work to investigate the efficacy of a more secure way of inputting a PIN number for individuals with dexterity disabilities and limitations. We present a fully operational bespoke eye-tracking solution prototype with custom software. We test the prototype in a pilot test to test for the usability compared to a traditional input system, and the effects of an over-the-shoulder attack with promising results and feedback from the participants. Our system showed promising results and favorable feedback usability-wise from our participants. Currently, our participants were not suffering from any dexterity issues. In future, we aim to expand the test to persons with severe dexterity disabilities to verify further the ecological and external validity of our findings. We are currently building a framework to direct the development of similar systems. We also aim to expand our work to utilize biometric identification of users thus removing the need to insert a bank card for a truly hands-free authentication experience – particularly the use of pupillary biometrics given the technologies utilized in the scope of this project could potentially provide this information.

References

1. Abdrabou, Y., Khamis, M., Eisa, R. M., Ismail, S., and Elmougy, A. Just gaze and wave: Exploring the use of gaze and gestures for shoulder-surfing resilient authentication. In *Proceedings of the 11th acm symposium on eye tracking research & applications* (2019), pp. 1–10.
2. Briotto Faustino, D., and Girouard, A. Bend passwords on bendypass: a user authentication method for people with vision impairment. In *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility* (2018), pp. 435–437.
3. Chauhan, J., Hu, Y., Seneviratne, S., Misra, A., Seneviratne, A., and Lee, Y. Breathprint: Breathing acoustics-based user authentication. In *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services* (2017), pp. 278–291.
4. De Luca, A., Denzel, M., and Hussmann, H. Look into my eyes! can you guess my password? In *Proceedings of the 5th Symposium on Usable Privacy and Security* (2009), pp. 1–12.
5. De Luca, A., Weiss, R., and Drewes, H. 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 (2007), pp. 199–202.
6. Dhamija, R., and Perrig, A. Deja {Vu–A} user study: Using images for authentication. In *9th USENIX Security Symposium (USENIX Security 00)* (2000).
7. Fatima, K., Nawaz, S., and Mehrban, S. Biometric authentication in health care sector: A survey. In *2019 International Conference on Innovative Computing (ICIC)* (2019), IEEE, pp. 1–10.
8. Faustino, D. B., Nabil, S., and Girouard, A. Bend or pin: studying bend password authentication with people with vision impairment. In *Graphics Interface 2020* (2019).
9. Forget, A., Chiasson, S., and Biddle, R. Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2010), pp. 1107–1110.
10. Furnell, S., Helkala, K., and Woods, N. Accessible authentication: Assessing the applicability for users with disabilities. *Computers Security 113* (2022), 102561.
11. Helkala, K. Disabilities and authentication methods: Usability and security. In *2012 Seventh International Conference on Availability, Reliability and Security* (2012), pp. 327–334.
12. Katsini, C., Abdrabou, Y., Raptis, G. E., Khamis, M., and Alt, F. The role of eye gaze in security and privacy applications: Survey and future hci research directions. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (2020), pp. 1–21.
13. Kelly, N., and Petrie, H. Digital authentication and dyslexia: A survey of the problems and needs of dyslexia people. In *International Conference on Computers Helping People with Special Needs* (2022), Springer, pp. 18–25.
14. Kumar, M., Garfinkel, T., Boneh, D., and Winograd, T. Reducing shoulder-surfing by using gaze-based password entry. In *Proceedings of the 3rd symposium on Usable privacy and security* (2007), pp. 13–19.
15. Lewis, B., Hebert, J., Venkatasubramanian, K., Provost, M., and Charlebois, K. A new authentication approach for people with upper extremity impairment. In *2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* (2020), pp. 1–6.
16. Lewis, B., Hebert, J., Venkatasubramanian, K., Provost, M., and Charlebois, K. A new authentication approach for people with upper extremity impairment. In *2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* (2020), IEEE, pp. 1–6.
17. Lewis, B., and Venkatasubramanian, K. "i... got my nose-print. but it wasn't accurate": How people with upper extremity impairment authenticate on their personal computing devices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (2021), pp. 1–14.
18. MacKay, D. The united nations convention on the rights of persons with disabilities. *Syracuse J. Int'l L. & Com. 34* (2006), 323.
19. Olson, E. Apriltag: A robust and flexible visual fiducial system. In *2011 IEEE international conference on robotics and automation* (2011), IEEE, pp. 3400–3407.
20. Rozado, D., Niu, J., and Lochner, M. Fast human-computer interaction by combining gaze pointing and face gestures. *ACM Transactions on Accessible Computing (TACCESS) 10*, 3 (2017), 1–18.
21. Saxena, N., and Watt, J. H. Authentication technologies for the blind or visually impaired. In *Proceedings of the USENIX Workshop on Hot Topics in Security (HotSec)* (2009), vol. 9, p. 130.

22. Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G., and Furlong, M. Password sharing: implications for security design based on social practice. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (2007), pp. 895–904.
23. Yigitbas, E., Anjorin, A., Jovanovikj, I., Kern, T., Sauer, S., and Engels, G. Usability evaluation of model-driven cross-device web user interfaces. In *Human-Centered Software Engineering: 7th IFIP WG 13.2 International Working Conference, HCSE 2018, Sophia Antipolis, France, September 3–5, 2018, Revised Selected Papers 7* (2019), Springer, pp. 231–247.