A New Authentication Approach for People with Upper Extremity Impairment

Brittany Lewis*
Computer Science and Statistics
The University of Rhode Island
Kingston, USA
bflewis@uri.edu

Joshua Hebert
Computer Science
Worcester Polytechnic Institute
Worcester, USA
jahebert@wpi.edu

Krishna Venkatasubramanian*
Computer Science and Statistics
The University of Rhode Island
Kingston, USA
krish@uri.edu

Matthew Provost
TechAccess of Rhode Island
Cranston, USA
matthewp@techaccess-ri.org

Kelly Charlebois
TechAccess of Rhode Island
Cranston, USA
kellyc@techaccess-ri.org

***Abstract*—In recent years, people with upper extremity impairment (UEI) have been using wearable Internet of Things (wIoT) devices like head-mounted devices (HMDs) for a variety of purposes such as rehabilitation, assistive technology, and gaming. Often such wIoT devices collect and display sensitive information such as information related to medical care and rehabilitation. It is therefore crucial that HMDs can authenticate the person wearing them so that appropriate access control can be implemented for the sensitive information they manage. In this paper, we *explore a new authentication approach* for people with upper extremity impairment (UEI) for wIoT devices head-mounted devices (HMDs). The approach works by leveraging *ballistocardiograms* – representations of the cardiac rhythm – derived from an accelerometer and a gyroscope, mounted on an HMD for authentication. The derived ballistocardiograms are then fed into six *participant-specific* convolutional neural networks (CNNs) which act as our authentication models. Analysis of our approach shows its viability. Using data from 6 participants with UEI (and 22 able-bodied participants, for evaluation), we show that we can authenticate a participant in 4 seconds with an average equal error rate of 4.02% and 10.02%, immediately after training and ∼2 months later, respectively.**

***Index Terms*—authentication, biometrics, internet of things, wearable computers, assistive technology**

I. Introduction

In recent years, **wearable Internet-of-Things (wIoT)** devices such as head-mounted devices (HMDs) – i.e., augmented reality (AR) devices, and virtual reality (VR) devices — have become increasingly useful for people with **upper extremity impairment (UEI)** as an assistive technology [1]–[3], for gaming [4], and for rehabilitation [5], [6]. A person with UEI is someone who lacks range of motion, strength, endurance, speed, and/or accuracy associated with movement in the shoulders, upper arms, forearms, hands, and/or fingers [7]. As people with UEI use these wIoT for increasingly personalized tasks, being able to authenticate a person with UEI to their HMDs is becoming increasingly important. This is because people with UEI often must rely on caregivers (e.g., family, friends, staff in a group home) to help them with day-to-day activities, including the setup of their computing devices such as HMDs. People with disabilities are disproportionally affected by crime, including theft and burglary, often perpetrated by people who are their caregivers [8]. Caregiver crimes against people with disabilities include the theft and misuse of personal computing devices [9], which can lead to terrible consequences, including the loss of sensitive data. Authentication solutions on HMDs can help alleviate such threats for a vulnerable population group.

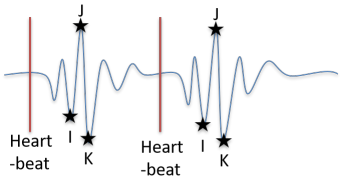


Fig. 1: A typical ballistocardiogram (BCG) waveform produced as a reaction to the beating of the heart. Note the characteristic I, J, and K peaks of the signal.

Our *goal* in this paper is to explore an authentication approach for HMDs that is specifically designed for people with UEI. Given the nature of the disability of people with UEI, we have designed an authentication approach that does not require any explicit action from the individual. All our approach requires is for an individual with UEI to wear the HMD and *sit still for a short period of time* to authenticate. Our approach works by collecting the subtle, natural movements of the head that occur while a person is sitting still using an accelerometer and gyroscope on the HMD. We use these measurements to derive a **ballistocardiogram (BCG)**. A BCG represents the body's motion as the blood flows through it, in response to the beating of the heart, and thus captures the characteristics of the cardiac process [10]. Figure 1 shows a typical BCG waveform with its characteristic peaks

* The bulk of this work was completed while the first and third authors were at Worcester Polytechnic Institute

usually referred to as I, J, and K peaks. A BCG waveform, due to its nature, appears after every rhythmic contraction of the heart muscle (heartbeat) [10]. Using the BCG we train participant-specific (i.e., personalized) convolutional neural networks (CNNs) which act as the authentication model in our approach. Once the model is trained, we can once again measure new accelerometer and gyroscope measurements from the HMD, derive a BCG from it, and use it to authenticate an individual.

Our approach has several *advantages:* (1) it does not require the individual with UEI wearing the HMD to use their limbs in any form; (2) it uses ubiquitous movement sensors rather than relatively rarer physiological signals/interconnects to work; and (3) the head-movements it uses for authentication are difficult for an adversary to copy as they are subtle.

To the best of our knowledge, HMD authentication has not been explored for the UEI population before. An analysis of our approach shows its viability. We used data from 6 participants with UEI (non-spastic cerebral palsy) and 22 other able-bodied participants to train six individual authentication models and to simulate adversarial attacks. We were able to authenticate an individual with UEI in 4 seconds with an average equal error rate[1] of 4.02% immediately after training and 10.02% after about two months.

The **contributions** of this paper are two-fold: (a) a novel authentication approach for people with UEI for HMDs using ballistocardiograms derived from subtle and involuntary head movements, and (b) a demonstration of the viability of this authentication approach.

II. Related Work

HMD Authentication: Authentication approaches have been previously explored for HMDs. Li et al. [11] use simple head movements in response to a specific song for authentication. The head movements used, however, can be easily imitated by adversaries who are able to observe the head patterns. Schneegass et al. [12] induce white noise into participants' skulls through the bone conduction speakers of an HMD. The response is then measured to identify the wearer. This is more effective at imitation attack resistance, but requires bone conductance speakers, which not all HMDs possess. Further, the white noise was found by the authors to be uncomfortable to some participants. Rogers et al. [13] present a user identification approach using blinking and head movement patterns of the participant while they watch a video. However, this approach requires 34 seconds for identification, presenting a temporal barrier to usefulness. Further, none of these approaches have been focused on the context of people with UEI.

Authentication for People with Disabilities: Recent years have seen the development of several authentication solutions specifically designed for people with disabilities. However, most authentication work has focused on people with visual impairments [14]–[19] or people with cognitive disabilities (e.g., Down syndrome) [20], [21]. Very few solutions have been proposed or designed for the needs of people with UEI. Solutions for people with UEI often focus on voice traits [22] or password dictation [23], [24] which can present barriers for people with UEI who often have co-morbid voice/speech impairments [25] – something we wish to avoid in this work.

Authentication using Ballistocardiography: Ballistocardiography has been tried for user identification on previous occasions [26]–[28]. In Guo et al. and Vural et al. [26], [28], ballistocardiography was used on movement sensors on an individual's torso. In the context of our work, however, this would require the use of an additional device to measure BCGs to authenticate into an HMD, which we would like to minimize given the ability of most HMDs to measure movement themselves. In Hernandez et al. [27], the authors measured BCGs using a smart-watch; however, owing to the distance from the person's heart, the signals produced were noisy and produced only 66% accuracy rate, which is rather low. Further, none of these previous works were evaluated using people with UEI or over time (as we shall see later in the paper).

III. Problem Statement and Threat Model

Before we delve into our authentication approach, we detail our problem statement, threat model, and assumptions about the adversaries that underlie this work.

Problem statement: The main problem that we address in this paper is to determine if ballistocardiograms derived from subtle head movements of an individual with UEI using an HMD is capable of authenticating them to that HMD.

In this work, we use a Google Glass as the HMD device. The principal reasons for choosing Google Glass are that it: (1) is used as head-mounted device by people with UEI [1], [2], and (2) has the accelerometer and gyroscope sensors that we need to implement our approach. *Our approach is not specific to Google Glass.*

Imitation attack threat: People with UEI often require caregivers (e.g., family, friends, staff in a group home) to help with routine daily activities, including assisting with computing [29]. Unfortunately, this has often led to the theft and unauthorized access of personal computing devices by caregivers [9]. Consequently, we assume that the principal adversaries to our authentication approach are malicious caregivers, having intimate access to a particular individual with UEI. These adversaries can observe the individual with UEI and have access to their computing devices and HMD. Since our approach involves no overt gestures/actions, that is, the individual sits still for authentication, we assume the adversaries can only perform *imitation attacks* where they try to imitate (mimic) the individual's subtle head movements by sitting still while wearing their HMD.

Adversarial assumptions: For the purposes of this work, we assume that adversaries: (1) do not have access to the authentication model; (2) are not present for the training phase and cannot pollute the model during this stage; (3) do not have any cardiac signals from the individual with UEI, past

[1]The point at which the false accept and false reject rates are equal.

TABLE I: Demographics of participants

Set	Avg. Age	SD Age	Male	Female
Model	40	11.06	3	3
Validation	32.83	13.13	4	8
Impersonation	28.50	10.91	8	2
All	**32.82**	**12.06**	**15**	**13**

or present; and (4) access the HMD surreptitiously without forcing the HMD to be unlocked through intimidation or violence.

IV. Data Collection

The first stage in our authentication approach is to collect head movement data from participants. We obtained approval from our institution's institutional review board (IRB) and collaborated with a local non-profit organization to obtain the data. We asked each participant to remove their glasses, if applicable, and sit comfortably, upright, and still. We then situated an HMD on their face such that it fit comfortably. We then collected 10 minutes of accelerometer and gyroscope data from each participant, per session. In order to minimize fatigue, we collected the data in five 2-minute intervals, with ample breaks between intervals. We collected *two sessions* of HMD data measurements from our participants to measure the *effectiveness* of our authentication approach after a couple of months. The second session was conducted anywhere from 15 to 57 days after the first session depending on the availability of our participants.

We collect and divide data into 3 sets: model set, validation set, and impersonation set. The **model set** consists of data from 6 participants with UEI, specifically non-spastic cerebral palsy, for whom we build our participant-specific authentication models. The **validation set** consists of data from 12 able-bodied individuals and is used to train the authentication models and to test against imitation attacks from a generic version of our adversary. Finally, the **impersonation set** consists of data from 10 able-bodied participants whose data have not been seen by the authentication models during training and is used to simulate imitation attacks by an unseen adversary. The impersonation set is used to evaluate the generalizability of our models. This is a common approach that is used to evaluate authentication models [30]. The demographic breakdown of these sets is in Table I.

Data Preprocessing: During data collection, the accelerometer and gyroscope sensors in the HMD are set to sample at 50 Hz (as recommended in the Google Glass API [31]). We obtain six discrete, *raw sensor streams*: the three axes of the accelerometer and three axes of the gyroscope measurements. Sensor data from any Android device, like our HMD Google Glass, are not guaranteed to align exactly to a sampling rate nor will measurements from different sensors necessarily be synchronized. Therefore, we preprocess the sensor streams. We truncate the beginnings and endings of both the gyroscope and accelerometer measurements, such that the timestamp of the first and last samples of both sensor measurements are as close as possible. We then interpolate the data and align the samples with one another.

TABLE II: Maximum of the average of $(TAR+TRR)/2$ for various segment lengths. Based on these results, $w = 4$ was chosen.

w	2s	3s	4s	5s
	92.73%	95.77%	**97.5%**	96.63%

Deriving the BCG Waveform: Once we obtain the preprocessed sensor streams, we use them to derive the BCG waveform. To do this, we divide each stream into overlapped *segments* of size w seconds. Between two sequential segments, there is a $w-1$ second overlap. Hence, two segments with $w = 4$ seconds would share 3 seconds of data. Then, inspired by [27], we perform a three-step BCG derivation process. (1) *Normalization:* We normalize each of the six sensor streams to have a zero mean and unit variance within each segment. (2) *Rolling Average Filter:* We then subtract a rolling-average filter of 35 samples from each sensor stream to correct for large motions as well as gyroscope and accelerometer drift. (3) *Band-Pass Filter:* Finally, we apply a 4th-order band-pass Butterworth filter with cutoff frequencies at 4 and 11Hz to each sensor stream. In all, we derive six versions of BCG, one per axis of accelerometer and gyroscope, *per segment*. These six BCGs are used as input for our authentication model.

Once the BCGs have been extracted, we derive six participant-specific two-class convolutional neural networks (CNNs), each acting as an authentication model for one of the six individuals with UEI in our dataset. We use CNNs to avoid complex feature engineering.

V. Model Training and Authentication

We now describe how the individual CNNs, used as our authentication models, are parametrized and trained. However, before we go into the details, we provide quick descriptions of the metrics we use in our CNN setup and the eventual evaluation of the authentication accuracy.

Metrics: To evaluate the efficacy of our approach, we use the following core metrics: *true accept rate* (TAR), *false accept rate* (FAR), area-under-the-curve (AUC), and *equal error rate* (EER). These metrics were chosen because they are common metrics used for evaluating authentication models and they balance permitting correct users with preventing attackers from receiving access. TAR is the fraction of positively labeled test BCGs that were correctly classified as positive and represent providing access to the user. FAR is the fraction of negatively labeled test BCGs that were misclassified as positive, representing an attacker being mistakenly allowed access. For our results we plot *receiver operator characteristic (ROC)* curves which graph TAR vs. FAR at various operating points for our authentication models. ROC curves are a compact way of showing model performance. The area-under-the-curve (AUC) gives a measurement for describing the overall performance of the ROC curve. Given TAR and FAR, we can easily compute the complementary metrics of false reject rate (FRR) as $FRR = 1 - TAR$, and true reject rate (TRR) as $TRR = 1 - FAR$. EER is the equilibrium point where the total error $(FAR + FRR)$ is minimized.

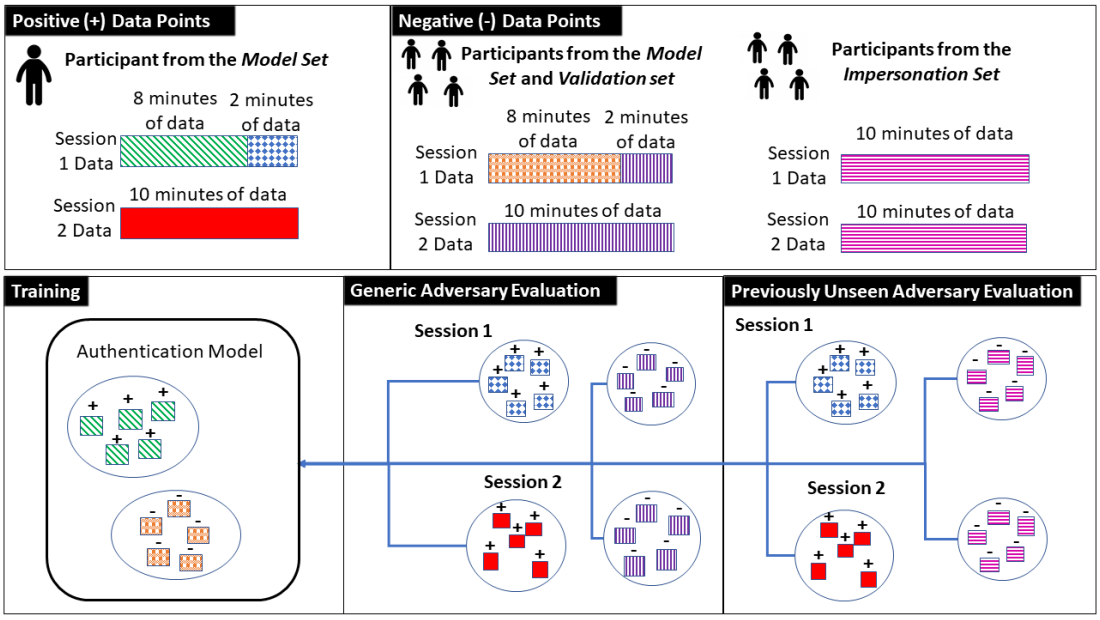


Fig. 2: Representation of how data from both sessions of our model set, validation set, and impersonation set are used for training and evaluation.

CNN Parameter Selection: We start with a base CNN model with 5 convolutional layers followed by 2 dense layers and an output layer. The output layer is a single neuron that produces a binary decision. For clarity and space reasons, we show our base CNN on our website[2]. The goal is to parametrize this CNN in a participant-specific manner so that it can authenticate our target population. We do this as follows. We have 2 sessions of data from the participants in the model set[3], validation set, and impersonation set. To build a custom CNN for each of the 6 participants in the model set, we use a *genetic algorithm-based method* to find the hyper-parameters of our CNN-based authentication model. This is because enumerating all possible values of these hyper-parameters and determining the best CNN configuration is prohibitively expensive. We optimize over 30 hyper-parameters that capture elements associated with convolutional and dense layers in the network. We use the first 8 minutes from session 1 of our model set and validation set (which forms the generic adversary) to train the models and the remaining 2 minutes of session 1 to test the model, for each generation of the genetic algorithm. Each generation is composed of 20 CNN configurations.

Previously, we had stated that we used (w) seconds of overlapping segments to generate the BCG waveforms. We determine the value of w simultaneously with determining the CNN hyper-parameters. We do this by running the genetic algorithm for 5 generations for segment lengths from w=2 seconds to w=5 seconds. This range was chosen as segments of less than 2 seconds may not be long enough to capture an entire cardiac rhythm if a person's resting heart rate is below 60 bpm, and longer segment times decrease usability. We then determine the maximum value of $(TAR+TRR)/2$ for each participant, over all 5 generations for a given segment length. We then compute the average of this maximum value (over our 6 participants) and choose the segment length that produced the maximum average. Table II shows the maximum of average $(TAR+TRR)/2$ observed for different segment lengths. Based on these results, we chose w=4 seconds. We input BCGs, derived from each segment of sensor measurements, into the CNN. Hence, the segment length determines how quickly we can authenticate a person. *A w=4 seconds, therefore, means we need only 4 seconds of movement sensor measurements to authenticate someone.*

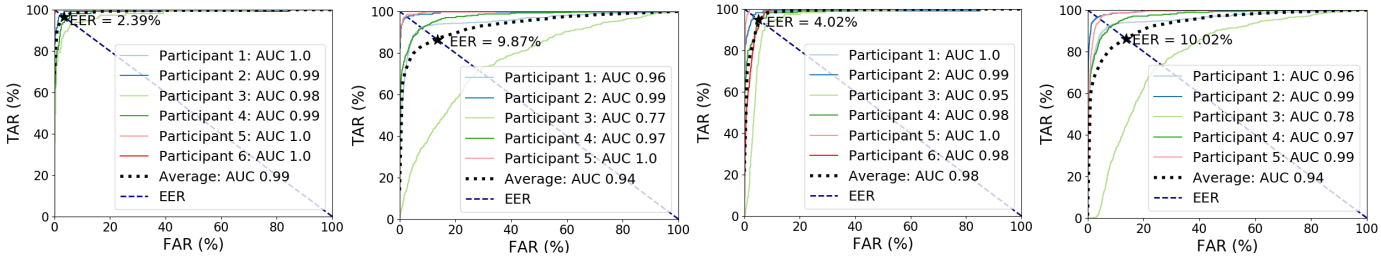
Once the segment length is chosen, we run the genetic algorithm for w=4 seconds for another 5 generations for a total of 10 generations. For each participant we pick the CNN hyper-parameters that produce the maximum value of $(TAR+TRR)/2$ in those 10 generations. For clarity reasons the CNNs, trained for the 6 participants in our study, are posted on our website[4].

Training and Authentication: Once we have the hyper-parameters, we train a participant-specific two-class CNN as the authentication model for each of the 6 participants in our model set. We use the participant's first 8 minutes of data from session 1 as positive class points and the first 8 minutes of data from both the other 5 participants in the model set and the 12 participants from the validation set as negative points and weight our model for the class imbalance. The usage of our data for training and evaluation can be seen in Figure 2. In the figure, positive and negative data points are marked with

[2]https://anonymoussubmissionuser.github.io/CNNs/

[3]We were able to collect only 1 session's worth of data for participant 6 in the model set.

[4]https://anonymoussubmissionuser.github.io/CNNs/



(a) Generic Adversary Session 1 (b) Generic Adversary Session 2 (c) Unseen Adversary Session 1 (d) Unseen Adversary Session 2

Fig. 3: Performance of our authentication approach

"+" and "-" symbols respectively. We train the CNN for 100 epochs, at which point the training loss of the model stabilizes to a minimum. Once the model is trained, we can authenticate an individual with UEI, by supplying their CNN with BCG waveforms obtained from a new (yet unseen) snippet for w=4 seconds of accelerometer and gyroscope measurements obtained from the HMD sensors. The CNN produces a binary decision, which can be evaluated for accuracy.

A. Performance under imitation attacks

Generic Adversary: As a first step in evaluating our models, we evaluate how well our six authentication models can differentiate a given participant from all the other participants in the *model set and the validation set*. The model set and validation set are used as a *reference for characterizing a generic adversary* for our authentication models. We perform our evaluations over two sessions using the unseen data from the last two minutes in session 1, and the full 10 minutes of unseen data collected for session 2. For our adversarial data, we treat the session 1 and session 2 data the same because these data do not have any temporal significance in relation to the positive data (i.e., the adversary can use data collected at any time to attack the authentication process).This process is detailed in the *Generic Adversary Evaluation* box in Figure 2. Figure 3 (a) and (b) show the ROC curves for the 6 trained models for session 1 and session 2 for the generic adversary, respectively. In session 1, the ROC curves show that the authentication models are accurate with average area-under-the-curve (AUC) values greater than 0.99. The average AUC drops to 0.94 in session 2. The EER shows an increase starting at 2.39% in session 1, and then increases to around 9.87% in session 2. We observe that the change in performance is largely due to Participant 3's data (whose AUC is 0.77). The reason Participant 3's data performed poorly is because they had relatively poor control of their neck muscles and could not sit still for sustained periods of time.

Previously Unseen Adversary: In practice, reference data for each potential attacker are not generally available. Therefore, we use data from both sessions of the *impersonation set* as negative data to evaluate our six authentication models. This process is detailed in the *Previously Unseen Adversary Evaluation* box in Figure 2. This simulates the actions of the primary adversary of our threat model, someone who views a participant authenticating and tries to mimic them. As the victim exhibits only subtle movements and no overt gestures during authentication, the adversary has nothing to copy and is reduced to using their own head movements. Figure 3 (c) and (d) show the ROC curves for the 6 trained models for session 1 and session 2 for the previously unseen adversary, respectively. The TAR is obtained using participants' unseen data as described earlier. The ROC curves for the 6 trained models have an average AUC that goes from 0.98 to 0.94 from session 1 to session 2, respectively (see Figure 3). Once again Participant 3's data performed relatively poorly for the same reasons as above. The EER shows an increase to 4.02% in session 1 and 10.02% in session 2. It is not surprising that the performance for the impersonation set is worse than when using unseen data from participants whose data are used to train the participant-specific models. However, the overall low error rate and high AUC shows that our authentication approach for people with UEI is promising.

VI. Discussion and Limitations

Our study has a three main limitations. First, during our study, motion artifacts from the lack of neck muscle control presented a problem with extracting noise-free signals for one participant. Therefore, we need strategies to compensate for artifacts induced by the participant. Second, in our current dataset the participants were alert during both data collection sessions. However, it has been shown that factors such as fatigue or recent physical activity affect an individual's physiology, movements, and posture [32]. It will be interesting to see how our approach works for individuals who are fatigued, sick, or even depressed. Third, physiological responses change over time, necessitating retraining. Approaches are required to determine when to retrain in order to balance the drop in authentication accuracy over time with the inconvenience of taking the system offline.

VII. Conclusions

In this paper, we have explored a new authentication approach for head mounted devices (HMDs), a type of wearable Internet-of-Things (wIoT) device, for people with UEI. Our approach used ballistocardiograms (BCGs) derived from subtle head movements captured by movement sensors in an HMD. In the *immediate future* we plan to extend this work in several directions including: (1) increasing the participant pool, and (2) making the approach tolerant to the motion from participants with poor neck control.

VIII. Acknowledgments

This work is supported in part by the National Science Foundation grant CNS-1947022. The authors would like to thank all the participants who helped with data for this work. We would also like to thank all the employees of TechAccess of Rhode Island for hosting us and helping us with our data collection.

References

[1] Alan Neuhauser, "Google Glass Offers Disabled People Access to a Bigger World," https://www.usnews.com/news/stem-solutions/articles/2014/06/10/google-glass-offers-disabled-people-access-to-a-bigger-world, 2014.

[2] Hayley Tsukayama, "Google Glass, other wearables could give the disabled a new measure of independence," https://www.washingtonpost.com/business/technology/with-wearable-technology-a-new-measure-of-independence-for-some-with-disabilities/2013/08/06/e258757e-fde4-11e2-96a8-d3b921c0924a_story.html, 2013.

[3] M. Cognolato, M. Atzori, and H. Müller, "Head-mounted eye gaze tracking devices: An overview of modern devices and recent advances," *Journal of rehabilitation and assistive technologies engineering*, vol. 5, p. 2055668318773991, 2018.

[4] O. Spakov, H. Istance, K.-J. Räihä, T. Viitanen, and H. Siirtola, "Eye gaze and head gaze in collaborative games," in *11th ACM Symposium on Eye Tracking Research and Applications, ETRA 2019*. ACM, 2019.

[5] S. H. Lee, H.-Y. Jung, S. J. Yun, B.-M. Oh, and H. G. Seo, "Upper extremity rehabilitation using fully immersive virtual reality games with a head mount display: A feasibility study," *PM&R*, 2019.

[6] X. Luo, T. Kline, H. C. Fischer, K. A. Stubblefield, R. V. Kenyon, and D. G. Kamper, "Integration of augmented reality and assistive devices for post-stroke hand opening rehabilitation," in *2005 IEEE Engineering in Medicine and Biology 27th Annual Conference*. IEEE, 2006, pp. 6855–6858.

[7] "Home Modifications for People with Upper Extremity Impairment," https://smartech.gatech.edu/bitstream/handle/1853/29027/k-10-6b2_9629.pdf, 2009.

[8] Erika Harrell, "Crime Against Persons with Disabilities, 2009-2012 - Statistical Tables," https://www.bjs.gov/index.cfm?ty=pbdetail&iid=4884, 2014.

[9] Kathy Wechsler, "Preventing and Dealing with Theft by Hired Caregivers," https://www.mda.org/quest/article/preventing-and-dealing-theft-hired-caregivers, 2014.

[10] J. Hernandez, Y. Li, J. M. Rehg, and R. W. Picard, "Bioglass: Physiological parameter estimation using a head-mounted wearable device," in *Wireless Mobile Communication and Healthcare (Mobihealth), 2014 EAI 4th International Conference on*, 2014, pp. 55–58.

[11] S. Li, A. Ashok, Y. Zhang, C. Xu, J. Lindqvist, and M. Gruteser, "Whose move is it anyway? authenticating smart wearable devices using unique head movement patterns," in *2016 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 2016, pp. 1–9.

[12] S. Schneegass, Y. Oualil, and A. Bulling, "Skullconduct: Biometric user identification on eyewear computers using bone conduction through the skull," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, ser. CHI '16, 2016, pp. 1379–1384.

[13] C. E. Rogers, A. W. Witt, A. D. Solomon, and K. K. Venkatasubramanian, "An approach for user identification for head-mounted displays," in *Proceedings of the The 19th International Symposium on Wearable Computers*, ser. ISWC'15, 2015.

[14] N. a. M. Barbosa, J. Hayes, and Y. Wang, "Unipass: Design and evaluation of a smart device-based password manager for visually impaired users," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, ser. UbiComp '16, 2016, pp. 49–60.

[15] M. Brown and F. R. Doswell, "Using passtones instead of passwords," in *Proceedings of the 48th Annual Southeast Regional Conference*, ser. ACM SE '10, 2010, pp. 82:1–82:5.

[16] A. Ali, "Sequential gestural passcodes on google glass," in *Proceedings of the 17th International ACM SIGACCESS Conference on Computers & Accessibility*, ser. ASSETS '15, 2015, pp. 359–360.

[17] K. Fuglerud and O. Dale, "Secure and inclusive authentication with a talking mobile one-time-password client," *IEEE Security Privacy*, vol. 9, no. 2, pp. 27–34, 2011.

[18] R. Kuber and S. Sharma, "Toward tactile authentication for blind users," in *Proceedings of the 12th International ACM SIGACCESS Conference on Computers and Accessibility*, ser. ASSETS '10, 2010, pp. 289–290.

[19] S. Saulynas and R. Kuber, "Towards brain-computer interface (bci) and gestural-based authentication for individuals who are blind," in *Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility*, ser. ASSETS '17, 2017, pp. 403–404.

[20] J. Hayes, X. Li, and Y. Wang, ""i always have to think about it first": Authentication experiences of people with cognitive impairments," in *Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility*, ser. ASSETS '17, 2017, pp. 357–358.

[21] Y. Ma, J. H. Feng, L. Kumin, J. Lazar, and L. Sreeramareddy, "Investigating authentication methods used by individuals with down syndrome," in *Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility*, ser. ASSETS '12, 2012, pp. 241–242.

[22] R. Johnson, W. J. Scheirer, and T. E. Boult, "Secure voice-based authentication for mobile devices: vaulted voice verification," in *SPIE Defense, Security, and Sensing*. International Society for Optics and Photonics, 2013, pp. 87 120P–87 120P.

[23] K. Fuglerud and O. Dale, "Secure and inclusive authentication with a talking mobile one-time-password client," *IEEE Security Privacy*, vol. 9, no. 2, pp. 27–34, 2011.

[24] S. Zhu, Y. Ma, J. Feng, and A. Sears, "Don't listen! i am dictating my password!" in *Proceedings of the 11th International ACM SIGACCESS Conference on Computers and Accessibility*, ser. Assets '09, 2009, pp. 229–230.

[25] M. Bottos, A. Feliciangeli, L. Sciuto, C. Gericke, and A. Vianello, "Functional status of adults with cerebral palsy and implications for treatment of children," *Developmental Medicine & Child Neurology*, vol. 43, no. 8, pp. 516–528, 2001.

[26] H. Guo, X. Cao, J. Wu, and J. Tang, *Ballistocardiogram-based person identification using correlation analysis*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 570–573.

[27] J. Hernandez, D. J. McDuff, and R. W. Picard, "Bioinsights: Extracting personal data from still wearable motion sensors," in *2015 IEEE 12th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, 2015, pp. 1–6.

[28] E. Vural, S. Simske, and S. Schuckers, "Verification of individuals from accelerometer measures of cardiac chest movements," in *2013 International Conference of the BIOSIG Special Interest Group (BIOSIG)*, 2013, pp. 1–8.

[29] S. Singh, A. Cabraal, C. Demosthenous, G. Astbrink, and M. Furlong, "Password sharing: Implications for security design based on social practice," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '07, 2007, pp. 895–904.

[30] S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic, "Evaluating behavioral biometrics for continuous authentication: Challenges and metrics," in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, ser. ASIA CCS '17, 2017, pp. 386–399.

[31] "Google Glass," http://www.google.com/glass/start/, 2014.

[32] J. Stern, D. Boyer, and D. Schroeder, "Blink rate as a measure of fatigue," *(Tech. Rep. No. DOT/FAA/AM- 94/17). FAA Civil Aeromedical Institute.*, 1994.