TWC: Small: Authenticating Smart Wearable Devices Using Unique Human Body Movement Patterns
Zhang, Rutgers University

This is the summary.

1 Introduction

We live in a world that has seen a generation of technological revolutions; from wired to wireless communications, immovable to mobile machines, large sized to hand-held devices. Today, we are witnessing what can be deemed as the next phase of mobile revolution through *wearable computers*. Research in wearable computers can be dated back to as early as 1980s when Steve Mann developed a prototype heads-up-display goggles [14]. Thanks to the advances in hardware miniaturization technology, cheap sensors/processor chips, and low-power sensing/computing, today, wearables are available off-the-shelf and have almost become an integral part of human lives [2, 4, 1].

With the onset of proliferation of wearable devices, preserving security and privacy of these devices and the data on the devices, is becoming critically important – most of the data is highly personal to the user. A solution for safeguarding the security and privacy of user's data on the wearable device, however, is only effective as long as the device itself is authenticated to the right user/owner.

Authentication on most commercially available wearable devices today [1, 4] relies on an indirect mechanism, where users can login to their wearables through their phones. This requires the wearable device to be registered and paired to the user's mobile device, which makes it inconvenient as the user has to carry both the devices. The security of this approach is also in question as it increases the chance of hacking into both the devices if either of the devices are lost or stolen. Some devices including Google Glass [2] and FitBit's health tracker [1], pair the device to the users email account instead of the phone for user's convenience; however, it does not add any security benefit. Though wearable devices today almost contain the same suite of sensors as a smartphone, the computing capacity and battery lifetime of wearables are far less comparable. This implies that, translating the same authentication solution from a phone to the wearable device, to enable direct authentication, is not only undesirable but also impractical. *Thus, the need for the day is a simple, low-power, and accurate direct authentication solution.*

Broadly speaking, there are two direct authentication methods that are commonly adopted: password based authentication and biometric based authentication. We argue that neither method is suitable for wearable devices. **** Collecting and recognizing these biometrics is subject to the availability of the sensing hardware and the computing capability on the wearable units, hence unrealistic in most cases.

In addition to password-based authentication and biometric-based authentication, there is another class of authentication method that relies upon the uniqueness of human behavior characteristics such as human walking gait, arm swings, typing patterns, body pulse beats, eye-blinks, etc. This way of authenticating users is called *behavioral* biometrics, which has been studied in the context of authenticating smart phones and tablets [18, 9, 19, 17, 15, 13, 6, 10]. In this proposal, we propose to authenticate wearable devices to users based on one type of behavioral biometric characteristics – our unique body movement patterns. We believe body movement patterns are well suited for authenticating wearable devices because ***.

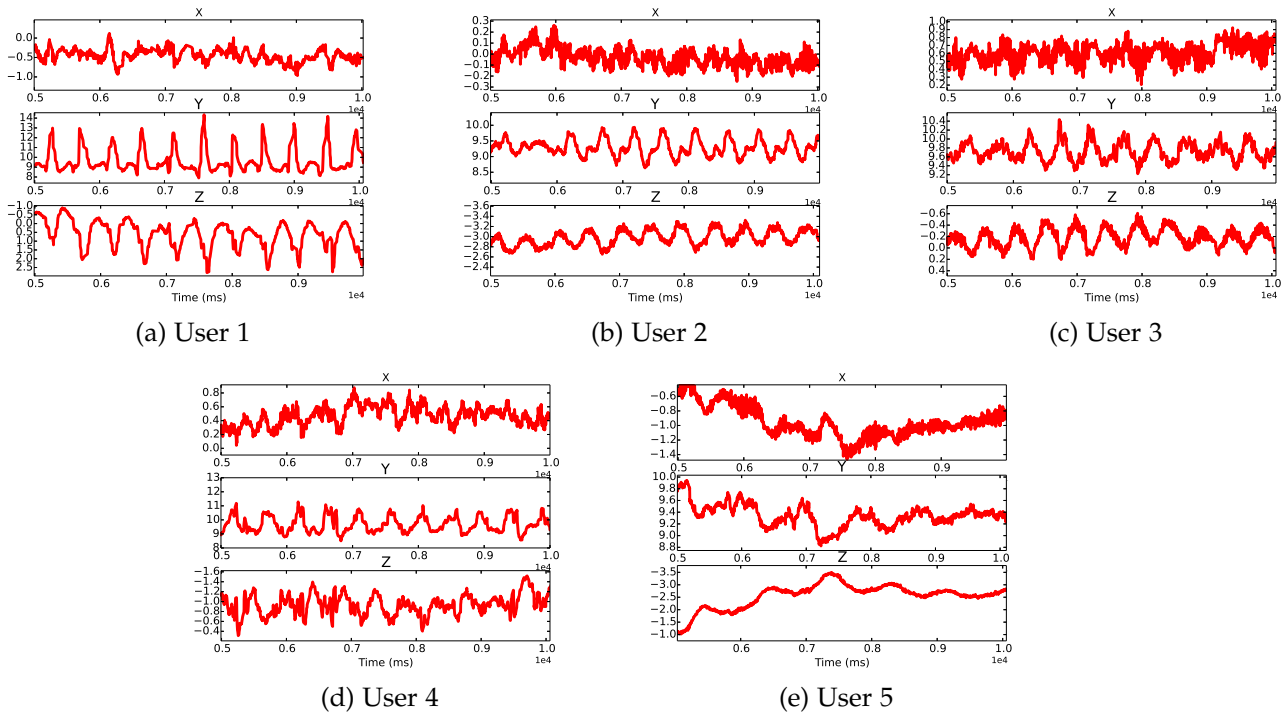
***Challenges ***

Our research involves a coordination of algorithm design and system evaluation, ultimately involving the construction of a realistic authentication system that can efficiently run on wearable devices. Our project also involves an important curriculum development effort. We intend to train next-generation workforces in the rapidly-growing mobile computing field, as well as recruit youth and women into research in this field.

2 Background and Overview

2.1 Background on Authenticating Wearable Devices

Authentication mechanisms for a wearable device can broadly be divided into two categories: (i) *Direct* authentication, where the users can directly authenticate themselves to their wearable device using the input/output interface and/or using signatures generated from the sensors available on the device, and (ii) *Indirect* authentication, where a secondary device – typically the user's smartphone – is used as a medium for authentication. Today's commercially available wearable devices predominantly use the latter approach where users login to their wearable devices through their smartphone – using a PIN or an email account.



(a) User 1 (b) User 2 (c) User 3

(d) User 4 (e) User 5

Figure 1: These plots show the raw accelerometer data in the time domain for five different users when they move their head in response to a music track wearing the same Google glass. The plots indicate that different users' head movement patterns appear distinctive from each other. The five users wore a Google Glass (in turns) and listened to a 10 second audio snapshot of a pop song.

Unlike the indirect approaches, that require a wearable device is registered to and connected (wireless) to a smartphone, direct mechanisms can leverage the built-in interfaces and sensors on the wearable device. The fact that wearable devices relate significantly to "what we wear" on the human body, biometrics can play a key role for direct authentication to wearable devices. Biometrics allow a system to identify a user based upon "who you are" (i.e., her physiology) instead of "what you have" (i.e., ID cards) or " what you remember" (i.e., passwords) [12, 16, 20]. Physiological biometrics such as DNA, ear shape, face, fingerprint, hand/finger geometry, iris, odor, palm-print, retinal scan, and voice, have been very effective and widely used in many prototype and commercial authentication systems. In addition, body shape such as body height, width, and body-part proportions can also be used as biometric cues to identify different people [8]. Even "soft" characteristics such as body weight and fat percentage have been considered as secondary biometrics for authentication purposes [5]. However, biometrics are not prominently used in wearable devices commercially available today, though there have been specific point commercial designs (e.g., Nymi [3]). This can be attributed to the fact that biometrics would require the specific hardware/sensor available on the wearable device. Also the overheads for physiological biometrics in wearable devices can be high, in both, cost for hardware as well as integration and computing.

An other approach to direct authentication is using behavioral biometrics where unique signatures from human behavior (subconscious or in response to external stimulus) provide cues for differentiating and authenticating users. For example, it has been shown that gait (e.g., stride length, the amount of arm swing) when the user is walking or running is a reliable identification cue, and irrespective of the environment [19]. Okumura et.al. [17] have shown that the human arm swing patterns can be used to create signatures to authenticate to their cell-phones. Monrose et.al. [15] show that keystroke rhythms, when users type on the keyboard, that include typing dynamics such as how long is a keystroke, how far is between consecutive strokes, and how is the pressure exerted on each key, can be used as a biometric to authenticate users. Similarly, mouse usage dynamics [13] and touchpad touching dynamics [6, 10] have also been shown to serve as potential biometrics.

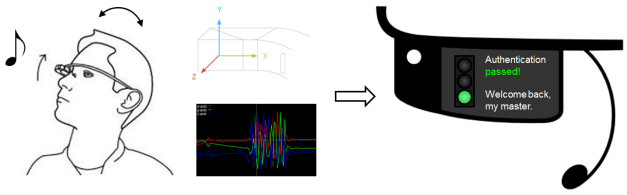


Figure 2: Illustration of Headbanger. The head-worn device authenticates the right user based on signatures generated from head-movement patterns in response to an audio snapshot played on the device.

In comparison to other means of authentication, behavioral biometric authentication can offer a more convenient (than physiological biometrics), and more secure (than indirect authentication) solution for wearable device authentication. With the increasing off-the-shelf availability and (almost) unlimited access to the sensors on the wearables, it has become possible to generate and/or infer unique behavioral signatures specific to users. We use these rationale as a motivation for our proposed design of a behavioral biometric based authentication that generates unique signatures from user's body movements. We design an authentication system, dubbed *Headbanger*, for wearable devices by monitoring user's unique body-movement patterns (e.g., head movements, arm movements, and hand movements) in response to an external audio stimulus.

2.2 Body Movement as a Behavioral Biometric

According to [12], a human characteristic can be considered as biometric as long as it is *universal*, *distinctive*, *repeatable*, and *collectible*. With the advancements in wearable computer designs it is becoming easier for collecting body movement patterns using the built-in sensors (e.g., accelerometer sensor, gyroscope sensor, motion sensor, etc). Such sensors are available on most wearable devices available today, thus making body movements that are universally available *collectible* in all aspects. It has been shown [21] that most people move their body as a natural response to external rhythmic stimuli such as music – even at a very early age, infants respond to music and their movements speed up with the increasing rhythm speed. We observed that even adults naturally perform head movements or hand movements when listening to a fast beat audio track.

Based on a preliminary analysis of the accelerometer signals from five Google Glass users, we also observed (see Figure 1 (a)-(e)) that these users *repeatedly* showed unique and *distinctive* head-movement patterns, when listening to the same music beats on the head-worn device. Motivated by this observation we hypothesize that head movements can be a good behavioral biometric characteristic to authenticate users to their smart glass.

Example Body Movement Patterns: Depending upon specific wearable devices, we can focus on different body parts. For example, head-mounted devices such as smart glasses/goggles can easily capture a user's head movements; wrist-mounted devices such as smart watches can easily capture a user's arm/hand movements. To facilitate natural and repeatable body movements, we can play short, fast-tempo music tracks on the wearable devices, and then measure the movement using built-in sensors such as accelerometer and gyroscope. In addition, eye lid movements such as blinking or winking can also be easily captured by head-mounted devices; for example, Google glass ***.

***YZ: Sugang, any other body movements we can study? ***

2.3 Overview of *Headbanger*

We envision that our proposed system will be used as an authentication interface on the wearable device. The system will run as a service in the device upon power-up, similar to the screen-lock in smartphones or the head-nod interface on Google Glass [2]. Upon usage, a short duration audio track will be played on the device, and the user makes body movements in response to the audio. *Headbanger*will then go through the following steps:

- *Sensor data collection*: *Headbanger* records the body movements in the form of raw sensor signals (e.g., accelerometer or gyroscope) using the built-in sensors on the wearable device.

- *Filtering*: The raw sensor signals are then filtered by applying filters such as low-pass filter to remove records of extraneous motion.
- *Signature generation*: The filtered signals are then processed to obtain the unique features for each user-audio pair.
- *Classification*: The signatures are classified to different users based on data mining and machine learning strategies, and labeled to the corresponding user.
- *Authentication*: The head-movement signature generated during system operation is compared with the original user-audio pair signature, and the user is authenticated access if there is a plausible match.

The illustration of *Headbanger* is shown in Figure 2.

2.4 Research Challenges

Specifically, the proposed research effort consists of the following thrusts:

- Developing signal processing and learning algorithms that can accurately identifying each user's body movement patterns.
- Developing a light-weight, low-cost authentication system that can run on wearable devices efficiently.

3 Establishing Body Movement Patterns as Behavioral Biometrics

3.1 Preliminary Results

In our preliminary study, we used Google glass to collect accelerometer data (*ACC* in short) when a user moves her head with music, and studied whether head movement patterns are distinctive and repeatable. After collecting raw *ACC* data samples, we went through the following steps to process the data:

1. *Filtering*: Since the frequency spectrum of the *ACC* samples is significantly concentrated within 5Hz, we filtered the raw samples using a low-pass digital Butterworth filter [7] by adopting a relaxed cut-off frequency of 10Hz. In this way, we removed spurious head movements and obtained smooth *ACC* data.
2. *Training Set Construction:* We constructed the training set to include m *ACC* samples from the legitimate user (which we refer to as *true ACC* samples), as well as m *ACC* samples each from N random users (referred to as *false* samples).
3. *Signature Generation*: Next, we generated signatures from the filtered *ACC* samples using the dynamic-time warping (DTW) tool [**?**]. DTW is generally used as a similarity matching tool for time-domain analysis of temporally varying signals. DTW compares a temporal signal with a reference signal over a certain time-window and yields a distance measure as the score. A low score (distance) implies that the test signal is in close match with the reference.

   Using DTW, we calculated the distances between true *ACC* samples and the distances between true samples and false samples, and refer to these two types of signatures as same-user distance signatures as well as across-user distance signatures.
4. *SVM Classification:* In the classification phase, we first calculated the DTW distances between the test sample and the true samples, and then feed these values and the signatures to a Support Vector Machine (SVM) for classification. SVM returns '1' to denote that the test user is legitimate and '0' to denote otherwise.

Distinctiveness: We designed the first set of experiments to show that even the simplest head movements are distinctive – i.e., it is hard to imitate other's head movements. In this set of experiments, we employed simplest head movement patterns: nodding. We have one owner for the Google glass who designed the nodding pattern and 15 imitators who imitated the movement. We collected 100 10-second *ACC* samples

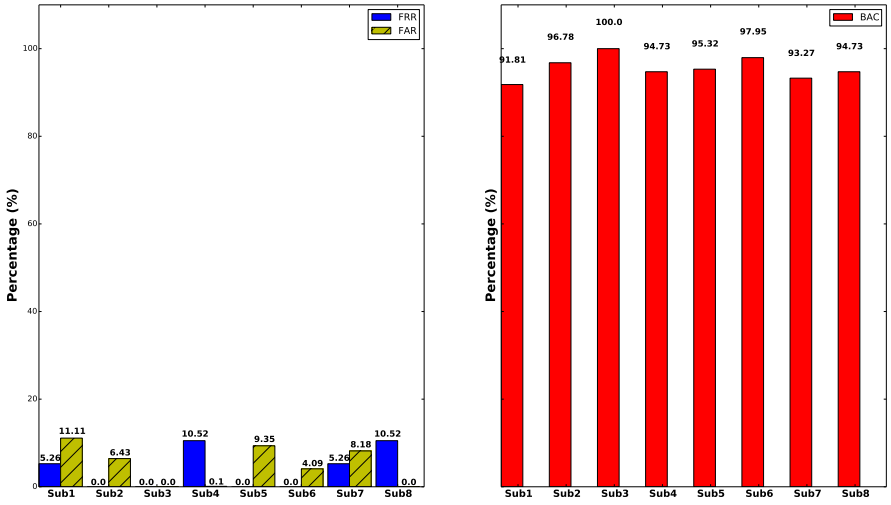


Figure 3: In this set of experiments, we studied whether a user can successfully repeat her own head-movement pattern. We had 8 subjects, each performing her own choice of head-movement patterns. We collected 38 samples for each subject. (a) shows the FRR and FAR results for each subject, and (b) shows the BAC results. Thresholding-based classification with top 3 voting was used to generate these results.

from the owner, during the course of 60 days (from 10/1/2014 to 11/30/2014), ensuring the owner's sensor data includes sufficient variation that naturally occurs with time. We also made a great deal of effort to make sure the imitators accurately imitate the owner's movement – the owner carefully explained his movement pattern to each imitator, and sat through each data collection session for all the 15 imitators to make sure their movement pattern looks the same to the owner's eye. For each imitator, we collected 40 10-second *ACC* samples. Using different combinations of training data and test data, we generated the classification results and summarized the mean FAR (false acceptance rate), FRR (false rejection rate), and BAC (balanced accuracy) in Table 1. The results show that *even simple nodding is not easy to imitate: nodding for 6 seconds can classify 95% of the users.*

Repeatability: We designed the second set of experiments to show that a user can successfully repeat her own head movement if each user is asked to come up with their own movement patterns. In this set of experiments, we had 8 subjects, and for each subject, we collected 38 *ACC* samples with sample duration of 10 seconds. Each subject performed different head-movement patterns of their choice. We report the average FAR, FRR, and BAC values in Figure 3, where Figure 3(a) shows the FRR and FAR values, while Figure 3(b) shows the BAC values. The results show that *head-movements are highly repeatable.* Among the 8 subjects that we studied, the highest BAC value is 100%, and the lowest is 91.81%, with the average BAC value of 95.57%.

Sample duration (s)	2			3			6			10		
	FRR (%)	FAR (%)	BAC (%)	FRR (%)	FAR (%)	BAC (%)	FRR (%)	FAR (%)	BAC (%)	FRR (%)	FAR (%)	BAC (%)
SVM	25.0	16.74	79.12	15.0	14.05	85.47	3.33	6.66	95.0	0.0	9.62	95.18

Table 1: Average FAR, FRR, and BAC for SVM-based classification when we choose different 4 imitators in the training set (from the total 15 imitators). We have the results for different sample durations. In these results, we use the earliest 40 owner samples in the training set.

3.2 Proposed Research

Our preliminary results show that head movement patterns have the potential to be used as a reliable biometric characteristic for wearable user authentication. However, in order to develop a full-fledged authentication system using unique body movements, we need to address several important challenges.

3.2.1 Authentication Accuracy

– feature selection
– how to increase the entropy of the signal (change music) ...

3.2.2 Reliability

Our preliminary results show that head movements are rather distinctive and repeatable in very controlled settings – all the data were collected when the participant was in a stationary setting, e.g., sitting on a chair. However, in reality, the behavior of body movement signatures over chaotic settings will be a key factor to decide on the effectiveness of this approach. In particular, we need to solve the challenge when the user is in a mobile setting such as walking or in a vehicle. It is unclear if the head movement patterns are repeatable in such a mobile environment, or if the ambiguities of vehicle motion versus head-motion can be separated.

In addition to a person's mobile setting, other factors such as a person's mood/energy level may also have an impact on her head movement signature; for example, a fresh and energetic user may provide significant head movements as compared to a sick or tired user whose signatures may not even be detectable. Inconsistencies in the accelerometer sensor such as drift and temporal bias can significantly affect the nature of inferred head-movement signature. Head-movements, on the other hand, may also evolve over time for a person which call for periodic calibration of the system and/or the training data.

YZ: Sugang, can you think about how to solve these challenges?

3.2.3 Multi-Modality

Smart-glass devices typically contain an array of motion sensors such as accelerometer, gyroscope, IMU. It is only a matter of time that motion sensor chips will be integrated into wearable devices. This opens up opportunities for multi-modal motion sensing. For example, accelerometer data can be combined with gyroscope measurements to provide multi-dimensional head-movement features that can improve the quality of the inferred signatures. Head movements can also be combined with other body movements to generate valuable, reliable signatures for authentication. For example, through a simple test experiment using the Google Glass infra-red light sensor[1] we observed that the blinking and winking patterns of users in response to the music stimulus were reasonably differentiable among users. Such patterns may also independently serve as another biometric that can be used for authentication purpose, or can be combined with head-movements for better results. Recent studies have shown that heart beat or pulse can also serve as reliable biometric for authentication purposes [11, 3] We reserve such potential enhancements to our system for future implementation.

***YZ: Sugang, can you write a few sentences about how to use gyro, blink sensor, and pulse data? ***

3.2.4 hand movements

***YZ: Sugang, any new challenges for hand movements? ***

4 Building the Body Movement Based Authentication System

4.1 Preliminary Work

Wearable devices have severe resource limitations in many aspects, such as energy, computing, networking and storage. Building a realistic authentication system that can smoothly run on such devices, therefore, becomes a significant challenge. In order to investigate whether such a goal is attainable, we have implemented

[1] we had to root the Google Glass to access the IR sensor unit.

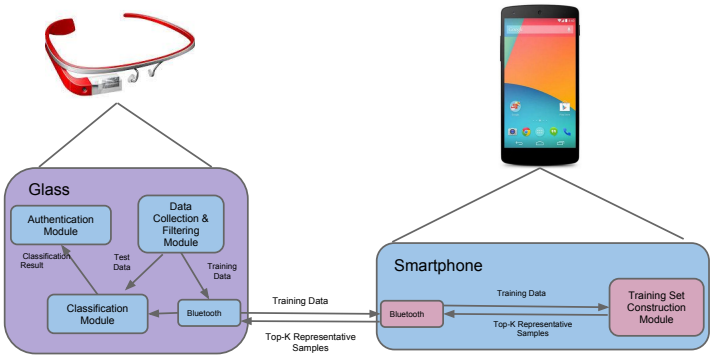


Figure 4: The software modules for the Headbanger authentication app we implemented in the preliminary study. Note that the Training Set Construction Module is executed on the bluetooth-paired smartphone because it is the most computing intensive module.

the a simple *Headbanger* system on Google glass. Figure 4 shows the software modules the app consists of. Among all the software modules, the "training set construction model" is the most computing-intensive, and as a result, we executed the model on the bluetooth-paired smartphone. The rest of the modules are implemented and executed on the glass. In our on-glass app, the classification module runs the thresholding-based classification. Table 2 shows the measured processing latency (the time that elapsed between when the test sample is collected and when the authentication result is generated). The results show that even after our aggressive optimizations, the processing latencies are still rather substantial, which suggests that further optimizations are needed.

sample duration (s)	processing latency (s)
2	1.29
3	2.74
6	9.04
10	2.48

Table 2: Measured processing latencies on Google Glass with different sample durations. We generated the results using Top 1 testing for thresholding based classification.

References

[1] Fitbit. http://en.wikipedia.org/wiki/Fitbit.

[2] Google glass. http://en.wikipedia.org/wiki/Google_Glass.

[3] Nymi band. http://www.nymi.com/.

[4] Smart watch. http://en.wikipedia.org/wiki/Smartwatch.

[5] Heikki Ailisto, Elena Vildjiounaite, Mikko Lindholm, Satu-Marja Makela, and Johannes Peltola. Soft biometrics – combining body weight and fat measurements with fingerprint biometrics. *Pattern Recognition Letters*, 2006.

[6] Cheng Bo, Lan Zhang, Xiang-Yang Li, Qiuyuan Huang, and Yu Wang. Silentsense: silent user identification via touch and movement behavioral biometrics. In *ACM MobiCom*, 2013.

[7] RE Challis and RI Kitney. The design of digital filters for biomedical signal processing part 3: The design of butterworth and chebychev filters. *Journal of biomedical engineering*, 1983.

[8] Robert T Collins, Ralph Gross, and Jianbo Shi. Silhouette-based human identification from body shape and gait. In *IEEE FGR*, 2002.

[9] Cory Cornelius, Ronald Peterson, Joseph Skinner, Ryan Halter, and David Kotz. A wearable system that knows who wears it. In *Proceedings of the 12th annual international conference on Mobile systems, applications, and services*, pages 55–67. ACM, 2014.

[10] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. Touch me once and i know it's you!: implicit authentication based on touch screen patterns. In *ACM CHI*, 2012.

[11] Javier Hernandez, Yin Li, James M Rehg, and Rosalind W Picard. Bioglass: Physiological parameter estimation using a head-mounted wearable device. In *IEEE MobiHealth*, 2014.

[12] Anil K Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 2004.

[13] Zach Jorgensen and Ting Yu. On mouse dynamics as a behavioral biometric for authentication. In *ASIACCS*, 2011.

[14] Steve Mann. Wearable computing: A first step toward personal imaging. *IEEE Computer*, 30(2):25–32, 1997.

[15] Fabian Monrose and Aviel D Rubin. Keystroke dynamics as a biometric for authentication. *Future Generation computer systems*, 2000.

[16] Lawrence O'Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 2003.

[17] Fuminori Okumura, Akira Kubota, Yoshinori Hatori, Kenji Matsuo, Masayuki Hashimoto, and Atsushi Koike. A study on biometric authentication based on arm sweep action with acceleration sensor. In *IEEE ISPACS*, 2006.

[18] Tauhidur Rahman, Alexander T Adams, Mi Zhang, Erin Cherry, Bobby Zhou, Huaishu Peng, and Tanzeem Choudhury. Bodybeat: a mobile system for sensing non-speech body sounds. In *Proceedings of the 12th annual international conference on Mobile systems, applications, and services*, pages 2–13. ACM, 2014.

[19] Sarah V Stevenage, Mark S Nixon, and Kate Vince. Visual analysis of gait as a cue to identity. *Applied cognitive psychology*, 1999.

[20] Roman V Yampolskiy. Motor-skill based biometrics. In *Annual Security Conference*, 2007.

[21] Marcel Zentner and Tuomas Eerola. Rhythmic engagement with music in infancy. *Proceedings of the National Academy of Sciences*, 2010.