# Cardiac Scan: A Non-contact and Continuous Heart-based User Authentication System

Feng Lin
CSE, University at Buffalo, SUNY
flin28@buffalo.edu

Chen Song
CSE, University at Buffalo, SUNY
csong5@buffalo.edu

Yan Zhuang
CSE, University at Buffalo, SUNY
yanzhuan@buffalo.edu

Wenyao Xu*
CSE, University at Buffalo, SUNY
wenyaoxu@buffalo.edu

Changzhi Li
ECE, Texas Tech University
changzhi.li@ttu.edu

Kui Ren
CSE, University at Buffalo, SUNY
kuiren@buffalo.edu

## ABSTRACT

Continuous authentication is of great importance to maintain the security level of a system throughout the login session. The goal of this work is to investigate a trustworthy, continuous, and non-contact user authentication approach based on a heart-related biometric that works in a daily-life environment. To this end, we present a novel, continuous authentication system, namely *Cardiac Scan*, based on geometric and non-volitional features of the cardiac motion. Cardiac motion is an automatic heart deformation caused by self-excitement of the cardiac muscle, which is unique to each user and is difficult (if not impossible) to counterfeit. *Cardiac Scan* features intrinsic liveness detection, unobtrusiveness, cost-effectiveness, and high usability. We prototype a remote, high-resolution cardiac motion sensing system based on the smart DC-coupled continuous-wave radar. Fiducial-based invariant identity descriptors of cardiac motion are extracted after the radar signal demodulation. We conduct a pilot study with 78 subjects to evaluate *Cardiac Scan* in *accuracy*, *authentication time*, *permanence*, *evaluation in complex conditions*, and *vulnerability*. Specifically, *Cardiac Scan* achieves 98.61% balanced accuracy (BAC) and 4.42% equal error rate (EER) in a real-world setup. We demonstrate that *Cardiac Scan* is a robust and usable continuous authentication system.

## KEYWORDS

Non-contact Sensing; Continuous Authentication; Biometrics.

## 1 INTRODUCTION

Continuous authentication improves upon one-pass validation by continuously verifying over the lifetime of a session that the system is operated by the same user as at initial login. It can prevent access by adversaries when the legitimate user is away or overwhelmed. Governments and private companies [14, 15] increasingly demand more secure authentication, because of credential compromises due to weak cryptographic mechanisms (hacking, password theft, etc.) and user carelessness. In 2014 alone, more than one billion personal records were illegally accessed including, health, financial, email and home address data, and other personal information like social security numbers [85].

Existing solutions for continuous authentication have certain limitations. Specifically, traditional methods demand the user to intentionally engage with the authentication system, such as scan a fingerprint or enter in a password after a certain period. Regardless of the vulnerability, these methods hurt the usability in practice. Several studies also have proposed advanced continuous authentication mechanisms based on the user's behavioral biometrics, such as keystroke dynamics and gaze pattern. However, keystroke dynamics [63, 73] require the user to keep typing on the keyboard, while gaze patterns [23, 54] requires the user to face and continuously look at the screen. Other methods, such as continuous face recognition [9] on Windows 10 Hello [20], are also reported to be vulnerable to spoofing or replay attacks [1]. Recently, the physiological biometrics-based approaches are emerging for continuous authentication, such as pulse response [67], however, they all require the human body to make contact with certain devices.

As a live individual trait, heart-based biometric is unique (i.e., distinguishable across subjects), measurable (i.e., hard to hide), non-volitional (i.e., unknown to the user), secure (i.e., difficult to counterfeit), and present in all living individuals (i.e., intrinsic liveness). Different from electrocardiogram (ECG) [70], we explore the cardiac motion, which is a heart-based functional behavior determined by the intrinsic geometric structure of the heart. We aim to develop a cardiac-motion-based continuous authentication scheme in a non-contact way. Specifically, there are three challenges involved: 1) how to obtain the high-resolution cardiac motion information unobtrusively? 2) how to extract invariant geometric-based features for each heart with regard to the cardiac motion mechanism? 3) how to examine the usability and security of the continuous authentication scheme?

To this end, we propose Cardiac Scan, a secure and trustworthy continuous user authentication scheme via non-contact cardiac motion sensing. Fig. 1 shows the working paradigm of transformative Cardiac Scan. The authentic user's credential is stored in the database prior to authentication, a new incoming cardiac motion will be matched to the stored credential to make the decision as to whether the access request is from an authorized user or a malicious adversary. Specifically, our work focuses on: 1) developing a smart DC-couple continuous-wave (CW) Doppler radar sensor to

*W. Xu is the corresponding author. F. Lin and C. Song contribute equally to this paper.


*MobiCom '17, October 16-20, 2017, Snowbird, UT, USA*

ACM ISBN 978-1-4503-4916-1/17/10…$15.00
https://doi.org/.1145/3117811.3117839

continuously capture the high-resolution cardiac motion information from the distance; 2) identifying fiducial descriptors of cardiac motion based on the heart geometric characteristics; 3) conducting intensive evaluations (e.g., accuracy performance, usability and complex use conditions) to validate its performance and examine its security against replay attacks. Through a pilot study with 78 subjects, Cardiac Scan achieves 98.61% balanced accuracy (BAC) and 4.42% equal error rate (EER). All these studies demonstrate that Cardiac Scan is a robust and usable continuous authentication system. *Moreover, Cardiac Scan can be conveniently integrated with existing one-pass user verification techniques (e.g., personal identification number [PIN], fingerprint, iris scan, and face) to enhance the continuous authentication capability of existing systems.*

In sum, our contribution in this work is two-fold:
1) We explore new cardiac motion-based biometrics for continuous authentication. Cardiac Scan exploits the unique and non-volitional components of individual cardiac motion and identifies users in a non-contact, unobtrusive, and secure manner. This approach holds the potential to transform existing authentication systems into a more undeceivable, disclosure-resistant and user-friendly solution.
2) We evaluate Cardiac Scan through a set of multi-scene evaluations, including authentication with unaligned sensors, authentication with different emotional states, authentication in motion, and authentication under replay attack.

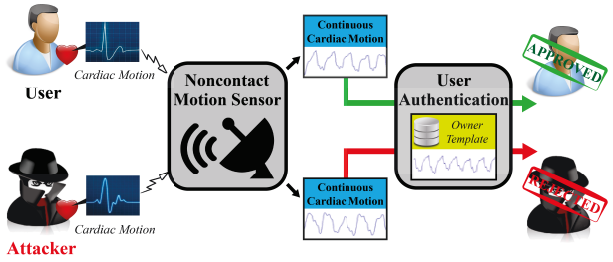



**Figure 1: A novel continuous authentication method using cardiac motion captured by a non-contact radar.**

## 2 DESIGN CONSIDERATIONS

### 2.1 Design Goals

A successful biometric system should possess some necessary properties. When designing our Cardiac Scan system, we have taken into account the following aspects.

**Intrinsic Liveness:** An essential requirement for a biometric system is intrinsic liveness detection, i.e., it should be able to distinguish if the authentication sample is a "live" user or a replay attack. Cardiac motion exists only in a "live" user and represents heart deformation when the heart is in contraction and relaxation states.

**Unobtrusive Authentication:** The authentication system should identify an authentic user in an unobtrusive way so that the user has no obligation to change his/her behavior to adapt to the system. Continuous authentication further requires the authentication process to be unobtrusive so that the user does not need to interrupt current work to authenticate. Cardiac Scan can perform unobtrusive authentication through a human-safe radio signal.

**Highly Secure:** The biometrics should be highly secure and unique, making it difficult to be forged and stolen. Cardiac Scan measures the live cardiac motion, which depends on the cardiac muscle structure of the user and therefore is impossible to completely mimic.

**Cost-effective and Easy-to-Use:** Some biometrics seem to have reliable and robust features, but the information acquisition requires expensive devices and specific conditions, such as an iris/retina authentication system. Cardiac Scan uses low-cost off-the-shelf components to build the radar sensor and is easy to use at a distance because of the propagation of the radio signal.

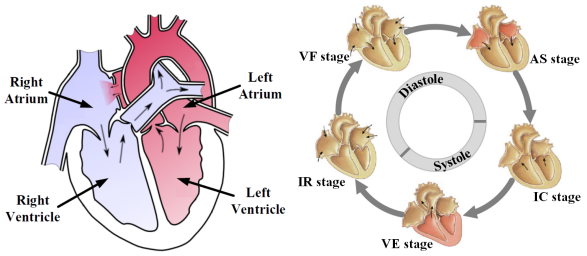
**Resilient to Background Noise and Use Conditions:** The biometric system should also be resilient to background noise and use conditions, no matter what the surrounding environmental conditions are. Camera-based systems, including face and iris recognition, usually have deteriorated performance with either too strong or too weak illuminations. Cardiac Scan uses a radio signal that is robust to the environmental change and can penetrate through obstacles to accurately sense the cardiac movement. Also, due to the essence that the sensing relies on the Doppler effect, static surrounding materials barely have an impact on the system performance.

### 2.2 Non-contact Cardiac Motion Sensing

*2.2.1 Rationale.* This work investigates cardiac motion as a new biometric to secure user authentication. Cardiac motion is a 3D automatic heart deformation caused by the self-excitement of the cardiac muscle [27]. As shown in Fig. 2(a), the human heart contains two upper cavities (atria) and two bottom chambers (ventricles) [33]. The successive contraction (systole) and relaxation (diastole) of both atria and ventricles circulate the oxygen-rich blood throughout the whole human body. The contraction and relaxation comprise the cardiac motion. In one cardiac cycle, ventricles relax and passively fill with the blood in approximately 70% of their total volume from atria through the open mitral valve. Then atria contract with heart muscles and pump blood. At the same time, ventricles continuously fill blood with the remaining 20%. (Ventricles, at least, free up 10% of the volume for the contraction.) After that, ventricles start to contract with all valves closed, and the blood volume remains unchanged. When the intraventricular pressures exceed the pressures within the aorta or pulmonary artery, blood is ejected and the heart volume reduces rapidly [8].

As shown in Fig. 2(b), one cardiac motion cycle consists of five distinct stages including: 1) ventricular filling (VF), 2) atrial systole (AS), 3) isovolumetric ventricular contraction (IC), 4) ventricular ejection (VE), and 5) isovolumetric ventricular relaxation (IR) [8]. These cycle stages are significantly different in volumes, surface shape, moving dynamics (speed, acceleration, etc.) and 3D deformation of the heart [12]. These stages vary from person to person due to the change in size, position, anatomy of the heart, chest configuration and various other factors [43]. No two persons have exactly the same heart, blood circulation system and other related tissues. Therefore, the cardiac motion is a unique identity marker for each individual [27]. Moreover, since cardiac motion is intrinsically connected to multiple biological functions, it is extremely difficult to counterfeit or to be hidden for a living individual.

*2.2.2 Feasibility.* Non-contact monitoring of human body motion, such as respiration and heartbeat rates using a Doppler radar motion sensor, has gone through a few decades of scientific study




(a) Heart structure. (b) Cardiac motion stages.

**Figure 2: Heart structure and dynamics.**

[16, 21, 41, 48, 49]. Efforts have been devoted to the development of radar front-end hardware, signal processing algorithms, and system on-chip/on-board integration. Compared with other techniques such as non-contact laser vibrometer [72] and infrared imager [53] that can only detect motion at body surface, it has been shown that the Doppler radar sensor can directly measure the motion of internal organs [62] and heart [68, 92]. However, research results in those works are incomprehensive for a real authentication system, e.g., the impact of random body movement is not considered. Although random body movement and clutter noise still require significant efforts to resolve, some progress has been achieved [40, 82] and preliminary clinical studies have been reported [35]. However, existing cancellation approaches either compromise the quality of the baseband signals [40] or require sweeping the carrier frequency and adjusting the target position [82], which is not applicable to capture the high-fidelity cardiac motion in a real-world setup. Because of the sensitivity required for the detection along with difficulty in maintaining the original motion pattern during demodulation, most research using biomedical radar sensors have focused on detecting heart rate [49]. Recently, some of our research results have proved that DC-coupled interferometry radar and Doppler radar with digital-IF architecture can avoid frequency-selective signal distortion and thus make it possible to recover accurate motion patterns using continuous-wave (CW) Doppler radar sensors.

## 3 CARDIAC SCAN PROTOTYPE

### 3.1 System Overview

By measuring the signal phase shift caused by physiological motion, biomedical radar can reveal heartbeat and respiration information. Compared with conventional biomedical radars that can only measure the rate of the heartbeat signal, the main novelty of the radar sensor developed in this work is using distortion-free front-end architecture and demodulation to measure cardiac motion pattern. A smart DC-coupled radar architecture was employed in the radar front-end to eliminate undesired DC offset and preserve the desired cardiac motion characteristic information.

### 3.2 Architecture with Dynamic DC Tuning

To monitor cardiac motion pattern, a smart DC-coupled CW radar sensor was employed by taking advantage of real-time signal processing and mixed-signal design in modern devices. For cardiac motion sensing, the DC offset due to reflection from other parts of the body not related to cardiopulmonary activities may easily saturate the receiver and create frequency-dependent distortion, and is an important factor for the central intelligence unit to handle. Details of hardware innovation are discussed below.

*3.2.1 Smart DC tuning.* As shown in Fig. 3, the DC-coupled adaptive tuning architecture includes RF coarse-tuning and baseband fine-tuning. For RF tuning, the electronically controlled phase shifter and attenuator add a portion of the transmitted signal to the receiver signal to cancel most of the DC offset caused by clutter reflections. However, due to quadrature imbalance, the phase variation of the received signals, and the limited resolution of the phase shifter and the attenuator, the RF tuning cannot completely remove all the DC offsets. To further eliminate the remaining DC offsets, a baseband fine-tuning block was implemented to dynamically adjust the amplifier bias to the desired level that allows the maximum dynamic range. With the above DC tuning realized by a smart center in real time, the radar will precisely measure cardiac motion pattern. The integration of the DC-tuning technique into portable devices will be addressed with the help of logic control circuits coordinated by the I2C bus and CMOS-integrated calibration DACs.

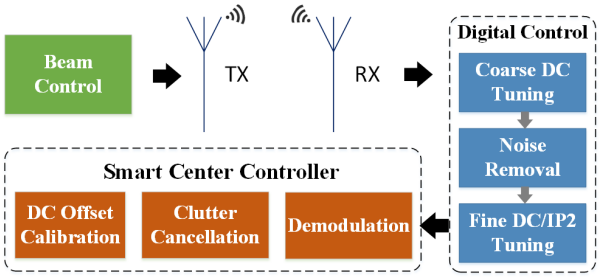



**Figure 3: Doppler radar sensor with adaptive DC tuning.**

*3.2.2 Optimal carrier frequency.* Besides manipulating the penetration depth, radar carrier frequency also determines the modulation sensitivity. Experiments were first carried out to compare the performance of carrier frequencies ranging from 2.4 GHz to 40 GHz. It should be noted that increasing the carrier frequency beyond 40 GHz may not help because as the wavelength approaches physiological motion amplitude, strong nonlinear phase modulation will generate harmonic interference [38] .

*3.2.3 Electronic beam control.* In this work, cardiac sensing will be realized from different angles to obtain sufficient information for biometrics applications. Also, multiple radars around a subject may "probe" cardiac signals simultaneously. To achieve this, it is essential that a radar can configure the radiation beam to precisely point at the location of interest. As shown in Fig. 3, digital beam control was implemented on the radar front-end. Conventional beamforming systems directly adjust the phase and amplitude of the signal of each element antenna. We demonstrated that it is much more convenient to simultaneously adjust the phase and amplitude in the complex domain than to adjust them separately. For a complex signal $x = \exp(-j2\pi ft)$ sent into each element antenna (where $f$ is the signal frequency), a vector multiplier was used to realize phase and amplitude modulation by first splitting the signal into in- and out-of-phase components and then by multiplying each one using a variable gain amplifier. Finally, by adding the amplified in- and out-of-phase components together, complex modulation to the original signal can be achieved thus effectively realizing radar

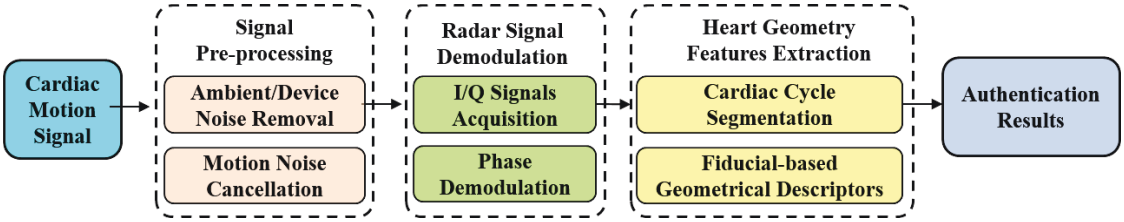



**Figure 4: The flowchart of Cardiac Scan, a heart-biometric-based continuous user authentication system.**

beam control. To align the radar beam with the user, a laser pointer can be used to indicate the beam direction.

# 4 RADIO SIGNAL PROCESSING SCHEMES

## 4.1 Scheme Overview

In this section, we elaborate on the radio signal processing schemes and correspondingly investigate user authentication methods to achieve secure and usable authentication results. As depicted in Fig. 4, our proposed approach is mainly comprised of three modules. First, the original sequential signal was preprocessed for noise reduction. Second, we performed de-noising aware radar signal demodulation. Third, we extracted fiducial-based descriptors using heart geometry features. Lastly, we obtained authentication results. Note that the existing heart-based biometrics, such as ECG, are recording the electrical activity of the heart, whose descriptors are extracted on the basis of the QRS complex [10]. As a new biometric modality, our non-contact cardiac motion is substantially different from the typical ECG signal in that it is a direct heart motion activity measured by an RF sensor. Therefore, it is crucial to explore new approaches in the non-contact cardiac motion authentication. To the best of our knowledge, no such work exists in the literature.

## 4.2 Pre-processing

Pre-processing is to reduce the noise level in the cardiac signal and simultaneously prevent the waveform from distortion. The noise includes low-band components (e.g., baseline wander), high-band components (e.g, power-line interference) and unpredictable-band components (e.g., arbitrary motion in the scene). Considering diverse and known frequency bands of the noise spectrum, we have addressed the noise level reduction in two areas: 1) one-pass noise reduction techniques (e.g., a Butterworth bandpass filter) and 2) adaptive noise canceling techniques [86] (e.g., a normalized least mean square adaptive filter [87]). These techniques have also been successfully applied in bio-artifact reduction [19, 87].

## 4.3 De-noising-aware Radar Demodulation

A novel signal demodulation is critical for distortion-free cardiac motion sensing because traditional Doppler radar is optimized for speed detection, which faces challenges when the movement pattern has very low frequency or stationary components [93].

*4.3.1 Challenges in signal demodulation.* The Doppler radar sensor transmits the continuous-wave signal $T(t)$:

$$T(t) = A_T \cos(\omega t + \phi(t)). \tag{1}$$

Then, the received signal is represented as $R(t)$:

$$R(t) = A_R \cos[\omega t - \frac{4\pi d_0}{\lambda} - \frac{4\pi x(t)}{\lambda} + \phi(t - \frac{2d_0}{c})], \tag{2}$$

where $A$ is the amplitude, $\lambda$ is the wavelength. $c$ is the speed of light. $\omega$ represents the angular velocity. $\phi(t)$ is the time-varying phase. $d_0$ is the distance between the Doppler radar and the subject. $x(t)$ denotes the time-varying displacement caused by cardiac motion. Then two baseband signals, the in-phase signal $I(t)$ and quadrature signal $Q(t)$ can be derived from $R(t)$ [47]:

$$I(t) = A_I \cos[\frac{4\pi x(t)}{\lambda} + \frac{4\pi d_0}{\lambda} - \phi(t - \frac{2d_0}{c})] + DC_I, \tag{3}$$

$Q(t)$ is the quadrature signal:

$$Q(t) = A_Q \sin[\frac{4\pi x(t)}{\lambda} + \frac{4\pi d_0}{\lambda} - \phi(t - \frac{2d_0}{c}) + \phi_0)] + DC_Q, \tag{4}$$

where $A_I$ and $A_Q$ are the amplitude of the in-phase signal and the quadrature signal, respectively. $DC_I$ and $DC_Q$ are the DC offsets in $I/Q$ channels, respectively. $\phi_0$ is the phase offset between $I(t)$ and $Q(t)$. The baseband radar signals, $I(t)$ and $Q(t)$, are sampled by NI USB-6008 at 100 Hz.

For simplicity, we neglect the constant phase offset $4\pi d_0/\lambda + \phi(t - 2d_0/c)$ in Eq. (3) and Eq. (4). We assume that the gain imbalance is 1 (i.e., the ratio of $A_I$ and $A_Q$ is 1), and phase imbalance ($\phi_0$) is 0. Thus, Eq. (3) and Eq. (4) can be simplified as:

$$\begin{cases} I(t) = A_0 cos(\frac{4\pi x(t)}{\lambda}) + DC_I \\ Q(t) = A_0 sin(\frac{4\pi x(t)}{\lambda}) + DC_Q \end{cases}. \tag{5}$$

According to trigonometric identities, we can transform Eq. (5) into Eq. (6)

$$(\frac{I(t) - DC_I}{A_0})^2 + (\frac{Q(t) - DC_Q}{A_0})^2 = 1, \tag{6}$$

which can be interpreted that the samples of $I/Q$ channels stay on a circle whose center is $(DC_I, DC_Q)$ with a radius of $A_0$. Then the least squares optimization [89] is employed to obtain the circle and obtain the three unknown parameters: $DC_I$, $DC_Q$, and $A_0$.

After identifying the DC component offsets, the displacement signal $x(t)$ can be derived using the arctangent demodulation method:

$$x(t) = arctan(\frac{Q(t) - DC_Q}{I(t) - DC_I}) \times \frac{4\pi}{\lambda}. \tag{7}$$

Traditionally, to detect the *weak* physiological signal $x(t)$, the small-angle approach was used [21, 40, 41, 48], which suffers from two inherent problems. First, when the distance between the target and the radar sensor changes, the detection sensitivity will also change, resulting in alternating *optimum* and *null* points [21]. Second, nonlinear harmonics and intermodulation products would appear when movement amplitudes are comparable to the carrier wavelength [37]. To solve this problems, an arctangent demodulation approach was proposed by calculating arctan$[\frac{Q(t)}{I(t)}]$, assuming $DC_I$ and $DC_Q$ can be properly calibrated [61]. Unfortunately, a direct arctangent function has a co-domain range of $(-\frac{\pi}{2}, \frac{\pi}{2})$. Once

the demodulation exceeds this range, phase unwrapping is required, which is challenging in practical detection when noise is strong and the movement amplitude is large [29]. This is especially a problem when random body motion exists, which introduces a significant phase change that could easily go beyond multiples of $2\pi$.

*4.3.2 Phase demodulation solution.* To overcome the limit of arctangent demodulation, we have investigated an extended differentiate and cross-multiply (DACM) algorithm to avoid the phase unwrapping problem. The algorithm computes a derivative to the arctangent-demodulated phase information first:

$$\omega(t) = \frac{\mathrm{d}}{\mathrm{d}t}[\arctan\frac{Q(t)}{I(t)}] = \frac{I(t)\dot{Q}(t) - \dot{I}(t)Q(t)}{I(t)^2 + Q(t)^2}, \tag{8}$$

where $\omega(t)$ is related to the velocity function of the cardiac motion, and $\dot{Q}(t)$ and $\dot{I}(t)$ denote the time derivative of $Q(t)$ and $I(t)$, respectively. To reconstruct the desired phase information, which represents cardiac motion, integration can be applied to the above result. Therefore, the signal phase can be recovered in the digital domain as:

$$\Phi_\theta[n] = \sum_{k=2}^{n} \frac{I[k]\Delta Q[k] - \Delta I[k]Q[k]}{I^2[k] + Q^2[k]}, \tag{9}$$

where $I[k]$ and $Q[k]$ are the discrete samples of the $I/Q$ channel outputs. $\Delta I[k] = I[k] - I[k-1]$ and $\Delta Q[k] = Q[k] - Q[k-1]$. The operation block diagram is also included in the "smart center" of Fig. 3. By introducing an accumulation procedure, noises can be effectively suppressed. Once $\Phi_\theta[n]$ is obtained, the cardiac motion $x[n]$ can be linearly obtained based on a single scale calibration.

# 5 CONTINUOUS AUTHENTICATION

## 5.1 Heart Geometric Features

*5.1.1 Segmentation.* To extract the invariant descriptors from the cardiac motion signal of the subject, we segmented the periodical signal sequence into discrete frames. For fiducial descriptors, there exist literature [3, 44, 50, 64] where multiple cardiac cycles were used. We have investigated the performance with various numbers of cardiac motion cycles. Though each segment (see Fig. 5) includes all five heartbeat motion stages, the variations across individuals within one cardiac cycle may not be sufficient for differentiation. This segmentation with disparate cardiac motion cycles benefits the signal alignment because it associates the segment with the physiological cardiac motion in one or multiple cycles.

*5.1.2 Fiducial descriptors.* The fiducial-based method extracts intrinsic geometrical descriptors (e.g., temporal, amplitude, area or angle) from fiducial points in the cardiac motion signal. Specifically, fiducial points are the biomarkers with physical meanings in clinics during the cardiac motion cycle. Fiducial points contain the biological information that is unique and non-volatile for individuals, and are also independent of the sensor location or state of the individual such as anxiety, nervousness, or excitement [28]. On the other hand, non-fiducial-based methods focus on the non-physical attribute features, which fails to reflect the intrinsic geometric features of the heart. Also, they are computationally demanding [5] and apt to be interfered with by parameters setting [79], making non-fiducial-based methods inapplicable for continuous real-time authentication.

In the fiducial-based method, the cardiac displacement signal is well matched to the cardiac activity rationale in Section 2. The first stage, Ventricular Filling (VF), is when the semilunar valves (SV) close and the atrioventricular valves (AV) open. The whole heart is relaxed and the blood charges into atria as well as ventricles, resulting in the outward expansion of the heart. The second stage, Atrial Systole (AS), is when atria contract to pump their contained blood into ventricles. The heart will contract inward first due to the emptying of atria. It will expand outward again because the extra blood in atria is squeezed into ventricles (SV will close to prevent blood from flowing into arteries). The third stage, Isovolumetric Ventricular Contraction (IC), is when ventricles begin to contract and SV/AV close. Since there is no change in volume, no significant displacement occurs. Lastly, Ventricular Ejection (VE), is when SV opens and ventricles are contracting and forcing blood into arteries. As a result, the heart will contract inward. During the fifth stage, Isovolumetric Ventricular Relaxation (IR), ventricles finish the blood ejection, stop contracting and begin to relax. This cycle ends and begins anew.

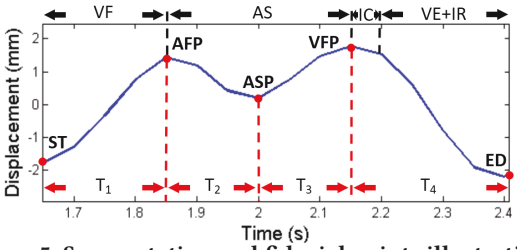



**Figure 5: Segmentation and fiducial points illustration.**

Fig. 5 is a complete segment which shows the changes of the cardiac displacement. Based on the cycle description above, the signal is typically further split into four sub-frames, each of which is labeled with the corresponding stage. We will refer to *ST* and *ED* as the starting point and ending point of the segment. The fiducial points that we plan to select are *AFP*, *ASP* and *VFP*, described as :
**AFP**: the first maximum point in the segment, which indicates the end of the VF stage and the onset of the AS period where the atrial muscles contract to squeeze the blood into the ventricles.
**VFP**: the second maximum point in the segment, which locates at the end of the AS stage. The blood flows into the ventricles and reaches the largest volume.
**ASP**: the local minimum point between *AFP* and *ASP*. It represents the end of atria contraction and the start of ventricles expansion.

Table 1 lists the descriptors based on the above fiducial points. Note that all the time descriptors $T_i$ are normalized by the duration of one cardiac cycle, such that these descriptors are *independent* of heart rate.

Fiducial point extraction is of great importance to accurately locate the feature point. Due to the potential clutter noise, the radius of curvature is more robust than the more straight-forward local extreme point or signal derivatives. Specifically, we selected three points $X$, $Y$ and $Z$ with a fixed time interval along the time sequence. The minimum (maximum) radius of curvature in the corresponding region is found by maximizing (minimizing) the value of $\delta$ using the vector cross product between the two directed line segments, as shown in Fig. 6.

## 5.2 Continuous Authentication Protocol

One time validation of a user's identity, referred to as static authentication, has shown its vulnerability to attacks. Specifically, malicious adversaries may access the system that has been logged in by an authentic user when the authentic user is not nearby. Unlike static authentication, continuous authentication represents a new security mechanism which continuously monitors the user's trait and use it as a basis to re-authenticate periodically throughout the login session. Therefore, continuous authentication significantly enhances the security level of systems. Cardiac Scan enables unobtrusive and non-contact continuous authentication with the radio frequency (RF) interrogation, during which RF signals transmit and measure the human target continuously. By demodulating the received echo signal, the cardiac motion pattern of the user can be extracted. In what follows, we will discuss continuous authentication parameters and three typical scenarios.

**Table 1: Fiducial-based descriptors.**

| List | Descriptor Definition |
|---|---|
| $T_1$ | Normalized Time interval between $ST$ and $AFP$. |
| $T_2$ | Normalized Time interval between $AFP$ and $ASP$. |
| $T_3$ | Normalized Time interval between $ASP$ and $VFP$. |
| $T_4$ | Normalized Time interval between $VFP$ and $ED$. |
| $H_1$ | Displacement difference between $ST$ and $AFP$. |
| $H_2$ | Displacement difference between $AFP$ and $ASP$. |
| $H_3$ | Displacement difference between $ASP$ and $VFP$. |
| $H_4$ | Displacement difference between $VFP$ and $ED$. |

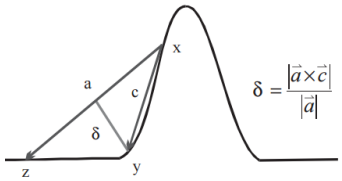



**Figure 6: The radius of curvature is calculated as the vector cross product between the two directed line segments.**

*5.2.1 Continuous Authentication Parameters.* Two parameters, refreshing interval $T_r$ and negative tolerance threshold $Th_{nt}$, are important in continuous authentication, which are unique compared to static authentication.

**Refreshing interval $T_r$:** It is defined as the interval between two consecutive authentications. The appropriate choice of $T_r$ has an impact on the performance and usability of continuous authentication. If $T_r$ is too large, malicious adversaries may not be detected in time, thus may lead to severe security issues. On the other hand, if $T_r$ is too small, some random activities (e.g., making phone calls, drinking water, turning around) or rhythmical body movement (e.g., listening to music) may compromise the system's recognition accuracy due to false alarms. Considering these random activities usually take about several seconds, we have set the refreshing interval as 5 sec. Note that the refreshing interval should be differentiated from the authentication time $T_a$. The latter is defined as the time duration for a single authentication process and will be discussed in subsection 7.2.

**False negative tolerance threshold $Th_{nt}$:** Usability is carefully considered in continuous authentication to make sure the authentic user will not frequently be interrupted by mistakenly logging out of the system. In other words, we aim to avoid the false negative event, which is the incorrect classification of an authentic user as an adversary due to motion artifacts. We noticed that false negative events are rare and appear sparsely in Cardiac Scan, which means there is a low probability that more than one "classified as adversary" event occurs consecutively when the authentic user is present. On the other hand, when the adversary is present, the "classified as adversary" event will occur consecutively. After observing such phenomena, we define the false negative tolerance threshold as the number of permitted consecutive "classified as adversary" events. Empirically, the value for this threshold can be 1 or 2. The larger value setting is more tolerant to false negative and the smaller value setting is more sensitive to risk. In the following scenarios, we adopt the threshold setting of 1 because the usability of continuous authentication will not be compromised given the low false negative rate of Cardiac Scan. In the mean time, this setting maintains a high sensitivity to unauthorized access.

*5.2.2 Continuous Authentication Scenarios.* We devise three scenarios in particular for Cardiac Scan enabled continuous authentication, including *Authentic user is present*, *Authentic user leaves*, and *Adversary is present*.

**Authentic user is present:** When an authentic user has logged into the system and is present within the range of the radar sensor, Cardiac Scan is able to detect whether cardiac motions are from the same person who was initially authorized. Thus, the permission of using the system for the user can be continuously granted without any interruption, unless the user logs off intentionally or leaves, as shown in Fig. 7 (a). By designing the false negative tolerance, Cardiac Scan allows one single "classified as adversary" event given that the classification results just before and after this event are both positive as "classified as authentic user". In case two or more than two consecutive "classified as adversary" events occur, though it has a low probability, Cardiac Scan will log out the initial user. Under such a circumstance, the user has to be re-authenticated by confirming his identity again using other complementary existing biometrics approaches, such as PIN, or fingerprint. Note that, for the scenario which has a specific requirement, the system tolerance level can be adjusted by changing the value of $Th_{nt}$.

**Authentic user leaves:** When the authentic user is away from the system and the radar sensor has detected the user's absence, as shown in Fig. 7 (b), Cardiac Scan will first check whether the user has logged off and the system has been locked up. If so, Cardiac Scan will classify the user's absence as a legitimate action and no further action needs to be taken. Otherwise, the system is at risk of unauthorized access, hence necessary actions such as locking the session, logging out the original user, or notifying the administrator [67], which depend on the system policy, have to be considered to address the security risks.

**Adversary is present:** In this scenario, an unauthorized adversary (the dark one in Fig. 7 (c)) is present and close to the system, and the system has been logged in initially by an authentic user. This can happen when the authentic user is under the coercion attack and being forced to be present or the adversary takes over the system before the system automatically locks up when the authentic user leaves. Therefore, immediate action is demanded to keep the adversary outside the system and prevent the leakage of sensitive

information. In this case, Cardiac Scan will immediately log out the initial user and lock up the system once $Th_{nt}$ is exceeded.

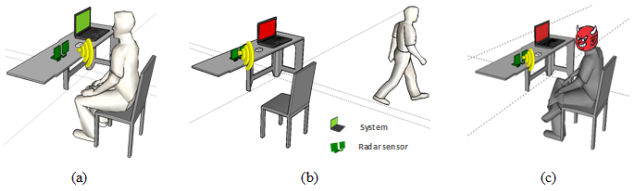



**Figure 7: Three scenarios: (a) Authentic user is present, the system remains unlocked. (b) Authentic user leaves, the system locks up. (c) Adversary is present, the system locks up. Green screen: system is unlocked. Red screen: locked.**

# 6 EXPERIMENTS AND VALIDATION

## 6.1 Experimental Setting

We conducted a pilot study to prove identifiability in cardiac motion. The Cardiac Scan system has been developed for the study, which works at the frequency of 2.4 GHz with the bandwidth of 5 kHz. The sampling frequency of 40 Hz. Though WiFi and Bluetooth also work at 2.4 GHz, our cardiac motion signal will not be interfered with because the motion information to be detected is only a few Hertz, which means both received signals and transmitted signals are only separated by a few Hertz, while other signals from potential interferences (e.g., WiFi and Bluetooth) have a much higher frequency separation and are conveniently rejected by the baseband signals. In other words, both transmitted signals and received signals are "coherent", whereas other signals are not coherent with transmitted signals. The Doppler radar has two antennas with the beam width of 45 degrees, i.e., one for transmitter and one for receiver. The power consumption of our radar is only 650 mW with 5 V voltage and 130 mA current. Note the transmission power level is within the human safety range because it is almost a thousand times less than the peak power of an ordinary global system for mobile communications (GSM) cellphone. The experimental setup is shown in Fig. 8, a subject sat in a chair in a relaxed condition. The customized Doppler radar sensor was placed in front of the subject with a distance of 1 m. A smartphone was placed close to a radar to record the subject identity and label the ground truth. The radar signal demodulation is done in a laptop equipped with Intel i7-3770 CPU @ 3.4 GHz. Motion compensation was carried out for the baseband complex signal obtained from subjects who breathed normally but randomly moved their body. A pulsed sensor (UFI 1010 pulse transducer) was attached to the subject's finger to provide a heartbeat reference. A chest belt (UFI 1132 piezo-electric respiration transducer) was used to provide a respiration reference.

## 6.2 Data Collection

As described above, our project evaluation relies on a strategically developed experiment that will involve a cohort of participants. We hold an existing active IRB protocol (# 502984/503753, Texas Tech University) that allows for recording body motion from adult human participants user identification. All the evaluations tightly follow the rule of IRB regulation. Seventy eight healthy subjects (46 males and 32 females) with their ages in the range of 16 - 54 participated in the study. Their weights are between 42 - 83 kg. None of them have any heart disease. Each subject has 20 trials, and each trial lasts eight seconds including 8 to 10 cardiac cycles. In each trial, all subjects are required to sit in front of the radar, unless specified in the evaluation, to get the cardiac motion signals collected. Therefore, in total there are 20 sets of data containing 14, 886 cardiac cycle samples in the evaluation. Currently, our work focuses on healthy people, the evaluation on subjects with pathologies or heart surgeries (e.g., heart diseases) is out of the scope of this work.

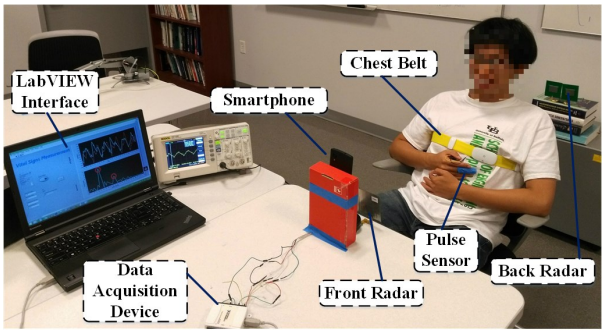



**Figure 8: Experimental setup for cardiac motion sensing. A subject is sitting one meter away from both radar sensors, a chest belt and a pulsed sensor is attached to the subject.**

## 6.3 User Classification

To prove the identifiability in cardiac motion, dynamic time warping (DTW) [81] is used as the similarity matching metric. Support vector machine (SVM) with a radial basis function (RBF) kernel classifier and 10-fold cross validation were employed for the 20 sets of data in the evaluation, among which 18 are for the training and 2 for the testing. The choice of the classifier will be further discussed in Section 7.1.4. In authentication, initially, the owner's cardiac motion template is stored in the system. Then, unknown users attempt to access the system by keeping still in front of the radar. Since there are total 78 participants, and each participant acts as an owner once while remaining participants act as attackers.

## 6.4 Body Movement Interference Suppression

Compared with cardiac motion, body movement may result in a large perturbation to the output DC offset, and thus confuse the radar demodulation algorithm or even saturate the baseband circuit. In the experiment, the time-domain signal had fluctuations due to the random body motion as shown in Fig. **??**(a). Strong near-DC spectral components were observed and the heartbeat was invisible in the spectrum (see Fig. **??**(b)). Simply reducing the front-end gain, as adopted in some communication systems, does not work because the radar will lose the sensitivity to the weak cardiac motion signal.

Because biomedical radar can detect cardiac motion from four sides of a human body, multiple radars can be installed at different locations around the human body to cancel out random body motion based on the different patterns of body motion and cardiac motion [40]. In the view of the two radars, the heartbeat-and-respiration-caused body movements are in phase, while the random body movements are out of phase. In the current setting, two radars

are detecting from the front and the back of the body. When the body is drifting toward one radar, it is moving away from the other; whereas heartbeat presents similar expansion/contraction patterns to the two radars [39]. Therefore, random body motion creates an opposite Doppler frequency shift to the signals of the radars, while cardiac motion leads to the same polarity. By properly combining the low-speed baseband signals from the radars, one type of motion can be canceled and the other type will be enhanced [40]. Note that although the random body movement can exist in the direction perpendicular to the radar direction, our body movement cancellation method still works effectively because only the movement in the radar direction is critical for the cardiac motion detection.

## 6.5 Signal Validation

We verified the validity of the collected data from our system. When the radar sensor detects the cardiac motion, the fingertip sensor simultaneously collects a signal as the ground truth signal. Both the radar sensor and fingertip pulse sensor were sampled at 40 Hz. We observed that the cardiac motion cycles are well aligned, each of which closely match the peaks in the fingertip signal. So we verified that our system could accurately detect the cardiac motion signal in a non-contact way.

# 7 EVALUATION RESULTS

As a potential breakthrough technology, it is necessary to evaluate the performance, flexibility, and vulnerabilities in practice of Cardiac Scan. Note that all the performance results are obtained after random body movement suppression except the one specified as "before random body movement suppression" in the evaluation of subjects in motion. We employed several statistics to describe the performance of Cardiac Scan.

## 7.1 Accuracy

*7.1.1 Balanced Accuracy and F-measure.* We provided the F-measure accuracy (F1 score) and balanced accuracy (BAC) for the accuracy measurement, both of which are non-sensitive to class distribution and can avoid misleading accuracy measurement when the true class distribution is unbalanced. F1 score is known as the harmonic mean of precision and recall, precision $p$ is the number of true positive (TP) divided by the number of positive calls (TP+FP) while recall $r$ (a.k.a. true positive rate) is the number of true positive (TP) divided by the number of condition positives (TP+FN) where FP is false positive and FN is false negative. F1 score reaches its best value at 1 and worst at 0. Simply, F1 score is defined as follows:

$$F_1(\%) = 2 \cdot \frac{precision \cdot recall}{precision + recall} = \frac{2TP}{2TP + FP + FN}. \quad (10)$$

And BAC is the equal combination of true positive rate (TPR) and true negative rate (TNR), which is defined as:

$$\begin{aligned} BAC(\%) &= 0.5 * TPR + 0.5 * TNR \\ &= \frac{0.5 * TP}{TP + FN} + \frac{0.5 * TN}{TN + FP}, \end{aligned} \quad (11)$$

where TN is true negative.

Table 2 shows the average F1 and BAC accuracies of the authentication with different configurations. BAC achieve 95.56%, 97.27% and 98.61% with the standard deviation (STD) of 0.92%, 0.65% and 0.38% for 1 cycle, 2 cycles and 4 cycles, respectively. F1 values are exactly mean values of BAC, which are 95.56%, 97.27% and 98.61% for 1 cycle, 2 cycles and 4 cycles. The results indicate that the increase of segment length improves accuracies. Furthermore, the performance benefits from the longer segment length and achieves the best accuracy of 98.61%. Note that the false positive events are not produced by the same pairs.

**Table 2: Accuracy comparison for different cardiac cycles.**

| | 1 cycle | 2 cycles | 4 cycles |
|---|---|---|---|
| **F1 (%)** | 95.56 | 97.27 | 98.61 |
| **BAC (%)** | 95.56 ± 0.92 | 97.27±0.65 | 98.61±0.38 |

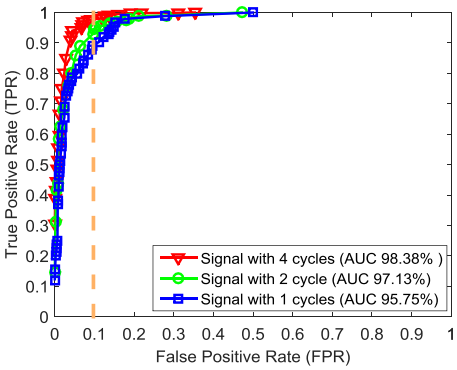



**Figure 9: The average ROC curves with AUC of 78 subjects with different number of cardiac cycles.**

*7.1.2 Receiver Operating Characteristic.* Receiver operating characteristic curve is created by plotting the true positive rate (TPR) against the false positive rate (FPR) at various threshold settings, which illustrates the performance of a binary classifier system as its discrimination threshold is varied. Fig. 9 depicts the average ROC curves of 78 subjects with different segment lengths. The signal with 4 cycles exhibits the best performance among three different segmentation configurations, which is consistent with the results of BAC and F1. Specifically, the corresponding area-under-curve (AUC) for each curve is also calculated as 98.38%, 97.13% and 95.75% for signals with 4 cycles, 2 cycles and 1 cycle, respectively.

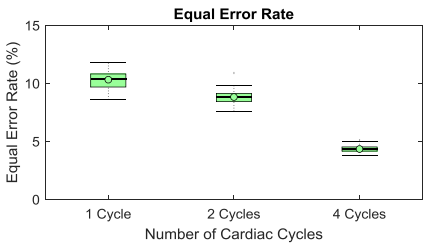



**Figure 10: The EER with a different number of cardiac cycles. Four cardiac cycles configuration has the lowest EER.**

*7.1.3 Equal Error Rate.* The equal error rate (EER) is a performance metric for authentication systems. It is a rate when the operating threshold for the accept and reject decision is adjusted such that the acceptance error (false positive rate, FPR) and rejection error (false negative rate, FNR) becomes equal. The lower the

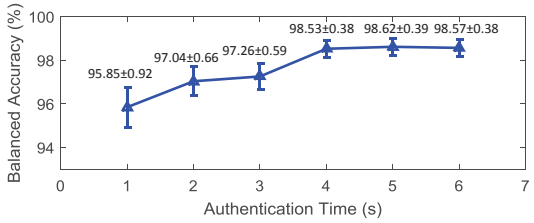



**Figure 11: The balanced accuracy of 78 subjects with different authentication time. Authentication with 4 sec duration is the optimal choice.**

equal error rate value, the higher the accuracy. Fig. 10 depicts the EER of 78 subjects with different segment lengths. The mean of EER is 10.37%, 8.79% and 4.42% for 1, 2, and 4 cycles, respectively.

**Table 3: The different classifiers comparison.**

| | kNN | SVM (linear) | SVM (polynomial) | SVM (RBF) |
|---|---|---|---|---|
| **BAC (%)** | 90.85 | 95.17 | 96.65 | 98.61 |
| **EER (%)** | 12.27 | 9.13 | 6.39 | 4.42 |

*7.1.4 Classifier Impact.* We compared two different classification techniques to select the best classifier for our application, including support vector machine (SVM) and $k$ nearest neighbors ($k$NN). A linear, a polynomial, and a radial basis function (RBF) kernel are adopted for SVM. Parameters of each classifier are tuned to achieve the best performance. The number of nearest neighbors $k = 4$, and $\gamma$ and $C$ of RBF function are 0.001 and 10000, respectively. Four cycles of cardiac motion are employed in this evaluation. The BAC and EER results are shown in Table 3. KNN has the lowest BAC of 90.85% and highest EER of 12.27%. SVM with RBF kernel has the highest BAC of 98.61% and lowest EER of 4.42%. SVM with linear and polynomial kernel have BAC of 95.17% and 96.65%, EER of 9.13% and 6.39%. The SVM with RBF kernel showed the best performance, which will be adopted in this paper for the classification.

## 7.2 Authentication Time

Another important performance metric for the user authentication system is the authentication time. Generally, a practical user authentication mechanism should not only be accurate in identifying the legitimate owners and the invalid attackers, but also time-efficient in processing authentication. We specifically defined the authentication time in terms of the total time elapsed, $T_a$, to make a final prediction for each user access attempt:

$$T_a = T_{cardiac\_motion\_sensing} + T_{processing}, \quad (12)$$

where $T_{cardiac\_motion\_sensing}$ is the minimum time that Cardiac Scan needs to collect the cardiac motion signals with the smart radar device. This depends on the number of cardiac cycles required to identify users. $T_{processing}$ is the time needed to process cardiac motion signals, including demodulation, denoise, feature extraction and user authentication.

To evaluate the authentication time efficiency, we applied different time restrictions on authentication time. Twenty subjects repeated the experiment with six different duration setups from 1 s to 6 s with increments of 1 s. The balanced accuracy with different authentication time is illustrated in Fig. 11. The error bars are the STD of BAC among 78 subjects. We observed that the authentication duration less than 3 sec are not long enough for reliable authentication, with low BAC (95.85% for 1 s, 97.04% for 2 s, 97.26% for 3 s) and high STD (0.92% for 1 s, 0.66% for 2 s, 0.59% for 3 s). The performance is improved when the duration is increased to 4 s with BAC of 98.53% and STD of 0.38%. Generally speaking, the accuracy increases with the longer authentication time. However, when the duration is greater than 4 s, the performance improvement is not significant. To be specific, BAC of 98.62% and 98.57%, and STD of 0.39% and 0.38% are for 5s and 6s, respectively.

We also provided the growth rate for different authentication duration to find the optimal duration in Table 4. The growth rate is calculated by the accuracy in the current duration and the previous duration. The growth rates for each second are 1.23%, 0.23%, 1.29%, 0.09% and -0.05%. Note that the duration of 4 s has the largest growth rate, and seems to be a significant turning point.

**Table 4: The BAC and growth rate.**

| Duration | 1 sec | 2 sec | 3 sec | 4 sec | 5 sec | 6 sec |
|---|---|---|---|---|---|---|
| **BAC (%)** | 95.85 | 97.04 | 97.26 | 98.53 | 98.62 | 98.57 |
| **Growth (%)** | - | 1.23 | 0.23 | 1.29 | 0.09 | -0.05 |

## 7.3 Evaluation in Complex Conditions

Another critical evaluation aspect is user experience. Typically, the user experience can be defined as: a person's perceptions and responses that result from the use and/or anticipated use of a product, system or service [36]. Therefore, the evaluation of user experience mainly focuses on the attitude/feeling of a person towards a product/system during its intended practical use. Traditionally, several methods have been widely adopted to maximally collect the feedback of a person on the product/system, such as interview, observation or survey. One unique aspect of the Cardiac Scan from many conventional authentication methods is that it is completely non-contact and passive to the user. Under normal conditions, the cardiac motion is not controllable or visible (even though it may be felt) to the user, which means that in most cases, the user will not be conscious of the interaction with the system in daily use. We also plan to evaluate usability with four variations: sensor distance, sensor alignment, emotional state, and subject in motion.

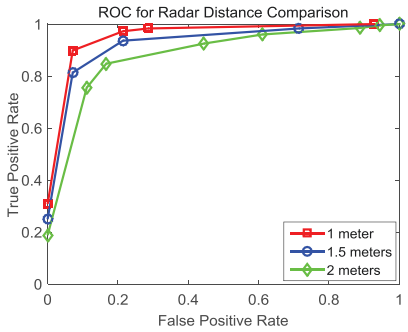



**Figure 12: The ROC of different radar distances.**

**Distance Impact:** We evaluated the impact of distance on the accuracy of cardiac motion authentication. The distance is defined as the length between the subject and the antenna of Doppler radar sensor. To make the Doppler radar sensor safe for human applications, we

have restricted the transmission power, so that the effective distance for the Doppler radar is 2 meters. Based on our observation, the amplitude of the baseband radar I/Q signal is inversely proportional to the distance between the subject and Doppler radar sensor. When the subject is far away from the Doppler radar sensor, the amplitude diminishes because it is difficult for the sensor to capture the slight cardiac motion. Fig. 12 illustrates the ROC of different radar distance comparison. Not surprisingly, the closest distance of 1 m has the best recognition performance. The accuracy decreases with the increasing distance between radar and subject.

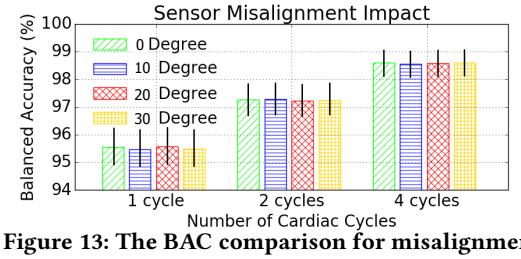



**Figure 13: The BAC comparison for misalignment.**

**Location Sensitivity:** As part of our understanding of how well non-contact cardiac motion can be utilized for identifying individuals, we investigated the relationship between various radar sensor orientation and identification performance. The hypothesis is that the extracted cardiac feature is insensitive to direction or orientation of the sensor beam. To test this hypothesis, we have collected a set of cardiac motion signals with a certain degree (10~30°) of orientation misalignment. Specifically, multiple radar sensors were used during the collection. One was placed in front of the subject, and others were placed out of alignment. The BAC comparison of each cycle length for different orientation misalignment is shown in Fig. 13. The BAC results for disparate misalignment with 0°, 10°, 20°, 30° are stable as observed from the figure which supports our argument that the extracted cardiac feature is insensitive to direction or orientation of the sensor beam.

**Emotional State:** A user's emotional state can change and is unknown to the identification system. The changes in emotional state will affect the cardiac motion (e.g, noise, heartbeat strength/cycle). The hypothesis is that the individualized features in cardiac motion are invariant to the user's emotional state. Research in heart-based biometrics [26, 28, 59] have demonstrated promising results for this hypothesis. To prove the usability and stability of Cardiac Scan under an unknown emotional state, we have conducted a set of experiments examining subjects in different emotional states. We have designated a special protocol to collect cardiac motion signals from low stress to high stress conditions. Specifically, selected subjects will perform two different task groups before collecting the data. The low stress tasks are meditation and listening to peaceful music. The high stress tasks are reading aloud, mathematical manipulation, driving in virtual reality, and intensive exercise. The BAC and EER comparison among all emotional tasks are shown in Fig. 14. The red bars with texture represent BAC and blue bars represent EER. The BAC and EER exhibit consistent performance across six different activities, including low stress and high stress conditions, which verifies that the emotional state will not impact the system performance.

**Subject in Motion:** Body movement may result in large perturbations to the output DC offset, and thus confuse the radar demodulation algorithm or even saturate the baseband circuit as described in detail in subsection 6.4. In this case, the recognition accuracy may be compromised, thus, the present user will experience logging out of the system. We investigated random movements in four activities ranging from tiny to large-range motions, including writing, drinking water, making phone calls, and one rhythmical movement when listening to music, to show the impact of body movement to the system performance. Twenty subjects participated in the experiment and each one performed all four body movement activities 10 times, a total of 200 trials for each activity are performed. Two radars are deployed in the front and at the back of the human body, and the measurement has to be performed simultaneously from both sides to cancel out the random frequency drift. With the current system setting, we evaluated how many times the authentic user is mis-classified as an unauthorized user before and after the body movement suppression approach described in subsection 6.4 is applied. The comparison results are shown in Fig. 15. Before body movement suppression, the mis-classified occurrence is 7 for making a phone call, 6 for drinking water, 5 for writing, and 18 for rhythmic movement. The rhythmic movement is more readily misclassified because it is periodic to some extent. The corresponding results after suppression are reduced to 2 for making a phone call, 1 for drinking water, 1 for writing, and 3 for rhythmic movement.

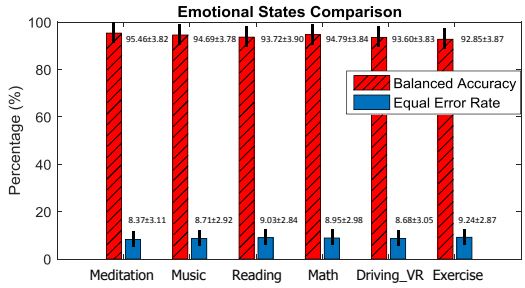



**Figure 14: The comparison among all emotional tasks.**

## 7.4 Continuous Authentication Stability

Besides maintaining a high true positive and true negative rate for authentication, we are particularly interested in low frequency false negative events that mis-classify an authentic user as an adversary in continuous authentication. As discussed in section 5.2.2, a usable continuous authentication system should always grant an access right to the authentic user as long as he/she is using the system. Otherwise, it is inconvenient even impossible to use the system if the user is being interrupted and asked to login again frequently. We conducted an evaluation on a continuous authentication session with four cardiac cycles setting. Under such configuration, the mean of false negative rate is as low as 0.4%. All 78 subjects participated in this evaluation and each session for each user lasts 40 minutes. Specifically, subject in turn acts as the user to login to the system and sit in front the system, browsing webpages or reading papers, until 40 minutes are reached or be logged out by the continuous authentication system. Not surprisingly, none of the subjects is forced to log out of the system due to a false negative, which is attributed to our continuous authentication protocol and

parameters setting to maintain a satisfactory usability as described in Section 5.2.2.

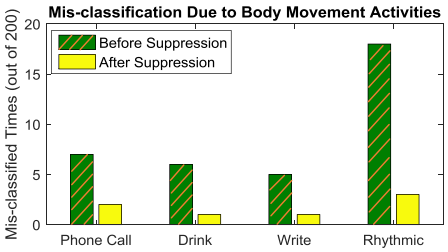



**Figure 15: Body movement suppression before and after.**

## 7.5 Longitudinal Study

It is important to prove the permanence of biometrics [30]. The permanence of heart-based biometrics was discussed in early experiments in many short-term studies [4, 25, 55]. In addition, each cardiac motion is independent, which means a prior result has no impact on the current result, so subsequent sessions study in short-term periods is not necessary. However, there are currently no longitudinal studies that establish this long-term persistence in any heart-based biometrics. Our generated dataset has included multiple sessions as part of a longitudinal approach to establish a baseline comparison of long-term persistence. 40 subjects (22 males and 18 females) participated in the longitudinal study lasting two months. Particularly, this study has two phases: enrollment phase and authentication phase. In the enrollment phase, training data were collected for each subject at the first day of this longitudinal study. Each subject finishes 20 trials in data collection events with the duration of each trial set as eight seconds. After that, the long-term authentication phase is carried out in the following two months. Each subject performed 20 authentication trials and each authentication duration is four seconds in this study. The BAC measurement is depicted in Fig. 16. In the 60-day duration, mean values of BAC measurement are between 98% and 99%, STDs are between 0.37 and 0.39. We concluded the BAC has no significant performance decreasing or ascending tendency, which demonstrates cardiac motion is robust against time change.

# 8 VULNERABILITY STUDY

Investigating the vulnerability of Cardiac Scan is crucial. Although cardiac motion is invisible and might possess better safety and security than other authentication approaches (e.g, PIN, fingerprint), it could become fallible under direct or spoofing attacks [51]. One immediate attack approach is the presentation of human characteristics to the acquisition device, including different living traits (i.e., zero-effort impostor attempts that try to take advantage of the false acceptance rate (FAR) of biometric systems) [31].

## 8.1 Replay Attack

One major risk of using biometrics is the danger that the biometric token can be intercepted and replayed by an unauthorized party. Compared to visual-based still biometrics (face/fingerprint/iris), the cardiac signal is more complex and dynamic to fake or replicate. However, there is still a chance to compromise cardiac signal under some extreme scenarios. Recently, Eberz *et al.* used a

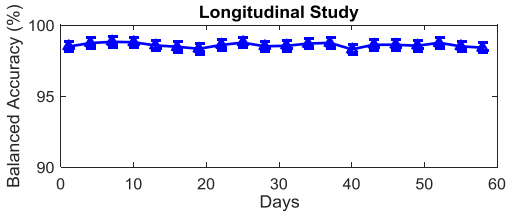



**Figure 16: The 2-month longitudinal BAC performance.**

hardware-based arbitrary waveform generator (AWG) and a sound card based AWG software to encode and emulate a set of pulse signals for attacking heart-based biometrics on the Nymi band [22]. Attackers might also hack into the database and obtain cardiac motion patterns or engineer the same cardiac motion sensing device to extract a user's cardiac signals. This work is to prove the possibility of a replay attack on Cardiac Scan if a legitimate user's cardiac signals are obtained by attackers. Our team has investigated the method of synthesizing cardiac motion and developed a programmable actuator to imitate the cardiac motion. As shown in Fig. 17, a linear actuator (ZABER TNA08A50) and a linear translational stage (i.e., ZABER TSB28-1) were placed 30 cm from the cardiac motion-sensing device. The actuator was programmed to perform a harmonic back-and-forth motion toward the radar for mimicking cardiac motion patterns.

## 8.2 Anti-Spoofing: Liveness Artifacts

Our team has also investigated a set of anti-spoofing approaches against a replay attack. The general idea of anti-spoofing is liveness detection [52, 80]. Liveness detection has been applied to existing biometrics systems by using affiliated living traits of humans by considering that it is relatively challenging to emulate multiple human traits at the same time during one spoofing attack section. For example, Pan *et al.* proposed the method to extract liveness information through eye blinks in face recognition [60]. Wei *et al.* detected counterfeit iris through texture analysis [84]. In this work, we have exploited the uniqueness of living traits in human cardiac motion to defend the above adversarial model. Specifically, we have tackled this challenge from two dimensions: hardware-based and software-based approaches. First, we integrated assisted sensors in Cardiac Scan, so that we can leverage additional information from these sensors to examine the legitimacy of subjects and capture the characteristics of multi-dimensional cardiac motions for liveness simultaneously. Specifically, as proposed in Section 6.4, the system employed multi-channel radars for noise reduction. Since the linear actuator only moves in rectilinear directions, the direction of arrival (DoA) [46] measurements with the linear actuator on these radars are different from DoA measured with real cardiac motion. Second, we have investigated software-based approaches. Because the sensor data from a live subject inevitably include vital sign (e.g., respiration) and other motion artifacts (e.g., body sway). These artifacts are not stored in the system database as credentials, so they are unable to be replicated and emulated for attack. Utilizing these vital sign detection and motion artifacts, liveness detection is conducted against the replay attack [26]. We programmed the actuator working with different moving amplitudes and frequencies to imitate cardiac motions of 12 subjects. *All replay attacks were rejected by our liveness detection method.*

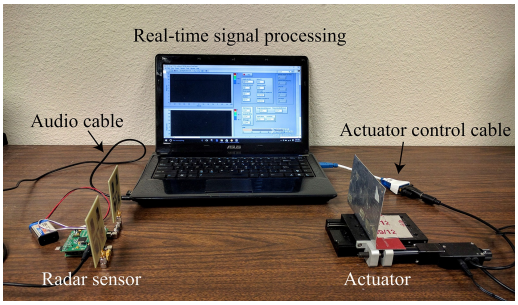



**Figure 17: A linear actuator imitates cardiac motion.**

## 9 RELATED WORK

**Heart-based Identification:** Heart-based identification has a long and rich research history in biometrics. There is sizable literature on user identification by analyzing heart-based signals. The most studied heart biosignals in identification application are the multi-lead electrocardiogram (ECG) body signals. Singh used both the analytical method of extracting fiducial features and the appearance method of extracting morphological features from the ECG trace for individual identification. The linear projection to a low-dimensional subspace is later applied to select the most significant features [74]. Zhao *et al.* extracted ECG feature for a human identification system by decomposing ECG signal into intrinsic mode functions using ensemble empirical mode decomposition [91]. Singh *et al.* delineated ECG waveform and extracted end fiducials from the heartbeat for individual authentication. The system is also evaluated in combination with face and fingerprint biometrics [75]. Silva *et al.* collected ECG from fingers for user authentication [18]. Safie *et al.* generated ECG features for authentication by using a pulse active ratio (PAR) technique [70]. To improve usability, other heart-related biosignals, such as Photoplethysmogram (PPG) [71, 78, 88], carotid pulse [17, 32], and finger pulse response [67], were investigated for human identification. Recently, there are some off-the-shelf user authentication products (e.g., the Nymi band [57]) using heart signatures from wrist pulse signals. However, these biosignals are not related to cardiac motion, in which case indirect or incomplete cardiac characterization will compromise the advantages of cardiac motion as a biometric. Moreover, these biosignals have to be obtained through skin contact, which is inconvenient and limits their applications for continuous authentication.

**Continuous User Authentication:** Most user authentication procedures, such as fingerprint or facial identification, only demand a one-pass session, which enables imposters to access the system until the user logs out. To address this security flaw, methods of continuous user authentication are explored. There are three categories. One category is to use soft biometric traits. Niinuma *et al.* used the color of user's clothing and facial skin for continuous monitoring [56]. This approach is readily counterfeited to confuse the system. The second category is to use behavioral biometrics. Keystroke dynamics, especially the rollover pattern, have been used for continuous authentication (e.g., Pinto *et al.* [63], Shepherd [73], Ali *et al.* [6]). Saevanee *et al.* utilize a text-based multimodal biometric including linguistic analysis, keystroke dynamics and behavioural profiling [69]. Behavioral screentouch features have also been explored for continuous authentication (e.g., Frank *et al.* [24] and Chan *et al.* [13]). Some studies leveraged eye movement biometrics (e.g., Eberz *et al.* [23], Mock *et al.* [54] and Song *et al.* [77]). Sitova *et al.* used hand gestures for continuous smartphone authentication [76], however, these methods require users to be obligated to continuously interact with systems for authentication. Khan *et al.* developed an implicit authentication (IA) framework for Android smartphone based on behavioral biometrics [34], yet there is no new biometrics proposed in this work. The third category is to use physiological biometrics. Rasmussen *et al.* utilized human body pulse-response as a continuous authentication mechanism[67]. However, this method demands the human body to make contact with electrodes, which is not user-friendly.

**Radio-based Human Sensing:** In recent years, there is a large wave of research work on radio-based (e.g., WiFi) human sensing applications. Pu *et al.* investigated gesture recognition by using radio signals [66]. Wang *et al.* studied radio signal analysis for people localization and motion tracking [83]. Li and Zhu explored the possibility of extracting fine-grained gait parameters from radio signals [45]. Adib *et al.* showed that a radio-based sensing system can collect physiological information, such as respiration, heartbeat, for health monitoring [2]. Obeid *et al.* obtained heart rate and heart rate variability (HRV) via microwave Doppler radar [58]. Boric *et al.* separated two subjects through multiple antenna systems [11]. Zhao *et al.* proposed EQ-Radio to infer a person's emotions from RF signals reflected off the body [90]. Scientists at Argonne National Laboratory have devised a millimeter-wave (mmW) system to remotely measure heartbeat, respiration and body motion [7]. However, little work exists for radio-based sensing identification. Identification is very challenging because it requires obtaining high-fidelity biometric information through non-contact radio sensing.

## 10 CONCLUSION AND FUTURE WORK

Existing biometric-based authentication systems are far from satisfactory. In this paper, we introduced a novel biometric system, Cardiac Scan, for non-contact continuous authentication. Specifically, Cardiac Scan can measure the unique cardiac motion of individuals with regard to the cardiac moving dynamics (e.g., speed, acceleration, etc.) and heart-blood circulation functionality in individuals. The system is unobtrusive, difficult to counterfeit, and easy to use. Our pilot study with 78 subjects showed that the system has a high balanced accuracy and low equal error rate. We evaluated the system in different complex conditions. As demonstrated in the longitudinal study, the cardiac motion biometric is robust

In the future work, we plan to evaluate Cardiac Scan with people of cardiovascular diseases, such as cardiac arrhythmia or using a cardiac pacemaker. Also, other methods, such as wavelet transformation [42] and area calculation upon phase portraits [65], will be further explored improve the system accuracy.

## ACKNOWLEDGEMENT

We thank our shepherd Lakshminarayanan Subramanian and anonymous reviewers for their insightful comments on this paper. This work was in part supported by the National Science Foundation under grant No. 1718483/1718375, No. 1564104, and No. CNS-1421903.

## REFERENCES


[1] 2016. Friends hacked into Windows using Windows Hello/camera-login. https://www.reddit.com/r/Surface/comments/4d9ykj/friends_hacked_into_windows_using_windows/. (April 2016). Accessed by August 2, 2017.

[2] Fadel Adib, Hongzi Mao, Zachary Kabelac, Dina Katabi, and Robert C Miller. 2015. Smart Homes that Monitor Breathing and Heart Rate. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, Seoul, Republic of Korea, 837–846.

[3] Foteini Agrafioti and Dimitrios Hatzinakos. 2008. ECG based recognition using second order statistics. In *Communication Networks and Services Research Conference, 2008. CNSR 2008. 6th Annual*. IEEE, 82–87.

[4] Foteini Agrafioti and Dimitrios Hatzinakos. 2010. Signal validation for cardiac biometrics. In *Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on*. IEEE, 1734–1737.

[5] Foteini Agrafioti, Dimitrios Hatzinakos, and Jiexin Gao. 2011. *Heart biometrics: Theory, methods and applications*. INTECH Open Access Publisher.

[6] Zaire Ali, Jamie Payton, and Vincent Sritapan. 2016. At Your Fingertips: Considering Finger Distinctness in Continuous Touch-Based Authentication for Mobile Devices. In *Security and Privacy Workshops (SPW), 2016 IEEE*. IEEE, 272–275.

[7] Argonne National Laboratory. 2012. Millimeter-Wave Systems Track Biometrics; Detect Chemicals, Gases and Radiation. https://www.anl.gov/sites/anl.gov/files/millimeter_wave_detector.pdf. (November 2012). https://www.anl.gov/sites/anl.gov/files/millimeter_wave_detector.pdf Accessed by August. 2, 2017.

[8] Kim E Barrett, Susan M Barman, and Scott Boitano. 2010. *Ganong's review of medical physiology*. New Delhi: McGraw Hill, 2010.

[9] Joe Belfiore. 2015. Making Windows 10 More Personal and More Secure with Windows Hello. https://blogs.windows.com/windowsexperience/2015/03/17/making-windows-10-more-personal-and-more-secure-with-windows-hello/ #tK-BXz8oqEQBUXG4q.97. (March 2015). Accessed by March 10, 2017.

[10] Lena Biel, Ola Pettersson, Lennart Philipson, and Peter Wide. 2001. ECG analysis: a new approach in human identification. *Instrumentation and Measurement, IEEE Transactions on* 50, 3 (2001), 808–812.

[11] Olga Boric-Lubecke, Victor M Lubecke, Anders Host-Madsen, Dragan Samardzija, and Ken Cheung. 2005. Doppler radar sensing of multiple subjects in single and multiple antenna systems. In *TELSIKS 2005-2005 uth International Conference on Telecommunication in ModernSatellite, Cable and Broadcasting Services*, Vol. 1. IEEE, 7–11.

[12] Marcus Carlsson, Peter Cain, Catarina Holmqvist, Freddy Stahlberg, Stig Lundback, and Hakan Arheden. 2004. Total heart volume variation throughout the cardiac cycle in humans. *American Journal of Physiology-Heart and Circulatory Physiology* 287, 1 (2004), H243–H250.

[13] Alexander Chan, Tzipora Halevi, and Nasir Memon. 2014. Touchpad input for continuous biometric authentication. In *IFIP International Conference on Communications and Multimedia Security*. Springer, 86–91.

[14] Chaos Computer Club (CCC). 2013. Chaos Computer Club Breaks Apple TouchID. https://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid. (September 2013). Accessed by November 10, 2016.

[15] Chaos Computer Club (CCC). 2014. Fingerprint Biometrics Hacked Again. http://www.ccc.de/en/updates/2014/ursel. (Dec. 2014). Accessed by November 10, 2016.

[16] Kunmu Chen, Yong Huang, Jianping Zhang, and Adam Norman. 2000. Microwave life-detection systems for searching human subjects under earthquake rubble or behind barrier. *Biomedical Engineering, IEEE Transactions on* 47, 1 (2000), 105–114.

[17] Mei Chen, Joseph A O?Sullivan, Alan D Kaplan, Po-Hsiang Lai, Erik J Sirevaag, and John W Rohrbaugh. 2009. Biometrics with physical exercise using laser doppler vibrometry measurements of the carotid pulse. In *International Conference on Biometrics, Identity and Security (BIdS)*. 1–6.

[18] Hugo Plácido Da Silva, Ana Fred, Andre Lourenco, and Anil K Jain. 2013. Finger ECG signal for user authentication: Usability and performance. In *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on*. IEEE, 1–8.

[19] Carlo J De Luca, L Donald Gilmore, Mikhail Kuznetsov, and Serge H Roy. 2010. Filtering the surface EMG signal: Movement artifact and baseline noise contamination. *Journal of biomechanics* 43, 8 (2010), 1573–1579.

[20] J. Decker. 2016. Windows Hello biometrics in the enterprise. https://technet.microsoft.com/en-us/itpro/windows/keep-secure/windows-hello-in-enterprise. (September 2016). Accessed by November 10, 2016.

[21] Amy D Droitcour, Olga Boric-Lubecke, Victor M Lubecke, Jenshan Lin, and Gregory TA Kovacs. 2004. Range correlation and I/Q performance benefits in single-chip silicon Doppler radars for noncontact cardiopulmonary monitoring. *Microwave Theory and Techniques, IEEE Transactions on* 52, 3 (2004), 838–848.

[22] Simon Eberz, Nicola Paoletti, Marc Roeschlin, Marta Kwiatkowska, I Martinovic, and A Patané. 2017. Broken hearted: How to attack ECG biometrics. In *NDSS*.

[23] Simon Eberz, Kasper Bonne Rasmussen, Vincent Lenders, and Ivan Martinovic. 2015. Preventing Lunchtime Attacks: Fighting Insider Threats With Eye Movement Biometrics.. In *NDSS*.

[24] Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. 2013. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE transactions on information forensics and security* 8, 1 (2013), 136–148.

[25] Jiexin Gao, Foteini Agrafioti, Hoda Mohammadzade, and Dimitrios Hatzinakos. 2011. ECG for blind identity verification in distributed systems. In *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*. IEEE, 1916–1919.

[26] Changzhan Gu and Changzhi Li. 2015. Assessment of Human Respiration Patterns via Noncontact Sensing Using Doppler Multi-Radar System. *Sensors* 15, 3 (2015), 6383–6398.

[27] John E Hall. 2010. *Guyton and Hall textbook of medical physiology*. Elsevier Health Sciences.

[28] Steven A Israel, John M Irvine, Andrew Cheng, Mark D Wiederhold, and Brenda K Wiederhold. 2005. ECG to identify individuals. *Pattern recognition* 38, 1 (2005), 133–142.

[29] Kazuyoshi Itoh. 1982. Analysis of the phase unwrapping algorithm. *Applied Optics* 21, 14 (1982), 2470–2470.

[30] Anil Jain, Brendan Klare, and Arun Ross. 2015. Guidelines for best practices in biometrics research. In *Biometrics (ICB), 2015 International Conference on*. IEEE, 541–545.

[31] Peter Johnson, Richard Lazarick, Emanuela Marasco, Elaine Newton, Arun Ross, and Stephanie Schuckers. 2012. Biometric liveness detection: Framework and metrics. In *International biometric performance conference*, Vol. 1.

[32] Alan D Kaplan, Joseph A O'Sullivan, Erik J Sirevaag, and John W Rohrbaugh. 2009. Laser Doppler vibrometry measurements of the carotid pulse: biometrics using hidden Markov models. In *SPIE Defense, Security, and Sensing*. International Society for Optics and Photonics, 730624–730624.

[33] Arnold M Katz. 2010. *Physiology of the Heart*. Lippincott Williams & Wilkins.

[34] Hassan Khan, Aaron Atwater, and Urs Hengartner. 2014. Itus: an implicit authentication framework for android. In *Proceedings of the 20th annual international conference on Mobile computing and networking*. ACM, 507–518.

[35] John E Kiriazi, Olga Boric-Lubecke, and Victor M Lubecke. 2012. Dual-frequency technique for assessment of cardiopulmonary effective RCS and displacement. *Sensors Journal, IEEE* 12, 3 (2012), 574–582.

[36] Effie Lai-Chong Law, Virpi Roto, Marc Hassenzahl, Arnold POS Vermeeren, and Joke Kort. 2009. Understanding, scoping and defining user experience: a survey approach. (2009), 719–728 pages.

[37] Changzhi Li and Jenshan Lin. 2007. Non-Contact Measurement of Periodic Movements by a 22-40GHz Radar Sensor Using Nonlinear Phase Modulation. In *Microwave Symposium, 2007. IEEE/MTT-S International*. IEEE, 579–582.

[38] Changzhi Li and Jenshan Lin. 2007. Optimal carrier frequency of non-contact vital sign detectors. In *Radio and Wireless Symposium, 2007 IEEE*. IEEE, 281–284.

[39] Changzhi Li and Jenshan Lin. 2008. Complex signal demodulation and random body movement cancellation techniques for non-contact vital sign detection. In *Microwave Symposium Digest, 2008 IEEE MTT-S International*. IEEE, 567–570.

[40] Changzhi Li and Jenshan Lin. 2008. Random body movement cancellation in Doppler radar vital sign detection. *IEEE Transactions on Microwave Theory and Techniques* 56, 12 (2008), 3143–3152.

[41] Changzhi Li and Jenshan Lin. 2013. *Microwave noncontact motion sensing and analysis*. John Wiley & Sons.

[42] Cuiwei Li, Chongxun Zheng, and Changfeng Tai. 1995. Detection of ECG characteristic points using wavelet transforms. *Biomedical Engineering, IEEE Transactions on* 42, 1 (1995), 21–28.

[43] Ming Li and Xin Li. 2014. Verification based ECG biometrics with cardiac irregular conditions using heartbeat level and segment level information fusion. In *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*. IEEE, 3769–3773.

[44] Ming Li and Shrikanth Narayanan. 2010. Robust ECG biometrics by fusing temporal and cepstral information. In *Pattern Recognition (ICPR), 2010 20th International Conference on*. IEEE, 1326–1329.

[45] Yan Li and Ting Zhu. 2016. Gait-Based Wi-Fi Signatures for Privacy-Preserving. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*. ACM, 571–582.

[46] Adrian Lin and Hao Ling. 2007. Doppler and direction-of-arrival (DDOA) radar for multiple-mover sensing. *IEEE transactions on aerospace and electronic systems* 43, 4 (2007), 1496–1509.

[47] Feng Lin, Yan Zhuang, Chen Song, Aosen Wang, Yiran Li, Changzhan Gu, Changzhi Li, and Wenyao Xu. 2017. SleepSense: A Noncontact and Cost-Effective Sleep Monitoring System. *IEEE transactions on biomedical circuits and systems* 11, 1 (2017), 189–202.

[48] James C Lin. 1992. Microwave sensing of physiological movement and volume change: A review. *Bioelectromagnetics* 13, 6 (1992), 557–565.

[49] Bram Lohman, Olga Boric-Lubecke, VM Lubecke, PW Ong, and MM Sondhi. 2002. A digital signal processor for Doppler radar sensing of vital signs. *Engineering in*

*Medicine and Biology Magazine, IEEE* 21, 5 (2002), 161–164.
[50] Justin Leo Cheang Loong, Khazaimatol S Subari, Rosli Besar, and Muhammad Kamil Abdullah. 2010. A new approach to ECG biometric systems: a comparative study between LPC and WPD systems. *World Academy of Science, Engineering and Technology* 68 (2010), 759–764.
[51] Sébastien Marcel, Mark S Nixon, and Stan Z Li. 2014. *Handbook of Biometric Anti-Spoofing*. Springer.
[52] Gian Luca Marcialis, Aaron Lewicke, Bozhao Tan, Pietro Coli, Dominic Grimberg, Alberto Congiu, Alessandra Tidu, Fabio Roli, and Stephanie Schuckers. 2009. First international fingerprint liveness detection competition??ivdet 2009. In *International Conference on Image Analysis and Processing*. Springer, 12–23.
[53] Manel Martinez and Rainer Stiefelhagen. 2012. Breath rate monitoring during sleep using Near-IR imagery and PCA. In *Pattern Recognition (ICPR), 2012 21st International Conference on*. IEEE, 3472–3475.
[54] Kenrick Mock, Bogdan Hoanca, Justin Weaver, and Mikal Milton. 2012. Real-time continuous iris recognition for authentication using an eye tracker. In *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 1007–1009.
[55] Gary Garcia Molina, Fons Bruekers, Cristian Presura, Marijn Damstra, and Michiel van der Veen. 2007. Morphological synthesis of ECG signals for person authentication. In *15th European Signal Processing Conference (EUSIPCO 2007)*. Poznan, Poland.
[56] Koichiro Niinuma, Unsang Park, and Anil K Jain. 2010. Soft biometric traits for continuous user authentication. *IEEE Transactions on information forensics and security* 5, 4 (2010), 771–780.
[57] Nymi. 2017. The Nymi band. https://nymi.com/product_overview. (August 2017). Accessed by August 2, 2017.
[58] Dany Obeid, Gheorghe Zaharia, Sawsan Sadek, and Ghaïs El Zein. 2012. Microwave doppler radar for heartbeat detection vs electrocardiogram. *Microwave and Optical Technology Letters* 54, 11 (2012), 2610–2617.
[59] Ikenna Odinaka, Po-Hsiang Lai, Alan D Kaplan, Joseph A O'Sullivan, Erik J Sirevaag, and John W Rohrbaugh. 2012. ECG biometric recognition: A comparative analysis. *Information Forensics and Security, IEEE Transactions on* 7, 6 (2012), 1812–1824.
[60] Gang Pan, Lin Sun, Zhaohui Wu, and Shihong Lao. 2007. Eyeblink-based anti-spoofing in face recognition from a generic webcamera. In *2007 IEEE 11th International Conference on Computer Vision*. IEEE, 1–8.
[61] Byung-Kwon Park, Olga Boric-Lubecke, and Victor M Lubecke. 2007. Arctangent demodulation with DC offset compensation in quadrature Doppler radar receiver systems. *Microwave Theory and Techniques, IEEE Transactions on* 55, 5 (2007), 1073–1079.
[62] Florian Pfanner, Joscha Maier, Thomas Allmendinger, Thomas Flohr, and Marc Kachelrieß. 2013. Monitoring internal organ motion with continuous wave radar in CT. *Medical physics* 40, 9 (2013), 091915.
[63] Paulo Pinto, Bernardo Patrão, and Henrique Santos. 2014. Free typed text using keystroke dynamics for continuous authentication. In *IFIP International Conference on Communications and Multimedia Security*. Springer, 33–45.
[64] Konstantinos N Plataniotis, Dimitrios Hatzinakos, and Jimmy KM Lee. 2006. ECG biometric recognition without fiducial detection. In *Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session on Research at the*. IEEE, 1–6.
[65] Emil Plesnik, Olga Malgina, Jurij F Tasič, and Matej Zajc. 2011. Detection of the electrocardiogram fiducial points in the phase space using area calculation. *Electrotechnical. Review* 78, 5 (2011), 257–262.
[66] Qifan Pu, Sidhant Gupta, Shyamnath Gollakota, and Shwetak Patel. 2013. Whole-home gesture recognition using wireless signals. In *Proceedings of the 19th annual international conference on Mobile computing & networking*. ACM, 27–38.
[67] Kasper Bonne Rasmussen, Marc Roeschlin, Ivan Martinovic, and Gene Tsudik. 2014. Authentication Using Pulse- Response Biometrics. In *The Network and Distributed System Security Symposium (NDSS)*. San Diego, CA.
[68] Dan Rissacher and Dan Galy. 2015. Cardiac radar for biometric identification using nearest neighbour of continuous wavelet transform peaks. In *Identity, Security and Behavior Analysis (ISBA), 2015 IEEE International Conference on*. IEEE, 1–6.
[69] Hataichanok Saevanee, Nathan Clarke, Steven Furnell, and Valerio Biscione. 2015. Continuous user authentication using multi-modal biometrics. *Computers & Security* 53 (2015), 234–246.
[70] Sairul I Safie, John J Soraghan, and Lykourgos Petropoulakis. 2011. Electrocardiogram (ECG) biometric authentication using pulse active ratio (PAR). *IEEE Transactions on Information Forensics and Security* 6, 4 (2011), 1315–1322.
[71] NSGR Salanke, Andrews Samraj, N Maheswari, and S Sadhasivam. 2013. Enhancement in the design of biometric identification system based on photoplethysmography data. In *Green High Performance Computing (ICGHPC), 2013 IEEE International Conference on*. IEEE, 1–6.
[72] Lorenzo Scalise, Ilaria Ercoli, Paolo Marchionni, and Enrico Primo Tomasini. 2011. Measurement of respiration rate in preterm infants by laser Doppler vibrometry. In *Medical Measurements and Applications Proceedings (MeMeA), 2011 IEEE International Workshop on*. IEEE, 657–661.
[73] SJ Shepherd. 1995. Continuous authentication by analysis of keyboard typing characteristics. In *Security and Detection, 1995., European Convention on*. IET, 111–114.
[74] Yogendra Narain Singh. 2014. Individual identification using linear projection of heartbeat features. *Applied Computational Intelligence and Soft Computing* 2014 (2014), 8.
[75] Yogendra Narain Singh and Sanjay Kumar Singh. 2011. Evaluation of electrocardiogram for biometric authentication. *Journal of Information Security* 3 (2011), 39.
[76] Zdeňka Sitová, Jaroslav Šeděnka, Qing Yang, Ge Peng, Gang Zhou, Paolo Gasti, and Kiran S Balagani. 2016. HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users. *IEEE Transactions on Information Forensics and Security* 11, 5 (2016), 877–892.
[77] Chen Song, Aosen Wang, Kui Ren, and Wenyao Xu. 2016. "EyeVeri: A Secure and Usable Approach for Smartphone User Authentication". In *IEEE International Conference on Computer Communication (INFOCOM'16)*. San Francisco, California, 1 – 9.
[78] Petros Spachos, Jiexin Gao, and Dimitrios Hatzinakos. 2011. Feasibility study of photoplethysmographic signals for biometric identification. In *Digital Signal Processing (DSP), 2011 17th International Conference on*. IEEE, 1–5.
[79] Fahim Sufi, Ibrahim Khalil, and Jiankun Hu. 2010. ECG-based authentication. In *Handbook of Information and Communication Security*. Springer, 309–331.
[80] Xiaoyang Tan, Yi Li, Jun Liu, and Lin Jiang. 2010. Face liveness detection from a single image with sparse low rank bilinear discriminative model. In *European Conference on Computer Vision*. Springer, 504–517.
[81] N Venkatesh and Srinivasan Jayaraman. 2010. Human electrocardiogram for biometrics using DTW and FLDA. In *Pattern Recognition (ICPR), 2010 20th International Conference on*. IEEE, 3838–3841.
[82] Fu-Kang Wang, Tzyy-Sheng Horng, Kang-Chun Peng, Je-Kuan Jau, Jian-Yu Li, and Cheng-Chung Chen. 2011. Single-antenna Doppler radars using self and mutual injection locking for vital sign detection with random body movement cancellation. *Microwave Theory and Techniques, IEEE Transactions on* 59, 12 (2011), 3577–3587.
[83] Guanhua Wang, Yongpan Zou, Zimu Zhou, Kaishun Wu, and Lionel M Ni. 2014. We can hear you with wi-fi!. In *Proceedings of the 20th annual international conference on Mobile computing and networking*. ACM, 593–604.
[84] Zhuoshi Wei, Xianchao Qiu, Zhenan Sun, and Tieniu Tan. 2008. Counterfeit iris detection based on texture analysis. In *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on*. IEEE, 1–4.
[85] Zack Whittaker. 2016. These companies lost your data in 2015's biggest hacks, breaches. http://www.zdnet.com/pictures/biggest-hacks-security-data-breaches-2015/. (January 2016). Accessed by August, 2016.
[86] Bernard Widrow, John R Glover Jr, John M McCool, John Kaunitz, Charles S Williams, Robert H Hearn, James R Zeidler, Eugene Dong Jr, and Robert C Goodlin. 1975. Adaptive noise cancelling: Principles and applications. *Proc. IEEE* 63, 12 (1975), 1692–1716.
[87] Chenxi Yang. 2015. *MOTION NOISE CANCELLATION IN SEISMOCARDIOGRAM OF MOVING*. Ph.D. Dissertation. STEVENS INSTITUTE OF TECHNOLOGY.
[88] Jianchu Yao, Xiaodong Sun, and Yongbo Wan. 2007. A pilot study on using derivatives of photoplethysmographic signals as a biometric identifier. In *2007 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. IEEE, 4576–4579.
[89] Mari Zakrzewski, Harri Raittinen, and Jukka Vanhala. 2012. Comparison of center estimation algorithms for heart and respiration monitoring with microwave Doppler radar. *IEEE Sensors Journal* 12, 3 (2012), 627–634.
[90] Mingmin Zhao, Fadel Adib, and Dina Katabi. 2016. Emotion recognition using wireless signals. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*. ACM, 95–108.
[91] Zhidong Zhao, Lei Yang, Diandian Chen, and Yi Luo. 2013. A human ECG identification system based on ensemble empirical mode decomposition. *Sensors* 13, 5 (2013), 6832–6864.
[92] Yan Zhuang, Chen Song, Feng Lin, Yiran Li, Changzhi Li, and Wenyao Xu. 2016. On the feasibility of Non-contact Cardiac Motion Sensing for emerging heart-based biometrics. In *2016 IEEE Radio and Wireless Symposium (RWS)*. IEEE, 204–206.
[93] Yan Zhuang, Chen Song, Aosen Wang, Feng Lin, Yiran Li, Changzhan Gu, Changzhi Li, and Wenyao Xu. 2015. SleepSense: Non-invasive sleep event recognition using an electromagnetic probe. In *Wearable and Implantable Body Sensor Networks (BSN), 2015 IEEE 12th International Conference on*. IEEE, 1–6.