Simultaneous Authentication of Multiple Users Using a Single mmWave Radar

Yao Wang, Tao Gu, *Fellow, IEEE,* and Haibin Zhang

***Abstract*—User authentication is crucial for maintaining privacy. However, most existing methods are designed for single-user scenarios and may not be efficient for multiple users. To address this issue, we propose *M-Auth*, a *M*ultiuser *Auth*entication system that utilizes a commercial mmWave radar to detect the unique breathing pattern. We exploit the phenomenon that chest movements due to breathing can alter radio frequency signals. To make *M-Auth* more effective in capturing signals from multiple users, we design an auxiliary rotating gadget to adjust the radar orientation dynamically. By using mmWave's high directivity, we can isolate individual components from blended RF signals and focus on reflections from different positions. We propose an energy comparison method to filter out irrelevant body movements and retain fine-grained respiration traits. Subsequently, we develop a feature selection pipeline to extract the most informative features and train a machine learning-based classifier to identify each user. *M-Auth* is practical because it is non-contact and passive, and it is secure because respiration is unique and challenging to forge. Extensive experiments with 37 participants demonstrate that M-Auth is effective in verifying legitimate users and thwarting spoofing attacks, with an authentication accuracy of over 96% and an attack detection rate of over 95%.**

***Index Terms*—Respiration, Authentication, mmWave Sensing**

I. Introduction

BIOMETRIC authentication has evolved significantly in recent years, with advanced algorithms that can analyze unique physical characteristics like fingerprints, irises, and facial features. However, despite these advancements, biometric authentication systems remain vulnerable to a variety of attacks, such as the use of fake fingerprints or contact lenses placed over photos of irises [1], [2]. To address these security concerns, continuous authentication has emerged as a promising solution. By continuously monitoring the user's biometric data in real-time, this approach can detect any anomalies or suspicious behavior and prevent unauthorized access to sensitive data. Moreover, continuous authentication can enhance the user experience by eliminating the need for repeated logins, as the system can automatically verify the user's identity throughout the entire duration of their session.

Existing solutions typically use behavioral biometrics, such as gait patterns [2], [3], keystroke dynamics [4], [5], and eye movements [6], [7], for continuous authentication. However, these solutions require active user engagement, such as walking a specific range, typing on a keyboard, or looking at visual stimuli on a screen. To avoid such laborious and tedious operations, various studies have proposed leveraging physiological biometrics, such as brain activity [8], fingertip pulses [9], and heart rhythms [10]. These methods, however, require users to wear additional cumbersome and obtrusive devices.

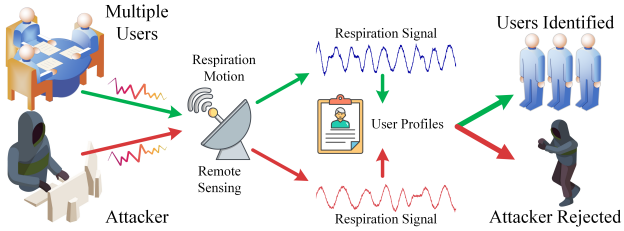


Fig. 1. A mmWave-based respiration sensing system for continuous multi-user authentication.

Wireless sensing and spontaneous physiological biometrics, such as respiration and heartbeat, have been used to propose non-contact and passive continuous authentication mechanisms. *Cardiac Scan* [11] and *BreathID* [12] are examples of these mechanisms, which use a continuous-wave Doppler radar and Wi-Fi infrastructure to capture heartbeat activities and respiration motions for continuous authentication, respectively. While these methods have the advantage of freeing users from getting involved in authentication and requiring no user contact, they have significant limitations. For instance, their restricted working range makes it inaccurate to identify far-field users, which is not suitable in larger spaces. Additionally, they only cater to single users, ignoring the broader applications of multiuser settings such as smart homes and workplaces, where multiple individuals are typically present. The primary reasons behind these limitations are that the frequency of the signals they adopt is fixed, and all reflections are inextricably mingled in both time and frequency domains.

Recent efforts have focused on enabling simultaneous authentication for multiple users [3], [13]. For example, Kong *et al.* [13] reused Wi-Fi signals to capture several predefined activities from different users and implemented a time-of-arrival measurement technique to distinguish between the components. Although this proposed system allows for multi-user authentication, it requires at least $0.8m$ spacing between users to achieve acceptable accuracy, which poses challenges when users are in close proximity, such as standing shoulder-to-shoulder or sitting abreast. Additionally, the system still suffers from the constraint of requiring users to complete specified tasks, and the average accuracy of 87.6% is not satisfactory compared to state-of-the-art works.

Yao Wang and Haibin Zhang are with the School of Cyber Engineering, Xidian University, China. E-mail: wangyao@xidian.edu.cn, hbzhang@mail.xidian.edu.cn.

Tao Gu is with the School of Computing, Macquarie University, Australia. E-mail: tao.gu@mq.edu.au.

Manuscript received month date, year; revised month date, year. (Corresponding author: Haibin Zhang.)

Design Goals. To address current limitations, we present *M-Auth*, a continuous multiuser authentication system that senses respiratory motions using a single commercial off-the-shelf mmWave radar. Fig. 1 provides a snapshot of *M-Auth*. Users enroll in the system to create profiles before being authenticated, and an incoming respiration signal is compared to stored profiles to identify whether the signal comes from a genuine user or an attacker. Specifically, the following are the highlights of our work:

Non-contact and Passive. We use radio frequency (RF) waves to remotely detect the unique, naturally occurring respiration motion, without the need for physical contact or exertion on the part of the user.

Ubiquitous and Trustworthy. All people must breathe, and it is difficult to fake breathing patterns. Meanwhile, authentications that rely on gait or hand movements are not practical for individuals with foot or hand disabilities and can easily be copied by a camera for imitation attacks [14].

Close Proximity. Our system enables concurrent authentication even when users have no separation spacing. This is in contrast to existing RF-based solutions, which typically require a separation of at least 0.8-1m [3], [13]. The limitation makes it difficult to authenticate users who are close to each other.

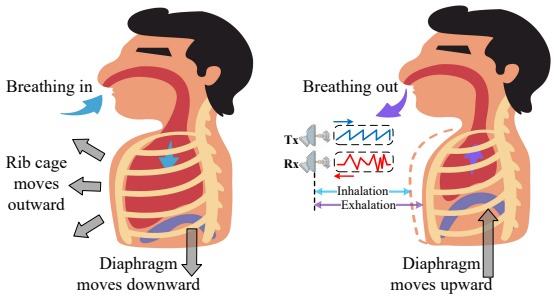
Technical Challenges. MmWave sensing has shown promise as a non-invasive method for monitoring respiratory rates by roughly identifying signal crests [15], [16]. However, when it comes to authentication, it is necessary to identify subtle differences in respiration signals between users. To fully unlock the potential of mmWave sensing in detecting subtle motion differences, we need to address the following technical challenges:

To ensure accurate authentication, it is important to consider the impact of angle-of-arrival (AoA) on signal-to-noise ratio (SNR). While existing beamforming techniques, such as phased array and beam steering, improve spectral efficiencies in a fixed direction [17], they are not well-suited for mobile users with unpredictable AoAs. To address this challenge, we have developed a rotating device that mechanically controls the radar and adjusts its orientation in response to the positions of users, thereby ensuring effective signal capture.

Respiration signals are susceptible to motion artifacts caused by body movements, which can overshadow the small chest movements caused by breathing. These interferences typically have larger amplitudes of reflected radio waves compared to respiratory movements. To eliminate them, we propose a comparison method that measures the energy of the signal within a defined time window.

Effective authentication requires identifiable features, which can be achieved by pinpointing the most representative features in the respiration signal. To do this, a feature selection pipeline is created. This pipeline combines the wavelet packet decomposition (WPD) and recursive feature elimination (RFE) techniques to analyze which features are most representative.

Applications. In IoT-rich environments, it is convenient to have support for multi-user authentication functionality. In a home setting, *M-Auth* can be used to provide personalized services to different family members. For instance, it can be used to monitor the sleeping patterns of each family member and adjust different temperature preferences and lighting levels accordingly to ensure a peaceful and comfortable sleep. In a large corporate setting with multiple people, *M-Auth* can be used to verify personnel for access control, ensuring that only authorized users are permitted to remain in the area. Besides, *M-Auth* can improve the continuous authentication capability over traditional one-time confirmation mechanisms, making it an essential tool for ensuring data privacy and security in today's connected world.



(a) Inhale Motion (b) Exhale Motion

Fig. 2. Respiratory motion cycle and sensing rationale.

In summary, this paper makes the following contributions:

- We develop a secure, passive, and contactless continuous authentication system for multiple users based on their unique breathing patterns. Through extensive experiments, we demonstrate the system's effectiveness, with an average authentication accuracy of over 96%.
- We design a dynamic mechanical device for effective radar sensing. We also provide a circuit schematic for interacting with the radar, making it easy for researchers to replicate its functions. This design promises to improve current static sensing solutions to be more cost-effective and dependable for coverage.
- We design a wavelet-based method for learning respiratory signals, which greatly shortens the authentication time and improves usability. We also develop a processing pipeline that includes segmentation, feature extraction, and optimal feature selection, which enhances the robustness of the system.

II. Preliminaries

A. Respiratory Biometrics

This paper explores the use of respiratory motion as a unique factor for user authentication. By analyzing the two phases of the respiratory cycle, inhalation and exhalation, we can establish a person's unique physiological profile. During inhalation, as shown in Fig. 2(a), the contraction of intercostal and abdominal muscles pulls the ribs outward, while the diaphragm moves downward, causing the chest cavity to expand. Exhalation, on the other hand, occurs when the muscles relax and the diaphragm returns to its original position, causing the chest cavity to decrease in size as shown in Fig. 2(b). As each individual has a unique physiological structure, such as lung volumes and chest movement dynamics, their respiratory phases differ, which makes respiratory motion a distinctive biometric factor. Respiratory motion is more difficult to forge than traditional biometric modalities such as face and voice, as it is inherently linked to physiological activities, thus providing a higher level of security.

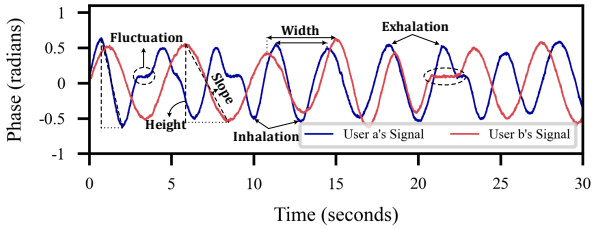


Fig. 3. Variations of phase due to respiration.

B. Feasibility Study

The radar device works by having the transmitter (Tx) send periodic sawtooth waves to the user, as illustrated in Fig. 2(b). As the user inhales and exhales, the chest movements alter the incident signal. This alteration in the signal is then reflected back to the receiver (Rx), which analyzes the changes to determine the user's breathing patterns. A frequency-modulated continuous wave (FMCW) signal can be used to detect chest movements that are caused by respiration and differentiate between individuals. By calculating the phase changes between consecutive measurements, the displacement of the chest can be tracked over time. In particular, the linear relationship between signal phase $\phi(t)$ and distance $d(t)$ is calculated as follows [18]:

$$d(t) = \frac{\lambda}{4\pi}\phi(t), \tag{1}$$

where λ and $\phi(t)$ are the wavelength and phase, respectively. It has been observed that short-wavelength signals are more sensitive to distance variations. In this work, we use a $4mm$ wavelength mmWave. With a phase change of $\Delta\phi = \pi$, Δd can be as high as $1mm$, which is sufficient to detect the small chest displacements produced by respiration.

We will further study the correlation between respiration and the captured signals. Two participants are asked to sit facing the device and breathe normally. As shown in Fig. 3, their respiration waveforms are significantly different. Morphological characteristics, such as pulse height, width, slope, and fluctuations, showed apparent variations between User a and User b. These distinctions are primarily due to individual differences in intercostal muscle strength and lung volume. This study shows that mmWave can capture even the smallest differences in respiratory movements, which motivates us to use these unique characteristics for authentication purposes.

C. Threat Model

In this work, we assume that the end device is secure and resistant to tampering or theft attempts by attackers targeting the matching mechanism or biometric templates. The user data collected by the device has been de-identified, removing any personally identifiable information. Additionally, this de-identified user data is stored locally, adding an extra layer of security to prevent potential leaks or unauthorized access. While respiration motion is a complex method and may be more secure than other authentication types like passwords and fingerprints, we will consider the following social engineering attacks to ensure its reliability:

Blind Attack. An adversary is uncertain about the genuine user's breathing patterns, such as their rate, depth, and rhythm changes. During the attack, the adversary may resort to performing arbitrary respiration motions to *M-Auth* in an attempt to produce similar effects on the system as the genuine user does.

Impersonation Attack. An attacker could potentially observe the breathing patterns of a legitimate user through shoulder surfing or video recordings. They may attempt to imitate the user's breathing in order to bypass security measures, relying on their own understanding of the pattern.

Replay Attack. This attack is more sophisticated than the previous two. The attacker is assumed to have knowledge of the authentication principle, and can place a concealed mmWave sensor in close proximity to record the legitimate user's body-reflected signals. Additionally, the attacker can intercept internal communication and inject the recorded signal to deceive the system.

III. System Overview

Fig. 4 presents the workflow of *M-Auth*, which consists of the following modules:

Signal Capturing. Beamforming techniques typically enhance signals in a specific direction, making them unsuitable for improving signal quality when users are mobile. To capture echo signals from multiple users effectively, we first eliminate reflections from static objects (e.g., walls) and then measure the users' positions. Next, we implement a clustering algorithm to estimate the central position of the users. Finally, we develop a mechanical rotating device to dynamically adjust the radar's orientation toward the centroid for reliable sensing.

Signal Processing. After determining the direction, *M-Auth* authenticates users within range of the radar. This module eliminates noise from the captured signal by combining a band-pass filter and an adaptive filter. To eliminate irrelevant body motion reflections, we propose a signal comparison scheme that involves calculating signal energy for a specific time window. The system then uses extremum analysis to segment the respiration signal. Finally, we employ wavelet packet decomposition (WPD) and recursive feature elimination (RFE) techniques to select the features that are most associated with respiration.

Authentication. Once feature selection is complete, *M-Auth* labels the corresponding features and saves them in order to construct biometric templates. These stored features are then used to build a machine learning-based classifier that determines whether a given visitor is a legitimate user or an attacker. In addition, our system offers template updating to adapt to changes in respiration patterns that may result from mood swings or energetic exercises. Specifically, when new feature data becomes available, the system will retrain the matching model. This process is efficient because we use shallow machine learning models, and the time required for each update is less than 40 seconds, as described in Section VI-B.

IV. Signal Capturing Module

A. Signal Separation for Different Users

To understand the signal capturing and separation process, we consider a typical scenario with multiple people, as shown

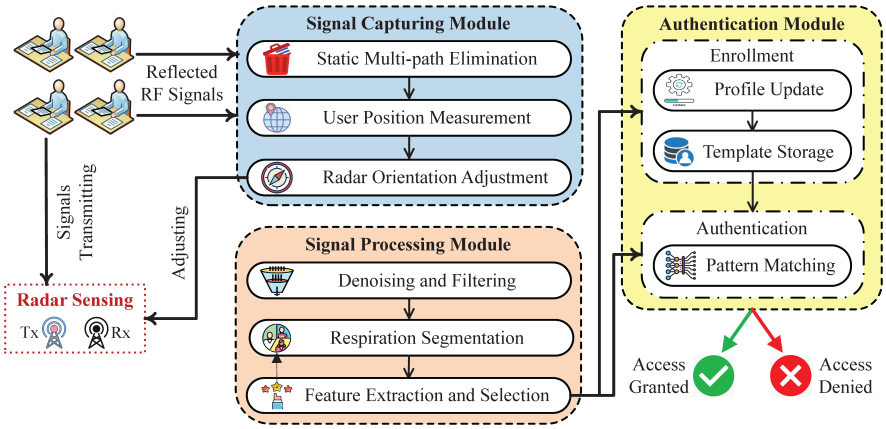
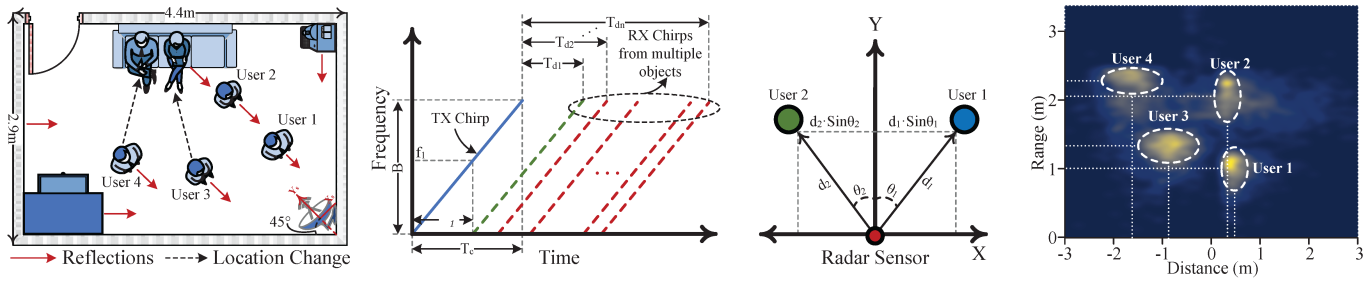


Fig. 4. System overview of *M-Auth*.



(a) Illustration of multi-user scenario (b) Time dependence of received chirps (c) Object location measurement (d) Signal separation for users

Fig. 5. Signal separation for multiple users and user location measurement.

in Figure 5(a). In this scenario, a mmWave radar is placed in the corner of a room with four people and several items of furniture. When the radar transmits RF signals into the room, the signals bounce off the users, furniture, and walls, and then return to the system. The resulting multi-path reflections superpose over the wireless channel and interfere at the receiving end. Our objective is to identify human-reflected signals from those reflected off other stationary objects and to separate individual signals from the multiple users in the environment. To achieve this, we take advantage of the intrinsic property of FMCW radar, which enables separating reflections from different objects. For this task, we use a MIMO FMCW radar with 3 TXs and 4 RXs, which supports multi-beam in a time-division multiplexing (TDM) fashion. In what follows, we detail the specifics of signal capture and isolation from multiple users[1].

Static Multi-path Elimination. For an object at a distance d_1 from the radar, the radar mixes the TX and RX chirps to generate an intermediate frequency (IF) signal. As illustrated in Fig. 5(b), we mark the RX chirp of the object in green dash line as an example. The corresponding sine-wave IF signal is expressed as follows:

$$S_{IF_1}(t) = A_1 \sin(2\pi f_1 t + \phi_1), \tag{2}$$

where A_1, f_1, and ϕ_1 are the amplitude, frequency, and phase of the IF signal, respectively. Given the slope of the chirp S, f_1 can be calculated as:

$$f_1 = S \cdot \tau_1 = \frac{B}{T_c} \cdot \frac{2d_1}{c} = \frac{2Bd_1}{cT_c}, \tag{3}$$

[1]For a better understanding of FMCW radar measurement, readers are suggested to refer to [15], [18], [19]. We just summarize the fundamental principles in our procedures.

where τ_1, B, T_c, and c are the time delay of the RX chirp, frequency bandwidth, chirp duration, and speed of light, respectively. As observed from Eq. (3), the distance of static reflectors (e.g., walls and appliances) to the radar remains constant over time, resulting in a frequency shift that does not change over time. Consequently, we can get rid of those time-invariant multi-path reflections by subtracting consecutive time measurements.

User Presence Detection. When a user appears in radar's (field-of-view) FoV, our system receives the reflected signal from the user. According to Eq. (1), the phase ϕ of the IF signal from the user is represented as $\frac{4\pi d}{\lambda}$. By combining Eq. (2) and Eq. (3), we can write the user's IF signal as:

$$S_{IF}(t) = A \sin(\frac{4\pi Bd}{cT_c}t + \frac{4\pi d}{\lambda}). \tag{4}$$

Dynamic body movements (e.g., limb, hand, and breathing motions) cause changes in d, consequently triggering strong responses in the IF signal. We use this phenomenon to detect the presence of users in the environment, and further estimate their positions in the next step.

User Position Measurement. By observing the phase change in the IF signal, the user's range information (i.e., distance between the user and the radar) can be calculated using Eq. (1). As illustrated in Fig. 5(c), using only range information is insufficient to distinguish between multiple users, as they are likely to have similar distances to the radar (i.e., $d_1 = d_2$) but be in different directions. Therefore, we introduce another horizontal distance parameter to determine the position of the user relative to the radar. For example, the horizontal distance from User 1 to the radar is calculated as $d_1 \sin\theta_1$, where

θ_1 represents the angle of arrival (AoA) that is measured as follows [18]:

$$\theta_1 = \sin^{-1}(\frac{\lambda \Delta\phi_1}{2\pi l}), \tag{5}$$

where λ, $\Delta\phi_1$, and l are the signal wavelength, phase change, and spacing between RX antennas, respectively. Accordingly, the $n'th$ user's position is expressed as $P_n(d_n \sin\theta_n, d_n)$.

Multiuser Signal Separation. In an environment with multiple users, each RX chirp is separated by a time delay proportional to the distance from the system to the user. A Fourier transform processes the IF signal, which consists of multiple tones, resulting in a frequency spectrum with discrete peaks for each tone. Each peak indicates the presence of a user at a certain distance. According to Fourier transform theory, frequency components can be separated if their frequency difference Δf is greater than $\frac{1}{T_c}$ Hz [18], where T_c is the chirp duration. By using Eq. (3), the relationship is represented as:

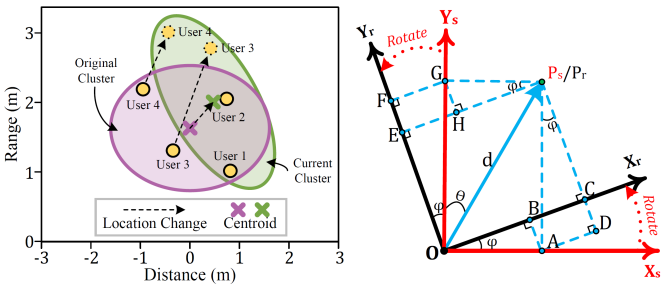
$$\Delta f = \frac{2B\Delta d}{cT_c} > \frac{1}{T_c} \Rightarrow \Delta d > \frac{c}{2B}. \tag{6}$$

In this work, the radar provides a $4GHz$ bandwidth, such that the range resolution Δd is calculated as $\frac{c}{2B} = \frac{3\times10^8}{2\times4\times10^9} = 3.75cm$. This means that we are able to differentiate between users as long as they are at least $3.75cm$ apart from each other. Our primary focus is on the chest movements of users, which are caused by respiration. Even when users are standing shoulder to shoulder (i.e., zero separation distance between them), our system is still able to distinguish the received chirps from each user because their chest positions are separated by their arms (which are typically spaced more than $3.75cm$ apart). As illustrated in Fig. 5(d), the reflections from multiple users are separated into distinct areas, allowing us to analyze their signals individually.

B. Dynamic Radar Orientation Adjustment

Design Motivation. In this study, we use a MIMO radar that has a FoV of 120° for multiuser detection, which is made possible by its channel diversity. Intuitively, it is not necessary to adjust radar orientation since a radar that is statically positioned in the corner of the room with configured beamforming can cover all the users. However, radar's phase change $\Delta\phi$ is sensitive to changes in AoA, the estimation of $\Delta\phi$ degrades as AoA approaches the boundary of FoV [19]. This means that the measurement of respiration motions becomes more error-prone as users draw closer to the border, resulting in a lower SNR. Our experiment in Section VIII-C also confirms that the authentication accuracy decreases by approximately 10% when the user's AoA changes from 0° to 60°.

Signal processing techniques, such as adaptive beamforming, beam steering, and beam switching, might be applied to address the issue of poor SNR [17], [20], [21]. However, these methods only improve the signal SNR in a specific direction and assume that the object's position is fixed. In our scenario, users are mobile and their AoAs are uncertain, signal processing-based methods are consequently not applicable. Instead, we propose an approach that physically adjusts radar's orientation in real time depending on the user's location. Specifically, we operate the following procedures to perform the adjustment.



(a) User clustering and centroid finding (b) Coordinate system converting

Fig. 6. Centroid estimation and location mapping.

Step 1 - Radar Direction Calibration. To begin with, we set up the sensor coordinate system to match the room coordinate system. By default, we align the radar direction at a 45° angle from the wall, as depicted in Figure 5(a).

Step 2 - User Centroid Estimation. The positions of the users relative to the room coordinate system are consistent with the current positions calculated by the sensor. A k-means clustering algorithm is then utilized to identify the centroid of the users with their positions serving as the feature. The sensor is subsequently adjusted to point towards the centroid to capture the reflected signals from the users. Specifically, the estimated centroid position is denoted as $P_c(h_c, d_c)$, where h_c represents the horizontal distance and d_c represents the range. The sensor is rotated by an angle of $\varphi = \sin^{-1}|h_c/d_c|$ in a direction determined by the positive/negative sign of h_c. This adjustment process is controlled by an auxiliary rotating device, which is further elaborated upon in Section IV-C.

Step 3 - Coordinate System Converting. As illustrated in Fig. 5(a), we consider the case that people might change their locations, and their centroid will also change accordingly. We describe the case in Fig. 6(a), after User 3 and User 4 move to the new locations, the system repeats Step 2 to estimate the current centroid of the users and rotates the sensor to point at it afterward. In this operation, the major challenge is that we cannot directly calculate the centroid for the current cluster since location measurements for User 3 and User 4 are relative to the sensor coordinate system (i.e., $X_s - Y_s$), whereas the locations of User 1 and User 2 are corresponding to the room (i.e., $X_r - Y_r$). To address this issue, we develop a mapping relationship between the two coordinate systems, as shown in Fig. 6(b). The mapping problem can be defined as follows:

- ***Condition:*** *Given user P's location measurement $P_s(\theta_s, d_s)$ in $X_s - Y_s$, rotating X_sY_s axes counterclockwise through an angle of φ into X_rY_r axes.*
- ***Resolve:*** *Determine the translation rule $\mathbf{T}(\varphi)$ to make the equation $\overrightarrow{OP_r} = \mathbf{T}(\varphi)\overrightarrow{OP_s}$ true.*

According to the measurement $P_s(\theta_s, d_s)$, we have $P's$ coordinate $P_s(d_s\sin\theta_s, d_s\cos\theta_s)$ in the sensor coordinate system. Then, $P_r(x_r, y_r)$ in the room coordinate system can be calculated as:

$$\begin{cases} x_r = OB + \underset{=AD}{BC} = d_s\sin\theta_s\cos\varphi + d_s\cos\theta_s\sin\varphi \\ y_r = OF - \underset{=HG}{EF} = d_s\cos\theta_s\cos\varphi - d_s\sin\theta_s\sin\varphi \end{cases}. \tag{7}$$

Vector $\overrightarrow{OP_r}$ can be represented in matrix form as:

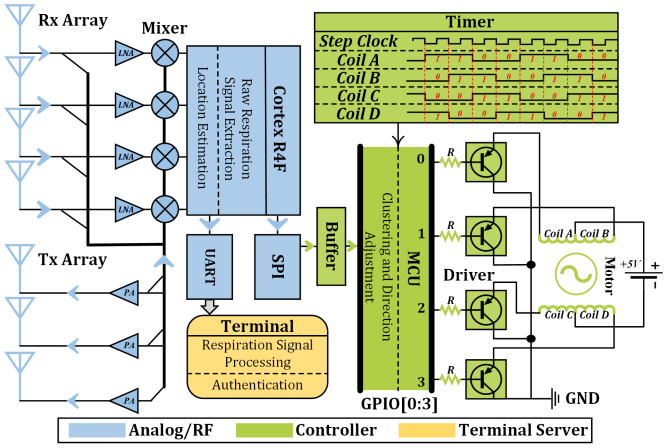


Fig. 7. The hardware design for operating mmWave sensor to adjust orientation.

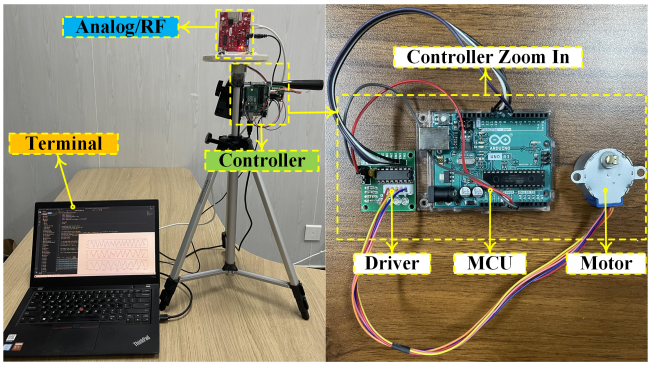


Fig. 8. The hardware setup.

$$\underbrace{\begin{bmatrix} x_r \\ y_r \end{bmatrix}}_{\overrightarrow{OP_r}} = \underbrace{\begin{bmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{bmatrix}}_{\mathbf{T}(\varphi)} \underbrace{\begin{bmatrix} d_s \sin\theta_s \\ d_s \cos\theta_s \end{bmatrix}}_{\overrightarrow{OP_s}}. \tag{8}$$

Using Euler's Formula, $\mathbf{T}(\varphi)$ can be further simplified as:

$$\mathbf{T}(\varphi) = \cos\varphi \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \sin\varphi \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = exp(\varphi \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}). \tag{9}$$

Since φ is the angle between the two coordinate systems that is obtained in the previous step, we can map the locations of User 3 and User 4 to the room with $\mathbf{T}(\varphi)$.

C. Rotating Device Design

Figure 7 illustrates the schematic diagram for controlling motor rotation, which dynamically adjusts the orientation of the sensor. The mixer component of the sensor combines the transmitted and reflected signals to produce an intermediate frequency (IF) signal. By processing the IF signal with Fourier transforms in the Cortex, we can extract respiration waves and estimate the user's location. Respiration-related signals are transmitted through the UART interface to the terminal computer for further authentication tasks, while location measurements are sent to the controller for adjusting sensor direction. Since the user's location may change frequently, we stream this information over SPI to the external buffer for faster data updates.

Fig. 8 shows the hardware setup. The controller primarily consists of the following parts:

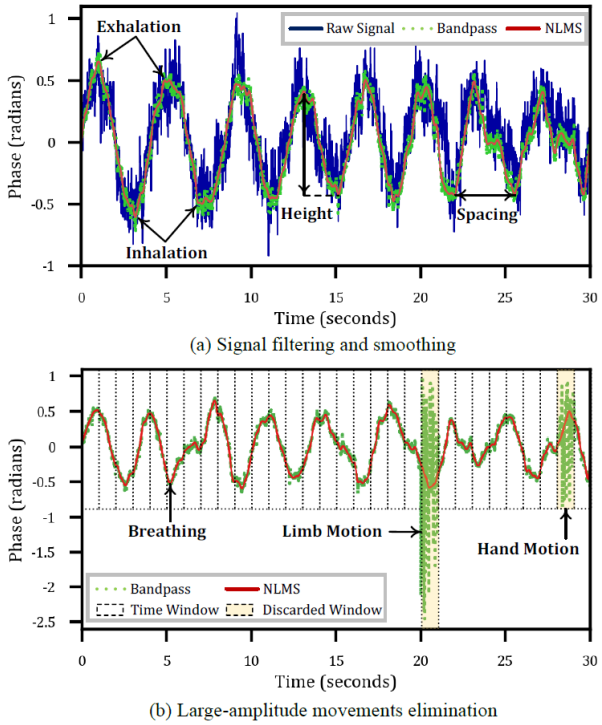


Fig. 9. Illustration of signal noise removal.

MCU. After reading the user's location information from the buffer, the MCU is programmed to cluster users and calculate the centroid. It also generates rotation instructions for the driver.

Driver. It is mainly composed of 4 transistors and a timer, which is in turn controlled by the MCU. The activation of the transistors provides the required voltage and current for the coils, and the timer controls its energizing timing. It controls the stepper motor in full step driving mode, and our designed driving sequences for the coils are are 1001, 1100, 0110, and 0011, as shown by the timing diagram.

Motor. It is controlled by the clock period and rotates to the desired direction. In our implementation, we employ an unipolar stepper motor which has 5 wires one for motor supply and the other for coils. The motor has 4 coils and they are connected as shown in Fig. 7.

The configuration of our stepper motor provides a step angle of 1.8° and a holding torque of $3.4kg\text{-}cm$, which is capable of rotating our sensor board to the desired direction. During direction adjustment, our system may cause authentication errors due to sensor movement. This vulnerability could be exploited by attackers. In our implementation, the motor speed is set to $150rpm$ for stability, taking only $0.1s$ to rotate 90° (i.e., the wall corner where our system is placed). It is highly unlikely for attackers to perform malicious activities within such a short time. In addition, our stepper motor only needs a $5v$ power supply. This low power consumption requirement allows for more convenient and flexible deployment in various task environments.

V. Signal Processing Module

A. Respiration Signal Separation

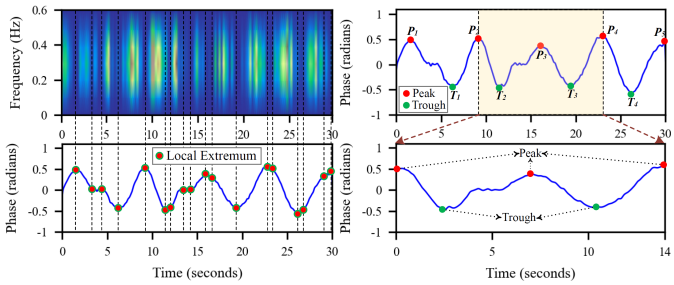
In general, the signal we capture includes high-frequency noises, such as power-line interference accompanied by several

harmonics; low-frequency noises, such as baseline wander due to physical instability; and other random interferences, such as limb motions. To minimize the negative effects of these noises, we employ the following optimizations to obtain a refined respiration waveform.

Bandpass Filtering. To ensure accurate user authentication, it is necessary to identify the signal that is predominantly influenced by respiration motions. In practice, if the energy of noise is stronger than that of respiration, it may lead to a spectral leakage effect [22], whereby strong energy at one frequency spills into other frequencies. This may cause the original respiration signals to spread into wider signals. To improve signal quality, we adopt a Butterworth bandpass filter [23] as our insight suggests that the respiratory frequency band typically lies between 0.2 and $0.5Hz$ [24]. The filter is used to eliminate irrelevant signals that fall outside this band. After bandpass filtering, the signal (i.e., green colored) shown in Fig. 9(a) exhibits higher resolution than the raw signal, allowing for clear separation of respiratory peaks and valleys. The sample depicted in this figure is obtained by asking a participant to remain stationary at a distance of $2m$ from the sensor in a typical office room.

Smoothing. Since unpredictable low-frequency interference is likely to fall into the frequency range of respiration, we need further refine the robustness against impulsive interference. To extract the most representative morphological features, we use a normalized least mean square (NLMS) adaptive filter [25] to smooth the respiratory waveform. Compared to the conventional smoothing methods, such as the moving average filter that interpolates the element of the signal with an average across its neighborhood, the NLMS adaptive filter is capable of stopping the adaptive update of the filter weight in the presence of impulsive interference. This indicates that the recovered respiration signal is much closer to the original. From Fig. 9(a), it is observed that the signal (i.e., red colored) is more smooth, and its morphology (e.g., height and spacing) is more prominent.

Outlier Removal. In practice, user might perform limb and hand movements, such as drinking or operating a phone. Figure 9(b) shows an example of how waving limb and hand creates irregular signal changes that interfere with respiration. Simply relying on filters is not enough to reject such interferences, because they are aperiodic and have larger amplitude than respiration. Therefore, we propose a method to reduce the impact of large movements based on signal energy calculation. The main idea is to slide a time window over the signal and calculate the energy for each window (i.e., $\int_t^{t+1} s^2(t)dt$). Then we compare the energy with the historical average of the signal and discard the window if the energy exceeds a certain threshold. This means that the window is dominated by non-respiratory movements. We empirically set the time window to 1 second and the threshold to 5 times the historical average of the window energy. Figure 9(b) also shows how we smooth the signal using NLMS after discarding the non-respiratory windows. In the following sections, we further analyze the fine-grained waveform of the smoothed signal to extract corresponding features.



(a) Extremum points determination (b) The result of segmentation

Fig. 10. Respiration segment extraction.

B. Respiration Segmentation

Respiration is a rhythmic motion that exhibits a periodic trend in the signal. Unique characteristics can be derived from its waveform, such as respiratory rate, depth, and rhythm changes. Since such characteristics are broadly similar between breathing cycles for a specific user, to facilitate and simplify the analysis of respiration, we suppose to partition the time-domain signal into segments according to its cycles. The most direct way to determine the cycles is to locate the peaks and troughs of the signal. As shown in Fig. 10(a), local extremums can be estimated by spectral analysis [26]. However, it is observed that multiple local extremums are generated on same peaks, troughs, and even slopes owing to the subtle fluctuation. Thus, to determine the exclusive points that denote the peaks and troughs in the cycles (a cycle is a "down-up" trend or "up-down" trend), we implement a distance limitation method as follows:

Extremum Classification. The peak represents exhalation that leads to a positive value in phase changes, while the trough stands for inhalation that results in a negative value. Based on this prior knowledge, we sort the extremums into maximums (i.e., positives) and minimums (i.e., negatives). Note that we delete zero-value points in this step. This is because exhaling and inhaling would produce the maximal absolute value of phase change, and the locations for peak and trough are not zero-value points.

Threshold Calculation. We introduce two thresholds T_{max} and T_{min} to select the unique peaks and troughs from the two categorized groups, respectively. In particular, the thresholds are the average distances between every two adjacent values in the two groups, respectively. The average distance is calculated as: $\frac{1}{n-1}\sum_{i=1}^{n-1} t_i \times s$, where $n-1$ is the number of intervals in the group, t_i refers to the duration of the $i'th$ interval, and s denotes the sampling rate.

Peak/Trough Determination. We choose the first local maximum/minimum in the groups as a valid peak/trough, and the next valid peak/trough is selected such that the distance between the current local maximum/minimum and the previous valid peak/trough is greater than T_{max}/T_{min}. Using such restriction, we finally obtain the corresponding peaks and troughs for the signal, as shown in Fig. 10(b).

Since slight differences might appear between cycles, to ensure the robustness of the features extracted from the segment, we slice two cycles as a respiration segment in our implementation (the determination of cycles for a segment is

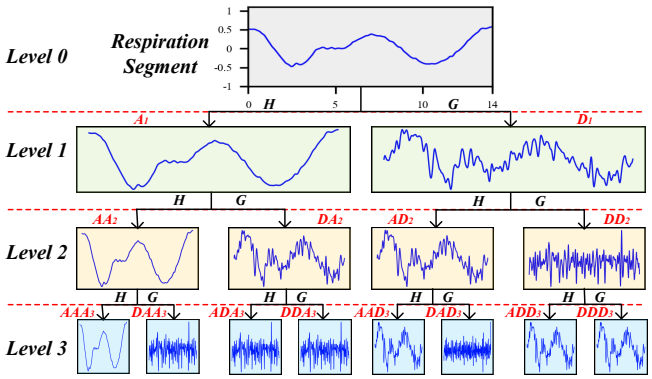


Fig. 11. Illustration of wavelet packet decomposition.

further studied in Section VIII-A). As illustrated in Fig. 10(b), we use the signal starting from P_2 to P_4 as one segment.

C. Biometric Features Extraction

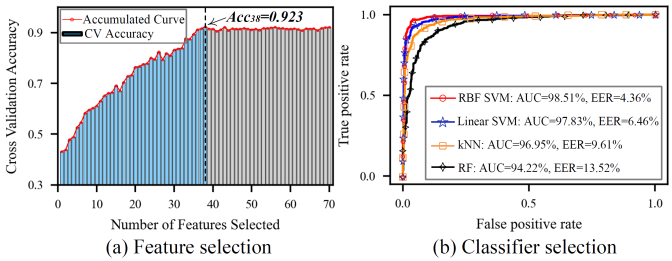
Respiration is non-stationary and contains periodic transient trends. Extracting statistic features alone may not capture minor changes between individuals. To accentuate minute changes, we use wavelet packet decomposition (WPD) for fine-grained analysis on respiration segments. We employ a 3-level WPD with $db1$ Daubechies wavelet, minimizing edge effects and allowing fast computation. As illustrated in Fig. 11, WPD decomposes the segment into detail (D) and approximation (A) components with corresponding high-pass (G) and low-pass (H) filters at each level. With WPD, we perform multi-resolution analysis in different frequency domains to capture representative biometrics and discern subtle differences in respiration motions between individuals. The original segment is zoomed in level by level, producing a total of $\sum_{i=1}^{3} 2^i = 14$ subspaces. Each subspace covers a part of the frequency spectrum and facilitates learning of distinctive features.

To better understand the important and unique information, we analyze and apply five different domain features to represent the signals, including skewness, kurtosis, shape factor, impulse factor, and root mean square (RMS). Skewness and kurtosis can detect abnormalities and irregularities. Shape factor and impulse factor describe the shape of the signal. Root mean square (RMS) reflects the signal's energy and lung function. Overall, these features help analyze the shape, dynamic changes, and energy of respiratory signals, providing insights into subtle differences between individuals. After applying the 5 measures to each respiration segment, we have a total of $14 \times 5 = 70$ features. These features are then analyzed to identify patterns for user template profiling and authentication model training. By using these various features, we gain a comprehensive understanding of the data and ensure accurate analysis for developing reliable authentication models in various settings.

VI. Authentication Module

A. Biometric Template Profiling

When an individual first enrolls in *M-Auth*, the biometric features are extracted from his/her respiration samples. In practice, not all the extracted features contribute the most informative



(a) Feature selection (b) Classifier selection

Fig. 12. Feature and classifier selection.

variables to represent the uniqueness of an individual. For instance, it is observed from Fig. 11 that there exist duplicate components after WPD process (e.g., DA_2 and AD_2), leading to producing same features. Therefore, to obtain robust features, we further study the 70 extracted features and select the most distinct ones using the recursive feature elimination (RFE) method [27].

Specifically, we employ a support vector machine (SVM) classifier with a linear kernel for RFE. We choose this method because of its ability to handle high-dimensional data and its success in previous studies. The training of the classifier is started by using all 70 features through 5-fold cross-validation. In this step, we randomly select data from 10 participants (data collection is discussed in Section VII-B). The algorithm accomplishes this by first fitting a model to the entire set of features. Then, it discards the least important features according to the model's coefficients and refits the classifier. This process is repeated recursively until the desired accuracy is reached with a specified number of features. By eliminating the least important features at each iteration, RFE is able to identify the most important features for the given problem, resulting in a more accurate and interpretable model.

In Fig. 12(a), we present the results of our analysis. The curve reaches an accuracy of 92.3% when 38 informative features are used. After that point, the accuracy remains stable even with the inclusion of additional features. This indicates that the first 38 features are the most sensitive to the classification task and represent respiration motions. Adding more features beyond this point does not lead to any improvement in accuracy, as the remaining features do not contribute to the classification task. In the following section, we leverage this insight by using the 38 selected features to train our matching model.

B. User Pattern Matching

By matching the incoming respiration segments with the built profiles, *M-Auth* identifies the unknown users and determines whether they are registered in the system. To facilitate the profile update and maintenance, we aim to transfer the classifier training process to our sensor board in practical applications, thus avoiding the cumbersome *offline training and online recognizing* procedure. For this purpose, we tend to adopt lightweight shallow machine learning classifiers instead of deep learning solutions as *M-Auth's* authentication model.

To determine the optimal classifier for our authentication system, we evaluated four machine learning techniques: Random forest (RF), k nearest neighbors (kNN), linear kernel-based support vector machine (Linear-SVM), and radial basis function-

TABLE I
CLASSIFIER PARAMETER SELECTION.

	RBF-SVM	Linear-SVM	*k*NN	RF
Parameter	$\mathcal{C}$=1, γ=0.01	$\mathcal{C}$=4	k=10	d=11, n=400
Accuracy (%)	95.77	93.04	94.07	76.69
Training Time (s)	39.22	2.02	0.24	35.74

TABLE II
MMWAVE CONFIGURATION.

Bandwidth	$4GHz$	ADC Sampling Rate	$2.5M/s$
Chirp Slope	$53MHz/\mu s$	Chirp Repetition	$184\mu s$
Chirps per Frame	128	Samples per Chirp	128

based support vector machine (RBF-SVM). We fine-tuned the parameters for each classifier using 5-fold cross-validation and grid search [28] to achieve optimal performance. We use the one-vs-the-rest multi-class strategy [29] to evaluate the performance of the classifiers. This strategy involves selecting users individually and assessing the classifier's performance for each user. Taking the random forest classifier parameter selection as an example, we have pre-set two parameter sets for the classifier: n and d. Among them, n represents the number of decision trees in the forest, with a value range between 0 and 500 and a step size of 50, resulting in 10 potential parameters. d represents the maximum depth of the tree, with a value range of 0 to 20 and a step size of 1, resulting in 20 potential parameters. After performing the grid search method on these two parameter sets, the RF classifier can be fine-tuned to achieve the best possible performance for our task.

Table I lists the parameters used for each classifier, as well as their corresponding accuracy and training time at their best performance. Among the classifiers, RBF-SVM achieves the highest accuracy of 95.77%, followed by kNN with an accuracy of 94.07%. Linear-SVM has an accuracy of 93.04%, while RF achieved the lowest accuracy of 76.69%. Despite having the longest training time at 39.22 seconds, RBF-SVM emerged as the best classifier on this task. In addition, Fig. 12(b) illustrates the distributions of FPR and TPR for the four classifiers. The results show that the RBF-SVM has the highest AUC value of 98.51% and the lowest EER of 4.36%, indicating that it is the most suitable classifier for our authentication system. Therefore, we have selected the RBF-SVM for user pattern matching in this study. For further details on the abbreviations used, please refer to Section VII-C.

VII. SYSTEM IMPLEMENTATION

A. System Setup

In our experiment, we employ a commercially available IWR1443BOOST mmWave radar equipped with 7 antennas (3 TXs and 4 RXs) [30] to demonstrate the feasibility of *M-Auth*. The radar board is configured according to Table II, providing a range resolution of $3.75cm$ and a displacement resolution of $1mm$, which satisfies the requirements of our scenario. As illustrated in Fig. 13, the sensor board transmitted and received signals, which were then streamed out via UART to a laptop featuring an Intel i7-8650U processor for further processing. We develop the *M-Auth* software in Python 3, which can be conveniently ported to portable embedded systems.

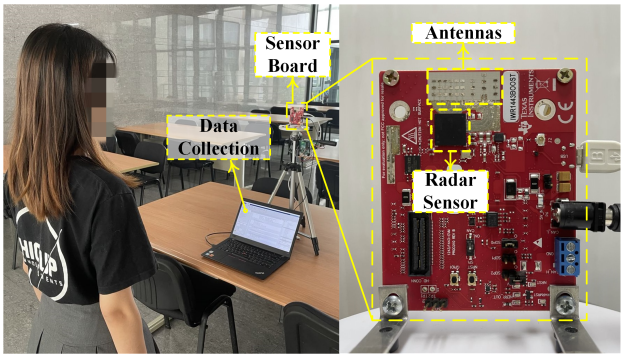


Fig. 13. Experimental setup.

B. Data Collection

Genuine Data Collection. We recruit 37 healthy participants (17 females and 20 males) between the ages of 19 and 35. Before data collection, participants are given the information that the experiment is to perform biometric authentication only and that their personal data would be stored securely and de-identified. Our experimental setup, as shown in Figure 13, involves having a participant sit or stand in front of the radar 2 meters away and breathe freely in a typical workplace environment without any restrictions on limb movement or smartphone use. The default settings are utilized unless otherwise specified. To minimize the impact of fatigue on the data and ensure data consistency, we collect each participant's data over multiple rounds lasting two months. For evaluation, we collect 400 respiration segments for each participant, resulting in a total of 14,800 samples.

Attack Data Collection. We collect attack data as follows:

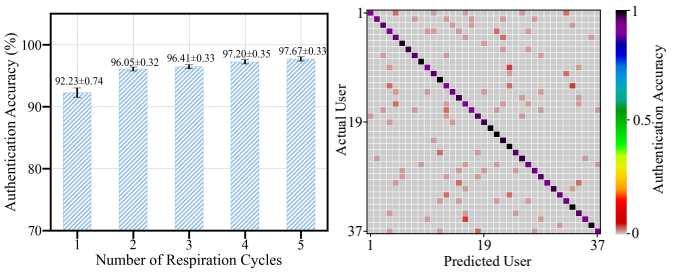
Blind Attack. We invite a total of 37 participants to take part in this study. 7 participants are assigned the role of legitimate users, while the remaining 30 participants are designated as attackers. Each attacker randomly performs 20 segments, resulting in a total of 600 segments. We then collect 4200 samples in total, which are used to analyze the performance of our system under blind attack.

Impersonation Attack. We select a group of 7 individuals to participate as victims and another group of 10 individuals to act as attackers. The attackers are specifically instructed to mimic the breathing patterns of the victims, paying close attention to their respiratory rhythm and depth. For each victim, we obtain 50 segments from each attacker, resulting in a total of 3500 samples.

Replay Attack. We invite 7 participants as victims and employ an additional mmWave radar to record the victim's respiration signals. It is assumed that the end device is secure, the attacker does not know the specifications such as the length of the respiration segment and the configuration of FMCW chirps. For each victim, we use the default chirp configuration to capture respiration for 10 minutes and slice the signal into segments by 5 seconds. In total, we collect 840 samples.

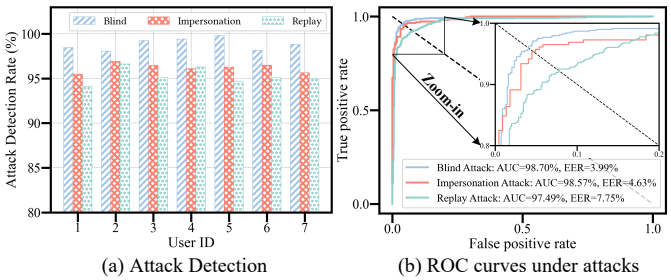
C. Evaluation Metrics

To evaluate the performance of *M-Auth*, we introduce the following metrics:



(a) Performance with different cycles (b) Confusion matrix

Fig. 14. Performance of legitimate user authentication.



(a) Attack Detection (b) ROC curves under attacks

Fig. 15. System performance under three attacks.

Authentication Accuracy. It denotes the percentage of genuine samples that are correctly verified. A system with high authentication accuracy is more reliable and secure. In addition, a high authentication accuracy also translates to a better user experience by reducing false positives and false negatives, which can lead to frustration and wasted time.

ROC Curve. The ROC curve presents the relationship between the true positive rate (TPR) and false positive rate (FPR) under different thresholds. The TPR represents the rate of attacks that are correctly detected, while the FPR denotes the rate of genuine samples that are falsely identified as attacks. A larger area under the ROC curve (AUC) means better performance of the system.

Equal Error Rate. EER is the rate at which the system incorrectly identifies genuine samples as imposters and the rate at which the system fails to detect an attack sample. It is calculated by finding the point where the ROC curve intersects the diagonal line. A lower EER indicates a better performance of the system in distinguishing between genuine and impostor samples.

VIII. Performance Evaluation

A. Overall System Performance

We first evaluate the impact of different segment lengths on authentication accuracy. Fig. 14(a) shows the results with different numbers of respiration cycles in a segment. We observe that when 2 cycles are chosen, the average accuracy leaps to 96.05% and remains roughly stable thereafter. We also notice that the standard deviation (STD) decreases from 0.74% to 0.32%, indicating that the results were more consistent. To further investigate this phenomenon, we find that the accuracy improves slightly when increasing the number of cycles from 2 to 5, reaching 97.67%. The STD slightly increases by 0.01% to 0.33% instead. These changes are not statistically significant, suggesting that choosing 2 cycles may provide the best balance between accuracy and computational resources. The result indicates that longer segments do not necessarily improve the performance, and may introduce additional noise and variability in the respiration signals. Based on these observations, we choose 2 cycles as the optimal segment length and the corresponding average accuracy demonstrates *M-Auth* is effective in verifying legitimate users.

Next, we evaluate the performance of specific user verification. We evaluate the authentication accuracy of 37 participants and generate a confusion matrix, which is displayed in Fig. 14(b). The matrix presents the corresponding authentication accuracy along the diagonal regions. It is color-coded to indicate the level of accuracy, with darker regions representing higher accuracy. Overall, we find that the authentication accuracy of our system is quite impressive, with the lowest and highest accuracy rates being 91.25% and 100% respectively, and a STD of only 2.69%. This low STD indicates that users' accuracy rates tend to cluster around the average, which is 96.05%. It is important to note that the darker areas of the confusion matrix highlight the system's ability to accurately identify specific users, which demonstrates that our system is reliable and effective in authenticating individuals.

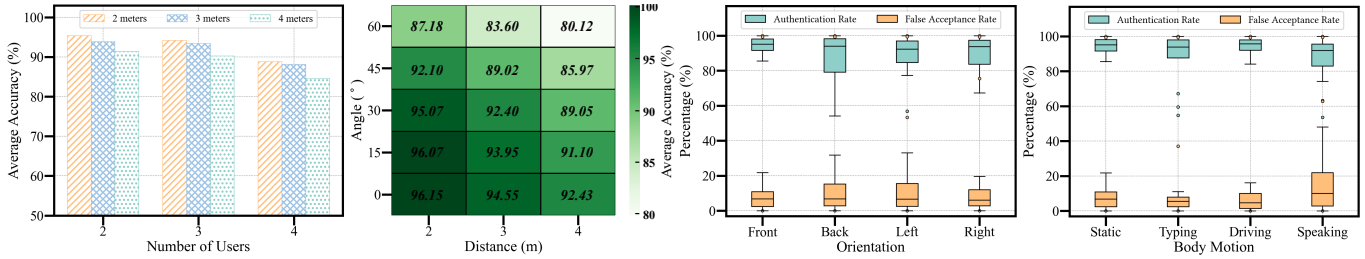
B. Performance of Resisting Attacks

We evaluate the resilience of *M-Auth* for the attacks discussed in Section II-C. As shown in Fig. 15(a), the detection rates of the three attacks are over 98%, 95%, and 94%, respectively, with mean values of 98.86%, 96.29%, and 95.34%, respectively. It is expected to have a high detection rate under blind attack since respiration motions are rarely the same between individuals as mentioned in Section II-A. We also observe a slight decrease in detection of impersonation attack, which suggests that imitating the victim's respiration can help attackers with their attack. However, the average detection rate of 96.29% indicates it is challenging to replicate someone else's respiration precisely. Furthermore, our system remains resilient to replay attacks, as verified by the results. Attackers lack detailed specifics of *M-Auth*, such as chirp configuration and signal segmentation, which makes it difficult for them to accurately replicate the system's unique features. Overall, these results demonstrate the robustness of our system against various attacks, ensuring a secure authentication process for our users.

In order to better understand the performance of the system, it is useful to examine the ROC curve depicted in Fig. 15(b). The curve provides a visual representation of the system's ability to distinguish between legitimate users and attacks. We can see from the AUC values that the system is highly effective at this task, with values of 98.70%, 98.57%, and 97.49% for the three attacks, respectively. Additionally, the EER values of 3.99%, 4.63%, and 7.75%, respectively, indicate that the system is able to accurately differentiate between legitimate users and attacks. These results demonstrate the robustness of our system and its ability to provide reliable security measures to protect against attacks.

C. Robustness Analysis

Impact of Multiple Users Under Variant Distances. We evaluate our system with up to four users with distances ranging



(a) Multiple users under different distances (b) AoAs under different distances (c) Different user orientations (d) Different body motions

Fig. 16. Robustness analysis for different scenarios.

from $2m$ to $4m$. We randomly select 2, 3, and 4 participants and ask them to stand shoulder-to-shoulder at distances of $2m$, $3m$, and $4m$, respectively. Fig. 16(a) shows the average authentication accuracy. It is observed that the accuracy values are all over 90% for the groups of 2-user and 3-user within $4m$. The accuracy values for the 4-user within $3m$ almost approach 90%. The results verify that *M-Auth* is capable of identifying multiple users simultaneously within a reasonable range. Note also that the increase of either users or the distance might decrease the accuracy, especially for the group of 4-user at $4m$, the accuracy decreases to 85%. It is expected due to the fast attenuation of mmWave signals and could be further improved by increasing respiration cycles in the segment.

Impact of AoA Under Variant Distances. To examine the effective sensing range, we evaluate performance under changeable AoAs and distances. The test requires the recruiter to be at $2m$, $3m$, and $4m$ away from the system, and positioned at angles ranging from $0°$ to $60°$ relative to the radar's orientation. The results are visualized in Fig. 16(b). We observe that the accuracy exceeds 92% when the angle is less than $30°$ and the distance is within $3m$. Like the previous experiment, the accuracy decays with the increase in distance. Moreover, the accuracy is above 92% when the user is on a straight line with the probe and reduces to less than 88% at $60°$. The results are expected since the estimation of phase change decays with the increase of AoA. This experiment motivates us to design the rotating device in Section IV-C, which can dynamically adjust the device orientation according to the user position.

Impact of User Orientation. We study the performance when users are not facing the device. Participants are asked to assume four different orientations, including facing the device, having their back to the device, and facing left or right to the device. The results are presented in Figure 16(c). We observed that the average authentication and false acceptance rates were the best (96.07% and 6.23%, respectively) when users faced the device. Across all orientations, the rates fluctuated slightly by 1%-3%, indicating the robustness of our system in verifying users in different orientations. This is due to the fact that when individuals breathe, their chest expands in all directions, and our system can capture the side expansions. This is a significant advantage over other methods of identity verification, which often require a specific body position to be successful.

Impact of Body Motion. We further investigate the performance under daily activities without requiring users to stop their ongoing work. Participants are invited to perform four different activities: static (as a control group), typing, imitating driving, and speaking. From Fig. 16(d), it is observed that the average authentication rate and false acceptance rate are close to those of the control group when typing or driving. The results are consistent with our methodology, where we introduce a signal energy comparison scheme to remove the outliers caused by limb or hand movements. In the case of speaking, the results drop by about 6% compared to the control group. This is due to the inherent nature of speaking, i.e., phonation relies on exhalation; it is not possible to phonate during inhalation [1]. The limitation could be alleviated by intermittent pauses during speaking.

Impact of Test/Train Split Ratio. We change the amount of training data used for building the user authentication model in our scenario to test system performance. To avoid other factors that may affect authentication accuracy, we use a fixed dataset to evaluate the performance by controlling the ratio of the testing and training sets. The results are presented in Table III. As we increase the proportion of the training set, the average accuracy shows a gradually rising trend, increasing from 93.49% to 95.59%. Meanwhile, the training time consumption also increases gradually from 5.63 seconds to 52.57 seconds. When the proportion of the training set is only 10%, the standard deviation is 0.52%. However, when the proportion of the training set exceeds 20%, the standard deviation is consistently below 0.35%. This is because a small training set may not provide enough information for the model to learn from. Therefore, choosing the optimal test/train split ratio is crucial for balancing performance and training time. In our scenario, it is suggested to adopt the ratio of 3/7 to achieve good results ($95.77 \pm 0.24\%$) within a reasonable training time (38.61s).

D. Usability Improvement

In Section VIII-A, we conducted a series of experiments to determine the optimal signal length for our work. After careful analysis, we discovered that the most effective signal length is two breathing cycles. This length typically lasts more than 10 seconds, as demonstrated in the example shown in Fig. 10(b), where two breathing cycles occupied 15 seconds. This result is significant as it greatly improves the accuracy and reliability of authentication, with an average accuracy of 96.05%.

Using longer signal lengths allows for more data to be captured and provides more insights into the patterns and trends of the signal. However, longer signal lengths also require users to stand in front of the device for a prolonged period, which could negatively affect the overall comfort and convenience of the system. To improve usability, it is best to minimize the time spent on the authentication process while ensuring

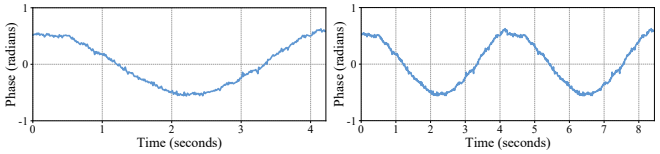
TABLE III
SYSTEM PERFORMANCE WITH DIFFERENT TEST/TRAIN SPLIT RATIOS.

Test/Train Ratio	1/9	2/8	3/7	4/6	5/5	6/4	7/3	8/2	9/1
Accuracy (%)	95.95 ±0.35	95.71 ±0.27	95.77 ±0.24	95.73 ±0.30	95.59 ±0.20	95.45 ±0.21	95.27 ±0.24	94.78 ±0.30	93.49 ±0.52
Training Time (s)	52.57	45.89	38.61	32.39	26.78	20.71	15.47	10.26	5.63

Algorithm 1 Wavelet-based Signal Generation

Input: x, respiration signal of length 1 cycle;
Output: z, respiration signal of length 2 cycles;

$wavelet = pywt.Wavelet('sym5')$;
$coeffs = pywt.wavedec(x, wavelet, level = 4)$;
for $i = 1$ to $len(coeffs)$ **do**
    $coeffs[i][-2:] = coeffs[i][-2:] * 0$;
end for
$y = pywt.waverec(coeffs, wavelet)$;
$z = np.concatenate(x, y)$;
Return z;



(a) Signal with 1 cycle (b) Generated signal with 2 cycles

Fig. 17. Signal generation using wavelet transform.

the accuracy and robustness of the system. We propose to analyze the signal pattern of a respiratory signal with only one cycle and generate a new respiratory signal containing two cycles. By doing this, we can halve the user's authentication time without shortening the signal length. Specifically, we employ wavelet transform to learn signal patterns, enabling us to examine different aspects of a signal in detail, such as its frequency content and time localization. By analyzing these properties, we can gain insights into the underlying patterns of the signal and use this information to generate new signals with similar characteristics.

Algorithm 1 presents the use of the PyWavelets[2] Python library to learn and generate new respiration signals. We begin by defining a wavelet named $sym5$ because this basis function can finely detect the local features of the signal, and performs well in extracting low-frequency signals while removing high-frequency noise. Next, we perform wavelet decomposition on signal x, using the specified wavelet and setting the transformation level to 4. This produces a list of five coefficient arrays, $coeffs$, each corresponding to a wavelet decomposition level. For each coefficient array, we multiply the last two arrays (corresponding to high-frequency wavelet coefficients) by 0 to remove unimportant high-frequency information. We then perform wavelet reconstruction on the trimmed coefficients to obtain a new signal y. Finally, we concatenate x and y to obtain the desired signal z containing two breathing cycles. Fig. 17 shows an example of generating a long signal using the algorithm described above. The algorithm learns the pattern of the single-cycle signal in Fig. 17(a), and then generates a signal containing two cycles as shown in Fig. 17(b). By doing so, users can complete the authentication process within one breathing cycle, thereby improving the system's usability in practice.

[2]https://github.com/PyWavelets/pywt.

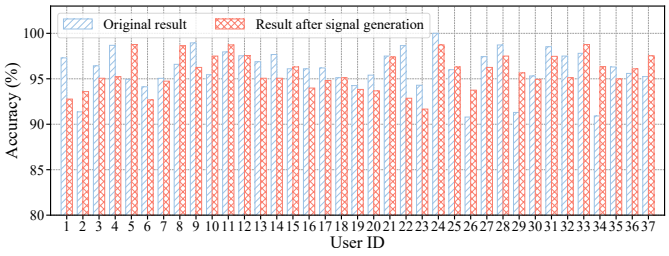


Fig. 18. System performance when using signal generation.

Next, we verify the effectiveness of the proposed method, especially its impact on system performance. We use the data collected in Section VII-B to generate test signals for our 37 participants and evaluate them using the authentication classifier established in Section VI-B. Fig. 18 compares the average authentication accuracy before and after using signal generation for each individual. Before using signal generation, the overall average accuracy is 96.05%, and the average accuracy of each individual ranges from 91.25% to 100%, with a STD of 2.69%. After signal generation, the overall average accuracy is 95.69%. For each individual, the minimum accuracy is 92.77% and the maximum accuracy is 98.77%, with a STD of 2.23%. While the proposed method may slightly reduce the system's performance, its lower STD improves the system's stability. Most importantly, this method significantly shortens the time required for user authentication, which enhances practical usability.

IX. RELATED WORK

Continuous Authentication. Traditional physiology-based authentications have been the standard for a long time, such as fingerprint [31], iris [32], and face [33]. However, recent developments in technology have shown that they are vulnerable to artifacts, leading to the development of behavior-based continuous authentications such as gait patterns [2], [3], finger vibrations [34], vocal vibrations [35], and keystroke dynamics [4]. As traditional solutions only provide one-time authentication during the initial login phase, continuous authentications have been proposed as more reliable alternatives to traditional physiology-based authentications. While these methods have shown promise, they require continuous and active interaction, which may be obtrusive and inconvenient for users.

Vital Sign-based Authentication. To overcome the limitations mentioned above, vital signs are used for new passive authentications. For example, brain responses to visual stimuli are used for user authentication [8]. In continuous user authentication, electrocardiogram (ECG) signals are widely studied as biometric markers [10], [36]. To make it more

convenient, photoplethysmogram (PPG) is suggested as an alternative to ECG [9]. Another approach is *BreathPrint*, which uses breathing audio to authenticate users [37]. However, these methods require users to wear gadgets, which is inconvenient. To address this, wireless signals are used for non-contact authentication. *Cardiac Scan* uses radar to verify users based on unique cardiac motion [11]. *BreathID* extracts respiration signals from Wi-Fi signals for contactless authentication [12]. However, these methods either require a dedicated device or close-range sensing, limiting their applicability.

Among all the discussed works, the most similar research to ours is *BreathID*, where the authors use Wi-Fi signals to authenticate users based on their unique respiratory motions. However, there are key differences between their work and ours: *(i)* They can only test one user at a time, while we can verify multiple users simultaneously. This improves system efficiency, reduces deployment cost, and expands the application scenarios of RF-based authentication. *(ii)* They assume users to be still during authentication, ignoring physical interferences like limb and hand movements. Our work introduces a method to eliminate motion-corrupted segments, making our system more practical. *(iii)* They use over 500 features to describe the respiration signal, whereas we carefully select 38 representative descriptors, which improves authentication accuracy and user template update. With these unique factors, our authentication solution differs significantly from *BreathID*.

X. Discussion

We analyze the potential limitations of our system and provide suggestions for how to improve it in the future.

Single Radar Deployment. Our solution is based on a dynamic radar deployment that adjusts radar direction based on user locations, enhancing signal quality and enabling accurate activity recognition. However, there are limitations to consider. In wide-space settings, signal strength may be lost when two users move apart. The radar direction may not cover both users within its field of view (FoV), resulting in a significant drop in signal intensity. This can impact the system's ability to capture fine-grained signals. To address this, we recommend deploying our system in activity-intensive settings where users are likely to be close. Another option is to install multiple radars to cover a larger area and ensure sufficient signal quality for all users. This is a common challenge for single-deployed radar systems and can be overcome by using multiple radars in practice.

Quasi-static State. Our system requires users to remain quasi-static during usage to ensure accurate monitoring. This is a common challenge in wireless sensing since full-body movements result in phase shifts that can overpower those caused by respiration. Due to the low signal-to-noise ratio (SNR) of the submerged signal, isolating it is not easy. One possible solution is intermittent authentication, where users are periodically prompted to briefly pause their activities for authentication. This minimizes the impact of large body movements on system performance while maintaining security. It also helps prevent users from forgetting to log out, reducing security risks.

Emotions and Health. In our work, we use respiration data acquired from healthy individuals under normal physical conditions to construct the matching model. However, we recognize that even though most individuals have typical respiratory patterns, some individuals may experience irregular breathing for various reasons. For instance, individuals with breathing problems, such as asthma, pneumonia, or anxiety, may have significant fluctuations in their respiration motions, which can negatively impact the accuracy of our authentication system. To improve the resilience of our system, we can collect respiration data from individuals with different breathing problems like sleep apnea or chronic obstructive pulmonary disease to create a more diverse dataset that can be used to train our system. We can also develop algorithms to detect and adjust for abnormal respiration patterns during the authentication process.

XI. Conclusion

This paper presents a continuous multi-user authentication system by sensing non-contact respiratory motion using a single COTS mmWave radar. To obtain high-quality reflected signals from users, we design a rotating device to assist the radar in finding the best direction. We provide an interference reduction approach to eliminate the effects due to body movements. To accurately authenticate genuine users and block spoofing attacks, we experimentally determine the appropriate data segment, elaborately select the representative features, and build a fine-tuned classifier for pattern matching. Extensive experimental studies demonstrate that our system is resilient to different spoofing attacks and effective in authenticating legitimate users in various application scenarios.

Acknowledgment

We would like to express our gratitude to the editor and the anonymous reviewers for their insightful comments and constructive suggestions, which greatly improved this paper. We would like to thank Xiaoluan Zhang and Qianfeng Wang for their invaluable support throughout the entire project. This work is supported in part by the National Natural Science Foundation of China under Grant 62002278, and in part by the Natural Science Basic Research Program of Shaanxi under Grant 2022JQ-658 and 2022JQ-621.

References

[1] Y. Wang, W. D. Cai, T. Gu, W. Shao, Y. N. Li, and Y. Yu, "Secure your voice: An oral airflow-based continuous liveness detection for voice assistants," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, vol. 3, no. 4, 2019.

[2] X. Yang, J. Liu, Y. Y. Chen, X. N. Guo, and Y. C. Xie, "Mu-id: Multi-user identification through gaits using millimeter wave radios," in *in Proceedings of IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 2020, pp. 2589–2598.

[3] Y. Z. Zeng, P. H. Pathak, and P. Mohapatra, "Wiwho: Wifi-based person identification in smart spaces," in *2016 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*. IEEE, 2016, pp. 1–12.

[4] K. Ali, A. X. Liu, W. Wang, and M. Shahzad, "Keystroke recognition using wifi signals," in *Proceedings of the 21st annual international conference on mobile computing and networking (MOBICOM)*, 2015, pp. 90–102.

[5] J. Kim and P. Kang, "Freely typed keystroke dynamics-based user authentication for mobile devices based on heterogeneous features," *Pattern Recognition*, vol. 108, 2020.

[6] Y. Zhang, W. Hu, W. Xu, C. T. Chou, and J. Hu, "Continuous authentication using eye movement response of implicit visual stimuli," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, vol. 1, no. 4, pp. 1–22, 2018.

[7] S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic, "Looks like eve: Exposing insider threats using eye movement biometrics," *ACM Transactions on Privacy and Security (TOPS)*, vol. 19, no. 1, pp. 1–31, 2016.

[8] F. Lin, K. W. Cho, C. Song, W. Y. Xu, and Z. P. Jin, "Brain password: A secure and truly cancelable brain biometrics for smart headwear," in *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services (MOBISYS)*, 2018, pp. 296–309.

[9] Y. M. Chen, J. C. Sun, X. C. Jin, T. Li, R. Zhang, and Y. C. Zhang, "Your face your heart: Secure mobile face authentication with photoplethysmograms," in *in Proceedings of IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 2017, pp. 1–9.

[10] J. S. Arteaga-Falconi, H. Al Osman, and A. El Saddik, "Ecg authentication for mobile devices," *IEEE Transactions on Instrumentation and Measurement*, vol. 65, no. 3, pp. 591–600, 2015.

[11] F. Lin, C. Song, Y. Zhuang, W. Xu, C. Li, and K. Ren, "Cardiac scan: A non-contact and continuous heart-based user authentication system," in *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking (MOBICOM)*, 2017, pp. 315–328.

[12] J. Liu, Y. Chen, Y. Dong, Y. Wang, T. Zhao, and Y. D. Yao, "Continuous user verification via respiratory biometrics," in *Proceedings of IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 2020, pp. 1–10.

[13] H. Kong, L. Lu, J. Yu, Y. Chen, X. Xu, F. Tang, and Y.-C. Chen, "Multiauth: Enable multi-user authentication with single commodity wifi device," in *Proceedings of the International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (MOBIHOC)*, 2021, pp. 31–40.

[14] M. Muaaz and R. Mayrhofer, "Smartphone-based gait recognition: From authentication to imitation," *IEEE Transactions on Mobile Computing*, vol. 16, no. 11, pp. 3209–3221, 2017.

[15] S. Yue, H. He, H. Wang, H. Rahul, and D. Katabi, "Extracting multi-person respiration from entangled rf signals," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, vol. 2, no. 2, pp. 1–22, 2018.

[16] F. Adib, H. Z. Mao, Z. Kabelac, D. Katabi, and R. C. Miller, "Smart homes that monitor breathing and heart rate," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, 2015, p. 837–846.

[17] S. M. Islam, N. Motoyama, S. Pacheco, and V. M. Lubecke, "Non-contact vital signs monitoring for multiple subjects using a millimeter wave fmcw automotive radar," in *2020 IEEE/MTT-S International Microwave Symposium (IMS)*. IEEE, 2020, pp. 783–786.

[18] C. Iovescu and S. Rao, "The fundamentals of millimeter wave sensors," *Texas Instruments*, pp. 1–8, 2017.

[19] S. Rao, "Introduction to mmwave radar sensing: Fmcw radars," *Texas Instruments*, pp. 1–70, 2020.

[20] U. Guler, T. B. Tufan, A. Chakravarti, Y. Jin, and M. Ghovanloo, "Implantable and wearable sensors for assistive technologies," 2021.

[21] A. Ahmad, J. C. Roh, D. Wang, and A. Dubey, "Vital signs monitoring of multiple people using a fmcw millimeter-wave sensor," in *2018 IEEE Radar Conference (RadarConf18)*. IEEE, 2018, pp. 1450–1455.

[22] D. J. Jwo, I. H. Wu, and Y. Chang, "Windowing design and performance assessment for mitigation of spectrum leakage," in *International Symposium on Global Navigation Satellite System 2018 (ISGNSS 2018)*, 2018, p. No. 03001: 8.

[23] S. Daud and R. Sudirman, "Butterworth bandpass and stationary wavelet transform filter comparison for eeg signal," in *6th International Conference on Intelligent Systems, Modelling and Simulation*. IEEE, 2015, pp. 123–126.

[24] M. A. Russo, D. M. Santarelli, and D. O'Rourke, "The physiological effects of slow breathing in the healthy human," *Breathe*, vol. 13, no. 4, pp. 298–309, 2017.

[25] M. Abadi, S. Z. Moussavi, and A. Mahlooji, "Variable, step-size, block normalized, least mean, square adaptive filter: A unified framework," vol. 15, 2008, pp. 195–202.

[26] F. Scholkmann, J. Boss, and M. Wolf, "An efficient algorithm for automatic peak detection in noisy periodic and quasi-periodic signals," *Algorithms*, vol. 5, no. 4, pp. 588–603, 2012.

[27] K. Yan and D. Zhang, "Feature selection and analysis on correlated gas sensor data with recursive feature elimination," *Sensors and Actuators B: Chemical*, vol. 212, pp. 353–363, 2015.

[28] I. Syarif, A. Prugel-Bennett, and G. Wills, "Svm parameter optimization using grid search and genetic algorithm to improve classification performance," *Telkomnika*, vol. 14, no. 4, p. 1502, 2016.

[29] Y. Xue and M. Hauskrecht, "Active learning of multi-class classification models from ordered class sets," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 33, no. 01, 2019, pp. 5589–5596.

[30] T. Instruments, "Iwr1443 evaluation module (iwr1443boost) mmwave sensing solution user's guide," https://www.ti.com/tool/IWR1443BOOST, 2020, accessed May 19, 2020.

[31] O. Ogbanufe and D. J. Kim, "Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment," *Decision Support Systems*, vol. 106, pp. 1–14, 2018.

[32] H. Shahriar, H. Haddad, and M. Islam, "An iris-based authentication framework to prevent presentation attacks," in *2017 IEEE 41st annual computer software and applications conference (COMPSAC)*, vol. 2. IEEE, 2017, pp. 504–509.

[33] R. Raghavendra, K. B. Raja, and C. Busch, "Presentation attack detection for face recognition using light field camera," *IEEE Transactions on Image Processing*, vol. 24, no. 3, pp. 1060–1075, 2015.

[34] J. Liu, C. Wang, Y. Y. Chen, and N. Saxena, "Vibwrite: Towards finger-input authentication on ubiquitous surfaces via physical vibration," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2017, pp. 73–87.

[35] H. N. Li, C. H. Xu, A. S. Rathore, Z. X. Li, H. B. Zhang, C. Song, K. Wang, L. Su, F. Lin, K. Ren, and W. Y. Xu, "Vocalprint: exploring a resilient and secure voice authentication via mmwave biometric interrogation," in *Proceedings of the 18th Conference on Embedded Networked Sensor Systems (SENSYS)*, 2020, pp. 312–325.

[36] Z. Zhao, L. Yang, D. Chen, and Y. Luo, "A human ecg identification system based on ensemble empirical mode decomposition," *Sensors*, vol. 13, no. 5, pp. 6832–6864, 2013.

[37] J. Chauhan, Y. Hu, S. Seneviratne, A. Misra, A. Seneviratne, and Y. Lee, "Breathprint: Breathing acoustics-based user authentication," in *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services (MOBISYS)*, 2017, pp. 278–291.

Yao Wang received his B.S. and M.S. degrees in Software Engineering from Xidian University in 2009 and 2012, respectively. He then went on to earn his Ph.D. degree in Computer Science from Northwestern Polytechnical University in 2019. He is currently working in the School of Cyber Engineering at Xidian University. His research interests include mobile computing and information security.

Tao Gu (Fellow, IEEE) is a professor at the Department of Computing at Macquarie University. His research interests include Internet of Things, ubiquitous computing, mobile computing, embedded AI, wireless sensor networks, and big data analytics. Currently, he serves as an editor of IMWUT, an associate editor of TMC and IoT-J, and is a member of the ACM. For more information, please visit https://taogu.site.

Haibin Zhang received his B.S. degree from Ocean University of China in 2003, and his M.S. and Ph.D. degrees from Xidian University in 2007. He is currently a professor and serves as the vice dean of Hangzhou Institute of Technology at Xidian University. His research interests mainly focus on AI security, decision intelligence, and intelligent optimization.