Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 9361017, 11 pages
https://doi.org/10.1155/2019/9361017

Research Article

A Continuous User Authentication System Based on Galvanic Coupling Communication for s-Health

Fernando Nakayama,[1] **Paulo Lenz**,[1] **Stella Banou**,[2] **Michele Nogueira**,[1] **Aldri Santos**,[1] **and Kaushik R. Chowdhury**[2]

[1]*Department of Informatics, Federal University of Paraná, Curitiba, Brazil*
[2]*Electrical and Computer Engineering Department, Northeastern University, Boston, MA, USA*

Correspondence should be addressed to Michele Nogueira; michele@inf.ufpr.br

Received 23 August 2019; Accepted 8 November 2019; Published 28 November 2019

Guest Editor: Raquel Lacuesta

Smart health (s-health) is a vital topic and an essential research field today, supporting the real-time monitoring of user's data by using sensors, either in direct or indirect contact with the human body. Real-time monitoring promotes changes in healthcare from a reactive to a proactive paradigm, contributing to early detection, prevention, and long-term management of health conditions. Under these new conditions, continuous user authentication plays a key role in protecting data and access control, once it focuses on keeping track of a user's identity throughout the system operation. Traditional user authentication systems cannot fulfill the security requirements of s-health, because they are limited, prone to security breaches, and require the user to frequently authenticate by, e.g., a password or fingerprint. This interrupts the normal use of the system, being highly inconvenient and not user friendly. Also, data transmission in current authentication systems relies on wireless technologies, which are susceptible to eavesdropping during the pairing stage. Biological signals, e.g., electrocardiogram (ECG) and electroencephalogram (EEG), can offer continuous and seamless authentication bolstered by exclusive characteristics from each individual. However, it is necessary to redesign current authentication systems to encompass biometric traits and new communication technologies that can jointly protect data and provide continuous authentication. Hence, this article presents a novel biosignal authentication system, in which the photoplethysmogram (PPG) biosignal and a galvanic coupling (GC) channel lead to continuous, seamless, and secure user authentication. Furthermore, this article contributes to a clear organization of the state of the art on biosignal-based continuous user authentication systems, assisting research studies in this field. The evaluation of the system feasibility presents accuracy in keeping data integrity and up to 98.66% accuracy in the authentication process.

1. Introduction

Smart healthcare (s-health) applications have great potential to positively impact the daily lives of many people, contributing to early detection, prevention, and long-term management of health conditions. Health monitoring is a vital topic and an essential research field supported by sensors in wearable devices which are either in direct contact with the human body (invasive) or indirect (noninvasive). Healthcare is moving from a reactive approach to a proactive one, promoted mainly by the continuous monitoring of health conditions and the techniques of data analytics applied to the collected data. The monitoring system allows an individual to closely monitor their changes in vital signs and provide feedback in real-time, which helps to maintain optimal health status.

Data privacy is the main concern in s-health [1], given the vulnerabilities found in wearable devices related to data collection, resource constraints, and vulnerabilities in communication technologies, such as wireless communication [2]. Recent attacks against healthcare providers have exposed an increasing number of security and privacy breaches, as pointed out by CynergisTek on its 7th annual breach report [3]. Also, regulatory worldwide institutions,

e.g., the U.S. Food and Drug Administration (FDA), request public and private companies to develop high-quality and secure healthcare devices and applications [4] by acts such as the Health Insurance Portability and Accountability Act (HIPAA). However, preserving data privacy and access in s-health environment without affecting its usability is a challenging task.

In this context, user authentication systems are crucial to grant data access for authorized professionals [5]. Traditional methods follow one-time event authentication and demand the user to intentionally engage with the system, such as scan a fingerprint or key in a password every certain period [6]. However, the offered security of one-time event authentication solutions lasts for short periods, being prone to malicious actions and requiring regular attention and interaction from users [6]. Also, data transmission in current authentication systems relies on wireless technologies. These technologies are susceptible to eavesdropping during the pairing stage, being necessary to design a distinct and secure communication channel.

Hence, the significance and the challenges of s-health applications have led to the exploration of new forms of human-computer interactions and communication technologies for designing continuous and seamless user authentication [7]. The literature has highlighted a set of recurrent biosignals (e.g., electrocardiogram (ECG), electroencephalogram (EEG), galvanic skin response (GSR) [8]) and experimental communication channels (e.g., galvanic coupling (GC)) [9] applied to continuous authentication and less interaction from users. Furthermore, advances in microelectronics and nanoelectronics have assisted the development of different types of sensors that provide real-time vital signs acquisition. Thus, it is time to rethink current authentication systems to encompass new biometric traits and communication technologies that can protect data and provide continuous authentication.

This article presents the Biosignal Enhanced AuThentication system (BEAT), an original continuous authentication system based on photoplethysmogram (PPG) signals and data transmission through a secure galvanic coupling (GC) channel. The GC channel deals with one of the main issues regarding the communication between wearable devices, once there are a wide variety of security vulnerabilities affecting wireless communication technologies [10, 11]. The PPG biosignal is one of the easiest biosignals to collect, becoming popular in commercial wearable devices, such as fitness trackers. This article also fills a gap overviewing and organizing the state of the art on biosignal-based and continuous user authentication systems. It contributes with a substantial and relevant holistic view about future research directions in this crucial topic. The feasibility of the system has been evaluated by a prototype using PPG as biosignal and a synthetic skin as a transmission medium. Evaluation results show the system accuracy in preserving data integrity during transmission and up to 98.66% of true positive in the authentication.

This article proceeds as follows. Section 2 presents the literature review of existing biosignal-based continuous authentication systems. Section 3 details the proposed PPG-based user authentication system. Section 4 describes its performance evaluation and results. Finally, Section 5 shows future directions in this topic and concludes the article.

2. Related Works

This section presents a literature review and a classification of authentication systems that employ biosignals. Although various works in the literature use biosignals as user credentials for continuous authentication systems, they have not been organized. Observations from this study have led to identifying recurrent features, such as diversity in the type of sensors; focus on a single part of the body as the source of biosignal; the requirement or not of specific actions from users; and the heterogeneity in the explored communication channels. Based on this, Figure 1 summarizes a classification of these works, following four main categories: (i) sensors, (ii) sources of biosignals, (iii) actions required from users, and (iv) communication channels. Each category is explained, offering an overview of the main existing works.

2.1. Sensors. This category highlights the type of sensors employed in continuous user authentication systems, focusing on biosensors, which collect vital signs from users and are the basis for different services in the context of s-health. Among the biosensors, those commonly applied in continuous authentication systems are mechanical, electrical, and optical, as detailed next. Continuous authentication systems, such as in [12], rely on mechanical sensors that utilize mechanical force or pressure to identify the response of a muscle contraction, the push of a button, or the pressure of a footstep. Based on an occasional or repetitive movement, e.g., arm gesture, walking, and leg movement, the system can identify a pattern, which is employed to identify the user.

User authentication systems, such as found in [13, 14], employ electric biosensors to interpret the electrical activity of the body (e.g., muscle or heart activity) during a period to get biosignals that will later act as a unique characteristic to identify each registered user. These biosensors require direct contact (or the use of electrodes) to the activity area to allow signal acquisition. The sensors may require or not the use of conductive gel in the points of contact.

Optical sensors analyze the dilatation of blood vessels to calculate the user's heart rate, among other features. These sensors emit light against the user's skin and measure light reflection. Optical sensors can collect biosignals from the heart (PPG and heart rate) and lungs (respiratory rates). For instance, PPG biosignal is used as a unique identifier for continuous authentication in [15–17]. PPG generates a pulse wave in which several features are estimated, analyzed, and extracted. Those features are exclusive for each human being, making it feasible to use them for authentication purposes.

Few continuous user authentication systems also rely on multisensors, i.e., in general, devices carrying more than one sensor of different types. Multisensor devices have become popular given their miniaturization and cheapness. Multiple sensors in the same device may offer multiple biosignals,

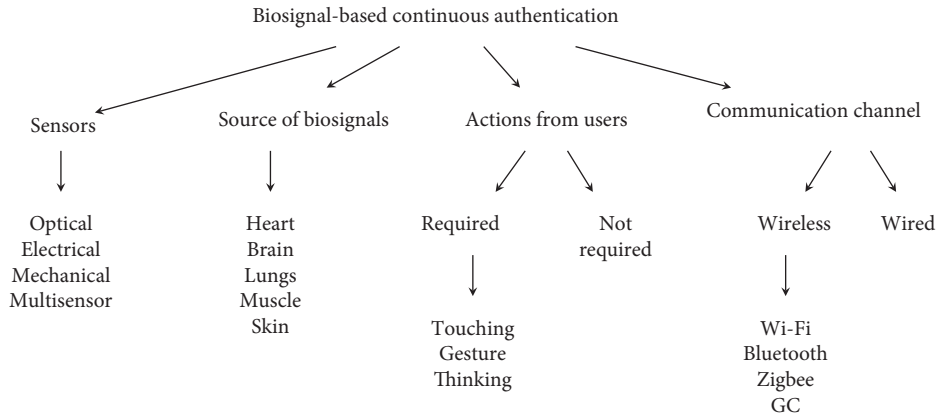


Figure 1: Taxonomy for biosignal-based continuous authentication systems.

improving efficiency by their combination. For instance, in [13] and [18], the authors employ multisensors for user authentication.

2.2. Sources of Biosignals. This category observes the continuous authentication systems under the perspective of the biosignal source. Identified works from the literature have commonly collected biosignals from the heart, brain, lungs, muscles movement, and skin. Each source of biosignals results in specific characteristics with advantages and disadvantages, as discussed next.

Biosignals from the heart are most commonly used in continuous authentication systems. PPG, ECG, and blood pressure are biosignals offering information about heart rate variation. PPG signals depend on optical sensors to be collected; ECG signals on electrical sensors; and blood pressure is usually measured from types of equipment with mechanical sensors. Authentication systems based on heart-related biosignals are available in the literature, such as [14, 15, 19].

Brainwaves are biosignals that originate in the brain. Studies have shown their feasibility to authenticate users, such as in [20], but it is required repetitive thinking from the user to create a pattern, e.g., think about an action, a picture or a geometric shape, or even memorize a speech. EEG is the most common biosignal from the brain; electrodes connected to sensors and placed on different spots on the head collect the signal. Less-invasive methods are also available like headsets and in-ear sensors.

Respiratory rate is a biosignal, once it is possible to create a breathing pattern, having the biosignal collected through microphones or the level of oxygen saturation measured through a PPG signal. This rate is the most common type of biosignal observed from the lungs. In [21], the authors presented an authentication system using the breathing pattern recorded from a microphone as a user identifier.

Upon contraction, muscles generate small electric signals. The signals are constantly measured and stored, aiding the extraction of a pattern that serves as a user identifier. The most common signal observed from muscles is the electromyogram (EMG). Muscles can trigger a mechanical sensor, pressing a button or activating a foot pressure sensor for plantar biometric recognition. Works such as [12, 22, 23] presented authentication systems based on muscle-related biosignals.

Finally, different skin properties can be measured and their values are considered biosignals. For instance, electrodermal activity (galvanic skin response) reflects the variation of the electrical characteristics in the skin by mirroring its conductance. Sudden changes in the electrical conductivity of the skin show stress, fear, and surprise, among other emotions. The galvanic skin response is unique for each user and has been employed to continuously authenticate a user. In [18], the authors evaluated the feasibility to use galvanic skin response biosignal to authenticate a user.

2.3. Actions from Users. Continuous authentication mechanisms are developed to authenticate a legitimate owner throughout their entire session [24]. Existing systems collect biosignal with or without the necessity of specific action from the user. Recent continuous authentication systems seek to perform authentication seamlessly, i.e., with low user interaction with the system or no user interaction at all. However, achieving seamless in this context is still a relevant challenge. In continuous authentication systems that require no user action, the sensor continually collects biosignals with no specific action from the user, e.g., a smartwatch that collects a biosignal continuously [15].

There are authentication systems that require interaction from the user within periods of time. Examples of interactions are touching the device to collect the biosignal [14], a specific gesture [23], walking [12], or thinking about a previously defined theme [20].

Touching is required in different systems, such as [14, 25]. For instance, ECG-capable smartwatches need signals from both sides of the body to authenticate a user. Hence, if the user wears the smartwatch on the right wrist, he/she will need to touch it with the left hand to generate the authentication signal. Similarly, gestures and thinking generate EMG and EEC signals, respectively. The first is collected through muscle contraction, whereas the second requires the user to think about something (shapes, colors,

speeches, etc.) to generate a pattern and then employed for authentication.

2.4. Communication Channels. Most biosignal-based authentication mechanisms use wireless radio frequency transmission as a communication channel. However, major communication technologies such as Bluetooth, Zigbee, and NFC have presented security flaws [10]. The galvanic coupling (GC) method is a promising communication channel by the human body, having the skin and tissues as conductors. Recently, we have observed an increase in the number of works employing GC as a communication channel, such as in [9]. Using human skin as a communication medium pursues a secure data transmission, once signal interception would not be possible without skin contact.

3. BEAT Authentication System

This section presents BEAT, a new biosignal-based and continuous user authentication system to attain seamless and secure authentication. BEAT authenticates a user based on PPG biosignals, collected continuously by wearable sensors and transmitted by GC from these sensors to a coordinator device, where the user needs access. BEAT acts within the s-health concept, considering a star network topology composed by a coordinator (e.g., a smartphone) as a central device and wearable devices connected to it. The network coordinator usually has higher computational resources (energy, memory and processing power) than other wearable devices in or on the human body. Furthermore, GC can protect data transmission between a wearable device and the network coordinator.

BEAT follows three steps: (i) data collection and preprocessing, (ii) data transmission by GC, and (iii) the authentication procedure, as shown in Figure 2. Hence, Figure 2(a) illustrates the network coordinator as a smartphone, but it could be any device in direct contact with the user's skin and able to serve as a communication gateway between the wearable network and other networks, e.g., a wireless local area network (WLAN) or the Internet. It is out of the scope of this work to handle the communication between the network coordinator and the Internet; or between the first and a WLAN.

Figure 2(a) also indicates multiple wearable devices positioned on different parts of the body, such as head, eyes, ears, clothing, wrist, and ankle. A wearable device lies in an autonomous, noninvasive device, performing a specific function related to the body, e.g., monitor a user's vital signs. Examples of wearable devices are smartphones, smartwatches, physical activity monitors, smart sneakers, and others. A generic architecture of a wearable device follows the modules: sensor, low-power processor, and communication. After data collection, wearable devices convert collected signals into raw data. Depending on the monitoring task, different types of sensors can be employed. BEAT is founded on optical sensors, such as those in smartwatches and physical activity monitors, once this type of sensors benefits from convenience and usability for users.

3.1. Data Acquisition and Signal Preprocessing. BEAT collects PPG signals, allowing the observation and extraction of unique user features, as the number of peaks and valleys, peak shapes, wave amplitude, and the distance between peaks and valleys, as shown in Figure 3. BEAT uses a combination of these features, using the time-frequency domain, to correlate the entire set of collected data by wave segments and improving robustness for user authentication. Regardless of the extracted trait, the identification of peaks and valleys is crucial, as the threshold authentication limit is based on peak overlapping.

After data acquisition, BEAT filters the collected signals to reduce noise from electromagnetic interference, light excess, and sudden user movements. Hardware filters are efficient and fast to extract specific data (e.g., data related to cardiac variation or breathing), but they are limited in terms of flexibility because they collect data in a specific range of frequencies. Similarly, to hardware filters, software filters limit the amplitude of the collected signal. Although these filters are slower than hardware filters, they are more flexible to adjust the filtered frequency band.

Among the filtering techniques, examples are frequency band segmentation and high-pass, low-pass, and band-pass filters. The choice for a given filter depends on the goals. Also, computational restrictions in wearable devices should be considered in the filter choice, and it is necessary to select filters with low computational complexity. Thus, high-pass, low-pass, and band-pass filters are preferable because they perform signal segmentation in several bands (multidimensional); their configuration allows a cutoff frequency and a reduced number of operations, leading to efficient energy use.

3.2. Data Transmission by Galvanic Coupling. BEAT adopts GC to significantly reduce vulnerability to attacks when compared to conventional communication technologies, such as Bluetooth, Zigbee, and others. In GC, data are encoded and transmitted by low-voltage electrical impulses sent through human skin, thus being immune to attacks, such as eavesdropping and others. GC acts on intracorporal communication, and it is within the scope of the IEEE 802.15.6 standard. In an intracorporal data transmission using GC, a differential electric signal is applied to two transmission electrodes on the skin. Most of the signals sent by the electrodes to the skin are dispersed. However, an amount of the signal is conducted by the skin and tissues, reaching the two contact electrodes in the receiver. The main feature of the differential signal in GC comprises the model of sending data through the two electrodes. At each electrode, the biosignals are reversed proportionally before transmission through the skin. The receiving device calculates the difference between the two received signals, getting the original signal. Figure 4 exemplifies the GC model.

Signal power is strongly influenced by the dielectric (insulating) properties of the body tissues. The body is the medium for sending (Tx) and receiving (Rx) data, the modulation and power of the signal being relevant issues. Modulation reflects the characteristics of the GC circuit,

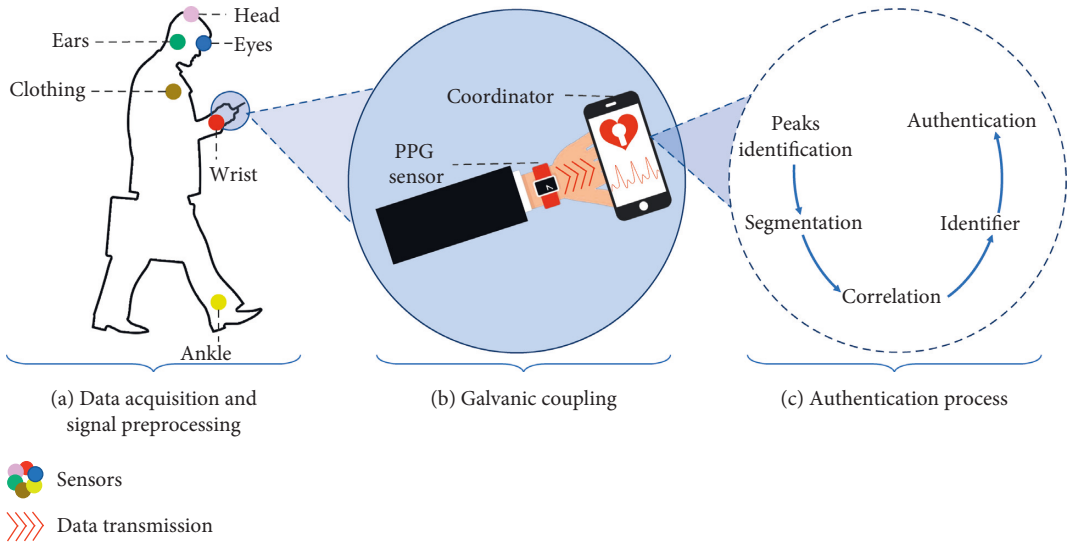


Figure 2: Steps of the BEAT authentication system.

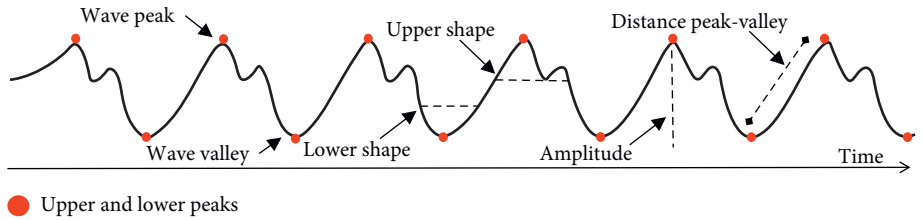


Figure 3: Main features in a PPG signal waveform.

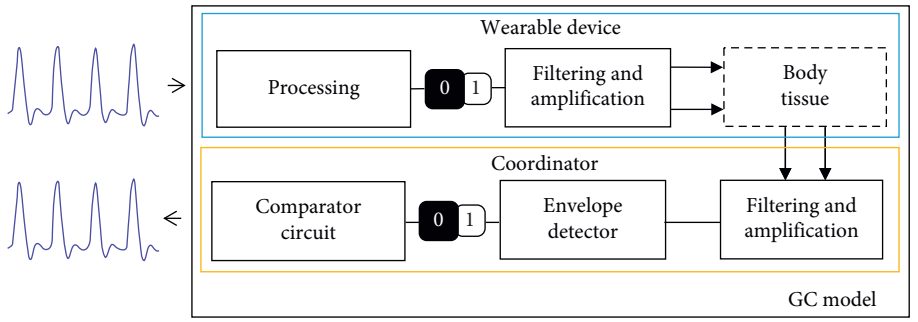


Figure 4: Galvanic coupling model.

emphasizing robustness and simplicity. BEAT follows the Pulse Width Modulation (PWM) for consuming less energy and conforming to the On-Off nature of digital devices. PWM represents the digital data through variations in amplitude and period in a carrier envelope. It estimates data through the presence or absence of an undercut and its percentage of duration in each state On-Off. The existence of a wave for a specific period means the binary 1, while its absence for a period means a binary 0.

3.3. Authentication Procedure. The authentication procedure (Figure 2(c)) occurs in the network coordinator. When the coordinator receives the preprocessed PPG signal, it assigns a function to extract features from the PPG waveform. The authentication procedure handles the waveform in four tasks: peak identification, segmentation, correlation, and user identifier calculation. The first one lies in identifying peaks along the entire length of the collected and preprocessed biosignal. This task is fundamental to define reference points for the segmentation phase. To identify peaks, BEAT employs specific algorithms, such as those based on moving averages or a set of features (e.g., peak and minimum height) for threshold calculation [26].

The second task segments the collected biosignal in cycles related to the wavelength. Thus, each cycle is identified, and then, all detected cycles are overlapped and aligned taking as reference the center of the previously

detected peaks. This allows us to make the correlation (the third task) of all segments and calculate their average. This average is referred to as a user identifier, its calculation being the fourth task. Thus, when the user identifier matches an existing reference model in the system, BEAT authenticates the user. Otherwise, it denies user access to services and data.

The authentication procedure relies on the previous registration of the users. The registration procedure takes place offline, and its tasks are similar to the authentication ones, but registration demands a higher amount of data, considering different user positions and physical states. User registration begins with data collection, following feature extraction and signal segmentation. Segmented cycles are aligned taking peaks as reference. This allows the correlation among all segments and their average calculation. Correlation defines an authentication threshold (user reference model), which is calculated by the minimum average value for a user to be authenticated. On an authentication attempt, the reference model is compared to the generated user identifier following authentication, as previously described.

Figure 5 summarizes the registration and authentication procedures. The registration procedure occurs before the authentication procedure and requires a higher amount of data compared to the authentication process; this is due to the need for more data to build the reference model. The authentication process occurs online, i.e., when the user needs to access the system or service.

4. Experimental Design and Analysis

This section details the real implementation of BEAT and its performance analysis. Evaluations have followed two approaches: (i) an experimental environment within the context of the NSF/RNP US-Brazil Healthsense project; (ii) based on a dataset available in the Physionet online repository. These two approaches aim at comparing their results.

4.1. Implementation of BEAT in an Experimental Environment. This implementation of BEAT employs the PPG Gravity Heart Rate Monitor Sensor from DfRobot, whose spectral response peak is 570 nm. It has been integrated into an open Arduino platform version R3, with a 16 MHz ATmega328 microcontroller, the same in several wearable devices. Figure 6(a) shows a picture from the data collection.

The galvanic coupling implementation and analysis employ two 72 MHz 32-bit Teensys 3.2 development boards acting as a signal transmitter (TX) and receiver (RX), powered by different sources and with no shared ground. The PPG signal is amplified, binary encoded, and injected into a synthetic skin tissue through jump wires that emulate contact skin electrodes. For evaluation purposes, we transfer a sample of real PPG signals from the emitter to the receiver through the synthetic skin using a distance of 8 centimetres. At the receiver, the signal is amplified once again, as the synthetic tissue has insulating properties, and then it is restored to the original form. We evaluate the data integrity of the signal by the transmitted sample to create an identifier model. This model is later compared to the reference model to perform user authentication, assuring the correctness and compatibility of the signal. Figure 6(b) shows a picture of the GC testbed.

The user registration procedure occurs in a controlled environment, protected from electromagnetic interference and from a direct incidence of light. We have collected PPG signals, and we have recorded both the time of capture and the numerical values of signal for each individual. The outcomes of the registration procedure are two datasets (NR2/UFPR#1 and #2), comprising data from 30 healthy individuals from 23 to 53 years old and with no record of cardiac issues. Each individual had their PPG signal collected and recorded in two positions: standing and sitting. The NR2/UFPR#1 dataset contains a set of files, one for each individual, with data from the seated individuals, whereas the NR2/UFPR#2 dataset contains a set of files, one for each individual, with data from standing individuals. Both datasets are publicly available at the Healthsense Project repository (https://github.com/Healthsense-Project). User registrations have occurred at different times as would happen in a real situation. Datasets hold a three-minute sample per individual. Figure 7 shows for a real sample the original PPG signal (as captured by the sensor); the filtered signal; and the filtered signal with detected peaks.

The testbed employs the eighth-order Chebyshev II low-pass filter over the collected signal using the R software. This filter fits wearable devices, which have low computational power microcontrollers. Feature extraction from the PPG signal uses the frequency band from 0.5 to 5.0 Hz. Earlier, peaks are detected and segments are overlapped; hence, the R Cross-Correlation Function (CCF) computes the correlation among all overlapping segments. CCF establishes the correlation between two distinct series and their respective confidence intervals. Hence, BEAT calculates the user reference model (authentication threshold), as seen in Figure 8.

The authentication procedure has input one-minute real-time collected data per user in each position. The evaluated metrics are the true- and false-positive rates, the true- and false-negative rates, and the total of inference and accuracy. Figure 9(a) compares the reference model recorded for a given user (red wave) and the identifier for the same user (blue wave) calculated on the authentication procedure. Although such waves are not fully identical, they are within the established threshold, showing the existence of enough similarity to allow user authentication. Figure 9(b) shows a comparison for a reference model and the identifier from different users, where the access was denied.

A low-pass filter removes the harmonics from the collected PPG signal, preserving the central band (FC = 100 kHz). Next, data are sent through the communication channel within the payload of a frame, which comprises a preamble (13-bit Barker code) for synchronization, a data length field, payload (64 bits), and 8-bit CRC. As the signal propagates through the synthetic skin, analog receiver hardware uses a high-pass filter to remove any low-frequency noise from interference. An amplifier (MAX4488 from Maxim Integrated TM) neutralizes the channel

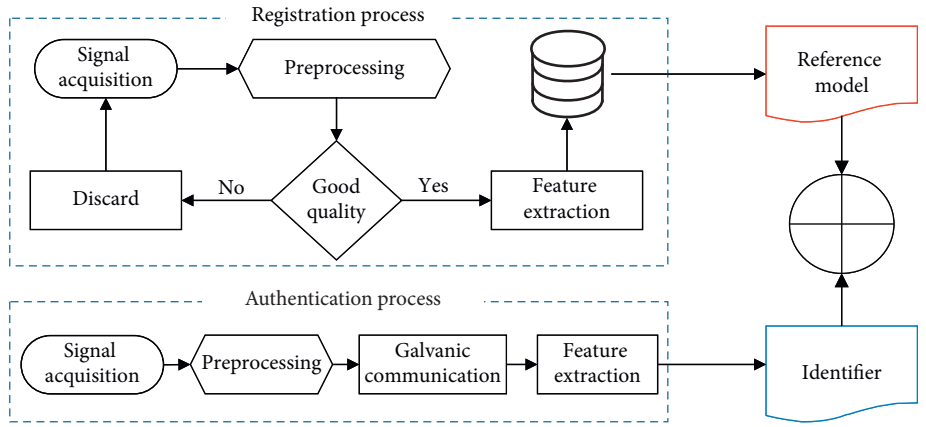
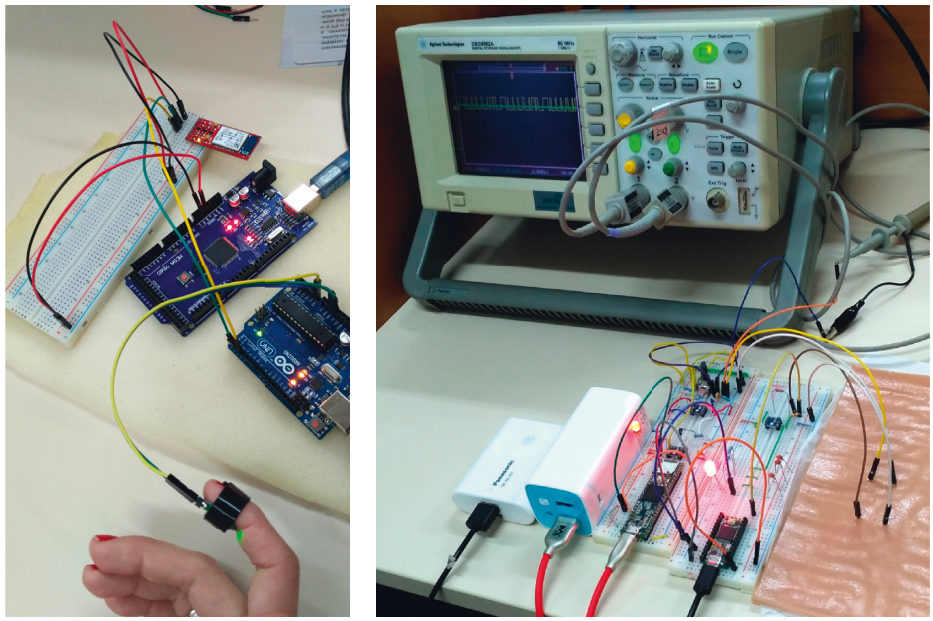


Figure 5: Register and authentication for the BEAT system.



(a) (b)

Figure 6: Testbeds. (a) PPG. (b) GC.

attenuation and the high-frequency filter raises the signal level to meet the activation voltage required for the diode. An envelope detector circuit converts the signal back to baseband and removes any possible carrier wave oscillations before delivering the signal to the comparator circuit.

Aside from the tests performed in the described experimental environment, the Beth Israel Deaconess Medical Center dataset from the Physionet repository [27] has served as the basis for comparative analysis. This dataset contains PPG signals collected from 30 individuals at the 125 Hz frequency by the Israeli center. The individuals suffer from some critical health conditions (e.g., heart, respiratory, and other problems), and when the data were collected, the individuals were resting in the hospital bed. It is worth to mention that there was no control over this last dataset creation, i.e., there was no management about the conditions of the environment in which data were collected or about the PPG sensor quality. Signal segments have resulted in handling three minutes of information from this dataset to create the user reference model (user registration) and one minute to calculate the user identifier employed for user authentication.

Table 1 summarizes the results for the analyzed metrics over the three evaluated datasets. BEAT has shown the best results for the NR2/UFPR#1 dataset, presenting an accuracy of 98.66%, 12 false positives, and no false negative. For the Physionet dataset, it has obtained an accuracy of 89.88% and no false negative but reached 91 false positives in 900 inferences. The NR2/UFPR#2 dataset has presented 26 valid users (peaks satisfactorily identified) of the initial 30 users and 676 inferences. For valid users, BEAT has achieved an accuracy of 92.15%, 3 false negatives, and 50 false positives for the NR2/UFPR#2 dataset.

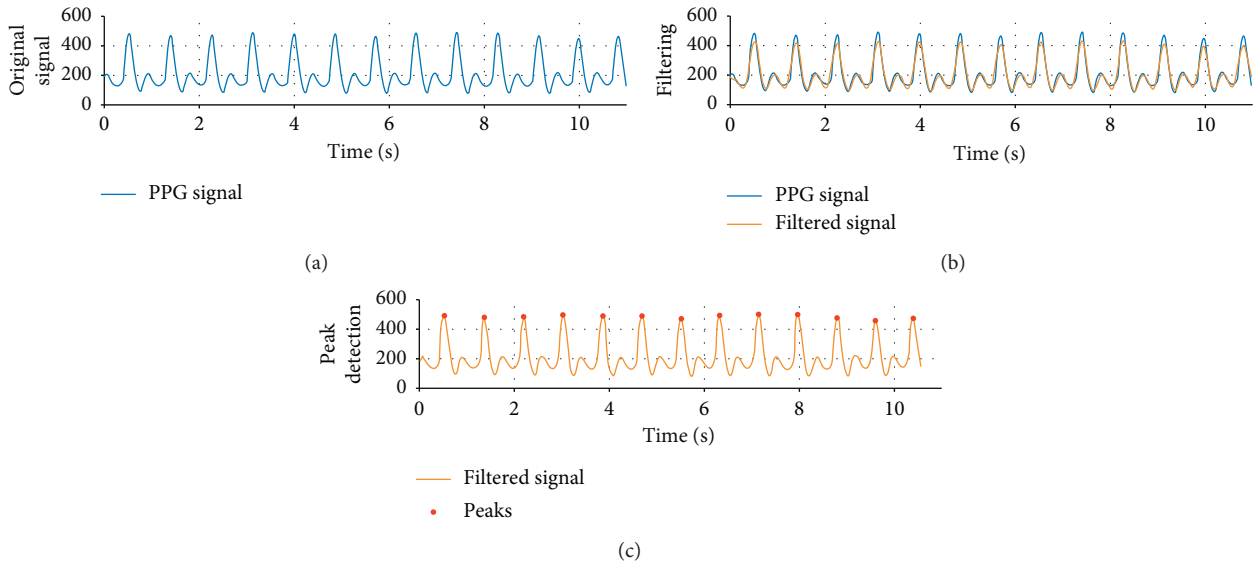


Figure 7: Signals and preprocessing.

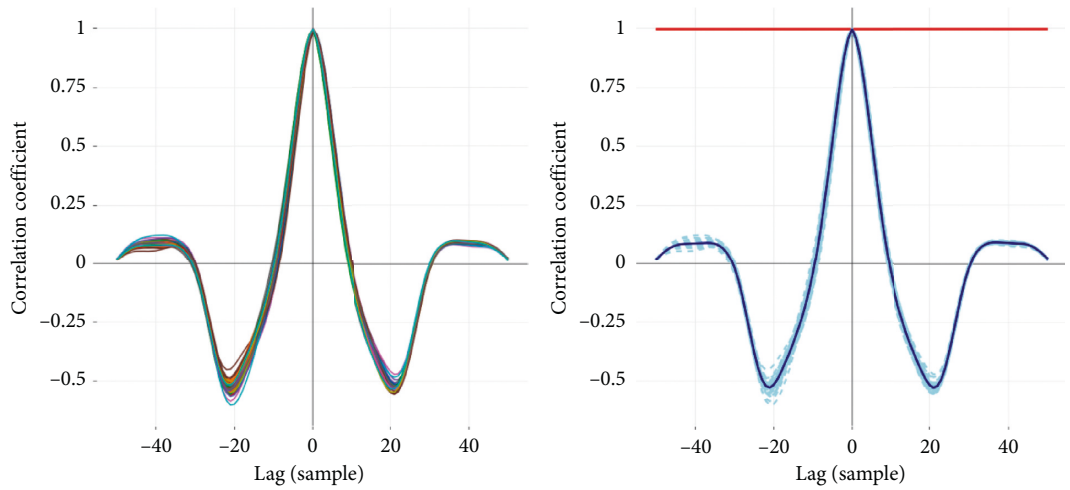


Figure 8: Authentication threshold.

Even with the application of filters, some factors could not be circumvented, such as an excessive movement during collection, electromagnetic interference, and other environmental issues. The best outcome of the NR2/UFPR#1 dataset is due to the stability offered by the sitting position, which allows the user's arm to be in rest position, which generates less movement and a stable PPG waveform.

Figure 10 shows the validation results for all individuals of the NR2/UFPR#1 dataset. The false-positive values in the authentication map indicate that the collected data are stable, making it possible to extract several features from the waveforms. Even with the signal collected from users with critical health conditions, the system has achieved accuracy close to 90% for the Physionet dataset. We suspect that the high number of false positives is due to the low-quality PPG signal, since four users from the dataset account for 60.4% of all false positives. Evaluating the two authentication maps, we observe that none of them got false negatives, showing that in every situation in which a legitimate user tried to authenticate, the authentication was successful. Authentication accuracy yielded by BEAT is equivalent to other PPG authentication systems such as [28, 29]. However, BEAT employs GC to provide a secure communication channel, making it difficult to perform a full comparison once; to the best of our knowledge, there is no other system that jointly applies PPG biosignal and GC to user authentication.

5. Conclusion

Smart healthcare (s-health) is an exciting topic that has led to a considerable number of research studies mainly concerned with the security of data, which are continuously collected from users by devices integrated into their clothing or worn on the body. To provide security, user authentication systems play a crucial role. However, it is imperative to redesign them considering the limitations of wearable devices, in

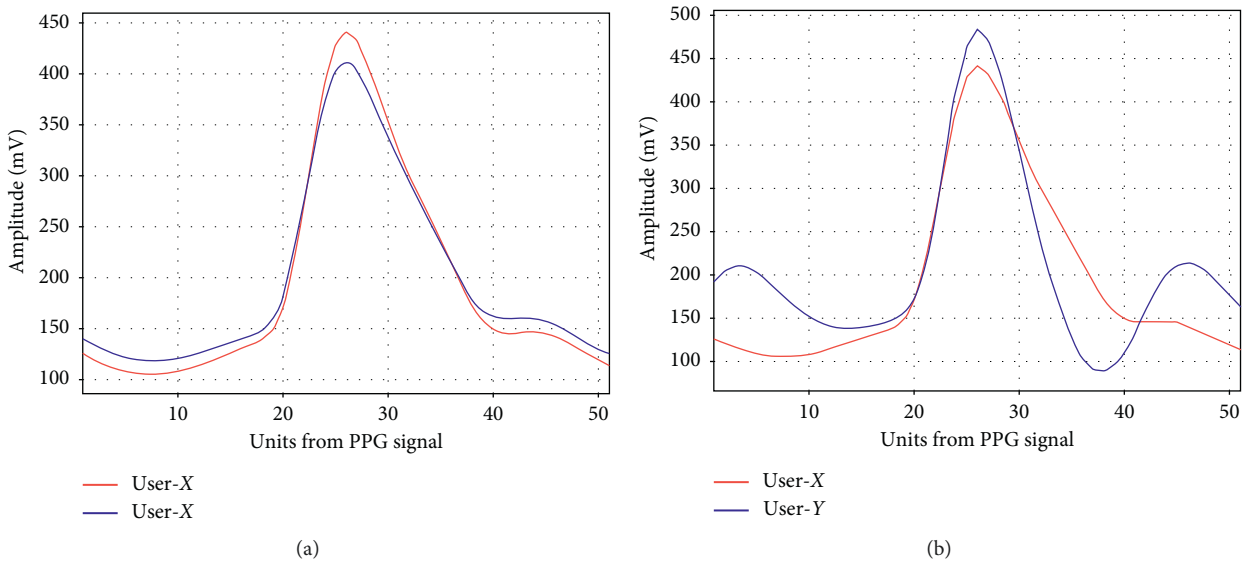


Figure 9: Authentication process. (a) Access granted. (b) Access denied.

Table 1: Comparing results from the NR2/UFPR and Physionet datasets.

	TP	FP	TN	FN	IT	Accuracy (%)
NR2/UFPR dataset #1	30	12	858	0	900	**98.66**
NR2/UFPR dataset #2	23	50	600	3	676	**92.15**
Physionet dataset	30	91	779	0	900	**89.88**

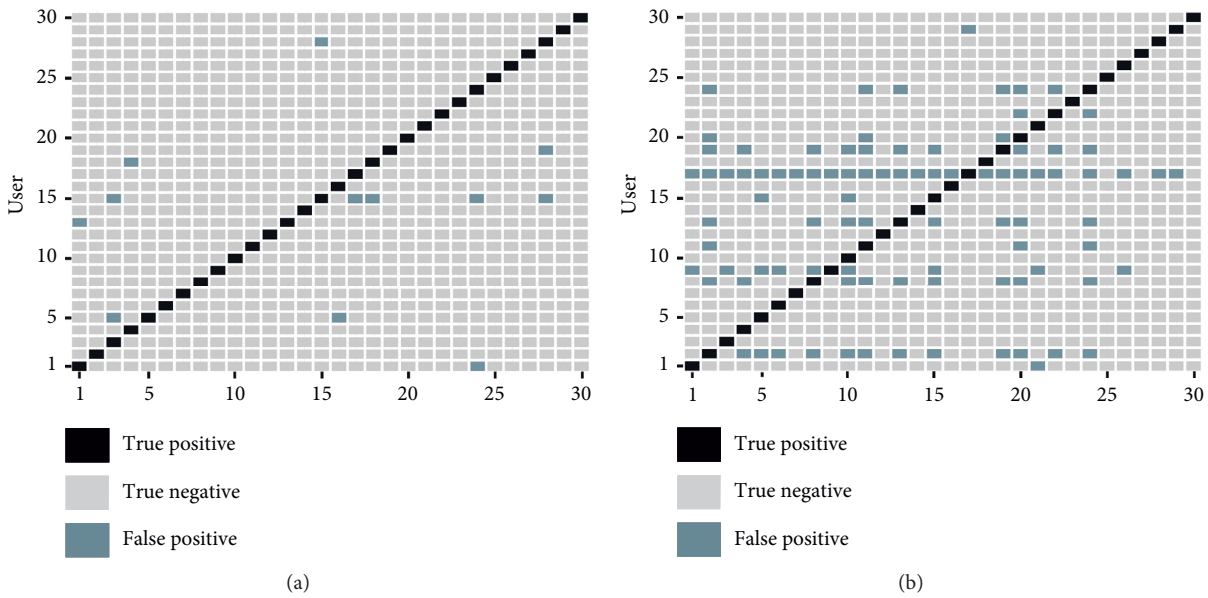


Figure 10: Authentication map. (a) NR2/UFPR dataset #1. (b) Physionet dataset.

which the human-computer interaction varies from the traditional perspective. For instance, one can expect no more the use of long-alphabetic passwords in wearable devices (mainly in the implanted ones) as a way to grant access to systems, once passwords lack convenience and require users' regular attention.

Based on the literature overview, this article presented BEAT, a new authentication system that uses PPG signals and galvanic coupling (GC), as a communication channel to authenticate users in a wearable network. BEAT aims at achieving seamless, i.e., high transparency to the user in the authentication process, and security. The acquisition of the

PPG signal is nonintrusive, and data are transmitted by GC, keeping the user continuously connected. Results from real experimentation have shown high accuracy, high true positives, and low false positives, being the incidence of false positives directly related to the quality of the PPG signal. The results of the experiments with the system indicate the feasibility of the PPG signal as a biometric authenticator; furthermore, using the galvanic coupling communication to transfer data raises security to a new level.

This article also presented an organization for the state of the art in biosignal-based user authentication. The organization follows four important categories considering the type of sensors: the employed biosignal and its source of the collection; the necessity or not of specific user actions; and the communication channel. This article highlighted each category and associated them with the main existing works from the literature.

Despite prominent advances, there are still challenges and opportunities for research studies on this fascinated topic. First, techniques to extract features and patterns from biosignals require improvements in efficiency (accuracy and low false-positive rates) to work on real-time over short time windows of collected data. Second, it is paramount to design resilient biosignal-based authentication systems to low quality in collected signals. A way in this direction would be aligned with the use of multisensors, which offer different biosignals or redundancy on the collection of the same signal. Third, designing user authentication systems that require no actions from users, i.e., seamless authentication to users, is urgent, given the rapid advances in nanotechnology that allow wearing devices in the body. Fourth, in the search for seamless, it is necessary to advance in an efficient communication interfacing body-implanted devices and network coordinators.

Data Availability

The datasets used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to thank CAPES, CNPq, and the Joint NSF and RNP HealthSense Project (Grant no. 99/2017 in Brazil).

References

[1] A. A. Abdellatif, A. Mohamed, C. F. Chiasserini, M. Tlili, and A. Erbad, "Edge computing for smart health: context-aware approaches, opportunities, and challenges," *IEEE Network*, vol. 33, no. 3, pp. 196–203, 2019.

[2] M. Kay, J. Santos, and M. Takane, "mhealth: new horizons for health through mobile technologies," *World Health Organization*, vol. 64, no. 7, pp. 66–71, 2011.

[3] R. CynergisTek, Breach Report 2016: protected health information (PHI), 2017.

[4] FDA, "Digital health innovation action plan," Tech. Rep., U.S. Department of Health and Human services food and Drug administration, Silver Spring, MD, USA, 2018.

[5] R. S. Sandhu and P. Samarati, "Access control: principle and practice," *IEEE Communications Magazine*, vol. 32, no. 9, pp. 40–48, 1994.

[6] 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'17*, pp. 315–328, ACM, Snowbird, UT, USA, October 2017.

[7] Z. Sitová, J. Šeděnka, Q. Yang et al., "HMOG: new behavioral biometric features for continuous authentication of smartphone users," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 877–892, 2015.

[8] J. Sancho, Á. Alesanco, and J. García, "Biometric authentication using the PPG: a long-term feasibility study," *Sensors*, vol. 18, no. 5, pp. 1525–1538, 2018.

[9] W. J. Tomlinson, S. Banou, C. Yu, M. Nogueira, and K. R. Chowdhury, "Secure on-skin biometric signal transmission using galvanic coupling," in *Proceedings of the International Conference on Computer Communications (INFOCOM)*, pp. 1135–1143, IEEE, Paris, France, April 2019.

[10] D. Celebucki, M. A. Lin, and S. Graham, "A security evaluation of popular internet of things protocols for manufacturers," in *Proceedings of the International Conference on Consumer Electronics (ICCE)*, pp. 1–6, IEEE, Las Vegas, NV, USA, January 2018.

[11] A. Lonzetta, P. Cope, J. Campbell, B. Mohd, and T. Hayajneh, "Security vulnerabilities in bluetooth technology as used in IoT," *Journal of Sensor and Actuator Networks*, vol. 7, no. 3, pp. 28–56, 2018.

[12] K.-H. Yeh, C. Su, W. Chiu, and L. Zhou, "I walk, therefore i am: continuous user authentication with plantar biometrics," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 150–157, 2018.

[13] A. Mosenia, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "CABA: continuous authentication based on BioAura," *IEEE Transactions on Computers*, vol. 66, no. 5, pp. 759–772, 2017.

[14] N. Belgacem, R. Fournier, A. Nait-Ali, and F. Bereksi-Reguig, "A novel biometric authentication approach using ECG and EMG signals," *Journal of Medical Engineering & Technology*, vol. 39, no. 4, pp. 226–238, 2015.

[15] G. Wu, J. Wang, Y. Zhang, and S. Jiang, "A continuous identity authentication scheme based on physiological and behavioral characteristics," *Sensors*, vol. 18, no. 1, pp. 179–199, 2018.

[16] Y. Y. Gu, Y. Zhang, and Y. Zhang, "A novel biometric approach in human verification by photoplethysmographic signals," in *Proceedings of the International Special Topic Conference on Information Technology Applications in Biomedicine (EMBS)*, pp. 13-14, IEEE, Birmingham, UK, April 2003.

[17] P. Spachos, J. Gao, and D. Hatzinakos, "Feasibility study of photoplethysmographic signals for biometric identification," in *Proceedings of the 17th International Conference on Digital Signal Processing (DSP)*, pp. 1–5, IEEE, Corfu, Greece, July 2011.

[18] J. Blasco and P. Peris-Lopez, "On the feasibility of low-cost wearable sensors for multi-modal biometric verification," *Sensors*, vol. 18, no. 9, pp. 2782–2802, 2018.

[19] T. S. Enamamu, N. Clarke, P. Haskell-Dowland, and F. Li, "Smart watch based body-temperature authentication," in *Proceedings of the International Conference on Computing Networking and Informatics (ICCNI)*, pp. 1–7, IEEE, Lagos, Nigeria, October 2017.

[20] L. Zhou, C. Su, W. Chiu, and K.-H. Yeh, "You think, therefore you are: transparent authentication system with brainwave-oriented bio-features for IoT networks," *IEEE Transactions on Emerging Topics in Computing*, 2017.

[21] J. Chauhan, Y. Hu, S. Seneviratne et al., "Breathing acoustics-based user authentication," in *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services—MobiSys'17*, pp. 278–291, ACM, Niagara Falls, NY, USA, June 2017.

[22] G. Peng, G. Zhou, D. T. Nguyen, X. Qi, Q. Yang, and S. Wang, "Continuous authentication with touch behavioral biometrics and voice on wearable glasses," *IEEE Transactions on Human-Machine Systems*, vol. 47, no. 3, pp. 404–416, 2016.

[23] H. Yamaba, A. Kurogi, S.-I. Kubota, T. Katayama, M. Park, and N. Okazaki, "Evaluation of feature values of surface electromyograms for user authentication on mobile devices," *Artificial Life and Robotics*, vol. 22, no. 1, pp. 108–112, 2017.

[24] S. Gupta, A. Buriro, and B. Crispo, "Demystifying authentication concepts in smartphones: ways and types to secure access," *Mobile Information Systems*, vol. 2018, Article ID 2649598, 16 pages, 2018.

[25] Y. N. Singh and S. K. Singh, "Evaluation of electrocardiogram for biometric authentication," *Journal of Information Security*, vol. 3, no. 1, pp. 39–48, 2012.

[26] H. S. Shin, C. Lee, and M. Lee, "Adaptive threshold method for the peak detection of photoplethysmographic waveform," *Computers in Biology and Medicine*, vol. 39, no. 12, pp. 1145–1152, 2009.

[27] A. L. Goldberger, L. A. N. Amaral, L. Glass et al., "Components of a new research resource for complex physiologic signals," *Circulation*, vol. 101, no. 23, pp. 215–220, 2000.

[28] T. Zhao, Y. Wang, J. Liu, and Y. Chen, "Your heart won't lie: PPG-based continuous authentication on wrist-worn wearable devices," in *Proceedings of the International Conference on Mobile Computing and Networking (MobiCom)*, pp. 783–785, ACM, New Delhi, India, October 2018.

[29] U. Yadav, S. N. Abbas, and D. Hatzinakos, "Evaluation of PPG biometrics for authentication in different states," in *Proceedings of the International Conference on Biometrics (ICB)*, pp. 277–282, IEEE, Gold Coast, QLD, Australia, February 2018.