




Article

# Biometric Authentication and Verification for Medical Cyber Physical Systems

Abdullah Alhayajneh <sup>1</sup>, Alessandro N. Baccarini <sup>2</sup>, Gary M. Weiss <sup>2</sup>, Thayer Hayajneh <sup>2,\*</sup>  
and Aydin Farajidavar <sup>1</sup>

<sup>1</sup> College of Engineering and Computing Sciences, New York Institute of Technology, New York, NY 10023, USA; aalhayaj@nyit.edu (A.A.); afarajid@nyit.edu (A.F.)

<sup>2</sup> Fordham Center for Cybersecurity, Fordham University, New York, NY 10023, USA; abaccarini@fordham.edu (A.N.B.); gaweiss@fordham.edu (G.M.W.)

\* Correspondence: thayajneh@fordham.edu

Received: 30 October 2018; Accepted: 11 December 2018; Published: 14 December 2018



**Abstract:** A Wireless Body Area Network (WBAN) is a network of wirelessly connected sensing and actuating devices. WBANs used for recording biometric information and administering medication are classified as part of a Cyber Physical System (CPS). Preserving user security and privacy is a fundamental concern of WBANs, which introduces the notion of using biometric readings as a mechanism for authentication. Extensive research has been conducted regarding the various methodologies (e.g., ECG, EEG, gait, head/arm motion, skin impedance). This paper seeks to analyze and evaluate the most prominent biometric authentication techniques based on accuracy, cost, and feasibility of implementation. We suggest several authentication schemes which incorporate multiple biometric properties.

**Keywords:** cyber-physical systems; WBAN security; biometric authentication; medical systems

## 1. Introduction

A Wireless Body Area Network (WBAN) is an interconnected network of wearable sensing devices. A WBAN network composed of medical sensors can be categorized as a Cyber Physical System (CPS). This subset of WBAN devices consists of special linked sensors made to work independently and continuously to connect with other medical devices, which can be planted either inside or outside the human body [1]. WBAN protocols are developed in such a way that will spread the communication between the body's sensors and the data center through the internet via web-servers. A WBAN can be installed inside a person's body in the form of intra-body sensors or on the surface of the skin. From here, the sensors record and transmit the data to the personal devices (such as smartphones) or dedicated hospital monitoring devices [2]. The sensors can be classified into two categories. They can be wearable outside the human body and implantable inside the human body. These sensors have become more practical because of advanced ingenuity, requiring them to be lightweight, small, and low-power.

Recent developments of low power fields in circuits and wireless communications such as Radio Frequency technology have advanced the achievements of WBANs [3]. This technology provides low-cost, accurate healthcare solutions for people which may, inevitably, enhance their quality of life [4]. There is significant interest from researchers, developers, and system designers in body network architecture technology [1,3–19]. These applications can be used in health care, security, wireless audio, and fitness monitoring. Given the dramatic population increase and growing cost of health care, these applications will be highly beneficial for future society. WBANs allow for continuous, real-time health monitoring for patients, military staff, and fire fighters to provide updated medical reports though the internet with the help of low-cost sensors [18]. Advancements in this field will

directly benefit elderly patients who require constant monitoring, but are often unable or unwilling to go to the doctor.

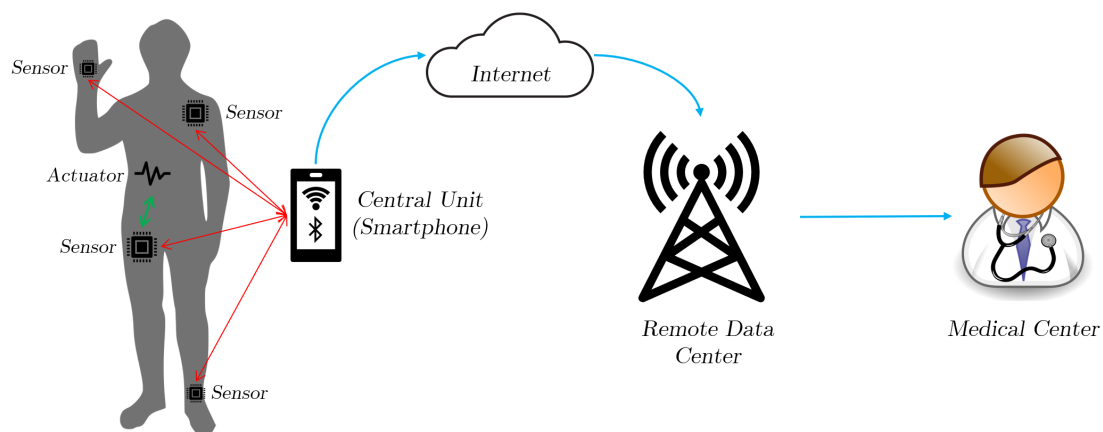
WBANs possess the potential to reduce healthcare costs as well as the workload of medical professionals, resulting in higher efficiency. Mobile sensing of the human body will become more widespread with new personal mobile devices which are capable of storing and processing large amounts of data [20].

The main purpose of this paper is to examine and evaluate the biometric techniques that have been used in several studies on WBANs to verify patient identities. We discuss the advantages and disadvantages of each technique, and we evaluate the studies based on their results. Additionally, we propose several authentication that will incorporate two or more biometric technologies.

The remainder of this paper is outlined as follows: Section 2 provides a foundational background for WBAN devices, specifically the hardware and network requirements. WBAN security is addressed in Section 3. We provide a general overview of authentication methodologies in Section 4, as well as how we can recognize whether or not the sensors are on the same body in Section 5. Section 6 provides a comprehensive analysis of currently available biometric authentication methods. Subsequently, our analysis of each technique is presented in Section 7. Section 8 proposes several potential authentication schemes and the future scope of WBAN devices. We conclude our analysis in Section 9.

## 2. Background of WBANs

WBANs consist of several or more miniaturized low-power devices connected wirelessly in or near a human body. An example WBAN network is depicted in Figure 1. The patient has several sensors and actuators that record data, which is transmitted to the central unit. This information is passed on via the Internet to a medical center. The devices often perform sensing functions in a two-hop star topology and transmit information to the central receiver. These devices are extensively used in areas including medicine, sports, gaming, entertainment, and emergency response [2]. We focus on medical applications of WBAN devices. Devices that fall under this scope include pacemakers, glucose monitors, blood pressure monitors, etc. We will discuss the foundational components of WBAN systems.



**Figure 1.** An example Wireless Body Area Network (WBAN) network.

WBAN networks are broadly composed of the following hardware components: Sensors, actuators, and personal devices (PD) [5,17]. The sensor node is responsible for responding to and recording information according to a physical stimuli. Data processing may occur if necessary prior to transmission. These sensors can either be external, as in added to clothing [21] or placed directly on the body (e.g., SpO<sub>2</sub>, ECG, EEG), or internal, as in injected under the skin or into the blood stream (e.g., electrical impulses to mitigate the effects of Parkinson's disease) [10]. An actuator responds to data

received from sensors or via direct instruction from the user. These can be responsible for administering medication or controlling a person's biometrics (e.g., blood pressure, body temperature). Physically, actuators and sensors share much of the same components (a power unit, a central processor (CPU), memory, and a receiver or transmitter). The personal device collects and processes all information from the sensors and actuators. Nowadays, these devices are typically smartphones, Personal Digital Assistants (PDAs), or dedicated unit. In some cases, the personal device can function as an actuator.

The fundamental limitations of WBAN devices is caused by their inherently small form factor. This directly affects power consumption, efficiency, and long-term reliability. Since these devices are typically battery powered, the sensors must be capable of continuous operation for several years (e.g., pacemakers are required to operate for a minimum of five years [11]). During their service, the devices must perform their functions reliably and consistently. The Quality of Service (QoS) must be guaranteed by the wireless protocols WBAN devices adhere to.

Furthermore, the various available WBAN applications demand a wide range of data transmission rates. The amount of data transmitted by the devices also depends on if the data is processed locally and only recorded parameters are transmitted [9]. Table 1 shows the data rate, bandwidth, and accuracy for several medical applications. Further research is necessary to improve cost, size, and lifespan of WBAN devices.

**Table 1.** Data transmission rates for several Wireless Body Area Network (WBAN) devices, adapted from [7].

Application	Data Rate	Bandwidth	Accuracy
ECG (12 leads)	288 kbps	1–1000 Hz	12 bits
ECG (6 leads)	72 kbps	1–500 Hz	12 bits
EMG	320 kbps	0–10,000 Hz	16 bits
EEG (12 leads)	43.2 kbps	0–150 Hz	12 bits
Motion Sensor	35 kbps	0–500 Hz	12 bits
Temperature	120 bps	0–1 Hz	8 bits
Blood Saturation	16 bps	0–1 Hz	8 bits
Glucose Monitor	1600 bps	0–50 Hz	16 bits

WBANs are typically designed to operate in a star topology, where all sensors are associated with a master node [6]. In some scenarios where devices are internally mounted, the human body can become an obstacle for radio transmission. A more optimal topology for this situation would be a multi-hop network, where sensors communicate to neighboring nodes to exfiltrate data. Relay-based protocols can also alleviate this issue by implementing a mixed integer linear programming formulation of the topology problem, which minimizes the network usage while accounting for energy considerations [22]. Several protocols are available for wireless transmission in WBANs, as specified by IEEE 802.15.6, including Bluetooth, Bluetooth Low Energy (BLE), Zigbee, Thread, and 6LoWPAN.

Another requirement for WBAN devices is true coexistence. Most devices communicate at the 2.45 GHz ISM band, which is shared with WiFi, Bluetooth, Zigbee, and other IEEE standards. This introduces the risk of interfering radio traffic, which can produce sub-optimal (and potentially fatal) outcomes for medical WBAN applications [11]. Fortunately, many researchers have proposed possible solutions to resolve these issues by implementing time and frequency spacing, code diversity, standards modification, standards adaptation, and hybrid solutions [6].

### 3. Security

Security is a fundamental requirement for WBANs as a result of the constant transmission of medical data. Since WBANs are transmitting important information, a security method is necessary to ensure communications remain private and to prevent security threats. Authentication, integrity authorization, availability, non-repudiation, and confidentiality must be implemented. Fraudulent instructions sent to actuators can have potentially fatal outcomes [17]. Patient data must not be

obtained by an adversary who could then use it to authenticate themselves as the wearer [15]. One of the marked challenges also is to answer the user's basic security questions. For instance, how does a user know if their critical health information is secure or not? How consistent or accurate is the data going to be? Sensor validations are subject to inherent communication and hardware constraints. Some of these constraints are experienced by the majority of the sensors, but are more apparent for medical sensors.

There are several protocols designed with the purpose to improve the energy efficiency of WBAN, and that means a longer life of the WBAN sensors [15,23]. The data access security requirements would need to have access control, accountability and non-repudiation. One of the biggest questions we ask with the WBAN technology is going to be regarding the authentication. How do we know if it is the right person using the WBAN? Confidentiality, integrity, and dependability are absolutely necessary for WBAN networks. We will discuss several studies about the verification techniques of the WBAN and their respective effectivenesses and accuracies.

#### 4. Authentication

Authentication is critical to ensure that the sensors, base station, and cluster heads are tested and authorized prior to providing or revealing information. These messages and information should be coming from the correct original source [16]. Several authentication procedures are outlined in Table 2.

**Table 2.** Available authentication procedures.

Procedure	Description
One-Way	A single message is sent from the sender to the receiver node.
Two-way	A communication link between two parties is certified.
Three-way	When clock synchronization fails, a third message is sent from the sender to the receiver
Implicit	Authentication is performed as a subset of another process.

Some authentication issues would be based on static and dynamic node deployment. In general, the authentication process starts with the mobile node to verify which of the sensor nodes are on the same body. After the authentication, the mobile node records the sensor data from the node. Until that time, all the data will be ignored [20]. In the personal health system, users will be able to connect to and read data from these sensors by using their cell phone and expecting the system to operate flawlessly. However, these sensors might not only be connected to the user's personal cell phones, but also unauthorized devices [20].

We consider a motivational example of two users living in the same house using identical sensor devices. User 1 should be able to put on either device and have the cell phone recognize which device is attached to the user. This will automatically create the phone-device association without an explicit pairing step. For this to happen, there needs to be two problems addressed first. User 1's device must be able to determine which sensors are attached to user 1. They must ignore other sensors that may be close but not attached to user 1. The next step would be to have the phone and sensor device agree on a shared encryption key to ensure their communications are secure. The cell phone would analyze the data coming from the sensors to verify the wearer by some biometric measure.

We can compose a solution by including an accelerometer sensor to every device, in addition to the primary sensors. Accelerometers are inexpensive additions, and can be used for biometric authentication (see [24,25]). First, the user wears the sensor on their body, and then turns it on. Next, the sensor will detect that it was utilized, and then it will transmit the accelerometer signal. Finally, the mobile receives the transmission, authenticates the device, and then connects with the sensor.

## 5. Location Recognition

It is necessary to discuss the different techniques that help to verify that the correct person is wearing a sensor, specifically biometric and cryptographic. Biometric authentication is the most popular option, with techniques that are capable of implementing an automatic verification of an individual identification by their physiological and behavioral characteristics. These characteristics can be used to measure the physiological or behavioral human patterns. In order to use the biometric techniques, there are several properties that must be satisfied [16]:

- Universal: Available to the entire population.
- Distinctive: It should be different between individuals.
- Permanent: It should remain unchanged for a period of time.
- Collectible: It means that the properties should be easy to collect and measure.
- Effective: Sufficient and stable for a period of time.
- Acceptable: The biometric system process has to be fast and accurate, have good memory storage and give a high performance with limited resources.
- Invulnerable: The biometric system should be hard to access or hacked by any fraud attempts.

The WBAN security system has to ensure that the sensor is on the correct user's body before it can authorize for information transfer. Biometric techniques use the human body's physiological or behavioral characteristics as an authentication identity in order to ensure a high security of the distribution for the cipher key inside the WBAN communications. The detection, collection, and transmission of human body data in the WBAN is sensitive and must be secured. The biometric tools can be implemented to verify the person who is wearing the sensor. If the verification is completed, then it will transmit the data through the WBAN network.

## 6. Device Authentication

There are several technical ways that have been used on the WBANs verification systems. In order to understand and analyze the techniques, we created the main categories below in Table 3 based on the user authentication devices with the techniques that were used on them.

**Table 3.** WBAN authentication categories based on device.

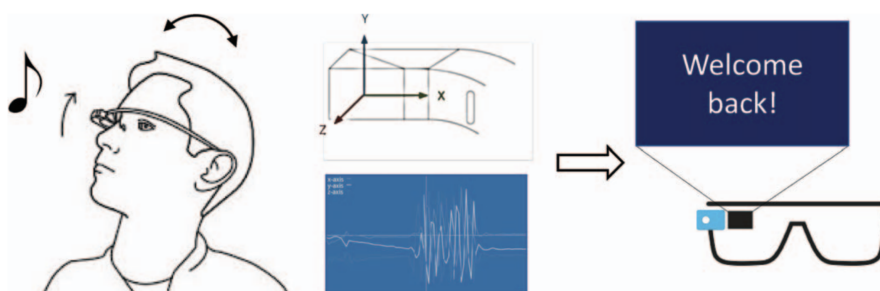
Category	Available Techniques
Head Wearable Devices	Head movement Eye blinking Skull Frequency response
Bracelet (Hand) Wearable Devices	Tomography system Behavioral biometric Bioimpedance
Body Portable Devices	Accelerometer from gait signal Fingerprint
Implantable Medical Devices (IMD)	Electroencephalography (EEG) Electrocardiography (ECG)

### 6.1. Head Wearable Authentication Devices

Head wearable devices including Virtual Reality (VR) headsets and smart glasses have become more common in the market for communication and entertainment. This new technology was also adopted by well-known companies such as Samsung, Google, and others, which made it available for users. Recent research of authentication WBANs used the available devices in the market such as Google Glass (GG) [16,26,27] in different techniques for authentication. The main focus was to create a software that uses the sensors of the smart glasses for authentication.

In some studies, the user will have to wear the GG which will display a series of changing images of numbers and letters in front of one or both eyes. By using the sensors, the device will be able to verify the users from their eye blinking and patterns of head movements [16]. This study used the blinking and head movements as a biometric for user identification and required a new software to be installed on the device for verification.

Another study uses the GG sensors to create WBANs authentication system by capturing the unique human head-movement patterns while a person listens to an audio stimulus or music and monitoring these movements for authentication (see Figure 2) [26]. The GG will record the data from the sensors and store it to the installed memory as a text file. The text file will be send to a PC to process the collected data using Python Script.



**Figure 2.** A biometric authentication system based off of head movement and auditory response, as presented in [26].

Another use of GG WBAN authentication involved creating a biometric authentication system using the audio signal inside the human skull to identify the users by recoding it. The users will be required to wear the GG in a controlled laboratory setting room in order to record the skull audio signal waves. This study showed the range of the recorded audio between 0 kHz to 8 kHz and all the details about it [27].

## 6.2. Bracelet (Hand) Wearable Authentication Devices

Hand wearable devices are considered one of most available and obtainable devices in the market nowadays. That's because of the new generation of smart hand wearable devices (watches) that were developed lately in the market by several companies such as Samsung, Apple, Huawei, and many other tech companies. Most of these devices were designed to be connected with the smartphones. Some of these watches contain accelerometer and gyroscope sensors that might be used for authentication. Several researchers used the idea of the smart watches to create WBAN authentication systems [25,28–31].

Some of the studies created a hand wearable device that contains eight sensors to read the internal impedance geometry of a user's arm using a tomography system [32]. A tomography system can analyze the internal structure of an object such as arm or leg by radiation and electricity. These waves go across the eight sensors and read the interior of the object. This research is an example of a wearable device that does not contain any verification system to validate if it is used by the actual owner. Some other studies presented an authentication scheme based on human body motions to verify a person wearing a wrist worn smart device using Samsung Galaxy Gear (SGG) [28].

The device is a behavioral biometric-based authentication method using three simple natural gestures and one special: Arm up, arm down, forearm rotation about 90 degree clockwise, and the special one is drawing a circle. In addition, an application was implemented based on the Android platform to apply dynamic time warping method (DTW) and histogram. This research used a smart watch available in the market (SGG) to create a new software and implement it.

One study used the LG G smart watch to perform gait-based biometric authentication [31]. The authentication models were generated using a variety of machine learning techniques, using the



accelerometer and gyroscope sensors on the watch, but evaluating each one separately. A subsequent study [25] by the same research group examined the simultaneous usage of both the accelerometer and gyroscope sensors, as well as physical activities other than walking to form the biometric signature. In total, this study evaluated the use of eighteen different physical activities (e.g., jogging, stair climbing) for biometric authentication.

Another example is a paper that describes a bracelet authentication which verifies the users while they are using a computer by monitoring how they type on the keyboard or how the user moves the mouse [29]. The bracelet contains accelerometer and gyroscope sensors that transfer the information to the computer over short range radio. The computer used in this experiment is a Mac, and a Python script was written to capture two different movement sources from the bracelet.

Another study on WBAN bracelet authentication systems used the bioimpedance technique to verify and authenticate that the WBAN sensors belong to the same body and identify who is wearing them [30]. Bioimpedance is a measurement of how tissue responds when exposed to an electrical current. A wrist-worn device was created with eight electrodes in contact with the wearer's wrist. With two of these electrodes, the device applies a small harmless current to the wrist so that it can measure bioimpedance. The wearable sensor was built on top of the shimmer platform which is an open-source, low-power wireless sensing platform.

### 6.3. EEG and ECG Authentication on IMDs

Several new studies discussed Implantable Medical Devices (IMD) authentication systems using Electroencephalography (EEG) and Electrocardiography (ECG) [14,33–35]. In general, most papers proposed IMD authentication based on the inter-pulse interval (IPIs). An ECG is used to provide a quantitative measurement of the electrical activity of a heart over a period of time [36]. An example ECG pulse is shown in Figure 3. The signals are recorded by attaching a series of electrodes to various locations on the the patient's body. An EEG signal is used to record brain activity, and is similarly recorded by using electrodes attached to the patient's head, as shown in Figure 4 [37]. Recent developments in the field of biomolecular sensing have widened the scope of IMDs. By implementing carbon nanotubes (CNTs) and graphene nanoribbons (GNRs), nano-sensors provide a noninvasive method of collecting biometric information. In addition to their passive applications, bio-nano-sensors have been developed to detect the presence of cancer [38], asthma attacks, and common viruses [39].

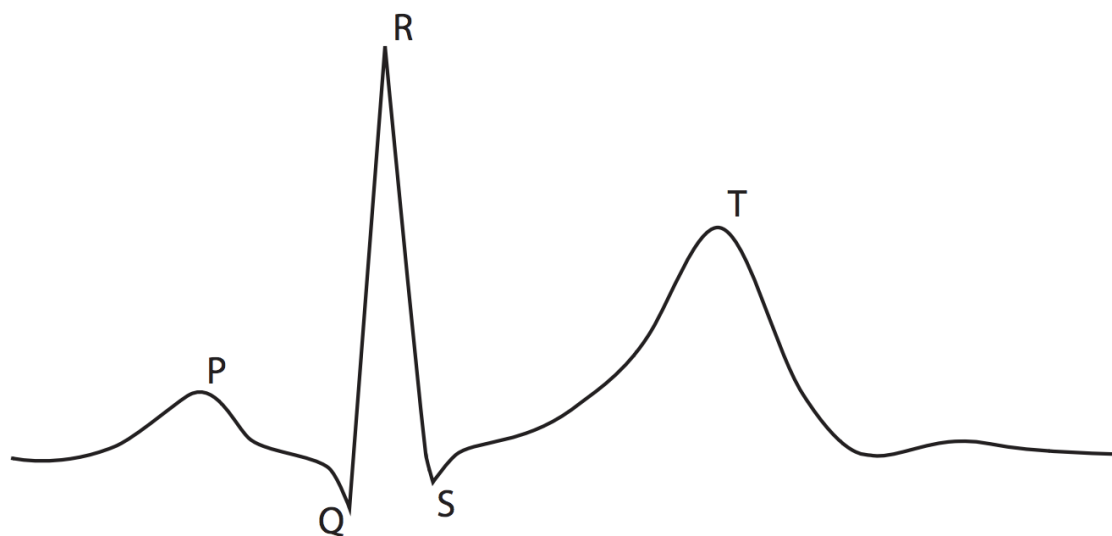
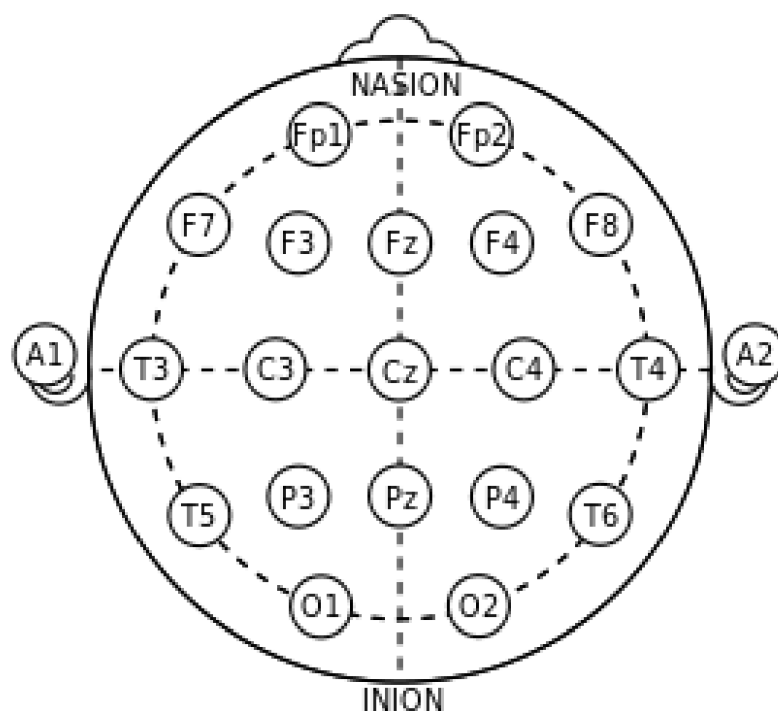


Figure 3. An example Electrocardiography (ECG) signal pulse.



**Figure 4.** The typical sensor layout for detecting Electroencephalography (EEG) signals.

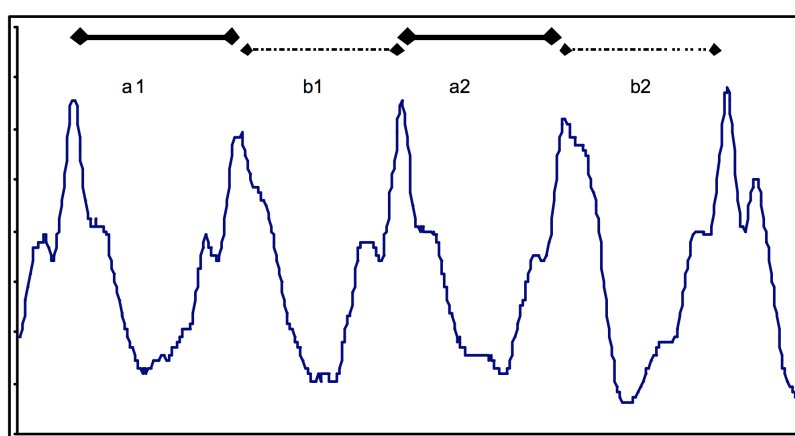
A study introduced an authentication system for the IMDs called Heart-to-Heart (H2H) [33]. This system used the ECG for the authentication mechanism, since the user's body should already have an IMD that can read the body's ECG and send out the information. A touchable medical instrument, generically called a "Programmer", was created and for it to work, the user needs to keep physical contact with it so that it can accept and authorize access to the user's IMD to read the signals. A H2H mechanism is used to compare the equality of the user's ECG from the touchable medical instrument (Programmer) and the IMD in order to access the IMD data. Another paper presented a secure scheme for IMDs with comprehensive techniques for the ECG-based keys with secure protocol and on the access control mechanism on the IMD external devices with an authentication proxy to protect it [35]. Another study implements a Discrete Cosine Transform to process real-time ECG signals for more resilient feature extraction [40]. An accuracy rate of 97.78% with an average 1.21 second processing time is reached for 15 subjects. A major drawback for most ECG authentication studies is the presumption that real-life users are perfectly healthy and have no preexisting medical conditions. Further testing is necessary for individuals with cardiac issues (e.g., arrhythmia and ischemia).

In [41], the authors incorporate an EEG-based authentication system with eye blinking. Several features are extracted (including event-related potential and morphological features) from EEG and eye-blinking signals. This information is passed to a convolutional neural network to score the two features. Least squares is used to produce their final estimation score. This method produced an improved accuracy of 97.6% (when compared to EEG-based authentication systems). Additionally, machine learning has been implemented to leverage brain EEG signals for authentication [42]. Raw EEG signals are filtered then segmented into sub-bands. These are used to extract several features to train an Error Correcting Code Support Vector Machine classifier. The input EEG vector and stored EEG vector are compared, and if a certain threshold is passed, then the user is authenticated [43]. Lower-cost, consumer-grade EEG authentication systems have been studied by [44], thus introducing the possibility of more widespread adaptation of this technology. Ref. [45] proposes an in-ear EEG sensor to collect data. This novel technique allows for even easier EEG authentication implementation.



#### 6.4. Body Portable Devices

This category pertains to any other WBAN devices that should be worn on any part of the body except the hands or head. Most of these studies used the Accelerometer Sensors and Fingerprint for WBAN Authentication [24,25,46]. These techniques were used several times and are often considered as the first and the oldest phase of the WBAN authentication. A paper identified the user using a portable device that records their accelerometer signals from gait signals. The device should be worn on a belt, similar to carrying a mobile phone attached to the waist [24]. The device consists of three dimensional accelerometer, two perpendicularly positioned Analog Devices ADXL202JQ accelerometers (Norwood, MA, USA). It will record the accelerometer signals of gait signal 256-Hz sampling frequency on a laptop with National Instruments Lab 1200 DAQ card (National Instruments, Austin, TX, USA). The user should walk 20 Meters in normal, slow, and fast walking speeds in order to detect the signals. A typical gait pattern is shown in Figure 5 It requires several other testing sessions to identify the users from their gait.



**Figure 5.** A typical gait pattern detected by an accelerometer, with steps “a” and “b” marked [24].

Personal devices, such as smartphones, typically include motion sensors, and another study utilized Google Nexus 5 and Samsung Galaxy S5 smartphones for biometric authentication [25]. The phones were placed in the subject’s pockets and both the accelerometer and gyroscope sensors were used for authentication. Eighteen activities, including walking (gait), were evaluated as biometric signatures. This study also evaluated biometric performance when the smartphone sensors were combined with the sensors on a commercial smart watch.

Other studies discussed the Fingerprint authentication system to give access to the person who will assist the patient [46]. This type of authentication access can be implemented by using fingerprint authentication systems which have become cheap and available in the market. The biometric fingerprint recognition system is used in the new generations of smart mobile phones such as Samsung and Apple. Other access devices are using electronic fingerprint recognition systems to grant access to doors or computer devices. Adding the fingerprint recognition system to the WBANS Body Portable Devices can be an advanced solution which should be considered in the near future.

### 7. Evaluation of Authentication Techniques

After discussing and analyzing the techniques and devices that have been used for WBAN authentication, it is necessary to determine the realistic effectiveness of each technology and assess their limitations. In some cases, biometric authentication performance was measured using Equal Error Rate (EER), which is the value at which the false identification rate equals the false rejection rate. To discuss the results of the WBANs authentication papers, each is classified into one of the categories that we used above for WBAN authentication analysis.

### 7.1. Head Wearable Devices

After discussing the techniques that were used on the head wearable devices (outlined in Table 4), we concluded that most of the studies used GG as a head wearable device. Focusing on the advantages of the head wearable devices for the WBANs authentication and identification studies, we can start with GG; using GG can be considered one of the advantages as it can be made available for patients as a low-priced, easy to use option. In addition, new head wearable devices can be built easily since the necessary equipment is readily available nowadays in the market. Another advantage is the high user identification accuracy of the papers such as 94% of 20 users [16] and 95.57% of 95 users [26].

**Table 4.** Head Wearable Device Evaluation by technique.

	Head Movement + Eye Blinking	Head Movement	Skull Frequency Response
<b>References</b>	[47]	[26]	[27]
<b>Accuracy</b>	94%	95.57%	97.0%
<b>Sample Size</b>	20	95	10
<b>Requirements</b>	GG with visual stimulation	GG with audial stimulation	GG in controlled setting
<b>Advantages</b>	GG (relatively low-cost, can be made available to patients)		
<b>Disadvantages</b>	Not viable for mentally, visually, and physically disabled individuals		Requires controlled laboratory setting

Regarding of the disadvantages, and talking about the security, most of the paper's systems did not mention the security methods that should be used to secure the transfer of the recorded data from the head wearable device to the other needed device (such as a computer). The security criteria was not addressed by the authors. Another disadvantage regarding the head-movement techniques is that the unique head-movements for human beings might not be functional for mentally or physically disabled individuals. This is one of the larger challenges for the head wearable device authentication system for the WBANs, including all the used techniques such as head movement and eye blinking. Adding to the disadvantages, some studies reading skull signal frequency used GG in a controlled laboratory setting [27]. This method is unlikely to be scalable to the point it can be used without specific laboratory conditions, thus increasing the cost and negatively affecting the availability.

### 7.2. Bracelet (Hand) Wearable Devices

Hand wearable devices, including smart watches, are considered the most common forms of WBANs authentication systems with high accuracy rates. A complete overview of hand wearable devices is shown in Table 5. Some studies used SGG [28], which can be considered an advantage because SGG is available in the markets and easy to use. A user study was implemented on 30 people and the equal error rate (EER) was less than 5%. Other studies created hand wearable devices for WBAN authentication systems [29,30]. The accuracy of this experiment was 85% with 11 s to verify in paper [29], and in paper [30] after testing the devices on 8 volunteers with a whole day of validation, the balance accuracy was 98%, which can be considered a good percentage.

Regarding the disadvantages, the security link between the smart watch and the other needed device (PC) was not mentioned as part of the security of the application and the implementation of the papers' mechanism. A second disadvantage of the hand wearable device authentication mentioned in the papers is that it requires hand movements for authentication [28,29], which might not be applicable for mentally or physically disabled individuals. A final disadvantage of the hand wearable systems is that they are not organized in a way to minimize the cost of energy consumption. An example of that

is a design that requires eight electrodes in contact with the wrist, but a system study that only used two electrodes at a time, which resulted in six unnecessary electrodes [30].

**Table 5.** Bracelet (Hand) Wearable Device Evaluation by technique.

	Tomography System	Behavioral Biometric		Bioimpedance	
<b>References</b>	[32]	[28]	[31]	[25]	[30]
<b>Accuracy</b>	Wrist: 97% & 87% Arm: 93% & 81%	EER < 5%	Accel: 97.2% (EER 2.6%) Gyro: 93.8% (EER 8.1%)	Accel: EER 13.2% Gyro: EER 17.2%	98%
<b>Sample Size</b>	10	30	59	51	8
<b>Requirements</b>	Hand wearable device with eight sensors	SGG, plus Matlab data processing application	LG G Watch		Wrist wearable device and a smartphone
<b>Advantages</b>	Low-cost device (roughly \$40)	Readily available equipment and application		Low-cost device (roughly \$60), very accurate	
<b>Disadvantages</b>	Difficult to evaluate, since results vary based on sensor location; other hand gestures not tested.	May not be applicable for disabled individuals		Difficult to implement due to the no. sensors required (8); sample size is limited compared to other methods	

### 7.3. Implantable Medical Devices

IMDs can be considered one of the newest and more novel forms of WBANs technology. Most of the studies used the data that the IMDs provided about the human body for authentication. We show in Table 6 that most of the studies used the ECG and EEG signals from the IMD for authentication [14,33–35]. Each human body provides unique ECG and EEG data, which can be considered one of the advantages for security and authentication. In addition to that, the IMD already provides the signals and will not require any extra cost for authentication as the device is already implanted inside the patient’s body. The only thing needed is another external device to read the same signal externally and compare it with the IMD’s reading to implement the security criteria.

**Table 6.** Implantable Medical Device (IMD) Evaluation by technique.

	Electroencephalography (EEG)			Electrocardiography (ECG)		
<b>References</b>	[42]	[41]	[45]	[48]	[49]	[50]
<b>Accuracy</b>	EER 0.0196	97.6 %	95.7%	96%	99%	97%
<b>Sample Size</b>	109	40	15	10	52	50
<b>Requirements</b>	Electrodes (typically 16) attached to the head (internal or external)		Single in-ear sensor	Electrodes (typically 10) attached throughout the body (internal or external)		
<b>Advantages</b>	Easily adaptable for users who have IMDs, accurate results.					
<b>Disadvantages</b>	Readings fluctuate heavily based on activity, expensive equipment and computationally exhaustive.					

The other requirement is to secure the connection between the external device and the IMD. Unfortunately, security issues with the connection might be considered one of the disadvantages of the

IMD authentication systems as none of the studies consider it. Further research is necessary to ensure that these methods of authentication are as secure as the others we discussed.

An important disadvantage of these techniques is their variability when the user is undergoing mental or physical activity. This can be mitigated by learning the user's biometric data while under load, but it further increases the complexity of an already computationally demanding process. Recoding all the signals with all the physical situations of the user for authentication requires a lot of time, memory space, and energy. Several papers [50,51] have sought to address this concern, but future research is necessary.

#### 7.4. Body Portable Devices

This category discussed the Body Portable Devices that can be worn on any part of the body except the hands and head. The accelerometer sensors were used in such devices in [24,25]. Our evaluation of this technique is presented in Table 7. In [24], the device was tested on 36 users and the equal error rate (EER) was 7% with signal correlation method, and 10%, 18%, and 19%, respectively in frequency domain method and two variations of data distribution statistics method. This technique required a laptop that should be carried by the users, which can be considered one of the disadvantages regarding the usability.

**Table 7.** Body Portable Device Evaluation by technique.

Accelerometer from Gait Signal		
References	[24]	[25]
Accuracy	EER of 7% with signal corr., 10%, 18%, and 19% with other methods.	EER of 9.4% with phone accel. EER of 9.8% with phone gyro. EER of 8.0% with combined accel. and gyro.
Sample Size	36	51
Requirements	Three-dimensional accel., worn on belt of user	Google Nexus 5 or Samsung Galaxy S5 placed in pant pocket
Advantages	Low-cost, easy to implement	Readily available, easy to implement
Disadvantages	Not viable for disabled individuals, results affected by shoes, leg injuries, walking surface	Not viable for disabled individuals, results affected by shoes, leg injuries, walking surface; some people do not carry their phone in their pockets

A second study [25] utilized the Google Nexus 5 and Samsung Galaxy S5, two popular smartphones, as body portable devices. These devices were placed in the subject's pant pocket and the accelerometer and gyroscope sensors were used, both independently and in tandem. Over a population of 51 participants, the average EER was 9.4% when using the accelerometer, 9.8% when using the gyroscope, and 8.0% when used the fused sensor values from the two devices. Both methods are relatively easy to implement, with [24] being the lower cost option, and [25] having better availability. However, both techniques are not viable for physically disabled individuals, and the results are highly affected by the surface walked on. Another disadvantage of [25] is its relying on the user to carry their phone in their pockets. A simple fingerprint verification can easily be added to both methods to enhance the overall security, and provide authentication when the user is not moving.

## 8. Future Scope of WBANs

WBANs are growing at an insurmountable rate in the market for medical fields and industry fields for entertainment. In the near future, WBAN systems will change the way people think about

managing and monitoring their health. This will also reduce healthcare costs because it will provide more preventive healthcare. WBANs require small, low-cost, low-energy devices such as sensor nodes. New generations of smartphones can store the medical data that is sent from the sensors, and in the future, with the growth of the smartphones, we will see improvements in this technology. The S-MAC and T-MAC protocols still need more research and improvements regarding the energy efficiency for the WBAN sensors. The user configuration systems and interfaces for the personal monitoring systems require more enhancements. This will be helpful for the users to interact efficiently with the device and improve their quality of life.

WBAN authentication and identification fields require further research and studies in terms of efficiency, accuracy, and reliability for the users' personal sensitive information. This will help to implement it in the market to increase the usability and availability.

We can now formulate several potential authentication schemes based on biometric techniques we discussed. Compared to the previous category that used the devices as a base form, on this analysis form we discussed the techniques that were used in papers [14,16,24,26–30,32–35,46,52]. Each technique has been used in a different way on the same device. For improved understanding and simplification, we re-categorized the use of each technique based on the way it is used and we added the possibility of combining two techniques or more together. We created new methods for improved comprehension of the WBAN authentication systems and the possibility of combining two or more techniques together.

### *8.1. External Authentication*

This method focuses on sensors located outside of the body. The two authentication techniques, head movement and eye blinking, were already used in [47]. Additionally, head movement was also used independently for WBAN authentication in [26]. The Skull Signal Frequency authentication technique was used in [27]. Since these techniques were both GG on similar head wearable devices, there will be an opportunity to incorporate these techniques together into a single device for enhanced accuracy, effectiveness, and security.

An additional combination is possible by incorporating several techniques designed to work on a bracelet. Several studies [28,30,32] used a hand wearable device in different ways for WBAN authentication systems. Combining these techniques to operate on a singular device will provide consistent results. Adding onto each technique (such as the Tomography System) with a fingerprint authentication technique may be feasible since the fingerprint devices can be seamlessly added to hand wearable devices. This new combination may be adopted and implemented into the market within the near future due to the high-speed developments on the smart watches by prominent tech companies such as Samsung and Apple.

### *8.2. Internal Authentication*

This method consists of the WBAN authentication techniques that have been used on IMDs and other wearable devices [14,24,33–35,46]. IMDs can read the ECG and EEG signals of patients and can be used for authentication. In order to use the ECG and EEG for authentication, it usually requires another portable external device to read the same signals and apply the authentication by comparing both readings to check if they are the same. To enhance the authentication techniques for the IMDs and make them more accurate, we added the fingerprint techniques on the external device or the wearable device. Since the fingerprint authentication devices are available in the market and easy to implement on any other device, it will be venerable and effective for them to be added for more privacy and security.

## **9. Conclusions**

WBAN is expected to be a very useful tool with the potential to offer a wide range of benefits to the health field and for society. This is going to be done by continuous monitoring and early detection

of possible health problems. As the technology continues to expand, WBANs will proportionally grow. We provided an overview of WBANs and discussed the challenges and security issues present in a WBAN. Hospitals and medical services are rapidly deploying CPS to enhance the level of care patients receive. Our framework provides a detailed overview of authentication methods that can be implemented in future Medical CPS.

The expanding utilization of remote systems and the constant scaling down of electrical gadgets has engaged the improvement of remote body wireless systems. These systems' sensors are connected to garments or on the human body. These systems offer numerous new useful and imaginative applications to enhance health care. We discussed several examples of research and studies regarding the technique to verify and authenticate that the WBAN sensors belong to the same body and identify who is wearing them. We evaluated the advantages and disadvantages of each study and offered means of improvement. We proposed several potential authentication systems that incorporates multiple biometric technologies.

Future work in this field encourages the development of a complete machine learning-driven biometric authentication suite. The system would use a range of biometric readings as the features for the algorithm to determine the authenticity of the patient and build a comprehensive profile for future use.

**Author Contributions:** Conceptualization, methodology, investigation, formal analysis, validation, writing—original draft preparation, and visualization, A.A. and A.N.B.; writing—review and editing, G.M.W.; supervision and project administration, T.H., A.F.

**Funding:** This research received no external funding.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Abbreviations

The following abbreviations are used in this manuscript:

CPS	Cyber Physical System
ECG	Electrocardiography
EEG	Electroencephalography
EER	Equal Error Rate
EMG	Electromyography
GG	Galaxy Gear
IMD	Implantable Medical Device
PDA	Personal Digital Assistant
QoS	Quality of Service
SGG	Samsung Galaxy Gear
WBAN	Wireless Body Area Network

## References

1. Davies, E.; Sanjay, K. A Survey on Wireless Body Area Network 1. *Int. J. Sci. Res. Publ.* **2014**, *4*, 1–7.
2. Wegmüller, M.S. Intra-Body Communication for Biomedical Sensor Networks. Ph.D. Thesis, ETH Zurich, Zürich, Switzerland, 2007.
3. Qadri, S.F.; Awan, S.A.; Amjad, M.; Anwar, M.; Shehzad, S. Applications, challenges, security of wireless body area networks (WBANs) and functionality of IEEE 802.15. 4/ZIGBEE. *Sci. Int.* **2013**, *25*, 697–702.
4. Ragesh, G.; Baskaran, K. An overview of applications, standards and challenges in futuristic wireless body area networks. *Int. J. Comput. Sci. Issues (IJCSI)* **2012**, *9*, 180.
5. Barakah, D.M.; Ammad-uddin, M. A survey of challenges and applications of wireless body area network (WBAN) and role of a virtual doctor server in existing architecture. In Proceedings of the 2012 Third International Conference on Intelligent Systems, Modelling and Simulation (ISMS), Kingston, ON, Canada, 8–10 February 2012; pp. 214–219.



6. Hayajneh, T.; Almashaqbeh, G.; Ullah, S.; Vasilakos, A.V. A survey of wireless technologies coexistence in WBAN: Analysis and open research issues. *Wirel. Netw.* **2014**, *20*, 2165–2199. [[CrossRef](#)]
7. Khan, J.Y.; Yuce, M.R. Wireless body area network (WBAN) for medical applications. In *New Developments in Biomedical Engineering*; InTech: London, UK, 2010.
8. Khan, P.; Ullah, N.; Ullah, S.; Kwak, K.S. Seamless interworking architecture for WBAN in heterogeneous wireless networks with QoS guarantees. *J. Med. Syst.* **2011**, *35*, 1313–1321. [[CrossRef](#)] [[PubMed](#)]
9. Lont, M.; Milosevic, D.; van Roermund, A. *Wake-Up Receiver Based Ultra-Low-Power WBAN*; Springer: Basel, Switzerland, 2013.
10. Salayma, M.; Al-Dubai, A.; Romdhani, I.; Nasser, Y. Wireless body area network (WBAN): A survey on reliability, fault tolerance, and technologies coexistence. *ACM Comput. Surv. (CSUR)* **2017**, *50*, 3. [[CrossRef](#)]
11. Cavallari, R.; Martelli, F.; Rosini, R.; Buratti, C.; Verdona, R. A survey on wireless body area networks: Technologies and design challenges. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1635–1657. [[CrossRef](#)]
12. Kim, E.J.; Youm, S.; Shon, T.; Kang, C.H. Asynchronous inter-network interference avoidance for wireless body area networks. *J. Supercomput.* **2013**, *65*, 562–579. [[CrossRef](#)]
13. Otto, C.; Milenkovic, A.; Sanders, C.; Jovanov, E. System architecture of a wireless body area sensor network for ubiquitous health monitoring. *J. Mob. Multimed.* **2006**, *1*, 307–326.
14. Poon, C.C.; Zhang, Y.T.; Bao, S.D. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Commun. Mag.* **2006**, *44*, 73–81. [[CrossRef](#)]
15. Saleem, S.; Ullah, S.; Yoo, H.S. On the security issues in wireless body area networks. *JDCTA* **2009**, *3*, 178–184. [[CrossRef](#)]
16. Singh, J.P.; Bilandi, N. Analysis of Biometric-Based Security in Wireless Body Area Network (Wban). In Proceedings of the International Conference on Information Technology and Computer Science, Liverpool, UK, 26–28 October 2015; pp. 50–56.
17. Ullah, S.; Higgins, H.; Braem, B.; Latre, B.; Blondia, C.; Moerman, I.; Saleem, S.; Rahman, Z.; Kwak, K.S. A comprehensive survey of wireless body area networks. *J. Med. Syst.* **2012**, *36*, 1065–1094. [[CrossRef](#)] [[PubMed](#)]
18. Vadehra, R.; Malhotra, J.; Chowdhary, N. Issues and Challenges in Implementation of Wireless Body Area Sensing Networks. *Int. J. Technol. Enhanc. Emerg. Eng. Res.* **2013**, *3*, 8–12.
19. Wang, L.; Goursaud, C.; Nikaein, N.; Cottatellucci, L.; Gorce, J.M. Cooperative scheduling for coexisting body area networks. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 123–133. [[CrossRef](#)]
20. Cornelius, C.T.; Kotz, D.F. Recognizing whether sensors are on the same body. *Pervasive Mob. Comput.* **2012**, *8*, 822–836. [[CrossRef](#)]
21. Azeez, H.I.; Chen, W.S.; Wu, C.K.; Cheng, C.M.; Yang, H.C. A Simple Resonance Method to Investigate Dielectric Constant of Low Loss Substrates for Smart Clothing. *Sens. Mater.* **2018**, *30*, 595–608. [[CrossRef](#)]
22. Jafari, R.; Effatparvar, M. Cooperative Routing Protocols in Wireless Body. *Int. J. Comput. Inf. Technol.* **2017**, *5*, 43–51.
23. Al Ameen, M.; Liu, J.; Kwak, K. Security and privacy issues in wireless sensor networks for healthcare applications. *J. Med. Syst.* **2012**, *36*, 93–101. [[CrossRef](#)]
24. Mäntyjärvi, J.; Lindholm, M.; Vildjiounaite, E.; Mäkelä, S.M.; Ailisto, H. Identifying users of portable devices from gait pattern with accelerometers. *IEEE Trans. Geosci. Remote Sens.* **2005**, *51*, 973–976.
25. Yoneda, K.; Weiss, G.M. Mobile sensor-based biometrics using common daily activities. In Proceedings of the 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, USA, 19–21 October 2017; pp. 584–590.
26. Li, S.; Ashok, A.; Zhang, Y.; Xu, C.; Lindqvist, J.; Gruteser, M. Whose move is it anyway? Authenticating smart wearable devices using unique head movement patterns. In Proceedings of the 2016 IEEE International Conference on Pervasive Computing and Communications (PerCom), Sydney, Australia, 14–19 March 2016; pp. 1–9.
27. Schneegass, S.; Oualil, Y.; Bulling, A. SkullConduct: Biometric user identification on eyewear computers using bone conduction through the skull. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, San Jose, CA, USA, 7–12 May 2016; pp. 1379–1384.
28. Yang, J.; Li, Y.; Xie, M. MotionAuth: Motion-based authentication for wrist worn smart devices. In Proceedings of the 2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), St. Louis, MO, USA, 23–27 March 2015; pp. 550–555.

29. Mare, S.; Markham, A.M.; Cornelius, C.; Peterson, R.; Kotz, D. Zebra: Zero-effort bilateral recurring authentication. In Proceedings of the 2014 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 18–21 May 2014; pp. 705–720.
30. Cornelius, C.; Peterson, R.; Skinner, J.; Halter, R.; Kotz, D. A wearable system that knows who wears it. In Proceedings of the 12th Annual International Conference on Mobile sYstems, Applications, and Services, Bretton Woods, NH, USA, 16–19 June 2014; pp. 55–67.
31. Johnston, A.H.; Weiss, G.M. Smartwatch-based biometric gait recognition. In Proceedings of the 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), Arlington, VA, USA, 8–11 September 2015; pp. 1–6.
32. Zhang, Y.; Harrison, C. Tomo: Wearable, low-cost electrical impedance tomography for hand gesture recognition. In Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology, Charlotte, NC, USA, 11–15 November 2015; pp. 167–173.
33. Rostami, M.; Juels, A.; Koushanfar, F. Heart-to-heart (H2H): Authentication for implanted medical devices. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, Berlin, Germany, 4–8 November 2013; pp. 1099–1112.
34. Venkatasubramanian, K.K.; Gupta, S.K. Physiological value-based efficient usable security solutions for body sensor networks. *ACM Trans. Sens. Netw. (TOSN)* **2010**, *6*, 31. [[CrossRef](#)]
35. Xu, F.; Qin, Z.; Tan, C.C.; Wang, B.; Li, Q. IMDGuard: Securing implantable medical devices with the external wearable guardian. In Proceedings of the 2011 Proceedings IEEE INFOCOM, Shanghai, China, 10–15 April 2011; pp. 1862–1870.
36. Agrafioti, F.; Bui, F.M.; Hatzinakos, D. Medical biometrics in mobile health monitoring. *Secur. Commun. Netw.* **2011**, *4*, 525–539. [[CrossRef](#)]
37. Khalifa, W.; Salem, A.; Roushdy, M.; Revett, K. A survey of EEG based user authentication schemes. In Proceedings of the 2012 8th International Conference on Informatics and Systems (INFOS), Cairo, Egypt, 14–16 May 2012; p. 55.
38. Kosaka, P.M.; Pini, V.; Ruz, J.J.; Da Silva, R.; González, M.; Ramos, D.; Calleja, M.; Tamayo, J. Detection of cancer biomarkers in serum using a hybrid mechanical and optoplasmonic nanosensor. *Nat. Nanotechnol.* **2014**, *9*, 1047. [[CrossRef](#)] [[PubMed](#)]
39. Rizwan, A.; Zoha, A.; Zhang, R.; Ahmad, W.; Arshad, K.; Ali, N.A.; Alomainy, A.; Imran, M.A.; Abbasi, Q.H. A review on the role of nano-communication in future healthcare systems: A big data analytics perspective. *IEEE Access* **2018**, *6*, 41903–41920. [[CrossRef](#)]
40. Hussein, A.F.; AlZubaidi, A.K.; Al-Bayat, A.; Habash, Q.A. An IoT Real-Time Biometric Authentication System Based on ECG Fiducial Extracted Features Using Discrete Cosine Transform. *arXiv* **2017**, arXiv:1708.08189.
41. Wu, Q.; Zeng, Y.; Zhang, C.; Tong, L.; Yan, B. An EEG-based person authentication system with open-set capability combining eye blinking signals. *Sensors* **2018**, *18*, 335. [[CrossRef](#)] [[PubMed](#)]
42. Kalshetti, U.; Goel, A.; Srivastava, P.; Ingole, M.; Bhide, D. Human Authentication from Brain EEG Signals using Machine Learning. *Int. J. Pure Appl. Math.* **2018**, *118*, 1–7.
43. Bashar, M.K.; Chiaki, I.; Yoshida, H. Human identification from brain EEG signals using advanced machine learning method EEG-based biometrics. In Proceedings of the 2016 IEEE EMBS Conference on Biomedical Engineering and Sciences (IECBES), Kuala Lumpur, Malaysia, 4–8 December 2016; pp. 475–479.
44. Ashby, C.; Bhatia, A.; Tenore, F.; Vogelstein, J. Low-cost electroencephalogram (EEG) based authentication. In Proceedings of the 2011 5th International IEEE/EMBS Conference on Neural Engineering (NER), Cancun, Mexico, 27 April–1 May 2011; pp. 442–445.
45. Nakamura, T.; Goverdovsky, V.; Mandic, D.P. In-ear EEG biometrics for feasible and readily collectable real-world person authentication. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 648–661. [[CrossRef](#)]
46. Mocanu, S.; Mocanu, I.; Anton, S.; Munteanu, C. AmIHomCare: A complex ambient intelligent system for home medical assistance. In Proceedings of the 10th International Conference on Applied Computer and Applied Computational Science, Trieste, Italy, 20–22 September 2011; pp. 181–186.
47. Rogers, C.E.; Witt, A.W.; Solomon, A.D.; Venkatasubramanian, K.K. An approach for user identification for head-mounted displays. In Proceedings of the 2015 ACM International Symposium on Wearable Computers, Osaka, Japan, 7–11 September 2015; pp. 143–146.
48. Camara, C.; Peris-Lopez, P.; Gonzalez-Manzano, L.; Tapiador, J. Real-time electrocardiogram streams for continuous authentication. *Appl. Soft Comput.* **2018**, *68*, 784–794. [[CrossRef](#)]

49. Brás, S.; Pinho, A.J. ECG biometric identification: A compression based approach. In Proceedings of the 2015 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), Milan, Italy, 25–29 August 2015; pp. 5838–5841.
50. Pathoumvanh, S.; Airphaiboon, S.; Hamamoto, K. Robustness study of ECG biometric identification in heart rate variability conditions. *IEEJ Trans. Electr. Electron. Eng.* **2014**, *9*, 294–301. [[CrossRef](#)]
51. Sriram, J.C.; Shin, M.; Choudhury, T.; Kotz, D. Activity-aware ECG-based patient authentication for remote health monitoring. In Proceedings of the 2009 International Conference on Multimodal Interfaces, Cambridge, MA, USA, 2–4 November 2009; pp. 297–304.
52. Holz, C.; Knaust, M. Biometric touch sensing: Seamlessly augmenting each touch with continuous authentication. In Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology, Charlotte, NC, USA, 11–15 November 2015; pp. 303–312.



© 2018 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).