Biometric Systems utilising Health Data From Wearable Devices: Applications and Future Challenges in Computer Security

SAAD KHAN, Department of Computer Science
SIMON PARKINSON, Department of Computer Science
LIAM GRANT, Department of Computer Science
NA LIU, Department of Logistics, Marketing, Hospitality and Analytics
STEPHEN MCGUIRE, Department of Computer Science

Health data is being increasingly sensed from the health-based wearable Internet of Things (IoT) devices, providing much-needed fitness and health tracking. However, data generated also presents opportunities within computer security, specifically with biometric systems used for identification and authentication purposes. This paper performs a systematic review of health-based IoT data collected from wearable IoT technology. This involved performing research in the underlying data sources, what they are collected for in terms of their health monitoring, and the underlying data characteristics. Furthermore, it explores existing work in computer security using these data sources, identifying key themes of work, key limitations and challenges. Finally, key opportunities are provided as summaries to the potential of health-based IoT data, highlighting challenges that are yet to be addressed, which motivate areas of future work.

CCS Concepts: • **Security and privacy → Biometrics**.

Additional Key Words and Phrases: Health Data, Wearable Technology, Biometrics, Authentication

ACM Reference Format:
Saad Khan, Simon Parkinson, Liam Grant, Na Liu, and Stephen McGuire. 2020. Biometric Systems utilising Health Data From Wearable Devices: Applications and Future Challenges in Computer Security. 1, 1 (May 2020), 29 pages.

1 INTRODUCTION

Health data is now being collected on a large-scale, primarily driven by the Internet of Things (IoT) for healthcare [42] and the curiosity of public citizens in understanding their health. There is a wide range of devices available that collect, analyse and report health-related data of the end-user. There are also many electronic devices dedicated to providing health data functionality, and these can include fitness watches and consumer heart rate monitors. Furthermore, fitness capabilities are embedded as secondary functionality in other devices, such as smartphones. These devices and companion apps are often sold as lifestyle accessories but can provide a valuable data source for both health analysis and biometric systems. A fundamental difference is often both the quantity and quality of information being sensed. For example, a smartphone will mostly record movement

Authors' addresses: Saad Khan, saad.khan@hud.ac.uk, Department of Computer Science, University of Huddersfield, Huddersfield, West Yorkshire, HD1 3DH; Simon Parkinson, simon.parkinson@hud.ac.uk, Department of Computer Science, University of Huddersfield, Huddersfield, West Yorkshire, HD1 3DH; Liam Grant, Liam.Grant@hud.ac.uk, Department of Computer Science, University of Huddersfield, Huddersfield, West Yorkshire, HD1 3DH; Na Liu, Na.Liu@hud.ac.uk, Department of Logistics, Marketing, Hospitality and Analytics, University of Huddersfield, Huddersfield, West Yorkshire, HD1 3DH; Stephen McGuire, stephen.mcguire@hud.ac.uk, Department of Computer Science, University of Huddersfield, Huddersfield, West Yorkshire, HD1 3DH.

data, whereas a smartwatch in physical contact with a person can sense other information (e.g., heart rate) in addition to movement data.

Although these devices are collecting data privately for utilisation by the sensed individual, their security is paramount as the data falls into the category of personal and sensitive data, which also raises privacy issues. There is a large body of research discussing techniques to improve security and minimise risk [8, 122]. However, this paper is focused on a different task – that of understanding health data generated through the wearable IoT technology and reviewing, discussing, and making recommendations as to its use as a biometric in computer security.

Techniques that utilise biometric data can involve automated recognition and authentication of a human being by their intrinsic biological data, which is based on physical or behavioural properties [85]. Using biometrics can provide a reliable, accurate, efficient, user-friendly and low-cost solution. A biometric data source should sufficiently satisfy the following properties among individuals to be utilised for security purposes:

(1) *Distinctive* – Should be distinguishable among individuals i.e., there is a high degree of uniqueness among individuals;
(2) *Permanent* – Should be sufficient, reproducible and remain constant over a significant time period, which is preferably the lifetime of an individual;
(3) *Universal* – Should be present in the entire population of individuals;
(4) *Measurable* – It has to be possible to collect and quantify among individuals;
(5) *Resource effective* – Should be easily acquirable in a reasonable time and consume a minimum amount of resources to process;
(6) *Invulnerable* – Should be challenging to reproduce and robust to malicious attacks; and
(7) *Acceptable* – Should be accurate, applicable and stable.

There are many forms of biometrics that are in wide-scale use for both identification and authentication of individuals. For example, fingerprint technology is used in applications from access control of electronic devices to the tracking of individuals involved in criminal activity. An individual's iris pattern is another biometric frequently used for authentication purposes, including passport control.

Both fingerprint and iris are an example of static biometric data, whereby the observed characteristic is static and is mostly stable, except fro slow deterioration due to ageing or injury. There are, however, dynamic biometric measures which are linked to individuals behavioural and biological characteristics. For example, an individual's written signature and their voice can be used as biometric measures. However, it is often the case that dynamic biometrics can suffer from reduced accuracy because of variation in samples and poor repeatably (i.e., an individual's signature is likely to have small differences every time).

Each biometric source involves a different collection method. For example, an iris pattern requires a photo to be taken, whereas a fingerprint requires a map of high/low markings. Taking a photo of an iris pattern is regarded as passive as it does not require too much involvement from the individual, whereas providing a fingerprint through a mechanism whereby an individual has to place their fingerprint on a reader is classed as invasive. In general passive biometrics are regarded as the most user-friendly; however, they often suffer from a reduced accuracy. Biometric systems aiming to use health data based on behavioural and biological characteristics are using data that is not classified as static. It is also the case that for the majority of applications, physical contact is required to sense the necessary information. The use of behavioural and biological characteristics, coupled with multiple sensing mechanisms of different accuracy, results in it being challenging to implement a biometric system.

Several surveys [6, 14] claim that as new security issues are found regularly, researchers are continuously researching effective authentication techniques by identifying and using new biometric mechanisms. Large-scale studies [56, 109] have also been conducted regarding health biometrics. Analysing data from over 400 subjects over the duration of 17-months results in an accuracy of over 90%. This demonstrates the continuing uptake of biometric applications by researchers in academia and industry along with the positive acceptance by end-users. However, these inevitably require the individual to be sensed in new ways. In this research, we are focused on understanding the potential of health data acquired through wearable IoT devices as a future biometric source. There are three reasons why this review of wearable devices based techniques has been undertaken. First, there has been a considerable increase in the usage of wearable devices due to wider availability, low cost and acceptance by users [92], encouraging the development and rigorous testing of novel biometric techniques. Second, the wearable devices perform non-invasive data collection [31]. This means, unlike conventional biometric systems, the wearable devices do not require large and complicated hardware setups, therefore, easier to deploy and utilise. Third, as a wearable device is essentially a set of portable sensors, it serves multiple and diverse purposes, such as financial payments, health-related monitoring and alerts, exercise and sports analytics, etc. Furthermore, a comparative study [123] has shown significant security advantages, such as reliable authentication, discouraging impostors and constrained access control. It is worth mentioning here that apart from the benefits, using wearable devices for biometrics can introduce new challenges and limitations that are usually not present in conventional biometric systems. Most of the wearable devices tend to be cheaper to target a larger market. This raises some concerns over the credibility and accuracy of the devices as cheap sensors might output noisy and inaccurate readings. Moreover, as the devices do not have sufficient computational resources, the data is off-loaded to other systems for processing and analysis, which brings data confidentiality and integrity related security risks. Such issues can compromise the authenticity and security of the biometric system itself.

The existing biometric identifiers fall under the following three categories [10]: *what you know*, *what you have* and *what you are*. The 'what you know' includes password, pin number, memorable phrase, signature, etc. The 'what you have' includes security badge, identity card, keys, etc. The 'what you are' includes face, fingerprint, heart rate, body odour, etc. Figure 1 shows a taxonomy of all 'what you are' biometrics that are or can be used for human identification and authentication. The figure is based on previously published surveys on biometric types, and is also used as a guide in this survey to conduct a systematic literature search. The 'what you are' category has further two subcategories: *extrinsic* and *intrinsic*. The extrinsic biometrics are based on the physical aspects of a human body, including fingerprint, face, gaze tracking, etc. The intrinsic biometrics considers inner body characteristics, depicted under *Medico-chemical* in the figure, such as heartbeats, brain activity, blood pressure, etc. This paper only discusses intrinsic 'what you are' biometrics, where the data is related to healthcare, can be acquired through wearable IoT devices and is currently used for human identification (details in Section 2).

The biometric data is acquired through wired/wireless sensor nodes/devices that are attached in-body, on-body and around-body, also known as Wireless Sensor Networks (WSNs) for healthcare monitoring. Using WSNs for obtaining the data is particularly beneficial in terms of costing, deployment/integration, portability, autonomy and longer hardware life. However, it should be noticed here that the heterogeneity and scalability of connected devices in WSNs also raise a number security-related concerns [16]. Therefore, the authors have recommended to integrate security when designing data storage, networking protocols, user applications, computing resource distribution and trust management components of WSNs. In fact, it is imperative for all types of connected devices (WSNs, Cyber Physical Systems, etc.) to be secure by design as they have impact on the daily lives of users [96]. The authors propose to implement the following practices:

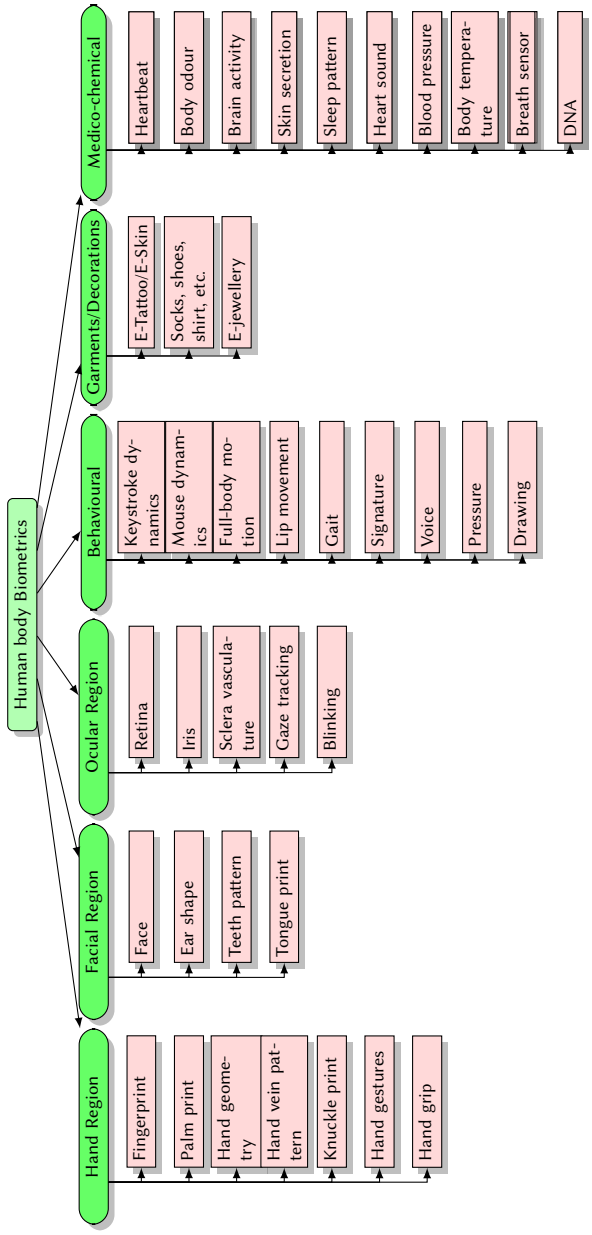

Fig. 1. List of all biometric types to guide literature search for biometrics. Gathered from multiple survey studies [14, 15, 92, 105]

strong password, least privilege access, segmentation, need-to-know, identity and authentication management, etc. Another research study presented a four-factor approach to build secure WSNs for healthcare systems: (1) anticipate potential security breaches and implement remedial actions accordingly, (2) design a transparent security infrastructure, (3) provide awareness of latest threat landscape to users, and (4) build trust in devices, applications and users [119].

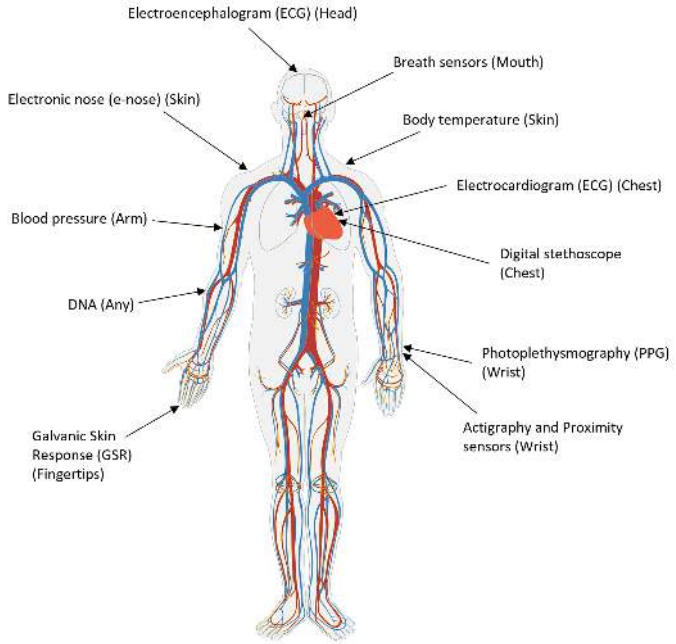

Fig. 2. Illustration of all data sources

To the best of the authors' knowledge, a systematic literature review of biometric systems utilising health-related data acquired from wearable devices is absent, taking an overview of this research discipline looking at both challenges and opportunities. The paper is structured in the following manner: it starts by surveying different health-based biometric data, followed by their uses within computer security. After that, a table is provided that summarises the current key works, the challenges they present, and the opportunities for the research discipline.

2 HEALTH DATA SOURCES

As mentioned before, the focus of this paper is to determine the applications of intrinsic 'what you are' biometrics that are related to healthcare. This section explores different types of data sources for such biometrics, along with the wearable IoT technologies that can extract the corresponding data. Figure 2 provides a graphical aid to help communicate the origin of existing 'what you are' data sources. The purpose of investigating these biometrics is to determine what research has taken place into its use in computer security. We adopt a categorisation, which is influenced by Figure 1 and also a recent survey into the IoT technologies within healthcare [42], to provide subsections discussing each category of health data. The following structured approach for discussing each different data source follows:

(1) What the data source is, why it is used in health, and generally how it is collected;
(2) Specifics on the data, including its structure, and where possible an example is provided; and
(3) What research is taking place that involves the progression of new technology and techniques to collect the data.

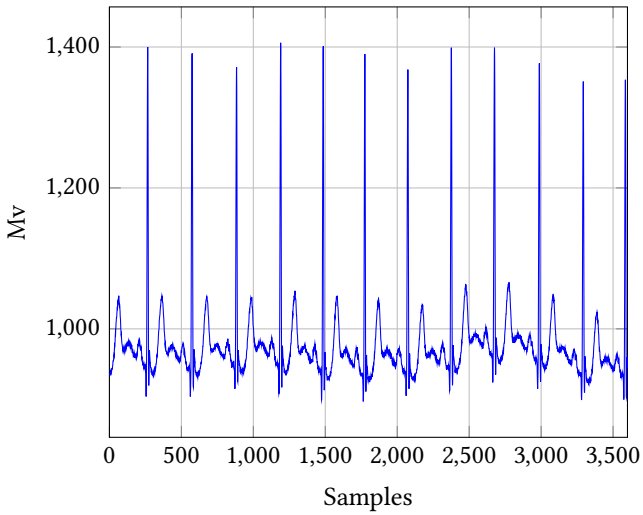

Fig. 3. ECG Example for a 10 second period comprising of 3600 data points. Data acquired from [79]

It is important to note that the below subsections contain a description of data sources and their acquisition technologies, whereas, their applications in computer security are presented later in Section 3.

2.1 Electrocardiogram (ECG) monitoring

Electrocardiograph (ECG) is widely acknowledged as being one of the most widely used biomedical sensing procedures [73]. The popularity of performing an ECG is down to its significance in diagnosing of heart-related diseases. This is performed by monitoring the electrical signals produced from the heart beating. An ECG can help to identify if a patient has a fast, slow, or irregular heartbeat (arrhythmias) and related conditions such as coronary heart disease. An ECG is typically conducted by attaching electrodes onto the patient's body in key areas to monitor electrical activity generated by the heart. In general, there are three main types of ECG: (1) a resting ECG, (2) stress or exercise ECG, and (3) an ambulatory ECG. The core technology and data acquisition stay the same; however, the key difference is the activity and setting of the patient during analysis. A resting ECG is where the patient is relaxing, a stress or exercise ECG involves them engaging in physical activity, and an ambulatory ECG is a portable device worn for a longer duration (e.g., one day) to acquire a longer data sample.

Performing an ECG requires the use of multiple strategically positioned sensors to measure the electrical potential difference. This process typically involves the positioning of multiple sensors to acquire sufficient information to produce a single data set constructed of amplitude (voltage) and time. There are two types of approaches that can be used to recognise ECG signals; fiducial dependent and independent [1]. The fiducial dependent methods employ spatial and temporal measures within heartbeats, whereas the independent fiducial methods utilise the entire heartbeats to formulate the ECG signal. A recent survey [64] has produced a comprehensive list of ECG signal databases, which have been used in several research studies. It also describes the acquisition of hardware, protocols, and methodologies of how data was collected. Figure 3 presents 3600 data points representing a 10-second segment of an ECG reading acquired and used in one recent study [79].

Considering the value of performing an ECG to determine and monitor heart-related conditions, researchers are consciously deriving new mechanisms to acquire, analyse and utilise ECG data for biometric identification. This is mainly due to the following reasons [21, 51]: (1) enables better classification ability due containing relatively large feature set, (2) difficult to spoof, (3) multi-purpose applications, (4) less affected by surrounding environment, (5) easy integration into the existing system and (6) does not require any special action from users during data acquisition phase. In one recent work, the authors develop an IoT ECG monitoring system where data is collected using a low-cost ECG monitoring device, shared via an internet connection to cloud servers, where it is processed and made available for healthcare practitioners [117]. This work concentrates on the development of the architecture design, both in terms of software and hardware; however, the work is focused purely on data acquisition and distribution and gives little insight into how the data might be processed. Furthermore, in another piece of work, researchers review challenges facing ECG devices in relation to the IoT [48]. The authors identify key challenges in data analysis, which centre around the ability to filter out interfering data adequately.

2.2 Photoplethysmography (PPG) monitoring

The photoplethysmography (PPG) sensor measures heart-rate based on detecting blood volume changes in the vessels [5]. A research study has demonstrated that there is a high similarity between heart rate signals/values measured by ECG and PPG devices [118]. Therefore, it is a suitable alternative of ECG that employs a simple optical technology. There are several reasons why PPG is preferred over ECG. It is a simple, low cost and portable sensor that also enables the multi-biometric system [115]. A multi-biometric is defined as a solution that contains two or more biometric identifiers collectively processing and recognising a single user. Due to the small form factor, the PPG sensors are easily embedded in wearable devices, such as wrist-worn smartwatches. They emit visible green or red light onto the surface of the skin from a moderate distance using Light Emitting Diodes (LEDs). The green light technology is more commonly used as the human blood (especially haemoglobin) is a good absorber of green and reflects red light. A PPG sensor records the variation in light intensity based on the quantity of absorption and reflection and applies signal processing to convert the variations into a heart rate. PPG technology is applicable in a wide range of clinical measurements, mainly in the cardiovascular systems. It can be used for measuring oxygen saturation, blood pressure, heartbeats, and also detecting heart-related abnormalities and diseases.

In terms of research and development in PPG monitoring, a recent survey has identified that the number of publications detailing research into PPG is continuing to increase [100], with recent advancements being discussed in terms of the portability of PPG technology and in data processing with the primary driver of improving data quality [65]. The survey and other recent publications also provide extensive coverage as to the development of PPG techniques for medical applications [65]. In one recent and related research paper, authors focus on establishing whether wearable devices implementing PPG can accurately measure heart rate variability, which concludes that they provide promising capability; however, further empirical-based analysis is necessary to establish their true capability [28].

2.3 Electronic nose (e-nose)

Each human body has different body odours due to different chemical composition, which can be used to distinguish individuals [29]. E-nose is a device that is used to detect body odours and flavours [88]. Researchers have developed and used it for different applications. The e-nose is created by combining an array of metal-oxide sensors that can detect volatile organic compounds (VOC). These sensors react to VOC, which decreases the density of O2 on the surface of the sensor

and reduces the electrons trapped; this is then translated into a measurable signal. A pattern recognition algorithm then analyses these signals with a reference database of known compound reaction. The body odour is considered safe for identification purposes as it is believed to a have high degree of uniqueness [83]. Unlike conventional methods, collecting body odour signals using e-nose is non-invasive and does not require any additional actions from the user [116]. This also makes it feasible for wearable IoT devices. For example, in recent advancements, a portable e-nose device has been developed, called TruffleBot, which is low-cost and recognises 9 distinctive odours in a chemical compound [111]. We believe TruffleBot is the first step towards a wearable e-nose sensor that can acquire and analyse body odour samples. Nonetheless, no such sensor has been found in biometric recognition/authentication related application.

2.4 Electroencephalogram (EEG)

Every human brain generates electrical activity and magnetic field due to the synchronised activity of thousands or millions of neurons [72]. The EEG is a non-invasive process that measures electrical activity (in volts) of the brain by placing electrodes in standardised locations over the scalp. The number of electrodes is typically between 4 and 256, and each operational electrode is called an EEG channel. The EEG signals have five major wave rhythms: Delta, Theta, Alpha, Beta, and Gamma. The Delta rhythm indicates deep sleep and has a frequency of $0.5 - 4$ Hz. The Theta rhythm is associated with the unconscious mind and arousal and has a frequency of $4 - 8$ Hz. The Alpha rhythm shows a relaxed state and has a frequency of $8 - 12$ Hz. The Beta rhythm indicates a busy/active state and has a frequency of $12 - 30$ Hz. The Gamma rhythm has a rare occurrence, is associated with cognitive functions and has a frequency of $30 - 45$ Hz. Although using EEG for user identification and authentication is still in its infancy stage [61], several biometric solutions can be found that have used EEG signals for the following reasons [18]: (1) EEG signals provide stable features and high recognition accuracy, (2) wealth of evidence that shows EEG signals are unique and invariable for each individual, especially Alpha rhythm, (3) brain waves change under stress removing the potential to force an individual to authenticate during an attack, and (4) EEG signals cannot be acquired in the absence of an individual.

2.5 Galvanic Skin Response (GSR)

The GSR sensor is used to detect the electrodermal activity/response of a human body, i.e., changes in the amount of skin sweat [87]. The sensor is situated anywhere on the body as it requires direct skin contact. It is composed of two Ag/AgCl (silver-chloride) electrodes, where one electrode sends the electric current, and the other one receives it. The GSR sensor determines the difference of intensity between sent and received current, and outputs the skin conductance level. The GSR signal has a sampling rate of $1 - 10$ Hz and shows the distinctive peaks that are a direct response and mapping of events, for example, physical activity, images, pain, anger, stress, relief and sounds stimuli. In other words, the GSR sensor is used to determine the emotional state of an individual.

According to the existing literature, GSR cannot be used as a standalone biometric but it can be combined with other (intrinsic or extrinsic) biometrics to improve the identification accuracy as evident by the following works: ECG and GSR [17], Gaze/Eye tracking and GSR [70], and possibly GSR and EEG [103]. The skin sweating is highly coupled with the nervous system, which controls the signals of the entire body. The signals are generated in a distinct manner/pattern and vary from person to person. Recognising and utilising such patterns contribute to the improvement of the underlying biometric system.

2.6 Actigraphy and Proximity sensors

Actigraphy and Proximity sensors are used to measure the sleep cycle [7]. The Actigraphy tracks the overall sleep cycle, which includes deep sleep, light sleep, and awake time during sleep. The state of sleep is commonly identified by the lack of movement of the wearable device. For this purpose, a sensor is used called Actimetric, which records and measures the body movements (both subtle and intense), and the output data is plotted on a graph and analysed to determine the sleep cycle. The additional Proximity-sensor is used to identify the presence of skin. This means if the wearable device is sitting idle on a table, that period would not be considered as asleep, hence providing an accurate sleep measurement. It should be noted here that considering sleep patterns whilst developing activity-related (i.e. using heartbeats, steps count, calorie consumption, intensity, etc. as features) biometric solutions have significantly improved accuracy. This is due to the uniqueness and invariability in the sleeping cycles and habits of each individual [108].

2.7 Digital stethoscope

Digital or electronic stethoscope [23] is a wearable device that is used to collect natural heart acoustic signals by placing it on a subject's chest. The signals are transmitted via Bluetooth to a computing machine, where they are stored in a digital format for analysis and usage. The signals are filtered, amplified, normalised and segmented for effective results. These signals have a strong potential to determine heart-related diseases and abnormalities due to their distinctive frequencies [101] and acoustic patterns [54]. Although the research is still on-going, many researchers have successfully used heart sounds as a biometric due to achieving high identification accuracy within a reasonable time.

2.8 Other potential sources

Several other data sources exist that are only used for healthcare and other related applications at this point. These sources include blood pressure, body temperature, breath sensor and DNA. However, current research suggests that these sources have the potential to be utilised for biometric authentication in future. Furthermore, multi-biometric systems can be developed as a wearable device can accommodate multiple sensors. This will enhance the accuracy, usage and adaptability of existing uni-biometric systems [34].

Blood pressure is a vital indicator in clinical and healthcare [84]. Diagnosis is performed by monitoring the patient's systolic (highest) and diastolic (lowest) pressure that their heart is producing. It can be used in the detection of hypertension which can increase the risk of stroke or heart failure, to hypotension, which can lead to fainting or dizziness. One way to collect this data, which a healthcare practitioner would usually opt for is a sphygmomanometer. As mentioned in ECG monitoring, similarly, a portable device can also be worn to measure BP over a prolonged period for a larger data sample, which can then be reviewed and analysed to detect any anomalies. The most common way to perform this fast, non-invasive procedure is to use and fasten the sphygmomanometer containing an inflatable fabric cuff to the patient's upper arm and let the machine take data readings for approximately one minute so that the systolic and diastolic results can be produced. Collection of this health data allows for endless possibilities in its use. In one interesting progress, Samsung Electronics has filed a patent [43] that will enable the user authentication through processing blood pressure patterns, measured by sensors in mobile phones and smartwatches. According to the patent, the atrial conduction system (contraction and expansion of heart muscles) of every human being is different. Therefore, the blood flow patterns are different as well.

Body temperature helps in the identification several health issues (e.g., infection and inflammation) [39] and should be appropriately monitored to allow the preservation of homeostasis (the

Technology	Origin	Location	Described in Section
Electrocardiogram (ECG)	Heart	Chest	Heart-based biometrics (3.1)
Photoplethysmogram (PPG)	Heart	Wrist	Heart-based biometrics (3.1)
Electronic nose (e-nose)	Skin	All body	Skin-based biometrics (3.3)
Electroencephalography (EEG)	Brain	Head	Brain activity based biometrics (3.4)
Galvanic skin response (GSR)	Skin	All body	Skin-based biometrics (3.3)
Actigraphy and Proximity sensors (AP)	Sleep	Wrist or All body	Sleeping patterns based Biometrics (3.2)
Electronic stethoscope (ES)	Heart	Chest	Heart-based biometrics (3.1)

Table 1. Specification and constraints of existing wearable technologies that have biometric applications

conditions where our body can function normally). Body temperature is of the utmost importance in health and is especially true for young children and the elderly alike to maintain bodily functions. In most cases, a digital thermometer is used to take readings. Advancements in body temperature sensing are on the rise. There is no work published regarding employing body temperature for biometric authentication; however, one research study [19] has developed a low-power, wireless sensor to measure body temperature that can be used in wearable biometrics and healthcare systems.

Breath sensors have long been used in healthcare monitoring and clinical applications [33]. They operate in a portable and noninvasive manner, and determine the composition/contents of breath in terms of over 870 compounds. The sensors are also capable of performing quick breath analysis by using an online system. Although the current research suggests no biometric-related application, we believe that breath sensors carry a strong potential for real-time and convenient user identification and authentication.

DNA (Deoxyribonucleic acid) is one of the best biometric for identifying human beings. It is unique and deemed impossible to fabricate or mimic [52]. However, it cannot be used in biometrics because it takes a significant amount of time to match, needs expensive equipment, and performs complex steps for extracting, inspecting and matching the DNA [36].

3 REVIEW OF APPLICATIONS IN BIOMETRICS

At this stage, a review has been performed to gain an understanding of what types of health-based data sources are collected and used by computing systems. The next stage is to perform a detailed literature review of how each data type, specifically those acquired from wearable IoT sensors, is used for biometric purposes. In this section, a systematic review is performed into the use of the identified data sources in computer security as biometrics. In order to perform this systematic literature review, Table 1 is followed whereby literature is searched to identify biometric uses of each data source (signal type), as well as searching for constraints affecting their use. These sources have biometric applications because the data generated is sufficiently distinctive, universal, permanent, measurable, resourceful, portable, consumes reasonable time, acceptable and reproducible. It should be noted here that some data sources (blood pressure, body temperature, breath sensor and DNA) are not included in this section as they remain unused in biometric systems based on the literature search and current technology status.

The biometrics discussed in this section are categorised based on the origin of data sources (presented in Table 1). The biometrics are organised in terms of the origin of signals, rather than the signals themselves. Therefore, all literature/information regarding a particular data source is accumulated into a single section. For example, ECG and PPG are different types of signals and acquired from different locations of a body; however, both signals are used for heart rate monitoring and have common underlying origin or data source. We have discussed all intrinsic 'what you are' properties (or features) of a human body, where signals can be acquired, processed and efficiently

used in biometric-related applications. Each section reviews key research, identifying key strengths and weaknesses.

3.1 Heart-based Biometrics

An ECG signal is a combination of three sub-sequences or electrical components; the *P* wave, the *T* wave, and the *QRS* complex (i.e., *PQRST* waves) that shows the depolarisation and repolarisation of the different muscles involved in a heartbeat [1]. The *P* wave reports the depolarisation of atrial muscles, which have a time duration of 120 milliseconds (ms) and the frequency of $10 - 15$ Hz. The T wave describes the repolarisation of ventricular muscles and is usually observed after 300 ms intervals. The QRS complex depicts the depolarisation of the right and left ventricles, and is significantly larger than the P wave and T wave. For a QRS complex, the duration is $70 - 110$ ms, the frequency is $10 - 40$ Hz and has steep slopes in terms of wave heights. A research study proposed a technique that extracts T wave, QRS Complex and P wave feature space from ECG signal, and formulates a polynomial function and coefficients (template) of heartbeats [98]. To authenticate an individual, it matches the template within the existing database using Polynomial Distance Measurement (PDM) method. Using PDM is deemed 12 times quicker than the existing mechanisms and requires 6.5 times less storage with up to 100% accuracy on 15 individuals. Another research work [95] proposed uni- and multi-biometric authentication scheme using ECG biometrics, which stores PQRTS features of each individual in the database, and later use a statistical matching threshold for authentication. The uni-biometric solution demonstrated 90% accuracy on 73 individuals, whereas, the multi-biometric system presented 96.98% accuracy with face and 98.48% accuracy with fingerprint. Although the ECG biometric systems rely on the QRS complex as it is dominant among others, in one paper, the authors used P and T waves to delineate (detect and track waves of) ECG signals [94]. These delineators are then utilised along with QRS complex to build a feature space consisting of time duration between heartbeats, amplitudes, and angles. These features are stored in the database, where the individual recognition process is performed using correlation-based Template Matching technique. This solution has presented an accuracy of 99% by evaluating 50 individuals.

A simple approach uses Multi-layer Perceptron (MLP) and Radial Basis Function (RBF) neural networks to classify QRS complexes to perform user authentication [60]. The MLP is a supervised linear classification technique that uses a feed-forward neural network. Similarly, the RBF determines input's similarity within the training set to perform classification. Both techniques were tested on 18 subjects containing 324 QRS samples and presented 98% accuracy for MLP and 97% for RBF. It should be noted here that the approach did not use P and T waves and generated viable accuracy. A similar paper [69] proposed the use of Neural Network (NN) to perform the classification of normalised QRS complexes in ECG signals for user authentication. This was tested on 90 individuals and presented 99.54% accuracy. Furthermore, this technique was embedded in a low-powered chip that authenticates the user based on heart rate and false negative rate. A study [57] proposed a new apparatus for ECG biometric system, which is attached to the subject hand (right thumb and left index fingers) without pre-gelled electrodes or conductive paste on the skin. The developed solution uses a fiducial approach, where a normalised waveform is created to represent a single mean of all heartbeat signals. The amplitudes of the waveform are directly considered as features. Upon testing the solution on 16 individuals, the extracted signal had more noise than the usual and showed 94.3% accuracy using Euclidean distance. The noise is a type of electromagnetic energy that is collected by transmission conductors. It is inversely proportional to the accuracy of the biometric-based authentication system.

In another study, the authors proposed a new ECG biometric recognition system that does not utilise P wave, QRS complex, and T wave [78]. This is known as the non-fiducial detection system.

It extracts features from heartbeat signals by conducting Discrete Cosine Transform (DCT) of the Autocorrelation (AC) and uses k-nearest neighbourhood (KNN) for classifying them to provide a correct and resource-efficient individual identification system. The AC method combines all heartbeat samples from an individual into one signal and DCT is used to reduce feature dimensionality of the signal. According to the evaluation of 14 healthy individuals with 1, 000 samples each, the proposed solution showed 100% recognition rate. However, the performance of non-healthy individuals is yet to be determined. Another research paper presents a similar DCT and AC based approach that additionally performs Template Matching (TM) before the dimensionality reduction process in order to prune the search space [2]. The TM is a high-performance classification that lowers the number of classes and reduces the overall classifier scope. This technique showed 96.3% accuracy on 27 subjects. Traditionally, the sensors for extracting ECG signals are strapped on the human chest.

A research study claims that the heart sound signal can also be used as a biometric [74]. It is claimed that the heart acoustics are distinct for everyone, even if two people have same heart disease, and does not require several electrodes to obtain the signal. The proposed solution employs a feature extraction scheme based on cepstral analysis to provide a low-dimensional and sufficiently unique discrimination feature space. The solution was developed in real-time using a combination Vector quantisation and Gaussian mixture modelling techniques, and can be used to identify/verify an individual. The empirical analysis consists of two different experiments; first, 128 heart sounds from 128 subjects produced 99% accuracy and second, 1000 heart sounds from 10 subjects generated 96% accuracy. Another research study proposed a new approach that combines heartbeat and acoustic signals to recognise the identity of individuals [26]. The heartbeat signals are obtained via ECG, whereas, the acoustic signals are collected by Phonocardiogram (PCG), a technique that records sounds and murmurs of heart. The Vernier sensor and Littmann Electronic Stethoscope Model 4100WS were used to conducting PCG. In order to extract features, the approach uses the entire ECG signal for heartbeats and the Short-Time Fourier Transform (STFT) along with the DCT coefficients to process heart acoustics. The developed solution was tested on 21 individuals and has presented an accuracy of 97% using Gaussian mixture modelling. Another paper [120] developed a heart sound biometric system for user identification by employing a new approach called marginal spectrum analysis (a feature extraction technique). This solution performs an additional step on the acoustic signal, where lung, body movement and other sounds are removed. The experiment was conducted on 280 heart sounds from 40 subjects, each in relaxed form for 10 seconds, using Vector quantisation algorithm. The results demonstrated the recognition rate of 94%, which is higher than the Fourier-based technique (84.32%) on the same data. An interesting fact about this study is that the heart sounds were acquired through stethoscope attached with a simple computer sound card.

A recent paper extracted RR-intervals from ECG signals and used an efficient 128-bit Random Binary Sequence (RBS) generation algorithm to improve security for biometric applications [76]. The algorithm is called Multiple Fiducial-points based Binary Sequence Generation (MFBSG) algorithm [121]. The RR-interval is the time between QRS complexes. The technique ensures that the RBS is random and distinct enough to be used for authentication and unique for every individual. It uses Hamming distance with a user-defined threshold to find the match between two RBSes. The empirical analysis has shown a reduction in execution time as the solution only uses inter-pulse intervals and an accuracy of 99.3% over 89 individuals. Another technique [55] starts by applying Discrete Waveform Transform (DWT) on ECG signals using heartbeat time intervals and extracts several features to represent the different cardiac states (resting, exercising and recovering) of an individual efficiently. The features are classified using Gaussian-mixture-model (GMM) and Hidden-Markov-Model (HMM) algorithms with user-specific thresholds. The GMM performs K-means clustering to depict a collection of features for an individual, whereas HMM is used to identify

the progression/changing of cardiac states for each individual. This solution has achieved 89% identification rate on 786 individuals. A new feature extraction algorithm, called Pulse Active Ratio (PAR) [90] performed ECG signal analysis for authentication purposes. The PAR determines the maximum amplitude and duration of the ECG signal and outputs a vector of 98 features as a pulse waveform. The users can also manually input the values into the PAR algorithm to generate ECG signals. The authors claim that the proposed solution is better in performance than the traditional methods. It was tested on 112 individuals (14 healthy and 98 with arrhythmia) with two samples each and demonstrated an accuracy of 94.54% using Euclidean distance.

The ECG signals are collected for longer periods of time to recognise subtle variations among the heartbeats of individuals. However, if the signal is short-term, the variations are significantly reduced, hence making it difficult to differentiate among individuals. To tackle this issue, a research study proposed a new technique that can distinguish among short-term ECG signals [110]. This technique first removes the noise from the QRS-centred signal and uses a deep learning procedure, known as Principal Component Analysis Network (PCANet), to extract the features. The PCANet identifies the linear patterns in the signal data and represents them (i.e., principal components or features) in lower dimensions without much loss of information. After the feature extraction, linear kernel support vector machine (or linear-SVM) is utilised for classification and recognition process. This technique achieved 94.4% accuracy on 12 samples with 5 heartbeats each. Another similar publication [20] created a non-expensive, portable chip for biometric authentication. The process begins by removing noise from a low-quality ECG signals using low/high-pass filters. After that, it extracts eight fiducial features and uses linear-SVM for classification. This solution achieved over 98% accuracy by testing 175 individuals.

Research has used heart rate variability (HRV) feature as well to authenticate the identity of a patient in a Wireless Body Area Network (WBAN) [75]. The HRV is a unique physiological phenomenon that determines the different time intervals between heartbeats. The proposed solution measures the HRV through R-peak detection of ECG waves. The R-peaks are easier to detect as they have the highest amplitudes among other waves. The HRV is used as an input to calculate the message authentication code (MAC), which is exchanged between the sender and receiver to maintain data integrity and authenticity of a biometric-based cryptosystems. This solution was tested on 24 healthy subjects and presented 99.3% accuracy. Another paper presents a solution for biometric authentication based on the long-term/historic ECG signals using Higher-Order Statistics (HOS) [97]. The HOS is a powerful technique that can represent the signals of arbitrary length in the third or higher power forms. It can also directly extract the features (PQRST complexes) in implicit form without needing fiducial points. So by using HOS, the proposed solution extracts the ECG signals, determines HRV feature space and reduces the dimensions to output a unique feature pattern for each individual. The patterns are compared with existing patterns in terms of similarity to perform the authentication. The authors also probed the effect of heart-related anomalies and their effect on classification accuracy. They determined that the more historical data is used, the more error rate is reduced. This technique showed 98.6% accuracy for 4 subjects using 5-minute time window samples. One paper proposed a new technique to create a heartbeat template for each individual based on a raw, noisy ECG signal [27]. The main contribution of this work lies in the detection and pre-processing of instrumental heartbeats for extracting templates. It takes the raw ECG signal, applies DWT to acquire a time-frequency domain, and then performs re-sampling and normalisation to extract PQRST waves. The DWT is an implementation of the wavelet transform that provides significant information about the signal within a reduced time. After getting the template, it uses the correlation technique to identifies a suitable match in the database. This solution has demonstrated an accuracy of 99.61% for 14 individuals.

Another study [53] used PPG signals with a feed-forward neural network to perform biometric authentication. The solution was tested on 708 datasets from 10 individuals and presented 95.1% accuracy. This is one of the long-term studes that established: (1) the feasibility of using PPG signals in biometric authentication based on features, such as wave angles, area and inflection point and (2) different physical and mental conditions might cause failure in the authentication as they introduce irregularities or abnormalities in the heart rate. Similar work [3] used PPG signals for HRV based biometric application where the authors designed a physical component to measure the RR-intervals, i.e., the time duration between two adjacent R-peaks of the signal. In this case, the RR-intervals were used as a feature to perform the *K*NN classification. This technique successfully recognised 92.26% of the 40 individuals. Due to motion artefacts (MA), the PPG sensors are prone to distortion and noise, which makes it difficult to collect signal features. Existing methods use manual feature selection and extraction techniques based on domain knowledge. To automate this process, a recent research study [25] presents a data-driven four-layer Deep Neural Network (DNN) that contains Convolution Neural Network (CNN) and Long and Short Term Memory (LSTM). The CNN automatically detects user-defined patterns in the data and uses as a feature extractor for PPG signal. The LSTM mines dependencies in the data, and is used for capturing the temporal dependency within the extracted features. The proposed DNN is capable of authenticating individuals based on heartbeat biometric collected through PPG sensors and has shown a 96% accuracy on 12 individuals. An extension of this work has been developed as a framework, called CorNET [12], for ambulant environments using custom sensors. It also uses a combination of CNN and LSTM, and presented 96% accuracy on 20 individuals (while doing different, voluntary physical activities). The CorNET is capable of biometric identification as well as heart rate estimation.

Most of the related work uses ECG biometric as it has a number of advantages in terms of easy to measure, difficult to mimic/replay signals for malicious reasons, as well as not requiring expensive equipment and applicable in practical environments. The key advantage of using ECG is high accuracy, which is integral to the authentication systems. There is an extensive study on using heart rates as a biometric and there are distinctive approaches with varying results. We believe it is beneficial to present a summary of the findings as shown in Table 2. Based on the literature, we have identified that the area of heart-related biometrics is the most developed and therefore, it is possible to construct a summary table, whereas, other areas are less mature and do not have enough articles to provide a comparison summary. Notice that the table presents a sorted list of research studies based on the highest-to-lowest number of subjects and classification accuracy.

3.2 Sleeping patterns based Biometrics

One research study has proposed the use of IoT bed sensors to determine and analyse sleep depth [35]. This is carried out by attaching sensors that are connected to the WiFi on a single bed mattress which in turn are connected to a remote server containing. The server has several features, for example, detecting if the user is laid flat and sleeping rather than just sat on the bed by use of body pressure in certain areas. A research study utilised actigraphy, which is a non-invasive monitoring technique containing 63 features, for the identification of sleep-wake states within infants [91]. The authors employed statistical and neural network-based algorithms, and showed an accuracy range of $77 - 92\%$ for 26 subjects. It is claimed that actigraphy is a comparable alternative to the similar polysomnography technique, which usually achieves $85 - 95\%$ accuracy. The polysomnography is an overnight examination of sleep, typically recorded by cameras and sensors that are attached to the head and chest of the subject. It is difficult to use and intrusive in nature. A recent patent proposed the use of sleep physiology for authentication of subjects by creating biometric profiles in order to either verify or disprove the identity of the individual [68]. The data suggested for collection during the different stages of sleep include heart rate, heart rate

Work	Signal / Technology	Features	Matching algorithm	Number of subjects	Classification Accuracy (%)	Additional information
[55]	ECG	Discrete Waveform Transform	Gaussian Mixture Model and Hidden Markov Model	786	89	Considers different cardiac and other user-specific conditions along with ECG signals
[20]	ECG	PQRST waves	Linear Kernel Support Vector Machine	175	98	Created a portable mobile chip to acquire, clean and classify ECG signals
[90]	ECG	Pulse Active Ratio	Euclidean Distance	112	94.54	Claims to develop a better feature extraction method and tested regular and arrhythmia heart signals
[69]	ECG	QRS waves	Neural Network	90	99.54	Developed a low-powered and fully operational electronic chip for authentication
[76]	ECG	RR-intervals using Random Binary Sequence	Hamming Distance	89	99.3	Demonstrates that using inter-pulse intervals reduces processing time, whilst, preserving accuracy
[95]	ECG	PQRST waves	Statistical Matching	73	90	Demonstrates that multi-biometric sytems are better than uni-biometric systems
[94]	ECG	Time duration between heartbeats, amplitudes and angles	Correlation-based Template Matching	50	99	Presents an efficient feature extraction technique
[120]	Heart acoustics	Marginal spectrum analysis	Vector Quantisation	40	94	Indicates that de-Noising of heart acoustic signals is crucial for better accuracy
[3]	PPG	RR-intervals	k-nearest neighbours	40	92.26	Proposed a new feature extraction mechanism that can measure RR-intervals of a PPG signal
[2]	ECG	Autocorrelation / Discrete Cosine Transform	Correlation-based Template Matching	27	96.3	Reaffirms that non-fuducial features produce promising accuracy
[75]	ECG	Amplitudes of R waves	Message Authentication Code	24	99.3	Proposed a cost and resource efficient solution that can be used in biometric cryptosystems
[26]	ECG and Heart acoustics	Short-Time Fourier Transform and Discrete Cosine Transform	Gaussian Mixture Modelling	21	97	Shows that heart acoustics is quite feasible for a multi-biometric system
[12]	PPG	Convolution Neural Network	Long and Short Term Memory	20	96	Presents a data-driven deep learning approach for ambulant environments using custom sensors
[60]	ECG	QRS waves	Multi-Layer Perceptron and Radial Basis Function Neural Networks	18	98	Affirms that only QRS waves are sufficient to obtain higher accuracy
[57]	ECG	Amplitudes of heartbeats waveform	Euclidean Distance	16	94.3	Uses subject's finger to collect signals, instead of chest
[98]	ECG	PQRST waves	Polynomial Distance Measurement	15	100	Presents a mechanism for quicker and efficient signal acquisition and processing
[78]	ECG	Autocorrelation / Discrete Cosine Transform	k-nearest neighbours	14	100	Provided a better and easier non-fiducial feature extraction technique
[27]	ECG	PQRST waves	Correlation-based Template Matching	14	99.6	Proposed an efficient pre-processing mechanism of raw, noisy ECG signals and feature extraction
[25]	PPG	Convolution Neural Network	Long and Short Term Memory	12	96	Presents a data-driven deep learning approach that does not require feature extraction
[110]	ECG	Principal Component Analysis Network	Linear Lernel Support Vector Machine	12	94.4	Developed a technique that can classify short-term ECG signals
[74]	Heart acoustics	Cepstral analysis	Vector Quantisation and Gaussian Mixture Modelling	10	96	Claims that heart acoustics are easier to obtain and similar to ECG in accuracy
[53]	PPG	Angles, area and inflection point of waves	Neural Network	10	95.1	Demostrated that PPG signals can be used for biometric authentication
[97]	ECG	PQRST waves	Higher-Order Statistics	4	98.6	Investigated the affect of heart-related anomalies on the user identification ability

Table 2. Summary of heart-related biometrics

variability, acceleration, and breathing rate. Using this data, a biometric profile can be created for each subject. Following on, classification algorithms, such as the random forest model, logistic regression, or neural network can be used for subject identification.

Monitoring sleep patterns for other purposes is a popular area and there are many pieces of new technology that have either been released or are in development. One such patent device covers the patients' nose and measures the air pressure produced. The purpose is to detect conditions, such as sleep apnea or airway blockage [99]. However, this device was created in 1993. A more recent patent recommends the use of a device that can be used for both medical diagnosis and identity verification [47]. This is achieved by the use of multiple sensors attached to the patient (or bed in the case of sleep analysis) constantly collecting data and authenticating the patient(s). After that, the collected data is sent to a remote location for analysis and diagnosis. A pulse oximeter on the patient's fingertip represents an example of this approach. A recent study employed Support Vector Machine (SVM) classifier for the identification and authentication of subjects based on a multi-biometric system [109]. The data set used in this paper was collected from the undergraduate students of the University of Notre Dame. The original data set, named as *NetHealth* [56], contained approximately 700 subjects but this paper considered and analysed 421 subjects. This is one of the large-scale studies that also extracted 108 (sedentary) and 109 (non-sedentary) features from sleep status, step count, heart beat, calorie burn and metabolic equivalent of task (MET). The results have shown 0.93% and 0.90% accuracy for sedentary and non-sedentary periods, respectively.

The potential of being able to utilise these techniques and analyse a user's pattern allows for an array of possibilities in identity verification and authentication. However, it is recommended that the data from wearable and non-invasive devices are collected for a minimum period of one to two weeks, and complemented by other sensors to achieve better accuracy. It is also not uncommon for actigraphs to misinterpret insomnia within patients, despite them not having it, making the use of them questionable for identification purposes.

3.3 Skin-based biometrics

A recent paper used skin temperature and electrodermal activity acquired through a smartwatch to perform the authentication process [24]. The signal features were extracted using wavelet entropy method, which is based on Shannon, energy, threshold, sure, norm and power entropy values. After that, it employed feed-forward neural network to perform the classification. This solution was tested on 30 individuals and achieved reasonable accuracy. A patent [4] proposed a mobile communication device coupled with electronic skin tattoo that is applied to the throat region. It consists of a microphone to capture audio signals, controller to process the signals, transceiver for wireless communication and a power supply. The main purpose of this device is to improve audio detection by reducing the signal-to-noise ratio.

Another study [40] proposed a theoretical framework that uses an electric nose (e-nose) to extract the body odour samples and perform biometric authentication. It uses a simple clustering technique for training and recognising the closest match of a given sample in the knowledge base. The e-nose apparatus consists of several expensive components for sniffing, delivering, receiving, computing and authenticating the body odour along with the complex electric circuitry that connects them. A similar paper [112] used e-nose to detect and recognise the individuals through the armpit odour. The proposed method uses Principal Component Analysis (PCA) to recognise patterns and achieved 95% accuracy by conducting multiple tests on 4 individuals. The authors claim that the accuracy of e-nose is affected by the degree of humidity and application of deodorant (noise). Therefore, they developed a novel methodology based on hardware and software that can perform noise correction. The hardware-based technique uses a heat bath to create a constant humidity level between the human skin and background environment and then allows the sensor to collect the

body odour sample. The software-based technique measures skin conductance at various noise levels and builds a mathematical model, which is then used to calibrate the acquired signal by identifying and eliminating the noise. Both hardware and software approaches are applied at the same time to gain maximum accuracy.

An extension of the aforementioned technique has also been proposed that takes sensor drift into consideration [113]. Sensor drift is caused by physical changes in the sensor over time due to external factors (heat, sweat, etc.) and leads to erroneous measurements. The sensor drift correction is performed by a mathematical model that was obtained by comparing the baselines of purified air and human odour signals. Another paper presents a technique that can convert a body odour into a unique digital signature/password [41]. All signatures are stored in a database, which is then used for the automated identification of individual's body odour by employing correlation techniques. Another paper applied multi-class SVM and kNN algorithms in order to perform the classification of the e-nose signals [32]. The technique was evaluated on 30 different combinations of 60 training samples and 20 test data samples. It achieved 87% and 86% accuracy for SVM and kNN, respectively. After that, the same test data was formulated into a decision tree structure, which increased the accuracy to 93% and 96% for SVM and kNN, respectively.

3.4 Brain activity based biometrics

A recent survey shows that the EEG signals have great potential of being used for biometric purposes, and a large community of researchers has started working in its practical deployment [104]. The EEG signals are well-suited in terms of stability and uniqueness. A study conducted on 50 individuals shows that the EEG signals have more distinct characteristics when collected in the resting/relax state [38]. It also suggests that the recording of EEG signals for training or identification should be approximately 2 minutes to obtain better accuracy. One of the initial work regarding the use of EEG for biometric authentication is based on feed-forward neural classifier [37]. This technique was tested on 6 individuals and resulted in the accuracy of 97.5%. Another paper proposed a two-step biometric authentication process using EEG signals [71]. The process starts by reducing the feature dimensions of the signals using PCA alongside removing the redundancies and overlapping. After that, it employs Manhattan distance based on two threshold values for reducing false accept/reject error and performs the authentication. This technique was tested on the EEG signals gathered from 5 individuals in different states, such as relax, solving mathematical problems, letter writing, etc. It showed 100% accuracy. Another paper utilised the MLP neural network to perform classification of EEG signals [93]. The technique applies two different methods, Discrete Fourier Transform (DFT) and Wavelet Packet Decomposition (WPD), to extract two different sets of features. It achieved 100% accuracy for 3 individuals in a relaxed and quiet state.

Bashar et al. proposed [9] three separate methods to extract features from the EEG signals in 2016: Multiscale Shape Description (MSD), multiscale Wavelet Packet Statistics (WPS) and Multiscale Wavelet Packet Energy Statistics (WPES). The features were extracted after removing the noise and artefacts through the band-pass filter. After that, it used the SVM algorithm for the training and recognition and achieved 94.44% on 9 individuals. A similar paper [45] followed the same approach, but added another feature extraction method, called Alpha-Beta Statistics, along with MSD, WPS, and WPES. It also used neural networks along with the SVM to perform a better classification process. Another study presents an EEG-based biometric authentication tool, called BrainID [44]. The EEG signals were collected by asking the user to visualise a predefined 4-digit number. After that, Common Spatial Patterns (CSP) approach is used for feature extraction that converts Alpha and Beta rhythms of the signal into a lower-dimension matrix. The extracted features were used as input to Linear discriminant analysis (LDA) algorithm that performed classification. At the time of authentication, the user is asked to visualise the same number that was used for training. The

evaluation of BrainID shows 96.97% accuracy on 12 individuals. A similar paper also employed LDA for the classification of EEG signals [50]. The features were extracted by analysing the relationship among EEG channels with the help of phase synchronisation approach. This technique achieved 95 – 99% accuracy in identifying individuals. Another paper proposed the use of Fuzzy Entropy (FE) to extract the features of EEG signals from different electrodes [66]. The FE measures and represents the degree of fuzziness in fuzzy sets based on numerical values. The Fisher distance algorithm is used to analyse and distinguish among the features using dissimilarity approach and outputs a matrix. After that, the technique used Back Propagation (BP) neural network for the classification of signals. Evaluation of this technique on 10 individuals shows that the accuracy is greater than 87.3%.

A paper proposed the use of a Convolution Neural Network (CNN) to perform the identification of individuals [59]. This system uses the EEG signals collected in a resting state with open/close eyes and yielded an accuracy of 88% on 10 individuals. Another paper used CNN for the EEG-based biometric identification [62]. The proposed system was tested on 100 subjects and showed high performance and accuracy of 97%. A research study applied two pattern matching methods, Euclidean Distance (ED) and Dynamic Time Warping (DTW), on EEG signals for identification [30]. The signals were acquired from 30 individuals by showing illegal strings and words, which is claimed to generate more distinguishable brain activity patterns. The ED method yielded a maximum accuracy of 81.17%, whilst DWT showed 67.17%. A recent paper proposed a new method to capture EEG signals using invisible visual stimuli [67]. An image is embedded in a video having a frame rate of 144 Hz and shown to the individual. The feature set from the EEG signals is acquired using the spectral difference of four different stimulation conditions, ranging from 0% (no visual stimuli) to 100% (visible visual stimuli). After that, the technique uses Euclidean distance to determine the match for identification and presented an accuracy of 80% on 20 individuals. Another recent study successfully demonstrates the use of Flower Pollination Algorithm (FPA) to reduce the number of sensors required to capture the EEG signal [89]. The FPA is an evolutionary-based optimisation algorithm that determines a sufficiently good solution. This paper used FPA to select the best subset and an optimum number of sensors without affecting the quality of EEG signal. For identification, the authors used Optimum-Path Forest algorithm, which is a graph-based classification process. The empirical analysis of this solution showed 87% accuracy while reducing the number of sensors in half as compared to other conventional systems. Another paper proposed a simple approach to use EEG as biometrics [86]. This approach removes the noise from the signal and uses time and frequency-based analysis to extract features template. After that, it uses neural network classifier to find a match between current and stored templates for identification.

3.5 Summary

Reviewing existing literature highlighted several medical-based biometric systems that can be used for enrolment, authentication, and identification of individuals. These systems possess a reasonable amount of accuracy and can be used in the real world. A general trend that has been followed in existing studies is described in the following:

(1) Acquire corresponding signals (heart, brain, etc.) from the individuals;
(2) Perform discretisation of the signals and extract the fiducials or non-fiducials features;
(3) Train the classification algorithm with one or more feature sets of the individuals to build a model. This is known as the enrolment phase; and
(4) Use the model to recognise individuals, also known as authentication and identification.

4 LIMITATIONS AND FUTURE CHALLENGES

At this stage, the use of health-based data within biometric systems has been investigated, looking at the different data sources and how they are utilised to build or improve security systems. In this section, we present limitations and their impact, and key future challenges of using wearable IoT health devices as a future biometric source. We also provide a brief discussion on each limitation and challenge, followed by a summary table at the end. Moreover, the limitations and impacts are linked to the survey/review of the existing literature presented in the previous sections for providing a reference.

Limitation 1. *Existing approaches are limited by the stability, variability and reliability of the biometric data source [53].*

Impact 1. *The inability to adequately handle the continuous change in biometric data source reduces wider adoption and usability due to a decreasing accuracy [97]. More specifically, an increase in false positives and a decrease in true positives.*

Challenge 1. *Unlike existing evaluation methodologies, researchers should conduct experiments over longer periods of time to consider greater variation and deteriorating characteristics.*

The physical and mental traits of a human body constantly change and behave differently depending on time, age, environment, and circumstances. For example, the heart rate changes under stress, coercion, intense physical activity, etc. This is one reason as to why heart-based authentication might result in lower accuracy, as it would be challenging to differentiate between participants. This is why it is not feasible to use a biometric data source, which is prone to constant change. Another example can be found in the use of EEG signals, which depict the amount of electric field (brain activity) around the scalp, but cannot explain the cause behind. This is generally known as 'inverse problem' [102]. The brain activity of the same individual might differ based on the varying physical and mental states. So, during the identification or authentication process, inconsistent EEG signal patterns can lead to poor quality results. Some existing solutions have attempted to resolve the inconsistent signals issue by taking multiple samples/templates of the same individual over longer periods of time [58]. Therefore, such algorithms and techniques should be created that are flexible enough to understand the constant variations in the human body and provide accurate results.

Limitation 2. *The electronic ageing of sensor's components (sensor drift) and deterioration over-time [113].*

Impact 2. *This limitation can increase signal acquisition time and reduce accuracy levels due to noisy, inaccurate and unreliable data samples [20, 110].*

Challenge 2. *Hardware that is not fit-for-purpose will generate erroneous results regardless of the data analysis technique. Therefore, electronic engineers should produce sensors of high quality, ensuring they are reliable and are also integrated with self-checking and even automated error compensation mechanisms.*

The wearable sensors are prone to physical damage depending on the adversity of external factors and output incorrect readings/signals [49]. This leads towards the failure of the overall biometric system. For example, the heart-related signals acquired from ECG and PPG sensors are usually distorted and/or have noise due to problems, such as a baseline drift, external interference, muscle noise, etc. Most of the existing techniques use frequency band filters to remove the noise. This is a complicated task and might not be sufficient due to difficulties in identifying the noise frequencies. A signal can have both internal (thermal and shot) and external (electrostatic and

electromagnetic) noise. The identification and elimination of all forms of noise and error require a more systematic and rigorous approach [107]. Furthermore, E-nose and other similar chemical-based sensors struggle with long stability in real operating conditions. Such sensors require constant error correction or replacement over time, depending on the sensor life that can be improved.

Limitation 3. *Current literature shows that most of the techniques have only been evaluated on healthy individuals. There is also a critical need to test biometric systems on large-scale datasets, representative of healthy individuals and also those deemed to have health conditions [75, 97].*

Impact 3. *Using datasets for development that are not representative of the general population will result in a biased evaluation along with representing incorrect capabilities [78]. This could result in a biometric system that either performs poorly for unhealthy subjects or unfairly discriminates against individuals with health conditions.*

Challenge 3. *The experiments should be performed on a larger and balanced population, having both healthy and unhealthy individuals, to determine the actual accuracy of the underlying technique. However, this requires researchers and developers of biometric systems to utilise a more inclusive test population, even if it results in a reduction in reported accuracy.*

There is a need for complete and reliable efficiency and accuracy analysis over large-scale datasets that includes both healthy and unhealthy individuals [22]. Without this, a wider adoption and utilisation of health-based wearable devices in biometric systems would be difficult. For example, the high risk of the instantaneous change in heart activity due to the physical and emotional state and various cardiac disorders can disrupt the biometric system. Furthermore, existing studies show that it is difficult to determine the individuality and scalability of heartbeat signals/patterns in a larger set of individuals. The sample sizes selected to test existing solutions are not insufficient to assess the performance and application in real-world, large-scale environments. It is possible that a certain selected population may (1) not possess a particular biometric identifier, (2) have a duplicate biometric identifier and (3) present properties that do not yield usable data for authentication. Furthermore, in most studies, training, and testing data were acquired in only one session, and the template ageing factor was ignored. Hence, balanced and large scale studies are required to determine the actual performance and accuracy over time.

Limitation 4. *Accurate sensor equipment is often expensive and there is no guarantee that expensive equipment results in a quality product [40].*

Impact 4. *This limitation impacts the wider and practical use of medical-biometric systems. The technology might be financially out of reach to many potential users, and even if it can be purchased, the quality might severely restrict its suitability and correctness for the target application [112].*

Challenge 4. *The sensors should have a balance between quality and cost along with a ubiquitous availability so that they can be utilised, tested, and integrated by a large number of researchers and developers.*

Regarding the issues in deployment, wearable biometric sensors are usually surrounded by several constraints, such as expensive hardware and intricate, time-consuming and cumbersome process for user authentication[80]. The second aspect of this limitation is that expensive sensing technology does not guarantee that it is fit-for-purpose for use in a biometric system. An example to demonstrate is that skin-based biometric requires pre-heated and pollution-free facilities [46] that are costly to build and setup as explained in the study. Besides, such facilities might not be available in every case due to portability concerns of bulky biometric sensor hardware. The current process of acquiring body odour signals also takes a relatively long time to train and recognise,

which result in it being unsuitable for practical use. Furthermore, there is not much discussion regarding the detection and removal of perfume, deodorant, lotion, or other external smells from the actual body odour signal. Failure to separate irrelevant smells might result in poor accuracy. Hence, electronic engineers should design and create new sensors that are small, portable and easy-to-use.

Limitation 5. *There is a lack of standardisation in medical-biometric techniques [82].*

Impact 5. *A lack of standardisation could result in the development and adoption of a biometric technology that is not suitable for the target domain [95]. This is because there is no appropriate methodology to determine whether a certain approach will perform better in a given situation, or what level of accuracy is permissible.*

Challenge 5. *The development of standards and best-practice guides required knowledge exchange and shared working between researchers and practitioners working within private companies and knowledge-based institutions, such as universities. Furthermore, the inclusion of special interest groups and governing organisations can help in achieving best practices and standardisation.*

Extensive studies have been conducted regarding the organised use of heartbeats, brain activity, skin sweat and so on for clinical diagnosis; however, its current biometric-related application has not been standardised [77]. For example, the existing works concerning feature extraction and selection (fiducials) only depends on the validity of empirical analysis by the respective authors. It is evident from Table 2 that different kinds of feature extraction mechanisms have been used. Therefore, a universally accepted, standard set of fiducials is yet to be defined. It has been widely accepted in literature that the manner in which features are selected can significantly improve the performance and accuracy of the overall biometric authentication. Also, the biometric systems are relatively difficult to design, develop and deploy as compared to traditional password/pin security systems. Hence the current biometric solutions lack wider accessibility and integration [13]. Furthermore, the number of standard, real-time and publicly available biometric datasets remain limited as compared to other similar areas. There is a need for a shared benchmark dataset that can be used to perform evaluation and cross-comparison between the developed techniques, wherever possible. Self- or home-made dataset may fulfil the requirements of individual experiments and depict accurate results, but such results cannot be considered as conclusive. Furthermore, some researchers may not have the tools and equipment to acquire an appropriate dataset for the development of methodologies. These are some of the reasons for biometric systems in lacking industry-wide standards.

Limitation 6. *There is an absence of considering security whilst collecting, storing and utilising signals in existing techniques [76].*

Impact 6. *The acquisition and usage of signals can raise privacy implications as they are not only the indication of health status but also the identity of the individual [81].*

Challenge 6. *Wearable devices and data processing tools are prone to several attacks during data communication and storage, such as leakage, theft, fabrication, and alteration. New security protocols should be developed in accordance with the needs of a biometric system and considered as an integral part of biometric systems to prevent such attacks.*

A large amount of personal and sensitive information is collected by biometric systems in the form of individuals' medical data and signals. This information can be used to expose the identity and record of the corresponding individual, along with violating several legal and ethical rules [63]. This is why it is crucial for a wearable IoT device to keep the data secure. The current

research studies are focused only on the application-side (authentication) and do not consider or present any procedure to secure the storage and communication of data. Although biometric systems are required to provide security, they need to be secured themselves as well by deploying certain protocols [11]. Lack of considering security aspects can lead towards serious attacks on the confidentiality (breach and theft of user's biometrics data) and integrity (forgery and altering of user's biometrics data) of the biometric system. There is a need to secure each layer or point of entry in the biometric system. Furthermore, there is a possibility of exploiting the biometric system by the malicious insiders, who in most cases have partial or full administrative access to the system. Insufficient security is limiting the wider usage and adaptability as the users are not comfortable in using biometrics technology.

Limitation 7. *The techniques used for the recognition and identification of individuals inherit all associated bottlenecks and related issues regarding Artificial Intelligence and Machine Learning algorithms, such as defining volume and quality of the training data, data labelling and building learning model confidence.*

Impact 7. *This negatively affects the accuracy and overall processing time of the proposed solutions alongside a large amount of consumption of computing resources.*

Challenge 7. *There is room to improve (or even create newly specialised) detection or classification algorithms for biometric data, such that they can increase the performance and accuracy of implementation and enable effective use of implemented technology. There is also a need to increase the feature quantity and uniqueness aspects.*

A general observation made from the reviewed literature is that there are several kinds of classification algorithms for the purpose of both authentication and identification processes. However, such algorithms have practical limitations due to the nature of the data and the context of the application. Moreover, the justification or explanation for using certain classification algorithm(s) for a particular kind of data that has a specific set of features is insufficient. The training set used by classification algorithms requires complete and large amounts of prepared and structured data that is also of high quality [106]. Without this, the algorithms would not be able to perform appropriate categorisation and distinctly identify the individuals, hence resulting in poor accuracy. The data is required to be effectively represented so that the algorithm can easily recognise biometric patterns [114]. These algorithms also demand larger computing resources in terms of memory and processing. In a traditional password-based system, the user will always be authenticated if correct credentials are entered. However, in the biometric systems, the user verification cannot be guaranteed, albeit inputting the correct signals, due to classification error. Another general trend seen in the existing studies is that they provide a minimal discussion of negative and non-significant results, hence their true accuracy and behaviour cannot be fully determined. A further issue regarding the biometric systems is the poor scalability. Larger datasets might have a higher error due to a lack of clear distinction among the training data items. Such issues can be tackled properly whilst building a new biometric-based authentication system.

4.1 Summary

Table 3 provides a list of limitations, their impact on the application and associated challenges determined in this survey of health-based wearable biometric technologies. Although derived from recent research activity, the presented knowledge gaps are speculative in nature. Furthermore, it is not an all-inclusive list and there is a potential that some have been missed. As the research continues in biometrics and related areas, many new gaps will be discovered and will need to be

Limitation	Impact	Challenge
The constant change of characteristics of a human body (i.e., deterioration of finger prints)	• Lack of adoption and usability • Poor accuracy	• Experiments need to be performed over longer duration's • Research required a wider and diverse range of human participants
Sensor ageing and deterioration	• Increased signal acquisition time • Increased noise in signals	• Adoption to constant change in sensors • Quality sensors • Automated error compensation mechanism
Lack of selecting an appropriate population for evaluating a biometric system	• Incomplete evaluation could lead to less accurate and reliable systems	• Standardised processes involving large-scale evaluation • Include a wide array of participants. E.g., healthy and unhealthy • Feasibility analysis of biometric identifiers
Sensor cost, hardware limitations and accuracy implications	• Reduced development and uptake of biometric-based authentication systems	• Establishing a between quality and cost • Increasing access to sensors
Unavailability of standardised techniques	• Lack of structured biometric approaches • Absence of reliable and shared dataset • Difficult distribution of new technology	• Development of International Standards and best practise guides • Release and maintenance of benchmark dataset • Public sharing and evaluation of datasets
Almost non-existence security measures in biometric systems	• Potential to damage confidentiality, integrity and availability of user data	• Development of standardised and easy to adopt security protocols • Integration of security into devices and software applications (security by deign)
Bottlenecks of Machine Learning and Artificial Intelligence	• Reduced accuracy of overall solution • Time and effort required for data pre-processing phase • Large computation resources for building learning models	• Improvements and advancements in classifications algorithms • Efficient use of developed technology • Defining high quality feature set • Effective data representation

Table 3. Summary of existing limitations of current approaches, their impact and future challenges

recognised. It should also be noticed that the elimination of knowledge gaps identified in this survey will require considerable research effort in both biometric hardware and software components.

5 CONCLUSION

This survey provides a review of state-of-the-art biometric-based technologies along with the discussion of applications, technology constraints, and further challenges. This was performed by first analysing data sources commonly used within the biometric systems that are also collected and processed for health purposes. Following on from this, a systematic analysis of current biometric systems was performed to identify current implementations and research utilising health-based data sources. This review resulted in the discovery of 7 key limitations, which all have different impacts and future challenges.

Literature has informed that the state of the research discipline is varied; new wearable biometric applications are being investigated and developed, but are yet to overcome limitations centred on usability and accuracy. It is foreseen that considering the 7 key findings when developing health-based biometric systems in the future would help improve both usability and accuracy. The wealth of research literature examined states the diversity of the research field and that wearable biometric solutions are gaining popularity, largely due to the increasing use of wearable devices collecting health data for purposes such as fitness tracking.

REFERENCES

[1] Foteini Agrafioti, Jiexin Gao, and Dimitrios Hatzinakos. 2011. Heart biometrics: Theory, methods and applications. In *Biometrics*. IntechOpen.

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

[3] Nazneen Akhter, Sumegh Tharewal, Hanumant Gite, and KV Kale. 2015. Microcontroller based RR-Interval measurement using PPG signals for Heart Rate Variability based biometric application. In *2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. IEEE, 588–593.

[4] William P Alberth Jr. 2013. Coupling an electronic skin tattoo to a mobile communication device. US Patent App. 13/462,881.

[5] John Allen. 2007. Photoplethysmography and its application in clinical physiological measurement. *Physiological measurement* 28, 3 (2007), R1.

[6] Abdulaziz Alzubaidi and Jugal Kalita. 2016. Authentication of smartphone users using behavioral biometrics. *IEEE Communications Surveys & Tutorials* 18, 3 (2016), 1998–2026.

[7] Sonia Ancoli-Israel, Roger Cole, Cathy Alessi, Mark Chambers, William Moorcroft, and Charles P Pollak. 2003. The role of actigraphy in the study of sleep and circadian rhythms. *Sleep* 26, 3 (2003), 342–392.

[8] Orlando Arias, Jacob Wurm, Khoa Hoang, and Yier Jin. 2015. Privacy and security in internet of things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems* 1, 2 (2015), 99–109.

[9] Md Khayrul Bashar, Ishio Chiaki, and Hiroaki Yoshida. 2016. Human identification from brain EEG signals using advanced machine learning method EEG-based biometrics. In *2016 IEEE EMBS Conference on Biomedical Engineering and Sciences (IECBES)*. IEEE, 475–479.

[10] Abhilasha Bhargav-Spantzel, Anna C Squicciarini, Shimon Modi, Matthew Young, Elisa Bertino, and Stephen J Elliott. 2007. Privacy preserving multi-factor authentication with biometrics. *Journal of Computer Security* 15, 5 (2007), 529–560.

[11] Andrea Bianchi and Ian Oakley. 2016. Wearable authentication: Trends and opportunities. *it-Information Technology* 58, 5 (2016), 255–262.

[12] Dwaipayan Biswas, Luke Everson, Muqing Liu, Madhuri Panwar, Bram Verhoef, Shrishail Patrika, Chris H Kim, Amit Acharyya, Chris Van Hoof, Mario Konijnenburg, et al. 2019. CorNET: Deep Learning framework for PPG based Heart Rate Estimation and Biometric Identification in Ambulant Environment. *IEEE transactions on biomedical circuits and systems* (2019).

[13] Ramon Blanco-Gonzalo, Chiara Lunerti, Raul Sanchez-Reillo, and Richard Michael Guest. 2018. Biometrics: Accessibility challenge or opportunity? *PloS one* 13, 3 (2018), e0194111.

[14] Jorge Blasco, Thomas M Chen, Juan Tapiador, and Pedro Peris-Lopez. 2016. A survey of wearable biometric recognition systems. *ACM Computing Surveys (CSUR)* 49, 3 (2016), 43.

[15] Jorge Blasco and Pedro Peris-Lopez. 2018. On the Feasibility of Low-Cost Wearable Sensors for Multi-Modal Biometric Verification. *Sensors* 18, 9 (2018), 2782.
[16] Ismail Butun, Patrik Österberg, and Houbing Song. 2019. Security of the internet of things: vulnerabilities, attacks and countermeasures. *IEEE Communications Surveys & Tutorials* (2019).
[17] Carmen Camara, Pedro Peris-Lopez, Juan E Tapiador, and Guillermo Suarez-Tangil. 2015. Non-invasive multi-modal human identification system combining ECG, GSR, and airflow biosignals. *Journal of Medical and Biological Engineering* 35, 6 (2015), 735–748.
[18] Patrizio Campisi and Daria La Rocca. 2014. Brain waves for automatic biometric-based user recognition. *IEEE transactions on information forensics and security* 9, 5 (2014), 782–800.
[19] Shih-Lun Chen, Ho-Yin Lee, Chiung-An Chen, Hong-Yi Huang, and Ching-Hsing Luo. 2009. Wireless body sensor network with adaptive low-power design for biometrics and healthcare applications. *IEEE Systems Journal* 3, 4 (2009), 398–409.
[20] Hyun-Soo Choi, Byunghan Lee, and Sungroh Yoon. 2016. Biometric authentication using noisy electrocardiograms acquired by mobile sensors. *IEEE Access* 4 (2016), 1266–1273.
[21] Adrian Condon and Grace Willatt. 2018. ECG biometrics: the heart of data-driven disruption? *Biometric Technology Today* 2018, 1 (2018), 7–9.
[22] Cory Cornelius, Ronald Peterson, Joseph Skinner, Ryan Halter, and David Kotz. 2014. A wearable system that knows who wears it. In *Proceedings of the 12th annual international conference on Mobile systems, applications, and services*. ACM, 55–67.
[23] Derek Kweku Degbedzui, Michael Tetteh, Elsie Effah Kaufmann, and Godfrey A Mills. 2018. BLUETOOTH-BASED WIRELESS DIGITAL STETHOSCOPE WITH MOBILE INTEGRATION. *Biomedical Engineering: Applications, Basis and Communications* 30, 03 (2018), 1850010.
[24] Timibloudi S Enamamu, Nathan Clarke, Paul Haskell-Dowland, and Fudong Li. 2017. Smart watch based body-temperature authentication. In *2017 International Conference on Computing Networking and Informatics (ICCNI)*. IEEE, 1–7.
[25] Luke Everson, Dwaipayan Biswas, Madhuri Panwar, Dimitrios Rodopoulos, Amit Acharyya, Chris H Kim, Chris Van Hoof, Mario Konijnenburg, and Nick Van Helleputte. 2018. BiometricNet: Deep Learning based Biometric Identification using Wrist-Worn PPG. In *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 1–5.
[26] S Zahra Fatemian, Foteini Agrafioti, and Dimitrios Hatzinakos. 2010. HeartID: Cardiac biometric recognition. In *2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*. IEEE, 1–5.
[27] S Zahra Fatemian and Dimitrios Hatzinakos. 2009. A new ECG feature extractor for biometric recognition. In *2009 16th international conference on digital signal processing*. IEEE, 1–6.
[28] Konstantinos Georgiou, Andreas V Larentzakis, Nehal N Khamis, Ghadah I Alsuhaibani, Yasser A Alaska, and Elias J Giallafos. 2018. Can wearable devices accurately measure heart rate variability? A systematic review. *Folia medica* 60, 1 (2018), 7–20.
[29] Martin D Gibbs. 2010. Biometrics: body odor authentication perception and acceptance. *ACM SIGCAS Computers and Society* 40, 4 (2010), 16–24.
[30] Qiong Gui, Zhanpeng Jin, Maria V Ruiz Blondet, Sarah Laszlo, and Wenyao Xu. 2015. Towards EEG biometrics: Pattern matching approaches for user identification. In *IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2015)*. IEEE, 1–6.
[31] Kyeonghye Guk, Gaon Han, Jaewoo Lim, Keunwon Jeong, Taejoon Kang, Eun-Kyung Lim, and Juyeon Jung. 2019. Evolution of wearable devices with real-time disease monitoring for personalized healthcare. *Nanomaterials* 9, 6 (2019), 813.
[32] Selda Güney and Ayten Atasoy. 2012. Multiclass classification of n-butanol concentrations with k-nearest neighbor algorithm and support vector machine in an electronic nose. *Sensors and Actuators B: Chemical* 166 (2012), 721–725.
[33] Andreas T Guntner, Sebastian Abegg, Karsten Konigstein, Philipp A Gerber, Arno Schmidt-Trucksass, and Sotiris E Pratsinis. 2019. Breath sensors for health monitoring. *ACS sensors* 4, 2 (2019), 268–280.
[34] Mohammad Haghighat, Mohamed Abdel-Mottaleb, and Wadee Alhalabi. 2016. Discriminant correlation analysis: Real-time feature level fusion for multimodal biometric recognition. *IEEE Transactions on Information Forensics and Security* 11, 9 (2016), 1984–1996.
[35] Hyonyoung Han, Jun Jo, Youngsung Son, and Junhee Park. 2015. Smart sleep care system for quality sleep. In *2015 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 393–398.
[36] Masaki Hashiyada. 2011. DNA biometrics. In *Biometrics*. IntechOpen.
[37] Chengalvarayan Radhakrishnamurthy Hema, MP Paulraj, and Harkirenjit Kaur. 2008. Brain signatures: a modality for biometric authentication. In *2008 International Conference on Electronic Design*. IEEE, 1–4.

[38] Gabriel Emile Hine, Emanuele Maiorana, and Patrizio Campisi. 2017. Resting-state EEG: A Study on its non-Stationarity for Biometric Applications. In *2017 International Conference of the Biometrics Special Interest Group (BIOSIG)*. IEEE, 1–5.

[39] Barbara J Holtzclaw. 1993. Monitoring body temperature. *AACN Advanced Critical Care* 4, 1 (1993), 44–55.

[40] P Inbavalli and G Nandhini. 2014. Body odor as a biometric authentication. *International Journal of Computer Science and Information Technologies* 5, 5 (2014), 6270–6274.

[41] Mahmoud Z Iskandarani. 2010. A novel odor key technique for security applications using electronic nose system. *American Journal of Applied Sciences* 7, 8 (2010), 1118.

[42] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. Kwak. 2015. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access* 3 (2015), 678–708. https://doi.org/10.1109/ACCESS.2015.2437951

[43] Jawahar Jain, Vatche A Attarian, Sajid Sadi, and Pranav Mistry. 2018. Real time authentication based on blood flow parameters. US Patent App. 15/654,263.

[44] Isuru Jayarathne, Michael Cohen, and Senaka Amarakeerthi. 2016. BrainID: Development of an EEG-based biometric authentication system. In *2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. IEEE, 1–6.

[45] Urmila Kalshetti, Akshay Goel, Prakhar Srivastava, Mayuri Ingole, and Devika Bhide. 2018. Human Authentication from Brain EEG Signals using Machine Learning. *Int. J. Pure Appl. Math* 118 (2018), 1–7.

[46] Prathyusha Kanakam, KCB Rao, and S Mahaboob Hussain. 2015. Olfactory biometric technique: An emerging technology. *Journal of Advancement in Robotics* 1, 1 (2015), 1–11.

[47] Hani Kayyali. 2014. Medical device and method with improved biometric verification. US Patent 8,679,012.

[48] A. M. Khairuddin, K. N. F. Ku Azir, and P. E. Kan. 2017. Limitations and future of electrocardiography devices: A review and the perspective from the Internet of Things. In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*. 1–7. https://doi.org/10.1109/ICRIIS.2017.8002506

[49] Rachel C King, Emma Villeneuve, Ruth J White, R Simon Sherratt, William Holderbaum, and William S Harwin. 2017. Application of data fusion techniques and technologies for wearable health monitoring. *Medical engineering & physics* 42 (2017), 1–12.

[50] Wanzeng Kong, Bei Jiang, Qiaonan Fan, Li Zhu, and Xuehui Wei. 2018. Personal identification based on brain networks of EEG signals. *International Journal of Applied Mathematics and Computer Science* 28, 4 (2018).

[51] Ruggero Donida Labati, Enrique Muñoz, Vincenzo Piuri, Roberto Sassi, and Fabio Scotti. 2019. Deep-ECG: Convolutional neural networks for ECG biometric recognition. *Pattern Recognition Letters* 126 (2019), 78–85.

[52] Chien Le and R Jain. 2009. A survey of biometrics security systems. *EEUU. Washington University in St. Louis* (2009).

[53] Anthony Lee and Younghyun Kim. 2015. Photoplethysmography as a form of biometric authentication. In *2015 IEEE SENSORS*. IEEE, 1–2.

[54] Shuang Leng, Ru San Tan, Kevin Tshun Chuan Chai, Chao Wang, Dhanjoo Ghista, and Liang Zhong. 2015. The electronic stethoscope. *Biomedical engineering online* 14, 1 (2015), 66.

[55] Ching Leng Peter Lim, Wai Lok Woo, Satnam S Dlay, and Bin Gao. 2018. Heartrate-dependent heartwave biometric identification with thresholding-based GMM–HMM methodology. *IEEE Transactions on Industrial Informatics* 15, 1 (2018), 45–53.

[56] Shikang Liu, David Hachen, Omar Lizardo, Christian Poellabauer, Aaron Striegel, and Tijana Milenković. 2018. Network analysis of the NetHealth data: exploring co-evolution of individuals' social network positions and physical activities. *Applied network science* 3, 1 (2018), 45.

[57] André Lourenço, Hugo Silva, and Ana Fred. 2011. Unveiling the biometric potential of finger-based ECG signals. *Computational intelligence and neuroscience* 2011 (2011), 5.

[58] Eduardo José da S Luz, David Menotti, and William Robson Schwartz. 2014. Evaluating the use of ECG signal in low frequencies as a biometry. *Expert Systems with Applications* 41, 5 (2014), 2309–2315.

[59] Lan Ma, James W Minett, Thierry Blu, and William SY Wang. 2015. Resting state EEG-based biometrics for individual identification using convolutional neural networks. In *2015 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. IEEE, 2848–2851.

[60] Vu Mai, Ibrahim Khalil, and Christopher Meli. 2011. ECG biometric using multilayer perceptron and radial basis function neural networks. In *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. IEEE, 2745–2748.

[61] Emanuele Maiorana, Daria La Rocca, and Patrizio Campisi. 2015. On the permanence of EEG signals for biometric recognition. *IEEE Transactions on Information Forensics and Security* 11, 1 (2015), 163–175.

[62] Zijing Mao, Wan Xiang Yao, and Yufei Huang. 2017. EEG-based biometric identification with deep learning. In *2017 8th International IEEE/EMBS Conference on Neural Engineering (NER)*. IEEE, 609–612.

[63] Thomas Martin, Emil Jovanov, and Dejan Raskovic. 2000. Issues in wearable computing for medical monitoring applications: a case study of a wearable ECG monitoring device. In *Digest of Papers. Fourth International Symposium*

on Wearable Computers. IEEE, 43–49.

[64] Mario Merone, Paolo Soda, Mario Sansone, and Carlo Sansone. 2017. ECG databases for biometric systems: A systematic review. *Expert Systems with Applications* 67 (2017), 189–202.

[65] Jermana Moraes, Matheus Rocha, Glauber Vasconcelos, José Vasconcelos Filho, Victor de Albuquerque, and Auzuir Alexandria. 2018. Advances in photopletysmography signal analysis for biomedical applications. *Sensors* 18, 6 (2018), 1894.

[66] Zhendong Mu, Jianfeng Hu, and Jianliang Min. 2016. EEG-based person authentication using a fuzzy entropy-related approach with two electrodes. *Entropy* 18, 12 (2016), 432.

[67] Isao Nakanishi and Masashi Hattori. 2017. Biometric potential of brain waves evoked by invisible visual stimulation. In *2017 International Conference on Biometrics and Kansei Engineering (ICBAKE)*. IEEE, 94–99.

[68] Laurence Richard Olivier. 2018. System and Method for Biometric Identification Using Sleep Physiology. US Patent App. 15/821,206.

[69] Adam Page, Amey Kulkarni, and Tinoosh Mohsenin. 2015. Utilizing deep neural nets for an embedded ECG-based biometric authentication system. In *2015 IEEE Biomedical Circuits and Systems Conference (BioCAS)*. IEEE, 1–4.

[70] Anita Pal, Ajeet Kumar Gautam, and Yogendra Narain Singh. 2015. Evaluation of bioelectric signals for human recognition. *Procedia Computer Science* 48 (2015), 746–752.

[71] Ramaswamy Palaniappan. 2008. Two-stage biometric authentication method using thought activity brain waves. *International journal of neural systems* 18, 01 (2008), 59–66.

[72] RB Paranjape, J Mahovsky, L Benedicenti, and Z Koles. 2001. The electroencephalogram as a biometric. In *Canadian Conference on Electrical and Computer Engineering 2001. Conference Proceedings (Cat. No. 01TH8555)*, Vol. 2. IEEE, 1363–1366.

[73] Chulsung Park, Pai H Chou, Ying Bai, Robert Matthews, and Andrew Hibbs. 2006. An ultra-wearable, wireless, low power ECG monitoring system. In *2006 IEEE Biomedical Circuits and Systems Conference*. IEEE, 241–244.

[74] Koksoon Phua, Jianfeng Chen, Tran Huy Dat, and Louis Shue. 2008. Heart sound as a biometric. *Pattern Recognition* 41, 3 (2008), 906–919.

[75] Sandeep Pirbhulal, Heye Zhang, Subhas Mukhopadhyay, Chunyue Li, Yumei Wang, Guanglin Li, Wanqing Wu, and Yuan-Ting Zhang. 2015. An efficient biometric-based algorithm using heart rate variability for securing body sensor networks. *Sensors* 15, 7 (2015), 15067–15089.

[76] Sandeep Pirbhulal, Heye Zhang, Wanqing Wu, Subhas Chandra Mukhopadhyay, and Yuan-Ting Zhang. 2018. Heartbeats Based Biometric Random Binary Sequences Generation to Secure Wireless Body Sensor Networks. *IEEE Transactions on Biomedical Engineering* 65, 12 (2018), 2751–2759.

[77] Lukasz Piwek, David A Ellis, Sally Andrews, and Adam Joinson. 2016. The rise of consumer health wearables: promises and barriers. *PLoS medicine* 13, 2 (2016), e1001953.

[78] Konstantinos N Plataniotis, Dimitrios Hatzinakos, and Jimmy KM Lee. 2006. ECG biometric recognition without fiducial detection. In *2006 Biometrics symposium: Special session on research at the biometric consortium conference*. IEEE, 1–6.

[79] Paweł Pławiak. 2018. Novel methodology of cardiac health recognition based on ECG signals and evolutionary-neural system. *Expert Systems with Applications* 92 (2018), 334–349.

[80] Norman Poh, Thirimachos Bourlai, Josef Kittler, Lorene Allano, Fernando Alonso-Fernandez, Onkar Ambekar, John Baker, Bernadette Dorizzi, Omolara Fatukasi, Julian Fierrez, et al. 2009. Benchmarking quality-dependent and cost-sensitive score-level multimodal biometric fusion algorithms. *IEEE Transactions on Information Forensics and Security* 4, 4 (2009), 849–866.

[81] Carmen CY Poon, Yuan-Ting Zhang, and Shu-Di Bao. 2006. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine* 44, 4 (2006), 73–81.

[82] Shahrzad Pouryayevali, Saeid Wahabi, Siddarth Hari, and Dimitrios Hatzinakos. 2014. On establishing evaluation standards for ECG biometrics. In *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 3774–3778.

[83] Revathi Rajan, N Fakhuruddin, N Hassan, and MN Islam. 2013. Chemical fingerprinting of human body odor: An overview of previous studies. *Malaysian Journal of Forensic Sciences* 4, 1 (2013), 33–38.

[84] Revathi Rajan, N Fakhuruddin, N Hassan, and MN Islam. 2013. Chemical fingerprinting of human body odor: An overview of previous studies. *Malaysian Journal of Forensic Sciences* 4, 1 (2013), 33–38.

[85] Sofia Najwa Ramli, Rabiah Ahmad, Mohd Faizal Abdollah, and Eryk Dutkiewicz. 2013. A biometric-based security for data authentication in wireless body area network (wban). In *2013 15th International Conference on Advanced Communications Technology (ICACT)*. IEEE, 998–1001.

[86] KC Reshmi, P Ihsana Muhammed, VV Priya, and VA Akhila. 2016. A novel approach to brain biometric user recognition. *Procedia Technology* 25 (2016), 240–247.

[87] Kenneth Revett, Farzin Deravi, and Konstantinos Sirlantzis. 2010. Biosignals for user authentication-towards cognitive biometrics?. In *2010 International Conference on Emerging Security Technologies*. IEEE, 71–76.

[88] Frank Röck, Nicolae Barsan, and Udo Weimar. 2008. Electronic nose: current status and future trends. *Chemical reviews* 108, 2 (2008), 705–725.

[89] Douglas Rodrigues, Gabriel FA Silva, João P Papa, Aparecido N Marana, and Xin-She Yang. 2016. EEG-based person identification through binary flower pollination algorithm. *Expert Systems with Applications* 62 (2016), 81–90.

[90] Sairul I Safie, John J Soraghan, and Lykourgos Petropoulakis. 2011. Electrocardiogram (ECG) biometric authentication using pulse active ratio (PAR). *IEEE Transactions on Information Forensics and Security* 6, 4 (2011), 1315–1322.

[91] Edward Sazonov, Nadezhda Sazonova, Stephanie Schuckers, Michael Neuman, CHIME Study Group, et al. 2004. Activity-based sleep–wake identification in infants. *Physiological measurement* 25, 5 (2004), 1291.

[92] Suranga Seneviratne, Yining Hu, Tham Nguyen, Guohao Lan, Sara Khalifa, Kanchana Thilakarathna, Mahbub Hassan, and Aruna Seneviratne. 2017. A survey of wearable devices and challenges. *IEEE Communications Surveys & Tutorials* 19, 4 (2017), 2573–2620.

[93] Howida AbdelFattah Shedeed. 2011. A new method for person identification in a biometric security system based on brain EEG signal processing. In *2011 World Congress on Information and Communication Technologies*. IEEE, 1205–1210.

[94] Yogendra Narain Singh and Phalguni Gupta. 2011. Correlation-based classification of heartbeats for individual identification. *Soft Computing* 15, 3 (2011), 449–460.

[95] Yogendra Narain Singh and Sanjay Kumar Singh. 2012. Evaluation of Electrocardiogram for Biometric Authentication. *J. Information Security* 3, 1 (2012), 39–48.

[96] Houbing Song, Glenn Fink, and Sabina Jeschke. 2017. *Security and Privacy in Cyber-Physical Systems*. Wiley Online Library.

[97] Sebastijan Šprager, Roman Trobec, and Matjaž B Jurič. 2017. Feasibility of biometric authentication using wearable ECG body sensor based on higher-order statistics. In *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. IEEE, 264–269.

[98] Fahim Sufi, Ibrahim Khalil, and Ibrahim Habib. 2010. Polynomial distance measurement for ECG based biometric authentication. *Security and Communication Networks* 3, 4 (2010), 303–319.

[99] Colin E Sullivan and Christopher Lynch. 1993. Device and method for monitoring breathing during sleep, control of CPAP treatment, and preventing of apnea. US Patent 5,245,995.

[100] Yu Sun and Nitish Thakor. 2015. Photoplethysmography revisited: from contact to noncontact, from point to imaging. *IEEE Transactions on Biomedical Engineering* 63, 3 (2015), 463–477.

[101] Supreeya Swarup and Amgad N Makaryus. 2018. Digital stethoscope: Technology update. *Medical devices (Auckland, NZ)* 11 (2018), 29.

[102] Albert Tarantola. 2005. *Inverse problem theory and methods for model parameter estimation*. Vol. 89. siam.

[103] Paweł Tarnowski, Marcin Kołodziej, Andrzej Majkowski, and Remigiusz Jan Rak. 2018. Combined analysis of GSR and EEG signals for emotion recognition. In *2018 International Interdisciplinary PhD Workshop (IIPhDW)*. IEEE, 137–141.

[104] Kavitha P Thomas and AP Vinod. 2017. Toward EEG-based biometric systems: the great potential of brain-wave-based biometrics. *IEEE Systems, Man, and Cybernetics Magazine* 3, 4 (2017), 6–15.

[105] JA Unar, Woo Chaw Seng, and Almas Abbasi. 2014. A review of biometric technology along with trends and prospects. *Pattern recognition* 47, 8 (2014), 2673–2688.

[106] Jason Van Hulse. 2007. Data quality in data mining and machine learning. (2007).

[107] Saeed V Vaseghi. 2008. *Advanced digital signal processing and noise reduction*. John Wiley & Sons.

[108] Sudip Vhaduri and Christian Poellabauer. 2016. Design and implementation of a remotely configurable and manageable well-being study. In *Smart City 360*. Springer, 179–191.

[109] Sudip Vhaduri and Christian Poellabauer. 2019. Multi-modal Biometric-based Implicit Authentication of Wearable Device Users. *IEEE Transactions on Information Forensics and Security* (2019).

[110] Di Wang, Yujuan Si, Weiyi Yang, Gong Zhang, and Tong Liu. 2019. A Novel Heart Rate Robust Method for Short-Term Electrocardiogram Biometric Identification. *Applied Sciences* 9, 1 (2019), 201.

[111] Jason Webster, Pratistha Shakya, Eamonn Kennedy, Michael Caplan, Christopoher Rose, and Jacob K Rosenstein. 2018. TruffleBot: Low-Cost Multi-Parametric Machine Olfaction. In *2018 IEEE Biomedical Circuits and Systems Conference (BioCAS)*. IEEE, 1–4.

[112] Chatchawal Wongchoosuk, Mario Lutz, and Teerakiat Kerdcharoen. 2009. Detection and classification of human body odor using an electronic nose. *Sensors* 9, 9 (2009), 7234–7249.

[113] Chatchawal Wongchoosuk, Taweesak Youngrod, Hirihattaya Phetmung, Mario Lutz, Theeraporn Puntheeranurak, and Teerakiat Kerdcharoen. 2011. Identification of people from armpit odor region using networked electronic nose. In *2011 Defense Science Research Conference and Expo (DSR)*. IEEE, 1–4.

[114] Jun Xu, Wangpeng An, Lei Zhang, and David Zhang. 2019. Sparse, collaborative, or nonnegative representation: Which helps pattern classification? *Pattern Recognition* 88 (2019), 679–688.
[115] Umang Natubhai Yadav. 2018. *On Establishing PPG Biometrics for Human Recognition: Feasibility and Variability.* Ph.D. Dissertation. Department of Electrical Computer Engineering, University of Toronto.
[116] Bin Yang and Wonjun Lee. 2018. Human Body Odor Based Authentication Using Machine Learning. In *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*. IEEE, 1707–1714.
[117] Zhe Yang, Qihao Zhou, Lei Lei, Kan Zheng, and Wei Xiang. 2016. An IoT-cloud based wearable ECG monitoring system for smart healthcare. *Journal of medical systems* 40, 12 (2016), 286.
[118] Jayasubha Yathav, Abhijith Bailur, AK Goyal, et al. 2017. miBEAT based continuous and robust biometric identification system for on-the-go applications. In *Proceedings of International Conference on Communication and Networks*. Springer, 269–275.
[119] Yuan Zhang, Limin Sun, Houbing Song, and Xiaojun Cao. 2014. Ubiquitous WSN for healthcare: Recent advances and future prospects. *IEEE Internet of Things Journal* 1, 4 (2014), 311–318.
[120] Zhidong Zhao, Qinqin Shen, and Fangqin Ren. 2013. Heart sound biometric system based on marginal spectrum analysis. *Sensors* 13, 2 (2013), 2530–2551.
[121] Guanglou Zheng, Gengfa Fang, Rajan Shankaran, Mehmet A Orgun, Jie Zhou, Li Qiao, and Kashif Saleem. 2016. Multiple ECG fiducial points-based random binary sequence generation for securing wireless body area networks. *IEEE journal of biomedical and health informatics* 21, 3 (2016), 655–663.
[122] Wei Zhou and Selwyn Piramuthu. 2014. Security/privacy of wearable fitness tracking IoT devices. In *2014 9th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE, 1–5.
[123] Alejandro Enrique Flores Zuniga, Khin Than Win, and Willy Susilo. 2010. Biometrics for electronic health records. *Journal of medical systems* 34, 5 (2010), 975–983.