3-2017

A Survey on Modality Characteristics, Performance Evaluation Metrics, and Security for Traditional and Wearable Biometric Systems

Aditya Sundararajan

Arif I. Sarwat

Alexander Pons

A Survey on Modality Characteristics, Performance Evaluation Metrics, and Security for Traditional and Wearable Biometric Systems

ADITYA SUNDARARAJAN, ARIF I. SARWAT, and ALEXANDER PONS, Florida International University

Biometric research is directed increasingly towards Wearable Biometric Systems (WBS) for user authentication and identification. However, prior to engaging in WBS research, how their operational dynamics and design considerations differ from those of Traditional Biometric Systems (TBS) must be understood. While the current literature is cognizant of those differences, there is no effective work that summarizes the factors where TBS and WBS differ, namely, their modality characteristics, performance, security and privacy. To bridge the gap, this paper accordingly reviews and compares the key characteristics of modalities, contrasts the metrics used to evaluate system performance, and highlights the divergence in critical vulnerabilities, attacks and defenses for TBS and WBS. It further discusses how these factors affect the design considerations for WBS, the open challenges and future directions of research in these areas. In doing so, the paper provides a big-picture overview of the important avenues of challenges and potential solutions that researchers entering the field should be aware of. Hence, this survey aims to be a starting point for researchers in comprehending the fundamental differences between TBS and WBS before understanding the core challenges associated with WBS and its design.

1 INTRODUCTION

Biometrics is a field of science which deals with the exploitation of unique, identifiable and quantitatively measurable characteristics of humans in order to authenticate and/or identify them [181].
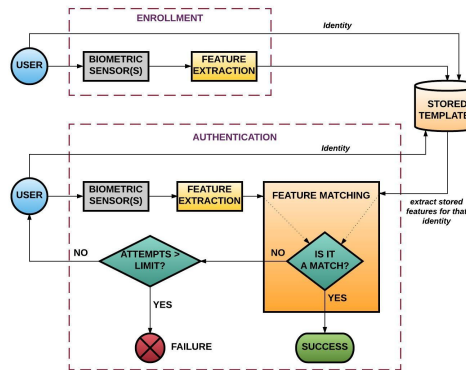
39

Fig. 1. Block diagram for the system model of a typical TBS.

Over the years, pattern recognition and machine learning algorithms have found immense significance in user authentication. A hardware-software-based technology that applies such algorithms to human biometrics for authentication and, more recently, identification, fall under the class called *biometric systems*. Although biometric devices are used more commonly, biometric systems has been used in this paper to emphasize that the scope of study is beyond the physical device itself, and considers communications and other applications that use the data from the individual devices. Traditionally deployed as standalone systems, the biometric systems require separate, mutually exclusive "enrollment" and "authentication" phases [31]. Figure 1 illustrates the system model of *traditional biometric systems (TBS)*. During enrollment, the user registers their traits or "modalities" as a template, created by selecting and extracting specific features from the sample recorded by sensor(s), such that it is enough to uniquely identify that user [192]. Their identity and corresponding template are then stored in the database.

At this point, security of template becomes critical, as they cannot be revoked once the database is compromised. Owing to plenty of additive noise common during measurement, hashing the template is counter-productive [199]. There are many template protection methods like secure sketch schemes whose strength is measured by the average min-entropy of the original template given the secure sketch [200], fuzzy commitment scheme based on binary error-correcting codes [108], and the use of mutual information to measure dishonesty among users [45]. The Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST) recommends standards for biometric data exchange, system accuracy and interoperability [213].

Another class of systems are emerging, referred to in this paper as *wearable biometric systems (WBS)*, which are miniaturized, mobile, flexible, comfortable, less invasive, and aesthetically pleasing. It is worth noting that WBS also come under another broader group, the wearable devices, which also include token and smartcards. However, this paper focuses only on WBS. TBS and WBS ensure user security in different ways.

- TBS consider each modality of the user as a separate entity while WBS consider the entire user (along with all of their individual modalities) as one [152]
- TBS can be optionally connected to the Internet, while WBS are inherently online, exploiting the principles of Internet of Everything (IoE) [178]
- The authentication and identification processes for TBS are static and user-initiated while for WBS are dynamic and autonomous
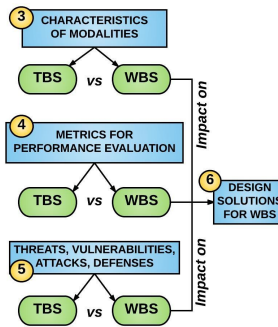
Fig. 2. Flowchart showing the outline of this paper.

- While traditional modalities such as fingerprints, gait, motor, iris, and retina can be integrated into wearables using less-invasive sensors embedded in eyewear, waist-belts, etc., modalities considered invasive in TBS such as ECG, EEG, and Electromyogram (EMG) could be less invasive in WBS domain
- Threats, attacks and defense landscapes for TBS is very different from those for WBS, considering they have different operating dynamics, characteristics and context
- While TBS are widely used in research institutes, hospitals, libraries, airports and universities, WBS currently find their use more in healthcare and personal fitness than in security [129]

It is clear that the future of biometric systems research is geared towards WBS, especially factors like modality characteristics, performance, security and privacy, and how they impact system design and operation. However, prior to looking deeper into this area, it is important to better understand the differences between TBS and WBS highlighted above. To this end, the paper makes the following *three key contributions*: **1)** Summarize and compare TBS and WBS in terms of the factors identified above and discuss how they contribute to the differences listed earlier; **2)** Contribute to the literature by reviewing and summarizing observations of how the modality characteristics, evaluation metrics and security impact the future design solutions for WBS; and **3)** Present important open challenges and future research directions in biometric systems that researchers should pay attention to. Hence, this survey is one of the first efforts in summarizing the research conducted beyond the widely explored TBS, and serves as a strong starting point for researchers entering/in interrelated fields.

The rest of the paper is organized as follows based on the outline illustrated by Figure 2. Section 2 introduces WBS, their system model, and Wireless Body Area Networks (WBANs). It also summarizes various products in the market that leverage the technology. A comprehensive summary of the different key characteristics of various WBS modalities is tabulated and discussed in Section 3. Section 4 reviews various metrics to evaluate the performance of TBS and WBS. Metrics for WBS are summarized in contrast with those of TBS. The threats, attacks and defenses for TBS and WBS are reviewed in Section 5. Attacks are summarized based on whether they target the modality, technology or both to provide a cohesive organization of the literature. Defenses available against the surveyed attacks are also presented. A brief discussion on how the modality characteristics, performance evaluation metrics, security and privacy affect future design solutions for WBS is discussed in Section 6. While Section 7 presents the open research challenges and future directions for research in the area of WBS, Section 8 concludes the survey by summarizing the key findings.

2 WEARABLE BIOMETRIC SYSTEMS (WBS)

Today, wearable applications quantify and personalize every action and movement undertaken by users in order to monitor their health and upgrade their lifestyles. However, in the context of security, the complexity faced by attackers increases multi-fold when such wearable applications are networked to form a WBAN, with many independent, body-friendly and reliably accurate sensors measuring and sharing data to yield a composite template. In tomorrow's fast-paced world where multiple devices are capable of interacting with each other, such dynamic and self-reliant security technologies will be required. Companies like Nymi, Google, Motorola, Apple, and Fitbit are releasing wearable devices like heart-rate monitors, physical fitness trackers, smartwatches, mobile operating systems, assisted living, elder-care, ambient-assisted living, remote automotive and home appliance control, and even navigation control [1, 43]. This implies there is a strong future in WBS security for user authentication and identification.

WBS also double up as "virtual keys" that people use to protect their sensitive assets. Their sensors are tasked with data acquisition, information communication, and decision making with little to no user intervention [118]. Additionally, the nodes of WBS can be implanted, surface-mounted, or even invisible [77]. While surface-mounted WBS are in the form of Smartwatch [122], Fitbit [137], MOTOACTV [4] and Jawbone UP, implanted or embedded WBS have also started making appearances in global markets. Invisible WBS, however, are still nascent in terms of their commercial availability, although two of the leading biometric garment companies, OMSignal and Hexoskin, have launched shirts and garments designed with specially fabricated textiles made of sensors that collect and visualize body statistics in real-time [150]. WBAN is discussed in Section 2.1. Section 2.2 describes the system model for WBS, while Section 2.3 details the products available in the market that use WBS.

2.1 Wireless Body Area Network (WBAN)

A central notion to WBS is WBAN. Wearable sensors, implanted or surface-mounted or invisible, constitute WBAN with a typical range of 1 to 2 meters around the body. WBAN is derived from "Wireless Personal Area Network (WPAN)", a term coined by Zimmerman in 2001 when he studied the effect of electronics brought near human body [221]. With improvements in Microelectromechanical System (MEMS), data analytics and wireless communications, sensors have seen successive improvements with respect to reliability and robustness [130]. The data collected in real-time by these sensors is communicated to a sink, which could be smartphones, Personal Digital Assistants (PDAs) or Personal Computers (PCs). The collected data is fused, processed, and analyzed to offer personalization, authentication and/or identification [63].

Wearable sensors are pervasive in nature. As identified in [59], a pervasive wearable is a colony of biometric sensors, more formally called "passive biometrics" that is unobtrusively measurable (non-invasive) and has maximal independence. They are auto-configured and do not need human intervention during enrollment. However, due to this reason, data collected by them is usually more than that collected by active biometrics like TBS. In addition, passive biometric sensors should be able to discover their peers within the same body, distinguish between those that belong to other bodies in their range, maintain secure communication, and identify the individual to whom they belong. They must also have small size and lean form-factor, and be energy-efficient and independent of positioning with respect to their target organ [79].

A typical WBAN, shown in Figure 3, is an interconnection of multiple independent wearable sensors, each of which measure specific signals from a modality included but not limited to be one of the following: brainwaves associated with stimuli, iris structure [30], retinal patterns [194], vocal resonance while speaking prerecorded phrases [149, 195], skull conduction in response to
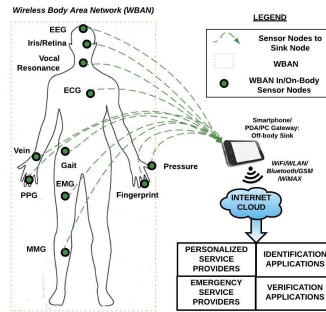
Fig. 3. Block diagram of a typical WBAN with wearable sensor and sink nodes.

audio waves propagating within the head [184], signals from the heart [23, 180], vein pattern on the underside of the skin, gait while walking or striding [64, 81], signals generated by muscles in motion [[201], Mechanomyograph (MMG) signals generated by muscles upon activation [25], fingerprint patterns [57], readings of pressure applied by fingertips when holding objects like pens, car keys, steering wheel, computer mouse, door handle, etc., patterns from signature and body odor [135], and Photoplethysmograph (PPG) denoting the absorption of light through a body part in accordance with heartrate pulses [53, 123].

In WBAN, each sensor is termed a "node". The network itself can be scaled by connecting more nodes on/in the body. These nodes use wireless protocols to communicate among themselves and are coordinated by an on/in-body master "sink", forming a star topology, or communicate among themselves and independently connect to an off-body sink, forming a star-mesh hybrid topology [9, 72, 134, 203]. The protocols for communication between WBAN nodes and sink require low power communication protocols since sensors run on batteries. The IEEE 802.15.6 is considered as the primary standard that defines the Medium Access Control (MAC) architecture for in- and on-body wireless communications [3]. According to the standard, every node and sink has a Physical (PHY) layer (constituting a narrowband, ultra-wideband and human body communication PHY layers) and a MAC sublayer [131]. The MAC Service Data Units (MSDUs) are transferred from the MAC client layer to the MAC sublayer through the MAC Service Access Point (SAP). The MAC frames are then transferred to the PHY layer through the PHY SAP. The reverse happens at the receiving end, which would be a sink in a star topology, or a node/sink in a star-mesh hybrid topology. Network and Application layers provide configuration, routing and management, and functional requirements, respectively [15, 16].

Standard protocols for WBAN MAC communication such as ZigBee-MAC, Baseline-MAC (BMAC), SPARE-MAC, T-MAC and D-MAC have been widely used to implement WBANs, which account for traffic resolution, collision contingencies, energy-saving, auto-configuration, throughput, and delay [113]. MAC layers employ Time Division Multiple Access (TDMA) and its hybrid variants such as λ-MAC, and A-MAC [165, 179]. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) technologies are also used for energy-efficient communication through sleep scheduling, high channel utilization and low latency [188]. A Low-Energy Adaptive Clustering Hierarchy (LEACH) routing protocol was presented to uniformly distribute energy load among WBAN nodes. This method is a significant attempt towards reducing energy dissipation through randomization, and also supports scalability, adaptiveness, and robustness [94]. WBAN communication should be cognizant of electromagnetic wave diffraction due to the continuous absorption and reflection
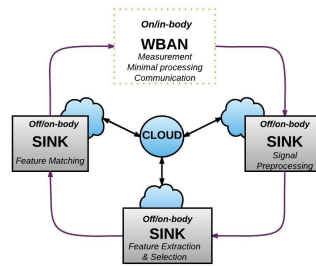
Fig. 4. System model of a typical Wearable Biometric System.

as waves pass through tissues and cells which predominantly contain water. If the sink is located off-body, normal human body movements and posture when stationary would determine the quality of information transmitted. This in-turn determines channel conditions and factors like latency and throughput, which indirectly affect energy consumption [79].

2.2 System Model of WBS

The system model of WBS is shown in Figure 4 is a cyclical "continuous/online" process, where wearables authenticate or identify users not on-demand but continuously. WBS comprise the WBAN represented in Figure 3, the sink, and storage, which may or may not belong to the sink. WBAN is bounded by constraints related to memory for storage and computation, network bandwidth for communication, and energy consumption, among other key factors like interoperability, form factor and bio-friendliness [42]. Some WBANs are also capable of doing minimal signal processing. Sink can be functionally decomposed into a signal preprocessing unit, feature extraction and selection unit, feature matching unit, and optionally a data storage and management unit. In some cases like Fitbit or Google Glass, the sensor and sink nodes are integrated into one device, while the storage and maintenance is pushed to cloud. Signal preprocessing involves operations such as smoothing, interpolation, and normalization. Feature extraction and selection employ standard methods like Principal or Independent Component Analysis (PCA/ICA), Linear Discriminant Analysis (LDA), logistic regression for minimal hardware complexity, and Short Time Fourier Transform (STFT) for minimal memory and computation complexity [40, 163, 189]. Feature matching uses one-class models for authentication and multi-class models for identification based on kNN, Support Vector Machines (SVMs), Bayesian Networks and NaÃŕve Bayes, and Artificial Neural Networks (ANNs) for supervised learning; and Hidden Markov Models (HMMs) and Gaussian Mixture Models (GMMs) for unsupervised learning. Sink-level storage lowers vulnerability to external threats, but limits computational capabilities and increases form factor.

2.3 Products In the Market Using WBS

It was estimated that the market for WBS in sports and healthcare would reach at least 170 million devices by the end of 2017 [5]. WBS use both physical as well as behavioral modalities, defined later in Section 3, where the former are more static and the latter more dynamic. The behavioral modality-based systems employ hand-eye coordinations, user interactions, pressure, tremors, and other finer movements in addition to the modality itself to capture the data needed for authentication. This sophistication can be more easily achieved by WBS than TBS given their mobility and proximity to the human body. Behavioral modalities have also been used in continuous authentication, sometimes with randomized selection of features from a pool to base the analysis

on. For example, EEG-based sensors, which measure stimulus-specific brainwaves to authenticate users, have been of recent interest to the research community, and their application to WBS has attracted decent attention. Below are a few other examples of emerging and recently available products in the market that leverage WBS and mostly behavioral modalities:

(1) **EEG:** It is difficult with today's technological advancement to consider EEG as one of the unobtrusively measurable biometrics, since it needs the user to be stationary and calm, and to wear a head-cap comprising electrodes. However, products developed by Muse and Kokoon can be viewed as a productive step towards realizing EEG-based WBS in the future
  - Muse has developed an application which measures EEG from the user's temples to which its sensors are attached [7]
  - Kokoon provides a set of EEG headphones which measure user's mental state or mood using brainwaves emitted, and accordingly play music [169]

(2) **ECG:** It measures signals emitted by one's heart that are unique to the individual and is more applicable for WBS [187]. Unlike EEG, ECG can be unobtrusively measured using just an electrode attached to the skin
  - Bionym is a company that has developed the Nymi wristband to use heartbeat profiles for uniquely identifying users and improving their lifestyle by personalizing their living environment [1]

(3) **Electromyogram (EMG):** It being leveraged by sports clothing companies, Athos and Myontech, to design sportswear more conducive for superior athletic performance [116]
  - MyoWare has developed a hardware that facilitates the control of video games, robotic movements, and actions of prosthetics based on movement profiles exhibited by the user's motor neurons [38]

(4) **Vocal resonance:** It refers to the voice of a user measured as the vocal sound waves propagate through their body as against traditional voice recognition systems that use the waves captured over air [60]. Placing contact microphones on the neck of the user, the system can unobtrusively measure and model their vocal resonance

(5) **TIAX LLC** has designed and developed wearable sensors and algorithms which can derive vital signs and bio-signatures
  - To facilitate seamless coordination and communication with minimal user intervention, the company has adopted sensor-fusion methods that combine different streams of physiological data such as EEG and ECG, fingerprints, and EMG response
  - The application of learning algorithms for discovering and exploiting unprecedented patterns is also being conducted [95]

(6) In December 2016, **Valencell** and **STMicroelectronics** launched a Scalable Development Kit (SDK) for biometric wearable and Internet of Things (IoT) sensor platform
  - It uses SensorTile of the STMicroelectronics, an IoT sensor module with one STM32L4 microcontroller, a Bluetooth Low Energy chipset, a host of MEMS sensors including accelerometer, magnetometer, pressure and temperature sensors that are both highly accurate as well as energy-efficient, and a digital MEMS microscope [125]
  - It is combined with Valencell's Benchmark biometric sensor system platform, and together enable the development and support of advanced wearable applications, including biometric authentication and identification
  - Valencell has also introduced technologies to measure heart-rate using forearm, and earbud-based sensors for evaluating energy expenditure, net calories burned and maximum oxygen consumption, and magnetic sensors for measuring cadence [74, 75, 120]

(7) **Skull Conduction:** An integrated bone conduction speaker was designed and proposed at the CHI Conference on Human Factors in Computing Systems in May, 2016, where the authors introduced an embedded wearable, SkullConduct, integrated with wearable computers like Google Glass [184]
  - A 1-Nearest Neighbor (1NN) classifier was used in conjunction with Mel Frequency Cepstral Coefficient (MFCC) features to analyze and interpret unique frequency response registered by the skull in response to the propagation of soundwaves within its bone structure
  - It was touted to be stable, universal, collectible, non-invasive and robust. It was proposed both as a verification as well as an identification system

(8) **Signature:** The work focused on using it as a form of identification, where an unknown signature was used as an input to verify if a claimed identity was forged [156]

(9) **Touch:** This work leveraged touch-based behavioral modality and combined it with smart eyewear to conduct continuous user authentication
  - To reduce the invasiveness in authentication, the authors in this work proposed an eyewear that captures user interactions such as single tap, forward, downward and backward swipes, and backward two-finger swipes to perform continuous, online authentication of the user [167]
  - This has been touted to achieve a detection rate of 99% and a false alarm rate of 0.5% under an equal probability of occurrence of all six perceived user events

All of the above applications more often than not consider the use of individual biometrics as wearables, in which case certain significant challenges fail to come to the forefront. However, when a colony of sensors are networked together to constitute a WBAN, security concerns become more pronounced, as will be explored in Section 5.2.

Key Takeaway Points: The following are the key takeaway points from this section:

(1) WBAN is a central component of WBS and has a typical range of 1 to 2 meters around the user's body and comprises multiple sensors that can be implanted, embedded or invisible, each dedicated to unobtrusively and independently measure specific modalities. Such wearables are called passive biometric systems

(2) The nodes of WBAN use wireless protocols to communicate among themselves and are coordinated by an on, in or off-body sink

(3) WBAN communication protocols must account for traffic resolution, collision contingencies, energy-saving, auto-configuration, throughput and delay

(4) WBS system model comprises WBAN, and units for signal preprocessing, feature extraction and selection, feature matching, and cloud-powered data storage and management

(5) There exist multiple WBS products in the market that utilize different modalities, either in isolation or combination, such as EEG, EMG, vocal resonance, fingerprints, skull conduction, signature, PPG, heart-rate, and touch

(6) Some of the forerunner companies that have released WBS products include Google, Fitbit, Nymi, Myontech, Valencell, Apple, Motorola, Muse, Kokoon, TIAX LLC, and MyoWare

3 KEY CHARACTERISTICS OF WBS MODALITIES

Modalities can be categorized in various ways depending on the criteria. For instance, based on their type, they can be classified as physiological (iris, hand, retina, fingerprint, DNA, earlobe, Electrocardiogram (ECG) and odor among others), cognitive (Electroencephalogram [EEG]) and behavioral (signature, keystroke, voice and gait among others) [28, 35]. All of these modalities comprise certain characteristics like *universal*- should be possessed by every person, *unique*- should

distinguish any two individuals, *permanent-* should not be drastically affected by age or fatigue, *collectible-* should easily be acquired by non-invasive means, *acceptable-* should be approved by the public for widespread use, and *circumventive-* should not allow adversaries to easily bypass it [44, 61]. The modality characteristics for TBS was summarized in an earlier work [197].

Ideally, the modalities used by WBS, in addition to the above six characteristics for TBS, must have the following characteristics: **1) Security:** overall confidence that users can invest in the modality against the loss of confidentiality, integrity or availability, **2) Reliability:** extent to which the modality can be trustworthy, **3) Mobility:** extent to which the modality's use does not get impacted by constant or intermittent motion with respect to sink, **4) Variability:** extent to which the above characteristics change with respect to time, **5) Interference:** extent to which the above characteristics get adversely affected by the presence of physical or electromagnetic impediments, and **6) Invasive:** extent to which measurement of the modality creates user discomfort.

The constraints of WBANs like communication latency, throughput and amount of energy consumed, in addition to security and resiliency, can be regarded as factors to determine the characteristics. Table 1 summarizes the different WBS modality characteristics, where each fares differently in satisfying the identified factors. The extent to which each modality contributes to enhance favorable factors (like throughput, goodput, security, resiliency) and reduce unfavorable factors (like energy consumed, latency, size) is used to qualitatively rank their suitability to a particular characteristic: H stands for High suitability, M for Medium and L for Low. As explained earlier in Section 1, the modalities, irrespective of being applied to TBS or WBS, must be unique, universal, permanent, collectible, acceptable and circumventive in nature.

The Table shows how the modalities shown in Figure 2 fare with the key characteristics identified for WBS. It can be inferred that while some modalities fare poorer for certain characteristics when implemented in TBS, they fare better on WBS. For example, iris or retinal pattern might be cumbersome to measure when implemented in TBS since the users are required to place their eye in line and close to the camera. However, the same when implemented in WBS is very easy to measure, considering users can use smart eye-wear like Google Glass to efficiently measure iris structures and even retinal patterns in a less invasive manner.

Key Takeaway Points: The following are the key takeaway points from this section:

(1) Biometric modalities must have six fundamental characteristics. They should be universal, permanent, collectible, unique, acceptable, and circumventive

(2) The modalities used by WBS have additional characteristics: security, reliability, mobility, variability, interference and invasiveness

(3) The constraints of WBANs like communication latency, throughput/goodput, and amount of energy consumed, can be regarded as primary factors that determine the system's operational dynamics

(4) While some modalities fare poorer for certain characteristics when implemented in TBS, they fare better on WBS as they could be easier to measure

(5) Modalities that have a "Low" suitability for a particular characteristic in TBS domain might possess a "High" suitability for the same characteristic in WBS domain, considering the two systems have different operational dynamics

(6) It can, hence, be understood that the operational dynamics identified in point number (3) significantly shape the extent to which the modalities contribute favorably to their different characteristics, thereby showcasing a strong dependency between the two

(7) Between physiological and behavioral modalities, further explained in Section 3, the latter have more dynamism, and hence are better suited for continuous authentication applications that would also not increase the invasiveness or jeopardize the privacy of users

Table 1. Summary of Key Characteristics of Different Modalities for Wearable Biometric Systems

	Vein	Odor	Signature	Fingerprint	Retina	Iris	Face	Gait	Pressure	EMG/MMG	Voice	ECG	EEG	PPG	Skull
Unique	H	M	M	H	H	H	M	M	M	H	M	H	H	H	H
Universal	H	M	L	M	H	H	H	M	M	H	M	H	H	H	H
Permanent	H	M	M	H	H	H	M	M	M	H	M	H	H	H	H
Collectible	H	M	M	H	H	H	M	M	M	H	M	H	H	H	H
Acceptable	H	M	M	H	H	H	M	M	M	H	M	H	H	H	H
Circumventive	H	M	M	H	H	H	M	M	M	H	M	H	H	H	H
Secure	H	M	M	H	H	H	M	M	M	H	M	H	H	H	H
Reliable	H	M	M	H	H	H	M	M	M	H	M	H	H	H	H
Mobile	H	M	M	H	H	H	M	M	M	H	M	H	H	H	H
Variable	H	M	M	H	H	H	M	M	M	H	M	H	H	H	H
Interferential	H	M	M	H	H	H	M	M	M	H	M	H	H	H	H
Invasive	H	M	M	H	H	H	M	M	M	H	M	H	H	H	H

4 PERFORMANCE EVALUATION METRICS FOR TBS AND WBS

Although modalities typically satisfy most characteristics described in Section 2.3, they focus on the modality itself but not on the products that use the modality. Performance is more applicable for products that use biometrics rather than the biometric itself. The characteristics summarized in Table 1 also affect the performance of such technologies. With the integration of high-end data fusion, analytics, processing, and personalization in order to securely authenticate and/or identify users, performance can be considered an important part of evaluating biometric systems.

4.1 Performance Evaluation Metrics for TBS

Evaluating the performance of TBS has been a widely studied topic in literature [8, 70, 85, 89]. A comprehensive summary of different performance evaluation metrics and charts used for TBS was described and summarized in [168]. The work documents that in accordance with the ISO/IEC standard 19795 Parts 1 and 2 for biometric system performance evaluation, multiple metrics are used for verification, such as:

- False Match Rate (FMR): probability of the technology wrongly authenticating an individual claiming to belong to his correct identity
- False Non-Match Rate ($FNMR$): probability of the system wrongly rejecting an individual claiming to belong to his correct identity
- EER or Crossover Error Rate (CER): probability that $FMR = FNMR$ or False Accept Rate (FAR) = False Reject Rate (FRR), where FAR and FRR are system-level errors
- True Acceptance Rate (TAR) which is $1-FRR$; and Weighted Error Rate (WER): the weighted sum of FMR and $FNMR$ [209]

Several curves have also been proposed in order to measure system performance more comprehensively, such as:

- Receiver Operating Characteristic (ROC) which plots $FNMR$, FRR or TAR on Y-axis and FMR or FAR in X-axis
- Detection Error Trade-off (DET) curve which uses nonlinearly scaled axes to show the regions of error rates of interest
- Expected Performance Curve (EPC) which uses a performance criterion like FMR to measure performance in terms of $FNMR$ or vice-versa

The first two curves are a posteriori as the evaluation is dependent on previous knowledge, and the last is a priori since it is independent of prior knowledge. A more comprehensive study was incorporated in [78], where TBS performance evaluation was restructured considering the international Common Criteria (CC) for Information Technology (IT) Security Evaluation and its Common Evaluation Methodology (CEM) guidelines, viewing TBS as IT systems.

This paper classifies TBS into *Verification* and *Identification* systems, the latter focused on determining the identity of an individual who may belong to the database (closed-set) or not (open-set). **Closed-set system performance evaluation** is done using a *Cumulative Match Characteristic (CMC)* curve proposed in [65], mostly used for systems which generate an ordered list of matches between the test subject and existing samples in the database, sorted from most likely to the least. Each of these matches are labeled as a rank. The first match, which is most likely, is called *Rank*-1, followed by the second most likely match labeled as *Rank*-2, and so on. CMC plots probability value on the Y-axis against rank on the X-axis. The probability value for a given rank k, known as "identification rate for rank k", depicts the percentage of time when the system correctly identifies the test individual within the first k ranks. Ideally, the system is expected to identify an individual in the first attempt (first rank). Hence, *Rank*-1 CMC is ideal. However, in real-world conditions, systems tend to have identification rates closer to 1 as the ranks increase. As a measure of performance, the

system whose identification rate hits 1 for the least rank value is deemed to be better. This metric is more widely used for face and iris recognition systems. **Open-set identification** is done using two approaches: exhaustive comparison where the system compares the test sample with all existing samples in the database, and retrieval-based systems where it employs two subsystems for filtering the samples to allow only those with a "score" above the predefined threshold to be considered for the matching process, and the actual matching with test sample. This class of methods consider two more metrics: Detection and Identification Rate (*DIR*), and False Alarm Rate.

4.2 Performance Evaluation Metrics for WBS

The performance of WBS under real-world conditions is more complex to measure owing to multiple external factors which vary with the type of modality, such as ambient noise, distractions, poor connectivity between the sensors and sink, lighting conditions, stress, and anxiety. Hence, most research efforts attempt to quantify their performance under laboratory or experimental conditions, making it idealistic.

Nevertheless, performance evaluation of WBS is very nascent. Metrics identified for TBS such as accuracy, FAR, FRR, ERR, and DIR are also applicable for WBS. However, the term "accuracy" has gained a deeper significance among others in wearable context, where it includes not just accuracy in the measurement of the signals, but also the confidence-level, immunity against external and bodily disturbances, quality of operation among sensors, communication latency and throughput, quality of assurance of results, efficient WBAN management to avoid congestion and collision, and energy consumption rate [6, 13]. In a preliminary survey conducted at the Biometrics Institute Asia Pacific Conference in May, 2016, fifty-four professionals were asked to provide their inputs on the potential applications for WBS, some crucial concerns they saw as hindrances to widespread adoption of the technology, and some potential formats in which they could be made available in the future [12]. This paper utilizes the results from the study to propose more metrics with respect to the components identified in the WBS system model earlier.

In literature, much emphasis has been laid on form factor and size as contributing factors towards achieving optimal or near-optimal performance, considering that the performance of WBS decrease with decreasing form factor. While reduced form-factor could sometimes imply greater comfort for the users, it limits local computation capability, necessitating the use of signal processing, feature extraction and matching to be located external to WBAN. This in-turn exposes the WBS to threats that TBS did not have to deal with. Before reviewing the evaluation metrics, the factors on which wearable performance depend are described below in brief.

(1) **Physiology:** Modalities are sensitive at different levels to different factors such as skin complexion, body shape and size. For example, the level of fat under the skin could affect the measurement of EMG signals, but it might not affect the measurement of a signal like EEG. Similarly, skin complexion could change the level of absorbed light (used by PPG)

(2) **Number and placement of sensors** directly correlates with the quality of signal measurement. Improper placement or implantation of sensors leads to weak or erroneous measurement, affecting quality and accuracy, and hence performance

(3) **Changes induced by mobility:** Quality of operation must not vary beyond an acceptable range when users are subject to movement, including rigorous physical exercise, true especially for ECG, PPG and EEG that are prone to interference with external noise

(4) **Environmental elements:** External noise due to ambient elements could significantly corrupt the measured signals. A technique called Active Signal Characterization (ASC), proposed by Valencell, measures biological, motion, and environmental signals as they come through optical and accelerometer sensors [119]. The required signal is then filtered to remove noise related to motion and other external signals. The separated noise could

be used as supplementary data to deliver crucial insights into the user environment and motion-related features. A preliminary study has also been conducted on PPG [14]

(5) **Crossovers:** Periodic movements made by a body could be mistaken by the system to represent a biometric modality. For example, the step-rate measured during activities like jogging or running could be mistaken for heart-rate and lead to miscalculations or wrongful verification/identification, both which bring down performance

(6) **Performance of the matching classifiers:** Whether one-class or multi-class, feature matching algorithms have their pros and cons with respect to performance. No matter how good a signal measurement, a less accurate classifier with poorly fit model could yield substandard results. The classifier model's performance for skewed training data (classification bias), precision, recall, and F1-score are some additional performance metrics that could be used to indirectly measure WBS performance [147]

(7) **Handling heterogeneity:** There are multiple types of wearable sensors that comprise WBAN, but measurement, signal preprocessing, feature extraction, selection and matching techniques for each of them vary significantly. Hence, the features that extractor and selector models look for also vary. However, in a comprehensive wearable environment, the extractor/selector and matcher are all embedded within a single device. Hence, the models used for performing such tasks must be adaptive to more than one type of signal, and the changing tolerance levels to different signals affects performance

Based on these factors, many performance evaluation metrics have been proposed recently in literature, including some patents [32, 34, 121, 182]. They have all been investigated for healthcare and personal fitness, specifically for PPG. It is noteworthy that, like characteristics, metrics for TBS performance evaluation are also applicable for WBS. Following are the metrics unique to WBS.

- **Accuracy:** Affected by factors 1-7; its calculation could be subjective due to the involvement of many subject-variant factors. Companies such as Valencell have attempted to deliver Precision Wearable Biometrics that account for these factors. Much emphasis has been laid on wearables for healthcare and fitness applications, but not user security

- **Flexibility:** Affected by factors 1, 2, 7; considering the dynamic and highly sensitive nature of WBS, much performance analysis has been typically done through validation testing by classes of users representing different physiologies such as skin tone, complexion and texture, body shape and size, and much more [115]. It has become a common practice employed by most wearable companies prior to releasing products. In other words, the WBS should be flexible enough to be used by majority of the human population

- **Interoperability:** Affected by factors 3, 4, 7; WBS must actively communicate either with other wearables within the same WBAN or to the sink(s). They must not only measure data with good quality, but also transmit them to the sink without losses or corruption. WBAN communication strategies discussed earlier in Section 2.1 provide an insight into the interoperability of WBS

- **Security:** Affected by factors 2, 4, 5; besides lossless and reliable communication, security is also key to performance. Encryption might not be suitable to secure signals from wearable sensors as it demands additional computation power. Efficient resource-aware key management and signal data scrambling methods are two alternatives, where descrambling could be performed by the sink during signal preprocessing

- **Resource allocation:** Affected by 2, 4, 5; prolonged battery life is one of the highly anticipated deliverables for WBS. Hence, the extent to which WBAN nodes manage their computation and communication powers to maximize functioning while minimizing consumption could be a metric for evaluating performance

- **Versatility:** Affected by factors 1-3, 7; it is the extent to which a WBS can be effectively molded into different consumer-friendly forms that encourage longer battery life and reduced form factor. People are fashion-conscious, and hence, WBS must not only be non-invasive and comfortable, but also be elegantly designed with appealing aesthetics in such a way that performance is not hindered
- **Power Consumption:** Affected by factors 2, 4-7; in order to optimize power consumption, the amount of energy expended by sensors for every bit of information could determine their performance [94]. Furthermore, as shown by [51] for Bluetooth-WBAN, synchronization strategies could help improve accuracy and limit unnecessary power consumption, thereby improving overall performance. Wake-up Radios (WURs) were proposed to listen to wireless channels in a power-efficient way through preamble sampling and continuous channel listening [145]
- **Network Efficiency:** Affected by factors 2, 4, 5; optimal use of communication bandwidth is a key concern for nodes within WBAN, between WBAN nodes and sink or, in some cases, between sink and cloud. Since most wearables today use wireless communication like WiFi, Bluetooth and cellular networks, they operate in the same frequency bands as other devices like mobile phones, laptops, and smart home appliances. While temporary solutions such as freeing up more bandwidth, spectrum sharing, and dynamic allocation and deallocation of bandwidth depending on the usage have been implemented, underlying bottlenecks of network congestion, noise, and subsequently performance degradation persist. Visible spectrum was proposed to establish wireless information transfer via Light Emitting Diodes (LEDs) [39]. Multi-tiered network architecture was also proposed, bolstering the emerging fifth generation (5G) mobile-communication systems where there exists one device, known as "seed", that connects to the internet and relays common information to the nodes subscribed to it [97]. Dynamic use of bandwidth can be feasible through the use of Cognitive Radios, which hop into underutilized bandwidths, lowering latency and maximizing performance [92]
- **Spectral Efficiency:** Affected by factors 2, 4, 5; measured in bits/s/Hz, it refers to the extent to which a physical or MAC layer protocol can effectively use the limited frequency spectrum bandwidth available (Hz) to maximize its information rate (bits/s). For WBS, this is very important given their limited resources and bandwidth. Spectral efficiency η has a probable mathematical formulation as shown below, where N_R and N_T are the number of receivers (sink) and transmitters (sensors) respectively; G_{ij} is the goodput (transmission of useful information bits between transmitter i and receiver j per unit time); D_{ij} is distance between transmitter i and receiver j; U_{ij} is mean societal value received by transmitter i from receiver j in return for every bit transmitted, where the societal value includes economic, social and environmental benefits; and A and B are area and bandwidth, respectively, in which transmitter i and receiver j operate [196]:

$$\eta = \sum_{j=1}^{N_R} \sum_{i=1}^{N_T} \frac{G_{ij}D_{ij}U_{ij}}{AB} \tag{1}$$

Key Takeaway Points: The following are the key takeaway points from this section:

(1) TBS performance has been conventionally measured using metrics like FAR, FRR, FMR, FNMR, EER/CER, TAR, ROC, DET, EPC
(2) Although the metrics used to evaluate TBS can be extended to evaluate WBS, the latter have more metrics owing to their differing operational dynamics

(3) Some of the key metrics that can be used to evaluate the performance of WBS include system accuracy, operation flexibility, device and application-level interoperability, systemic security, functional versatility, resource-efficiency, energy-efficiency, network efficiency, and spectral efficiency

(4) WBS performance measured by each of the above metrics is in-turn impacted by one or more of various factors such as physiology, placement and orientation of sensors, external environment, crossovers, system component performance, and heterogeneity in sensing and computation

5 THREATS, ATTACKS AND DEFENSES FOR TBS AND WBS

Before moving ahead, a primer on the terms related to biometric security is briefly presented. A *Threat* is anything that has the potential to inflict serious harm to the technology of concern. A *vulnerability* is a weakness that when successfully exploited manifests the threat into an attack [18]. An *attack vector* is a means by which a malicious entity can compromise a system by exploiting its vulnerabilities for a malicious outcome [183]. An *attack* is the execution of an attack vector by an adversary who successfully exploits a series of vulnerabilities in the concerned domain. A coordinated attack comprises multiple attacks, sequential or parallel, represented using attack vectors that may exploit the same vulnerabilities. An attack is applicable to both TBS as well as WBS in two ways: system attacks that tamper the hardware or firmware, or pattern recognition attacks where the feature extraction and feature matching modules are harmed. While system attacks are applicable to any domain, pattern recognition attacks target feature selection and extraction. It can be said that TBS and WBS are both prone to system attacks, but it is harder to conduct pattern recognition attacks on WBS. However, it is not impossible to do so, as will be discussed in Section 4.

The threats, attacks, and defense landscapes can be categorized for the purposes of this survey into different classes. The first, called *Technology Attack (T)*, considers attacks that exploit vulnerabilities of the system's technology, while the second, called *Modality Attack (M)*, considers attacks that exploit vulnerabilities of biometric modalities used by the technology. When an adversary exploits vulnerabilities of both technology as well as modalities, a *Hybrid Attack (H)* could be realized. These attacks can be applied to both TBS as well as WBS.There are also different *Agents* which enforce a threat into an attack: impostor that deliberately or accidentally pretends to be the authorized entity, attacker that intends to access or compromise the technology with malicious intent, snooper that intends to access or compromise the technology with no malice, and erroneous that compromises the technology accidentally. Sometimes, these agents could also be non-human [18]. Penetration testing is conducted to discover hidden vulnerabilities and establish attack vectors that can then be mitigated [41].

5.1 Threats, Attacks and Defenses for TBS

Figure 5 shows the system model of TBS with different points of attacks, as identified by the different works in literature [21, 66, 153, 166]. In this figure, only the authentication phase of the system is shown, since enrollment is subsumed in the authentication except for the template creation stage, the security-related significance of which was already described in Section 1. Considering how various components interact with each other, a successful attack on one component could pave way for subsequent compromise of other components. It is to be understood that the categorization of attacks described earlier in this section is made with a certain degree of independence between them. For example, a successful Modality attack does not guarantee a successful compromise of the entire system, since the technology might still remain unaffected. Similarly, a Technology attack might be conducted without directly compromising any of the modalities. Those attacks which require to disrupt both technology as well as modality are categorized as Hybrid to avoid any
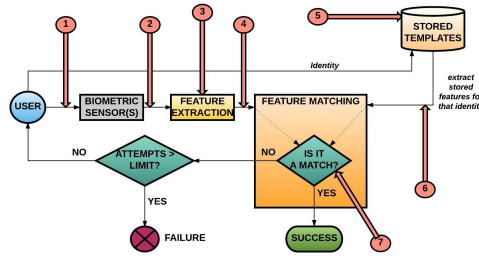
Fig. 5. Block diagram of attack model for TBS.

confusion. While a successful Modality attack affects confidentiality but not necessarily integrity and availability, a successful Technology attack impacts integrity and availability but not necessarily confidentiality. A Hybrid attack compromises all three cornerstones of security.

Table 3 summarizes the attacks, corresponding threats and defenses against them. Analysis of system-specific attacks and defenses have been extensively studied in literature [71, 193].

Table 2. Summary of class-wise TBS threats, attacks and defense mechanisms

Class	Attacks	Threats, Vulnerabilities	Defenses
M [48, 52, 73, 82, 83, 86, 88, 100, 101, 105, 172, 173, 191, 217]	Presentation attack, Collusion, Coercion	Easily reproducible, Poor manual supervision, Poor fault tolerance, Gullible to close relatives, Residuals	Supervised enrollment, PAD, Access controls
Sys [2, 19, 54, 68, 76, 103, 104, 110, 111, 148, 164, 176, 204–206]	Physical tamper, Replay, Man-in-the-Middle, Bad data injection, Template substitute, Template compromise, Denial of Service	Lack of policy enforcements, Sensor memory/ circuit limits, Flaw in sensor software, Poor key management, Weak/no encryption, Vulnerable communication, No perfect forward secrecy, Lack of interoperability between other systems, Susceptibility to Trojan horse, Trade-off between template security and system performance, Storage channel interception, Key discovery	Firewalls, Physical security, Fall-back systems for fault tolerance, Use of Session keys and timestamps, Digital signatures, Random/ cued challenges, Multi-factor authentication, Biometric cryptosystems, Template encryption, Template fusion, One-time biometrics

...continued

Class	Attacks	Threats, Vulnerabilities	Defenses
PR [20, 22, 36, 62, 107, 117, 132, 141, 154, 162, 174, 186, 198, 202, 216, 219]	Characterize feature extractor, Feature replay, Feature correlation, Trojan horse to alter match scores	Known template storage format, Information of data type created by feature extractor, Correlation among features, Matcher and decision-maker program error, Poor exception handling, Missing match upper bounds	Use biometric feature entropy, Revocable biometrics, Feature randomization from multiple input sets, Effective debugging with exhaustive use-case testing, Match-score quantization
H [26, 84, 87, 90, 93, 139, 147, 158, 215]	Buffer Overflow, Enrolling crafted samples to matcher, Hill climbing	Fraud during enrollment	Feature fusion from multiple modalities

5.1.1   M Threats, Attacks and Defenses. This class refers to attacks that exploit the vulnerabilities of the users or their modalities to successfully penetrate into the system. Spoofing or identity (ID) theft is the oldest form of attack (also called a Direct or Presentation Attack) where modalities such as fingerprints, iris, signature and others can be recreated or spoofed using gummy fingers, high resolution color printouts, 3D robotic eyes, and much more [52, 73, 100, 105]. In general, to protect against Class 1 attacks, proper enforcement of enterprise-level security such as access controls must be enabled. Additionally, security policies must be strictly enforced to avoid creating loopholes. Physical hardware of TBS must be capable of working without significant loss of performance in the event of an attack or outage [217]. Targeted direct attacks have lately been minimized by the use of sophisticated sensors equipped with Presentation Attack Detection - PAD (also called live-ness or vitality detection, or anti-spoofing) techniques [48, 82, 83, 86, 88, 101, 172, 173, 191].

5.1.2   Sys Threats, Attacks and Defenses. This class of attacks target the system components by exploiting vulnerabilities at different points identified in the system model (Figure 1) except the feature extractor and matcher: communication channels, modality residuals, and the template storage unit. Two forms of eavesdropping attacks exist. Passive eavesdropping intercepts the vulnerable communication channel between sensor and feature extractor modules but does not alter or steal it; active eavesdropping like Man-in-the-Middle (MITM) and storage channel interception usurp, swap, or corrupt legitimate data to disrupt rightful operation of the system [2]. While only a few employ encryption when sending the captured biometric signals, they do not enforce forward secrecy (a method to ensure the non-compromise of previously secure events even if the current event is compromised) [164]. Attacks and defenses related to biometric templates discussed in Section 1 are applicable here. Since TBS are database-oriented, they need to query the stored template in order to make the comparison, which an attacker could modify. If the encryption is not strong, the attacker can replace the query with malware to corrupt the database [76]. Template swapping is a special case of substitution. It deals with replacing a legitimate template with that of any user, even external to the system [104, 110]. Alternatively, template could be compromised by exploiting weaknesses in the database architecture or schema, enabling the attacker to insert, update or delete templates of legitimate users. DoS can be executed by feeding TBS with an overwhelming number of feature samples through Bad Data Injection (BDI), MITM, or replay [204].

Specific defense mechanisms such as tagging input signals with timestamps and using session keys to ensure forward secrecy have been developed [176]. Template encryption, where secure sketch schemes, homomorphic encryption, and chaotic theory, could be used, considering standard hashing and encryption methods which are applicable for other types of data fail for biometric templates [68, 148]. A modified Hill Cipher algorithm for encryption and a combinatorial Discrete Cosine and Discrete Wavelet Transforms for concealment were proposed that led to an overall improvement in template storage [111]. Templates could be alternatively stored separately on smart cards, backed by biometric cryptosystems. However, this imposes an additional restriction of users having to carry cards all the time and increases the overall system complexity. One-time biometrics deter storage channel interception by using statistical learning to create biometric representations, and then applies chaotic mixing to generate an encrypted template, constituting a self-generated, dynamic helper data [19]. Encrypted template is then decrypted into constituent biometric representations using well-trained Hidden Markov Models (HMMs) and iterative Blind Source Separation before being fed into fuzzy matcher. A multi-factor authentication can also provide defense against MITM attacks by combining modality samples with PINs or passwords [103]. However, such additional authentication mechanisms could prove counterproductive to the reason biometrics were introduced. Biometric cryptosystems, which generate a helper data using a secret key and biometric features, may also be used to prevent MITM attacks [206]. Here, only the helper data, which by itself is useless to an attacker, is stored by the system, while the secret key is reconstructed during authentication using extracted features and helper data [54, 205].

5.1.3   PR Threats, Attacks and Defenses. Attacks on feature extractor and matcher can be regarded mostly as *PR* in nature. Since randomness in modality features is hard to achieve for cryptosystems, fuzzy-based extractors using shielding functions, fuzzy commitment, and fuzzy vault schemes were proposed and applied to the key binding process [107, 117]. However, attacks using feature correlation are shown to significantly reduce performance [219]. If the attacker has prior knowledge about the feature extractor, optimization methods to estimate the unknowns can be devised using the knowns, exploiting statistical dependencies. Further, knowledge of feature extracting algorithms such as PCA and LDA which use the entire biometric sample to construct feature vectors, and Gabor filters and HMMs which select specific features of modalities prior to forming the feature vector, can be used to exploit the correlation between features of modalities that the extractors also use [20]. False Data Injection (FDI) could corrupt extracted features by the addition of random noise or intelligent data. Such attacks could either be aimed at feeding a large number of erroneous feature vectors to the matcher that would increase its FRR beyond acceptable limits, or at manipulating the vector to circumvent or bypass the matcher.

Probable defense mechanisms include measuring feature entropy to gauge the level of uniqueness of the modality and also the strength of cryptosystems for guaranteeing privacy [132]. Cancelable or Revocable biometrics, also referred to as template transformation, distort input features by a specific function by applying Gaussian noise models, and use multiple distorted features for different levels of authentication [154, 174]. They store not the original features but only the distorted ones. However, they have a potential of increasing the system's FRR considering the inherent feature variability among modalities. Feature extractors take this into account using error correction codes, adjustable filters, correlation, or quantization [141, 198, 202, 216]. Alternatively, randomization of biometrics could be used, where multiple samples of a biometric signal is taken (the number of samples varies), and a cumulative average of the samples is used to minimize the intra-class variance [36]. Multimodal feature fusion is also proposed, which differs from revocable biometrics by applying transformations and distortions to a single modality feature set to produce multiple feature vectors. Feature fusion has been successfully applied to feature extractors and

tested for its robustness against various attacks including spoofing and replay of extracted features, and potentially feature correlation attacks [22, 62, 162, 186]. However, practical significance of multi-factor authentication, revocable biometrics and biometric cryptosystems is limited.

5.1.4 H Threats, Attacks and Defenses. Attacks that are a hybrid of *M* and *Sys*: buffer overflow and residuals. Buffer overflow involves a system interacting with an external environment seeking inputs, in this case, the sensor(s) [26]. Flaws in sensor memory allocation protocols could be exploited by such an attack to overwrite codes important for system's rightful operation. System authentication could be bypassed in some cases. Further, residuals (latent fingerprints, signature imprints, or pressure points on specific keys in keystroke recognition systems) can be exploited to conduct replay attacks [87]. A Hill Climbing (HC) attack is a hybrid of *M*, *Sys* and *PR* attacks, made more powerful by Nelder-Mead simplex optimization [158]. It creates an application that sends random templates to the system, disturbed iteratively [84, 147]. The system works by reading output match score and proceeding with perturbed template only after score surpasses the acceptance threshold. Successful applications of HCA to TBS exist in literature [84, 139].

Since HCA targets matching scores of feature matching algorithms, defense mechanisms aim to immunize the matcher. Score-level fusion techniques namely, SVMs, likelihood ratio-based fusion, and sum rule-based method preceded by normalization, were analyzed for their performance and accuracy for multimodal biometric systems comprising fingerprints, face and finger vein [93]. Another contemporary method proposed the use of triangular norms to make score-level fusion faster and computationally efficient, again for multimodal systems [90]. HCA was applied for online signature TBS by modifying initialization, restart and centroid computation steps of traditional Nelder-Mead algorithm. It also proposed a Llyod-Max non-uniform score quantizer to determine quantization levels such that the Mean Square Error (MSE) between original and quantized versions is minimized. Additionally, decision-level template fusion was shown to degrade performance least when compared to fusion at sample, instance, or algorithmic levels [215]. Since matching and decision-making modules of the system contain program codes that have access to crucial parameters besides the match score, like FRR, FAR, FNMR, and EER, ineffective program blocks could be compromised through the use of Trojan horse.

5.2 Threats, Attacks and Defenses for WBS

WBS are associated with a new dimension of threats and vulnerabilities. Figure 6 shows their generic attack model. In WBS domain, Class *M* attacks exploit vulnerabilities of modalities and users, while *Sys* attacks are surveyed under two classes: *Sys-WBAN* and *Sys-Sink*. Attacks on WBAN sensors, intra-body communication, and the communication channel between WBAN and sink come under
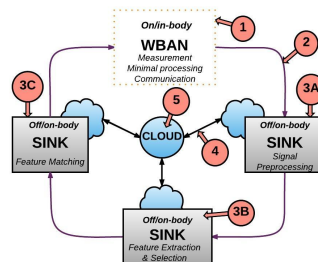

Fig. 6. Block diagram of attack model for WBS.

Sys-WBAN while those that target the sink's signal preprocessing unit, communication between sink and cloud, and cloud storage infrastructure itself. Class *PR* attacks target the sink's feature extraction and selection, and feature matching. Table 3 summarizes threats and vulnerabilities, attacks and corresponding defenses for WBS, organized class-wise.

Table 3. Summary of class-wise WBS threats, attacks and defense mechanisms

Class	Attacks	Threats, Vulnerabilities	Defenses
M [37, 50]	Motion-based keystroke inference, Collusion, Coercion	Poor manual supervision, Poor fault tolerance, Gullible to close relatives, Residuals	Supervised enrollment, PAD, Access controls
Sys-WBAN [27, 46, 49, 109, 142, 160, 161, 185, 208, 208, 214, 220]	Direct attacks, MITM, (D)DoS, Counterfeit sensors, Selective forwarding, Jamming, Brute-force search, Sybil/Wormhole	Sensors transmit only useful information, Difficult policy-making, Expensive to encrypt, Feature entropy, WBAN broadcasting, Noisy network, Half-duplex intra-WBAN communication	Multi-point fuzzy commitment, Cluster-based security, MBStar WBAN topology, Trust-based key management, Elliptic Curve, Cryptography Additional hardware filters, Defensive jamming, Hyper-quiet networks, Tamper-proof sensors, BCC
Sys-Sink [11, 33, 56, 69, 98, 99, 112, 114, 124, 127, 128, 133, 140, 143, 144, 146, 155, 157, 170, 171, 190, 210, 211, 218]	Sniffing, Data misuse by third party, Threats due to third party, Providing false trust credentials, SQL injection, CSRF, Traffic redirection, Malware, Privacy exposure, Session hijack, BDI, JTAG (-R), External device mis-bonding, Side-channel attack	Weak/no WBAN-to-sink authentication, Varied off-body sink network dynamics, Third party encryption, More data logged than revealed, Application of similar security levels for different kinds of data, Sink broadcasts to cloud, TLS could be bypassed, Location-related information storage, Obtrusive authentication, Untrusted applications installed, Vulnerabilities of sink, Weak device-application bonding policies	Cluster-based security, Proximity detection, Mutual authentication, Random challenge/response, Network segmentation, Administration of backups, Dedicated onsite cloud, Careful policy inspection, Data protection, Context-based data security, Trust revocation, HTTPS with SSL, Network segmentation, Data compartmentalization, Symmetric encryption, Timestamps to obfuscate patterns, OS-level device-application bonding

. . . continued

Class	Attacks	Threats, Vulnerabilities	Defenses
PR [58, 106, 207]	Cryptanalytic attacks	Noise/ redundancy in signals, Collection of geolocation and time-synchronized information, Time-variance of signals	Matching-level fusion, Multi-factor authentication, Feature-level fusion, Attribute-based encryption, Case-based reasoning, Spectral analysis of signals

5.2.1 M Threats, Attacks and Defenses. At the modality-level, WBS exhibit slight variations in attack surface than TBS. While direct attacks are possible in WBS too, they are not conducted using shoulder-surfing or spoofing of templates, since WBS employ passive authentication. Hence, such attacks are conducted at the system level (Class *Sys-WBAN*). **Collusion** and **coercion**, however, are still prevalent techniques that employ social engineering skills to deceive a legitimate WBS into authenticating or identifying an attacker. A **motion-based keystroke inference attack** on smartphones was demonstrated by [50], where its feasibility was shown despite the influence of noise, device dimensions and screen orientation. Using Long Short-Term Memory (LSTM) deep neural networks, motion sensors of wearable wristbands like smartwatches could be used to infer keys typed by the owner on other devices like PC or cellphone keypad for spying [37].

5.2.2 Sys-WBAN Threats, Attacks and Defenses. This class of attacks target WBAN and the communication between WBAN and sink. Owing to stringent energy and resource limits, WBAN sensors transmit only useful information, and go through sleep and wakeup cycles to conserve energy, relaying messages through half-duplex wireless broadcasts. By virtue of this, **direct attacks** by eavesdropping are prevalent. Thorough network reconnaissance could make an external wireless node privy to signals being exchanged between sensors, and sometimes even between sensors and sink. Decoded signals could reveal sensitive information that could then be stolen by the adversary, or even modified to make sensors act anomalously, causing life-threatening behaviors. Sometimes, counterfeited sensors could be deployed into WBAN which are prone to **jamming** attack where a malicious node reduces availability by causing collision to each packet of interest [208], **Sybil attack** where a sensor node exhibits dynamic personality by falsely claiming the identities of other surrounding nodes within the same WBAN through impersonation [160], or **wormhole attack** where a sensor node could trick other nodes in the network into thinking it is only a few hops away from them when in reality it could be otherwise, thereby not only confusing the routing algorithms, but also causing more energy and resource consumption [109]. Counterfeited or compromised sensors could also be manipulated to conduct **selective forwarding attacks**, where the node intercepts only specific packets of data but not all, thus prompting re-transfer or restart of packets that in-turn drains energy [49]. Most WBS use Bluetooth, WiFi, and ZigBee for communicating with their sinks [33]. For higher performance and comfort, most commercial WBS transfer sensitive geolocation in clear text, which could be easily intercepted through **brute-force** attacks. Most WBAN-sink communications only employ sink-to-WBAN authentication to minimize the overhead on WBAN. However, this makes the entire communication link vulnerable to **MITM** and **salami thefts**, the latter of which steals small chunks of sensitive data unrecognizable individually but compromises over time. No work in literature has studied the effect of salami attack on WBS, but an assessment of salami attacks and ID thefts on IoT, a superset of WBS, was conducted by [99].

A **multi-point Fuzzy commitment** scheme for key management using ECG was proposed, and its performance evaluated by augmenting Gray coding into its binary encoder and error correcting codes to fine-tune accuracy [46]. A unique **data scrambling** approach using interpolation and

random sampling was also applied instead of conventional symmetric cryptographic techniques. However, the practicality of this strategy in the presence of fading and distortions was only briefly addressed. Another energy-efficient key management and refresh scheme using **multiple clusters** was proposed, which used both predetermined as well randomly generated ECG keys for creating hybrid security [27]. This technique is applicable better to WBANs than data scrambling. A more reliable and secure protocol for the inherent star topology of WBANs was proposed, termed as **MBStar** [220], addressing the problem of long hyper-period communications required by TDMA in the MAC layer under varying schedule profiles by keeping a global hyper-period schedule on the gateway/sink side and assign node-specific local schedules with conflict resolution. It demonstrated co-existence functionalities with other standard protocols like Bluetooth, ZigBee and WiFi. A **trust key management** scheme for WBAN implemented using ECG utilizes ECG to generate symmetric session keys and manage them for end-to-end communication, also between sensors and sink [142]. Some approaches advocate the separation of signal measurement and authentication in sensors, where a separate middle-entity called **Guardian** was proposed for the Implantable Medical Devices (IMDs) scenario to protect against jamming, direct attacks, selective forwarding, and brute-force search through techniques like **defensive jamming** (jamming sensors when communication link is jammed by an attacker) [214]. Some defense methods consider non-Radio Frequency (RF) wireless data communication using **Body Channel Communications** (BCCs), where the human body is converted into a channel/medium to send messages, consuming power less than $1mW$ at rates greater than $100kbps$ [161, 185]. **Hyper-quiet network** principles and network segmentation employ layered architecture for isolating network traffic based on the type of data to be transmitted, thereby lowering network congestion. Although encryption is the most sought solution in networks, it is an expensive feature for WBAN-sink communications, especially with WBAN. Traditional Public Key Infrastructure (PKI) use RSA, but other methods such as **Elliptic Curve Cryptography** (ECC) in conjunction with symmetric encryption have been proposed [127]. In some cases, proximity detection can be used where the distance between WBAN and sink can ascertain whether the signal is fraudulent. However, simple proximity checking might not work in cases where wearables are designed to perform remote services. Hence, **context-aware proximity checking** is needed. **Mutual authentication** could also be used where wearable sensors and sink establish handshake to ensure secure communication channels using Physical Unclonable Function (PUF) that employs challenge-response methods to parry replay attacks [128], and an energy-aware mutual authentication by the use of hash and XOR operations over a star two-tiered topology [98].

5.2.3 Sys-Sink Threats, Attacks, and Defenses. This class targets the sink's signal processing and computation units, cloud, and communication link between sink and cloud. While some WBS feature local storage and processing capabilities, still many others like Google Glass and Fitbit opt for cloud-based data storage and processing. Although loss of privacy and **network impersonation** attacks could be conducted when sink communicates with cloud, **traffic redirection** and **Cross-Site Request Forgery** (CSRF) attacks are also emergent [218]. A greater number of organizations adopt Bring Your Own Device (BYOD) **policies**, where multiple sinks can access similar services offered by the cloud [112]. Multiple applications within a sink can also establish communication with the cloud, creating an environment vulnerable to sniffing or theft of legitimate information. WBS could use Software as a Service (SaaS) cloud platforms, which provide sleek front-end and monitoring features, pushing significant jobs like management, communication, computation, and storage to trusted third parties, thereby raising **privacy** concerns [11]. **Deceptive and ambiguous privacy policies** trap users, allowing parties to sell information they collect to third party-managed databases which might not have strong information security protocols in place. **Session hijacking** attacks (cookie and session thefts, brute-force) that steal sensitive data flowing into the sink have

also been studied [56]. Some WBS applications in the sinks grant permissions to other apps for exchange or access to their information, which could pose a threat for BDI. **Weak bonding policies** between the sink and its apps could pose a significant threat, causing external **device mis-bonding** attack (DMB) [157]. Additionally, **JTAG-Read** (R) and boundary scan based attacks have been shown to access the memory of sinks, and allow adversaries to read the contents in its memory [171]. **Side-channel attacks** such as differential power attack that monitor the power consumption profile of the sink to steal secret keys have also been successfully conducted [114, 140, 146, 155].

Providing **trust-based management** for the transfer and storage of user-sensitive data is a viable addition to secure communication channels [133, 144], as it limits data sharing to between WBAN sensors which have a valid trust in each other. With **trust revocation**, the system maintains a time-variant dynamic trust model, generating flags when one of the sensors has failed to establish trust with any other sensor in the same network. When one sensor is compromised, the trust model altered as a consequence would flag an alert and island that sensor to avoid further compromise [124]. **Compartmentalization** of wearable data has proven to be a good countermeasure against thefts and frauds [190]. Designing wearable applications to store vital information in segregated, encrypted, application-specific chunks restricts data replication. **Data protection** makes sure critical applications run un-preempted, data is securely backed up and recoverable, and allows administrators to map data and information flow between WBANs, sinks and cloud without jeopardizing integrity and privacy [69, 210]. In defense to hijacking, BDI and JTAG-R, data communication and storage protocol using two **pseudo-random numbers** generated through symmetric and secret keys was proposed [170], its implementation focused more on WBS where single-node WBAN and sink nodes are integrated into the same device. To counter DMB attacks, an OS-level protection method called **Dabinder** was proposed to enforce secure bonding policies whenever an app tried to establish Bluetooth connection or pair with the sink [157].

5.2.4 PR Threats, Attacks and Defenses. Most WBS today have feature extractor and matcher modules located in the same device: a separate sink, or wearable itself. Considering, WBS operate in noisy environments where other devices also communicate, signals are prone to noise and interference, which demand more processing from feature extractors and matchers [106]. This is in contrast with TBS that operate in controlled environments. More computation resources increase attack surface, paving way for **cryptanalytic attacks** that target pseudorandom number generators used by encryption methods in WBS [207]. Acoustic key search, electromagnetic attacks, ciphertext, birthday, preimage, and key generation also come under this category.

Defending these attacks ranges from resetting sinks and erasing any trace of stored data, to more advanced methods that look at **match-level fusion** of signals to increase complexity of an attack to demotivate the adversary. Alternatively, extractor and matcher modules could be designed to function in frequency-domain. Since signals measured by wearables are time-variant, they could be directly correlated with owner's activities. Transforming signals into frequency-domain and using **spectral analyses** to operate on the features could make inference less explicit. The viability of **one-step two-factor authentication** scheme was discussed for wearable biosensors in the contexts of keystroke, EEG, hand geometry, and hand gesture [58]. **Case-based reasoning** could be used between extractor-matcher modules and other associated modules of the sinks.

Key Takeaway Points: The following are the key takeaway points from this section:

(1) The literature on threats, attacks and defenses for TBS and WBS can be modality (*M*) or Technology (*T*) attacks, where *T* attacks can be System (*Sys*), Pattern Recognition (*PR*) or Hybrid (*H*) attacks for TBS, and *Sys* could be *Sys-WBAN* and *Sys-Sink* for WBS

(2) All the attacks discussed impact confidentiality, integrity and/or availability of the modality and/or template, and hence the privacy of users

(3) Physical attacks are harder to conduct on WBS than on TBS since the former employ passive authentication and are more complexly networked together

(4) Systemic security measures such as adversarial machine learning and game theory could be used to defensively learn adversary strategies and psychology before proactively resolving the attacks

(5) Most of the attacks that target TBS and WBS tend to indirectly affect their performance, especially factors like energy, network, and spectral efficiencies, and throughput/goodput, which establishes a strong coupling between security concerns and performance

(6) Modality characteristics determine the impact of M attacks while performance metrics determine that of T attacks. Security of TBS, on the other hand, depends on modality, sample measured, template, and feature matching/decision-making

6 FACTORS CONTRIBUTING TO WBS DESIGN SOLUTIONS

Despite numerous WBS products already in the market and many more emerging, the design considerations for WBS is still an evolving subject of research. Many principles impacting WBS design have been identified:[55, 80, 138, 175]

- Human interaction with WBS could be in four ways: audio, visual, tactile and haptic [151]. These interaction modes, which form a fundamental aspect of WBS design solutions, are influenced by different parameters like cognitive ease, cognitive overload, intuitiveness, comprehension and perception

- With the WBS required to be always online and support passive authentication and/or identification, the sensors generate ample amount of data over a given period of time. The WBS design must account for not just data acquisition, but appropriate data management-from sanitation, processing and storage to destruction. Some of the evaluation metric factors discussed earlier like accuracy, energy and network efficiencies, will play key roles in shaping WBS design with respect to its data handling requirements [175]

- Aesthetics have always been at the core of WBS, with designs catering to elegant, fashion-conscious models that are powerful as well as easily wearable [55]. It is a significant consideration, since a good design for WBS is a proper balance between the technology's intelligence and its appearance and user-friendliness

- The different WBS modality characteristics surveyed in Section 3 impact WBS design. This is so, because every modality has its own properties (such as uniqueness, universality, permanence, acceptability and robustness against circumvention), requirements for measurement (such as collectibility, susceptibility to interference from external signals and ambient noise, and invasiveness) and constraints for processing and maintenance (such as security, reliability, mobility and variability). The heterogeneity between different modalities requires WBS design to be tweaked accordingly. For example, a WBS designed to work on EEG might not be a good design for EMG or PPG

- As detailed in Section 4.2, different factors that impact WBS performance also contribute to their design considerations. Physiology, number and placement of sensors, environmental elements, and sensory heterogeneity affect the criteria for WBS designs

- Performance of WBS can be impacted by attacks, which affect security design aspects:
  (1) Attacks that delay or corrupt the data packets within WBAN or WBAN-Sink communication could affect throughput and goodput, an unchecked manipulation of which could result in faulted WBS that could even be life-threatening

(2) The M class attacks have a strong coupling with the modality characteristics like reliability, security and circumvention. They impact confidentiality and integrity of sensitive data. Considering revoking biometrics is impossible (unless revocable technology is fused with the system), a successful compromise can impact the system performance and operations adversely

(3) DoS and other attacks that target the availability of data could drain the battery of WBS or trigger excessive usage of critical resources like network bandwidth, causing WBS to undergo preemptive shutdown that, in certain use-cases, could not only be disruptive to system operation but also be fatal to the owner

(4) It is known that WBS are sensitive to external noises, considering their energy and spectral efficiencies depend on them. However, jamming attacks distort the legitimate signals by adding noise to impact WBS performance

- Many recent works have proposed novel WBS materials: stretchable silicon-based elastomers like polydimethylsiloxane or Ecoflex for substrates and metal-based conductors for electrodes [29]. They exhibit properties like biocompatibility, stretchability, conductivity, malleability, ability to withstand strain and stress, and have a low failure rate

7 OPEN RESEARCH CHALLENGES AND FUTURE DIRECTIONS

WBS have proven their mettle in healthcare and fitness, but their security concerns in these domains as well as when considered solely for authentication and identification purposes have significant rooms for improvement [24, 63, 96, 136, 212]. Specifically, key open research areas in WBS are:

- Evolving security scape: The increased adoption of IoE principles into WBS will continue to push boundaries in terms of signal processing, connectivity, data processing and management, measurement accuracy, convenience and aesthetics, but the constantly evolving nature of attacks will pose a significant and persistent threat to their tech-scape. Recently, the use of blockchain technology to store and analyze WBS data was explored to offer a personalized healthcare for customers [126]. The approach used distributed ledger technology and machine learning to store and access data of users in a secure manner. More work is foreseen in areas that combine data analytics, cyber-physical security, and biometrics

- Changes to business models: With cloud and edge-based decentralized data analytics becoming the norm for WBS, business models and intellectual property must be redefined to adapt and support the relevant advancements in this newly redefined environment. WBS are viewed as one of the first technologies that pave way for a customer-driven market where choices of end-consumers drive the industries

- WBS Big Data: With increasing adoption of WBS by consumers, the number of sensors collectively generating data will increase. Considering a single user can have a WBAN of multiple sensors that are always online and ubiquitously churn new data periodically, significant advances to manage, process and analyze the wealth of raw information in a decentralized manner must be developed. The data thus generated will find multiple uses ranging from consumer analytics to business intelligence and personalization of services

- Newer methods to leverage the power of emerging modalities such as voice, signature, iris and human interactions have recently been explored. Hand-worn devices such as smartwatches and fitness wear have been used to verify signatures and prevent frauds in the financial sector. A study used voice recognition to perform two-factor authentication on WBS [47]. This technology generates speech embedded with a random code that a browser then plays. The signals are then captured by the WBS to perform authentication. Google recently patented an iris scanning contact lens that uses the light reflected by the

iris to perform authentication [10]. These technologies increase the likelihood that the traditionally used modalities will now be exploited to solve the emerging challenges of security and also not jeopardize user privacy and invasiveness

- Revision to policies: With changes in business models, policymaking follows. With consumers demanding greater transparency, end-to-end analytics, peer-to-peer information exchange, localized privacy-aware processing, and much more, restructuring of policies and legislation will be inevitable
- Social behavior and acceptance: WBS are still viewed as invasive technologies by a majority of consumers in the market. Hence, besides revisions to policies, social analytics and acceptance testing through controlled experiments, surveys, interviews, awareness and outreach must be conducted by the companies manufacturing WBS, thereby creating a pipeline to gather consumer information from WBS data for offering personalized services

7.1 WBS Datasets and Access

To further the future research in WBS, data acquisition from different biometric modalities is important. However, setting up devices, recruiting the right mix of participants, and gathering measurements is not an easy task. This is where online data repositories come into importance. These repositories include, but are not limited to, the UCI's Machine Learning Repository, Kaggle, knowledge discovery in datasets, KDNuggets, Wiley online repository, and even research repositories such as the one hosted by the Biometrics Security Lab for the PPG datasets [67, 91, 102].

Although medical professionals have been collecting biometric data over years through clinical trials, experiments, patient examinations and observations, the WBS have increased the rate of data acquisition and the types of data being collected. This opens emerging challenges such as data mining, minimizing signal-to-noise ratio, determining the length and persistence of data collection and storage, respectively, for effective analysis and diagnosis of associated health risks in case of fitness applications and being adaptive to potential consumer preference changes in case of applications of leisure [177]. The lack of proper standardization to ensure data consistency, trust, and integrity in interpretation and analysis is a challenge to gain insights from WBS datasets.

One of the key research gaps identified in [159] is obtaining intelligence for diagnosis from raw WBS data without the involvement of human agents to manually parse and contextualize. Legal, ethical, administrative and technical concerns have been identified as barriers to widespread use of third party data collected by the above sources. The report also identifies the NIST Biometric & Forensic Research Database Catalog that serves as a central repository for publicly available biometric and forensic datasets [17]. Collaborative efforts by the U.S. Military Academy and the Defense Advanced Research Projects Agency (DARPA) have also enabled the process of biometric data measurement and collection, followed by dissemination. Wearable data acquisition and/or access is still an emerging research problem with significant administrative, ethical, legal, and technical implications that must be sorted out.

8 CONCLUSION

One of the important underpinning inferences visible from the emerging research in the area of WBS is that their operational dynamics are different from those of TBS which have been available in the market for a long time. Although the research community is aware of the key differences between the two systems, the factors that contribute to these differences are not well researched, summarized or discussed. To bridge this gap among the recent works of literature, this paper conducts a comprehensive survey on three distinct but interdependent aspects of biometric systems: the characteristics of modalities they use, the metrics used to evaluate their system performance, and their security and privacy. Initially, to help appreciate the differences between TBS and WBS,

the paper reviews and contrasts the above three aspects for both types of biometric systems with equal emphasis. However, given the future research is geared more towards the security and privacy concerns of WBS, the paper highlights how the design solutions to enhance security and privacy are impacted by WBS modality characteristics and performance factors. Thereby, the survey is aimed at not only summarizing, but also using the surveyed results to contribute to the literature a clear understanding of the differences between TBS and WBS, advancements in WBS technology and research, and the factors that impact their security and privacy design. It is inferred that most modalities considered invasive in TBS could be powerful in the wearable environment. WBS require additional metrics to measure their performance owing to their ubiquitous nature, and the landscape of security is often different from that of TBS. In the end, open research challenges and future directions for research in biometric systems was briefly discussed.

REFERENCES

[1] 2001. Nymi White Paper. (mar 2001). Retrieved March, 2017 from https://www.nymi.com/wp-content/uploads/2013/11/NymiWhitePaper-1.pdf
[2] 2007. *M1.4 Ad Hoc Group on Biometric in E-Authentication*. Study Report on Biometrics in E-Authentication. International Committee for Information Technology Standards (ICITS).
[3] 2012. *IEEE Standard for Local and Metropolitan Area NetworksâĂŤPart 15.6: Wireless Body Area Networks. IEEE Standards Association Std, 802.15.6*. IEEE Computer Society.
[4] 2013. *MOTOACTV User Manual*. Motorola Global Portal Archives. Motorola.
[5] 2013. *Performtek Precision Biometrics*. Valencell White Paper. Valencell.
[6] 2014. *Health wearables: Early days*. PwC Report. PwC.
[7] 2014. *Muse Technical Specification Sheet*. InteraXon Technical Report. InteraXon. Retrieved from http://www.choosemuse.com.
[8] 2014. *Understanding Biometric Performance Evaluation*. Precise Biometrics White Paper. Precise Biometrics.
[9] 2015. *IEEE Standard for Low-Rate Wireless Networks: IEEE Standards Association Revision of IEEE Std. 802.15.4-2011*. IEEE Computer Society.
[10] 2015. *Iris-Scanning Contact Lens Patented By Google*. Technical Report. https://www.biometricupdate.com/201701/researchers-authenticate-handwritten-signatures-with-wearables
[11] 2015. *Threat Outlook: Integrity Attacks, Ransomware-as-a-service & Connected Cars*. Threat Intelligence Times Technical Web Article. Threat Intelligence Times.
[12] 2015. Unisys Survey Finds Wearable Technology to Revolutionize Biometrics; Privacy Issues Yet to Be Addressed. (March 2015).
[13] 2015. *Wearables: Driving user outcomes in the Digital Age-the next leap*. PwC Report. PwC.
[14] 2016. *Accuracy in Biometric Wearables*. A Valencell Report. Valencell, Inc.
[15] 2016. *IEEE Standard for Low-Rate Wireless Networks Standard 802.15.4n: Amendment 1: Physical Layer Utilizing China Medical Bands*. IEEE Standards Association.
[16] 2016. *IEEE Standard for Low-Rate Wireless Networks Standard 802.15.4q: Amendment 2: Ultra-Low Power Physical Layer* (2 ed.). IEEE Standards Association.
[17] 2018. NIST Biometric and Forensic Research Database Catalog. (2018). https://tsapps.nist.gov/BDbC/
[18] Fargana Abdullayeva, Yadigar Imamverdiyev, Vugar Musayev, and James Wayman. 2009. *Analysis of Security Vulnerabilities in Biometric Systems*. Danish Biometrics Technical Report. Danish Biometrics. Archived.
[19] Aditya Abhyankar, Shailesh Kulkarni, Rajendra Talware, and Stepahnie Schuckers. 2010. One Time Biometric Transform to secure biometric templates. In *2nd International Conference on Computer and Automation Engineering*. https://doi.org/10.1109/ICCAE.2010.5451900
[20] Andy Adler, Richard Youmaran, and Sergey Loyka. 2009. Towards a Measure of Biometric Feature Information. *Pattern Analysis and Applications* 12, 3 (2009). https://doi.org/10.1007/s10044-008-0120-3
[21] Andy Adlerr. 2008. Biometric System Security. In *Handbook of Biometrics*. Springer, Chapter 19, 381–402.
[22] Zahid Akhtar, Giorgio Fumera, Gian Luca Marcialis, and Fabio Roli. 2012. Evaluation of Multimodal Biometric Score Fusion Rules under Spoof Attacks. In *IAPR International Conference on Biometrics*. IAPR. https://doi.org/10.1109/ICB.2012.6199784
[23] Nazneen Akhter, Sumegh Tharewal, Vijay Kale, Ashish Bhalerao, and K. V. Kale. 2016. *Heart-Based Biometrics and Possible Use of Heart Rate Variability in Biometric Recognition Systems*. Springer. https://doi.org/10.1007/978-81-322-2650-5_2

[24] Samaher Al-Janabi, Ibrahim Al-Shourbaji, Mohammad Shojafar, and Shahaboddin Shamshirband. 2017. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egyptian Informatics Journal* (2017), 10. https://doi.org/10.1016/j.eij.2016.11.001

[25] Mohammed R. Al-Mulla and Francisco Speulveda. 2014. Novel Pseudo-Wavelet Function for MMG Signal Extraction during Dynamic Fatiguing Contractions. *MDPI Sensors* 14 (2014), 15. https://doi.org/10.3390/s140609489

[26] Abdulmonam Omar Alaswad, Ahlal H. Montaser, and Fawzia Elhashmi Mohamad. 2014. An Overview of Face Liveness Detection. *International Journal of Information & Computation Technology* 4, 10 (2014), 9.

[27] Aftab Ali and Farrukh Aslam Khan. 2013. Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications. *EURASIP Journal on Wireless Communications and Networking* (2013).

[28] Md Liakat Ali, John V. Monaco, Charles C. Tappert, and Meikang Qiu. 2016. Keystroke Biometric Systems for User Authentication. *Journal of Signal Processing Systems* 86 (mar 2016), 15. https://doi.org/10.1007/s11265-016-1114-9

[29] Byeong Wan An, Jung Hwal Shin, So-Yun Kim, Joohee Kim, Sangyoon Ji, Jihun Park, Youngjin Lee, Jiuk Jang, Young-Geun Park, Subin Jo Eunjin Cho, and Jang-Ung Park. 2017. Smart Sensor Systems for Wearable Electronic Devices. *MDPI Polymers* (2017), 41. https://doi.org/10.3390/polym9080303

[30] Anderson. 2017. Wearable Retina/Iris Scan Authentication System. (mar 2017).

[31] Siddhesh Angle, Reema Bhagtani, and Hemali Chheda. 2008. Biometrics: A Further Echelon of Security. (2008).

[32] Arxan. 2014. *Precision Wearable Biometrics Provider, Valencell, Selects Arxan to Protect Intellectual Property.* Case Study. Valencell.

[33] Kat Austen. 2015. The Trouble with Wearables. In *Nature.* MacMillan.

[34] Muhammad Awais, Luca Palmerini, Alan K. Bourke, Espen A. F. Ihlen, Jorunn L. Helbostad, and Lorenzo Chiari. 2016. Performance Evaluation of State of the Art Systems for Physical Activity Classification of Older Subjects Using Inertial Sensors in a Real Life Scenario: A Benchmark Study. *MDPI Sensors* (2016). https://doi.org/10.3390/s16122105

[35] Aleksandra Babich. 2012. *Biometric Authentication. Types of Biometric Identifiers.* Master's thesis. Business and Information Technology.

[36] Lucas Ballard, Seny Kamara, Michale K. Reiter, and Fabian Monrose. 2008. Towards Practical Biometric Key Generation with Randomized Biometric Templates. *CCS* (2008). https://doi.org/10.1145/1455770.1455801

[37] Tony Beltramelli. 2015. *Deep-Spying: Spying using Smartwatch and Deep Learning.* Master's thesis.

[38] Lena Berglin. 2011. *Smart Textiles and Wearable Technology âĂŞ A study of smart textiles in fashion and clothing.* The Swedish School of Textiles Technical Report. The Swedish School of Textiles.

[39] M. V. Bhalerao, S. S. Sonavane, and V. Kumar. 2013. A Survey of Wireless Communication using Visible Light. *International Journal of Advances in Engineering & Technology* 5, 2 (2013), 9.

[40] Anna M. Bianchi, Omar P. Villantieri, Martin O. Mendez, and Sergio Cerutti. 2006. Signal Processing and Feature Extraction for Sleep Evaluation in Wearable Devices. In *Proceedings of the 28th IEEE EMBS Annual International Conference.* https://doi.org/10.1109/EMBC.2016.7591487

[41] Battista Biggio, Giorgio Fumera, Paolo Russu, Luca Didaci, and Fabio Roli. 2015. Adversarial Biometric Recognition : A review on biometric system security from the adversarial machine-learning perspective. *IEEE Signal Processing Magazine* 32 (2015), 10. https://doi.org/10.1109/MSP.2015.2426728

[42] Jorge Blasco, Thomas M. Chen, Juan Tapiador, and Pedro Peris-Lopez. 2016. A survey of wearable biometric recognition systems. *Comput. Surveys* 49, 3, Article 43 (2016), 35 pages. https://doi.org/10.1145/2968215

[43] Paolo Bonato. 2005. Advances in wearable technology and applications in physical medicine and rehabilitation. *Journal of Neuro-Engineering and Rehabilitation* 2, 3 (2005). https://doi.org/10.1186/1743-0003-2-2

[44] Nazmeen Boodoo-Jahangeer and Suniduth Baichoo. 2014. Choice of Biometrics. In *IST-Africa 2014 Conference Proceedings.* IIMC International Information Management Corporation. https://doi.org/10.1109/ISTAFRICA.2014.6880618

[45] Xavier Boyen, Yevgeniy Dodis, Jonathan Katz, Rafail Ostrovsky, and Adam Smith. 2005. Secure Remote Authentication Using Biometric Data. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques.* 147–163. https://doi.org/10.1007/11426639_9

[46] Francis Minhthang Bui and Dimitrios Hatzinakos. 2008. Biometric Methods for Secure Communications in Body Sensor Networks: Resource-Efficient Key Management and Signal-Level Data Scrambling. *EURASIP Journal on Advances in Signal Processing* (2008). https://doi.org/10.1155/2008/529879

[47] Chris Burt. 2017. *Researchers authenticate handwritten signatures with wearables.* Biometric Update Online Article. Biometric Update. https://www.biometricupdate.com/201701/researchers-authenticate-handwritten-signatures-with-wearables

[48] Christoph Busch. 2017. *The ISO/IEC Standards for Testing of Presentation Attack Detection.* Technical Report. TTT Working Group Biometrics.

[49] Leela Krishna Bysani and Ashok Kumar Turuk. 2011. A Survey on Selective Forwarding Attack in Wireless Sensor Networks. In *International Conference on Devices and Communications*. https://doi.org/10.1109/ICDECOM.2011.5738547

[50] Liang Cai and Hao Chen. 2012. On the Practicality of Motion Based Keystroke Inference Attack. In *International Conference on Trust and Trustworthy Computing*. https://doi.org/10.1007/978-3-642-30921-2_16

[51] Filippo Casamassima, Elisabetha Farella, and Luca Benini. 2013. Synchronization methods for Bluetooth based WBANs. In *IEEE International Conference on Body Sensor Networks*. IEEE. https://doi.org/10.1109/BSN.2013.6575489

[52] Saptarshi Chakraborty and Dhrubajyoti Das. 2014. An Overview of Face Liveness Detection. *International Journal on Information Theory (IJIT)* 3, 2 (2014).

[53] Samik Chakraborty and Saurabh Pal. 2016. Photoplethysmogram signal based Biometric Recognition using Linear Discriminant Classifier. In *2nd International Conference on Control, Instrumentation, Energy & Communication (CIEC)*. https://doi.org/10.1109/CIEC.2016.7513792

[54] Yao-Jen Chang, Wende Zhang, and Tsuhan Chen. 2004. Biometrics-Based Cryptographic Key Generation. In *IEEE International Conference on Multimedia and Expo*. IEEE.

[55] Huei-Huang Chen, Chien-Hsu, ChenZheng-Yu, and HoeZong-Xian Yin. 2016. Ergonomic Consideration for Wearable Device Design in Frozen Shoulder Rehabilitation. *Advances in Intelligent Systems and Computing* (2016), 10. https://doi.org/10.1007/978-3-319-41694-6_40

[56] Ke Wan Ching and Manmeet Mahinderjit Singh. 2016. Wearable Technology Devices Security and Privacy Vulnerability Analysis. *International Journal of Network Security & Its Applications* (2016). https://doi.org/10.5121/ijnsa.2016.8302

[57] John Chuang. 2014. One-Step Two-Factor Authentication with Wearable Bio-Sensors. In *Symposium on Usable Privacy and Security (SOUPS)*.

[58] John Chuang. 2014. One-Step Two-Factor Authentication with Wearable Bio-Sensors. In *CMU Report.*

[59] Cory Cornelius, Zachary Marois, Jacob Sorber, Ron Peterson, Shirang Mare, and David Kotz. 2012. Passive Biometrics for Pervasive Wearable Devices (Poster Paper). In *Workshop on Mobile Computing Systems and Applications (HotMobile)*. ACM Press, 1.

[60] Cory Cornelius, Zachary Marois, Jacob Sorber, Ron Peterson, Shirang Mare, and David Kotz. 2014. *Vocal Resonance as a Passive Biometric.* Computer Science Technical Report Series 1. Dartmouth College.

[61] 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*. IEEE, 55–67. https://doi.org/10.1145/2594368.2594369

[62] Jia Cui, Jian-Ping Li, and Xiao-Jun Lu. 2008. Study on Multi-Biometric Feature Fusion and Recognition Model. In *International Conference on Apperceiving Computing and Intelligence Analysis*. https://doi.org/10.1109/ICACIA.2008.4769972

[63] Ashraf Darwish and Aboul Ella Hassanien. 2011. Wearable and Implantable Wireless Sensor Network Solutions for Healthcare Monitoring. *MDPI Sensors* 11 (2011), 34. https://doi.org/10.3390/s110605561

[64] Saad M. Darwish. 2016. Design of adaptive biometric gait recognition algorithm with free walking directions. *IET Biometrics journal* (2016). https://doi.org/10.1049/iet-bmt.2015.0082

[65] Brian DeCann and Arun Ross. 2013. Relating ROC and CMC curves via the biometric menagerie. In *IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems*. IEEE. https://doi.org/10.1109/BTAS.2013.6712705

[66] Anthony Delehante. 2011. Security Issues in Biometric Identification. In *University of Minnesota Computer Science Spring Seminar*. Springer.

[67] Dua Dheeru and Efi Karra Taniskidou. 2017. UCI Machine Learning Repository. (2017). http://archive.ics.uci.edu/ml

[68] Michael Dorn, Peter Wackersreuther, and Christian Bohm. 2012. Efficient Comparison of Encrypted Biometric Templates. Springer-Verlag.

[69] Yitao Duan and John Canny. 2005. Protecting User Data in Ubiquitous Computing: Towards Trustworthy Environments. *Privacy Enhancing Technologies* 3424 (2005), 18. https://doi.org/10.1007/11423409_11

[70] Mohammad El-Abed and Christophe Charrier. 2012. Evaluation of Biometric Systems. In *New Trends and Developments in Biometrics*. 149–169. https://doi.org/10.5772/52084

[71] Mohamad El-Abed, Romain Giot, Baptiste Hemery, Jean-Jacques Schwartzmann, and Christophe Rosenberger. 2012. Towards the Security Evaluation of Biometric Authentication Systems. *International Journal of Engineering and Technology* 4 (2012).

[72] Jocelyne Elias and Ahmed Mehaoua. 2012. Energy-aware topology design for wireless body area networks. In *IEEE International Conference on Communications*. https://doi.org/10.1109/ICC.2012.6363949

[73] N. Erdogmus and S. Marcel. 2014. Spoofing Face Recognition with 3D Masks. *IEEE Transactions on Information Forensics and Security* (2014). https://doi.org/10.1109/TIFS.2014.2322255

[74] Chris Eschbach. *Validation and Reliability of PerformTek Earbud Heart Rate Sensor Utilizing 12 Lead ECG*. Valencell White Paper. Valencell.

[75] L. C. Eschbach, S. Long, B. Stillwaggon, and J. A. Bunn. *Applicability of a Forearm-based Biometric Sensor for Measuring Heartrate during Exercise*. Valencell White Paper. Valencell.

[76] Mohammad Esmalifalak, Zhu Han Ge Shi, and Lingyang Song. 2013. Bad Data Injection Attack and Defense in Electricity Market Using Game Theory Study. *IEEE Transactions on Smart Grid* 4, 1 (2013).

[77] Javier Espina. 2014. *Network Topologies, Communication Protocols, and Standards* (2nd. ed.). Springer-Verlag, London. https://doi.org/10.1007/978-1-4471-6374-9

[78] Belen Fernandez-Saavedra, Raul Sanchez-Reillo, Judith Liu-Jimenez, and Oscar Miguel-Hurtado. 2013. Evaluation of biometric system performance in the context of Common Criteria. *Journal of Information Sciences: an International Journal* (2013), 14. https://doi.org/10.1016/j.ins.2013.05.022

[79] Luis Filipe, Florentino Fdez-Riverola, Nuno Costa, and Antonio Pereira. 2015. Wireless Body Area Networks for Healthcare Applications: Protocol Stack Review. *International Journal of Distributed Sensor Networks* (2015). https://doi.org/10.1155/2015/213705

[80] Shaun Fynn. 2014. 10 Considerations for Making Wearable Devices More Wearable. (Feb. 2014). Retrieved November 2017 from http://www.studiofynn.com/journal/10-considerations-making-wearable-devices-more-wearable

[81] Davrondzhon Gafurov, Einar Snekkenes, and Patrick Bours. 2007. Gait Authentication and Identification using Wearable Accelerometer Sensor. In *IEEE Workshop on Automatic Identification Advanced Technologies*. IEEE. https://doi.org/10.1109/AUTOID.2007.380623

[82] Javier Galbally, Julian Fierrez, and Javier Ortega-Garcia. 2007. Vulnerabilities in Biometric Systems: Attacks and Recent Advances in Liveness Detection. In *Spanish Workshop on Biometrics*. Springer, Spain.

[83] Javier Galbally, Marta Gomez-Barrero, Arun Ross, Julian Fierrez, and Javier Ortega-Garcia. 2014. Securing Iris Recognition Systems against Masquerade Attacks. In *Biometric and Surveillance Technology for Human and Activity Identification Proceedings of SPIE*, Vol. 8172. SPIE, London. https://doi.org/10.1117/12.2015690

[84] Javier Galbally, Chris McCool, Julian Fierrez, Sebastian Marcel, and Javier Ortega-Garcia. 2010. On the vulnerability of face verification systems to hill-climbing attacks. *Pattern Recognition* 43, 3 (2010), 11. https://doi.org/10.1016/j.patcog.2009.08.022

[85] Romain Giot, Mohamad El-Abed, and Christophe Rosenberger. 2013. Fast Computation of the performance evaluation of biometric systems: Application to multibiometrics. *Future Generation Computer Systems* (2013), 29. https://doi.org/10.1016/j.future.2012.02.003

[86] Ines Goicoechea-Telleria, Belen Fernandez-Saavedra, Judith Liu-Jimenez, and Raul Sanchez-Reillo. 2016. An Evaluation of Presentation Attack Detection of Fingerprint Biometric Systems Applying ISO/IEC 30107-3. In *International Biometric Performance Conference*. Gaithesburg, MD.

[87] Alex Goldschmidt. 2016. *Intercept-Replay Attack Vulnerabilities and Mitigation Strategies*. ECE Senior Capstone Project 2016 Tech Notes. Tufts University.

[88] Marta Gomez-Barrero, Javier Galbally, Pedro Tome, and Julian Fierrez. 2012. On the Vulnerability of Iris-Based Systems to a Software Attack Based on a Genetic Algorithm. In *CIARP*. Springer-Verlag, London, 114–121.

[89] Dmitry O. Gorodnichy. 2009. Evolution and evaluation of biometric systems. In *IEEE Symposium on Computational Intelligence for Security and Defense Applications*. https://doi.org/10.1109/CISDA.2009.5356531

[90] Madasu Hanmandlu, Jyotsana Grover, Ankit Gureja, , and H. M. Gupta. 2011. Score-level fusion of multimodal biometrics using triangular norms. *Pattern Recognition Letters* (2011).

[91] Dimitrios Hatzinakos and Umang Yadav. 2017. BioSec.Lab PPG Dataset - Benchmark Dataset for PPG Biometrics. (2017). https://www.comm.utoronto.ca/~biometrics/PPG_Dataset/contact.html

[92] Simon Haykin. 2005. Cognitive Radio: Brain-Empowered Wireless Communications. *IEEE Journal on Selected Areas in Communications* 23, 2 (2005). https://doi.org/10.1109/JSAC.2004.839380

[93] Mingxing He, Shi-Jinn Horngg, Pingzhi Fan, Ray-Shine Run, Rong-Jian Chen, Jui-Lin Lai, Muhammad Khurram Khan, and Kevin Octavius Sentosa. 2010. Performance evaluation of score level fusion in multimodal biometric systems. *Pattern Recognition* (2010).

[94] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan. 2000. Energy-Efficient Communication Protocol for Wireless Microsensor Networks. In *Proceedings of the Hawaii International Conference on System Sciences*. https://doi.org/10.1109/HICSS.2000.926982

[95] Charlotte Hill. 2015. *Wearables âĂŞ the future of biometric technology?* Online Magazine 8. Biometric Technology Today.

[96] Katrin HÃďnsel, Natalie Wilde, Hamed Haddadi, and Akram Alomainy. 2015. Challenges with Current Wearable Technology in Monitoring Health Data and Providing Positive Behavioural Support. In *Proceedings of the 5th EAI International Conference on Wireless Mobile Communication and Healthcare*. 4. https://doi.org/10.4108/eai.14-10-2015.

2261601

[97] Ekram Hossain, Mehdi Rasti, Hina Tabassum, and Amr Abdelnasser. 2014. Evolution Toward 5G-Multi-Tier Cellular Wireless Networks: An Interference Management Perspective. *IEEE Wireless Communications* (2014). https://doi.org/10.1109/MWC.2014.6845056

[98] Maged Hamada Ibrahim, Saru Kumari, Ashok Kumar Das, Mohammad Wazid, and Vanga Odelu. 2016. Secure anonymous mutual authentication for star two-tier wireless body area networks. *Computer Methods and Programs in Biomedicine* (2016). https://doi.org/10.10106/j.cmpb.2016.07.022

[99] Assessing Identity Theft in the Internet of Things. 2014. IT CoNvergence PRActice (INPRA). In *Nature*, Vol. 2. 15–21.

[100] ISO-IEC. 2016. *Information Technology – Biometric Presentation Attack Detection Part 1: Framework*. ISO Standard for Biometric Presentation Attack Detection. ISO/IEC 30107-1:2016.

[101] ISO-IEC. 2017. *Information Technology – Biometric Presentation Attack Detection Part 3: Testing and Reporting*. ISO Standard for Biometric PAD. ISO/IEC 30107-3:2017.

[102] Elena S. Izmailova, John A. Wagner, and Eric D. Perakslis. 2018. Wearable Devices in Clinical Trials: Hype and Hypothesis. *Journal of American Society of Clinical Pharmacology and Therapeutics* 104, 1 (2018). https://doi.org/10.1002/cpt.966

[103] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar. 2008. Biometric Template Security: Review Article. *EURASIP Journal on Advances in Signal Processing* (2008). https://doi.org/10.1155/2008/579416

[104] Anil K. Jain, Arun Ross, and Umut Uludag. 2005. Biometric template security: Challenges and solutions. In *13th European Signal Processing Conference*.

[105] Prabhakar Pankanti Jain. 2003. Biometric Recognition: Security and Privacy Concerns. *IEEE Computer Society* (2003).

[106] Adehayo Kolawole John, Adekoya Adewale M., and Ekwonna Chinnasa. 2016. Temperament and Mood Detection Using Case-Based Reasoning. *International Journal of Intelligent Systems and Applications* 3 (2016), 11. https://doi.org/10.5815/ijisa.2014.03.05

[107] Ari Juels and Madhu Sudan. 2002. A Fuzzy Vault Scheme. (2002).

[108] Ari Juels and Martin Wattenberg. 1998. A Fuzzy Commitment Scheme. In *Proceedings of the 6th ACM Conference on Computer and Communications Society*. 28–36. https://doi.org/10.1145/319709.319714

[109] Chris Karlof and David Wagner. 2003. Secure routing in wireless sensor networks: attacks and countermeasures. In *IEEE International Workshop on Sensor Network Protocols and Applications*. https://doi.org/10.1109/SNPA.2003.1203362

[110] Manvjeet Kaur, Dr. Sanjeev Sofat, and Deepak Saraswat. 2010. Template and Database Security in Biometric Systems: A Challenging Task. *International Journal of Computer Applications* 4, 5 (2010).

[111] Emad Taha Khalaf and Norrozila Sulaiman. 2015. A New Secure Storing System for Biometric Templates Based Encryption and Concealment. *Journal of Applied Sciences* (2015). https://doi.org/10.3923/jas.2015.773.782

[112] Arjun Kharpal. 2015. *Biggest Hacking Threat to Business? Wearables*. Technical Web Report. CNBC.

[113] Sarika Khatarkar and Rachana Kamble. 2013. Wireless Sensor Network MAC Protocol: SMAC & TMAC. *Indian Journal of Computer Science & Engineering* 4, 4 (2013).

[114] Paul Kocher, Joshua Jaffe, and Benjamin Jun. 1999. Differential Power Analysis. In *Advances in Cryptology*.

[115] Markos Kos and Iztok Kramberger. 2017. A Wearable Device and System for Movement and Biometric Data Acquisition for Sports Applications. *IEEE Access* (2017). https://doi.org/10.1109/ACCESS.2017.2675538

[116] Nissan Kunju, Neelesh Kumar, Dinesh Pankaj, Aseem Dhawan, and Amod Kumar. 2009. EMG Signal Analysis for Identifying Walking Patterns of Normal Healthy Individuals. *Indian Journal of Biomechanics: Special Issue* (2009).

[117] Maryam Lafikh, Patrick Lacharme, Chsirtophe Rosenberger, Mounia Mikram, and Sanaa Ghouzali. 2015. Vulnerabilities of fuzzy vault schemes using biometric data with traces. In *International Wireless Communications and Mobile Computing Conference*. https://doi.org/10.1109/IWCMC.2015.7289189

[118] Benoit Latre, Bart Braem, Ingrid Moerman, Chris Blondia, and Piet Demeester. 2010. A survey on wireless body area networks. *Journal of Wireless Networks* 17, 1 (Nov. 2010), 18. https://doi.org/10.1007/s11276-010-0252-4

[119] S. Leboeuf. 2016. *Medical Active Signal Characterization Boosts Accuracy of Wearables*. Sensors Online Article. Valencell, Inc.

[120] Steven Francis Leboeuf, Michael E. Aumera, William E. Kraus, Johanna L. Johnson, and Brian Duscha. 2014. Earbud-Based Sensor for the Assessment of Energy Expenditure, HR, and VO2max. *Medicine & Science in Sports & Exercise* 46, 5 (2014). https://doi.org/10.1249/MSS.0000000000000183

[121] Steven Francis LeBoeuf, Jesse Berkley Tucker, Michael Edward Aumer, Eric Douglas Romesburg, and Joseph Norman Morris. 2014. *Apparatus and Methods for Monitoring Physiological data during environmental interference*. Patent. United States Patent Application Publication Number US 8,888,701 B2.

[122] Dan Ledger and Daniel McCaffrey. *Inside Wearables: How the Science of Human Behavior Change Offers the Secret to Long-Term Engagement*. Endeavor Partners LLC Technical White Paper Report. Endeavor Partners LLC.

[123] Anthony Lee and Younghyun Kim. 2015. Photoplethysmography as a form of biometric authentication. *IEEE Sensors* (2015). https://doi.org/10.1109/ICSENS.2015.7370629

[124] Hyun-Ju Lee, Woo-Young Kim, and Ji-Yeon Yoo. 2015. Wearable DevicesâĂŹ Security Risk Analysis and its Counter-measures: Korean cases. *International Journal of Innovative Science, Engineering & Technology* 2, 7 (2015).

[125] Justin Lee. 2015. STMicroelectronics, Valencell launch biometric sensor platform for wearables, IoT. (mar 2015). Retrieved March, 2017 from https://www.biometricupdate.com/201612/stmicroelectronics-valencell-launch-biometric-sensor-platform-for-wearables-iot

[126] Justin Lee. 2017. *University of Surrey testing blockchain for wearable biometric data storage and analysis.* Biometric Update Online Article. Biometric Update. https://www.biometricupdate.com/201705/university-of-surrey-testing-blockchain-for-wearable-biometric-data%e2%80%8e-storage-and-analysis

[127] Young Sil Lee, Esko Alasaarela, and Hoon Jae Lee. 2014. An Efficient Encryption Scheme using Elliptic Curve Cryptography (ECC) with Symmetric Algorithm for Healthcare System. *International Journal of Security and its Applications* (2014). https://doi.org/10.14257/ijsia.2014.8.3.07

[128] Young Sil Lee, Hoon Jae Lee, and Esko Alasaarela. 2013. Mutual Authentication in Wireless Body Sensor Networks (WBSN) based on Physical Unclonable Function (PUF). In *9th International Wireless Communications and Mobile Computing Conference.* https://doi.org/10.1109/IWCMC.2013.6583746

[129] D. C. Leonard, A. Pons, and S. Asfour. 2009. Realization of a Universal Patient Identifier through Biometric Technology. *IEEE Transactions of Biomedicine* 13, 4 (2009).

[130] V. Leonov, P. Fiorini, S. Sedky, T. Torfs, and C. Van Hoof. 2005. Thermoelectric MEMS Generators as a Power Supply for a Body Area Network. In *13th International Conference on Solid-State Sensors, Actuators and Microsystems.* https://doi.org/10.1109/SENSOR.2005.1496414

[131] Miaoxin Li and Mingjie Zhuang. 2012. An Overview of Physical Layers on Wireless Body Area Network. In *International Conference on Anti-Counterfeiting, Security and Identification.* https://doi.org/10.1109/ICASID.2012.6325342

[132] Meng-Hui Lim and Pong C. Yuen. 2016. Entropy Measurement for Biometric Verification Systems. *IEEE Transactions on Cybernetics* 46, 5 (2016). https://doi.org/10.1109/TCYB.2015.2423271

[133] Huang Lin, Xiaoyan Zhu, Y. Fang, Chi Zhang, and Zhenfu Cao. 2011. Efficient Trust Based Information Sharing Schemes over Distributed Collaborative Networks. In *Military Communications Conference âĂŞ Track 3 âĂŞ Cyber Security and Network Operations.* 1399–1403. https://doi.org/10.1109/MILCOM.2011.6127501

[134] M. Lont. 2014. *Wake-up Receiver based Ultra-Low-Power WBAN.* https://doi.org/10.1007/978-3-319-06450-5_2

[135] Panida Lorwongtragool, Enrico Sowade, Natthapol Watthanawisuth, Reinhard R. Baumann, and Teerakiat Kerd-charoen. 2014. A Novel Wearable Electronic Nose for Healthcare Based on Flexible Printed Chemical Sensor Array. *MDPI Sensors* 14 (2014), 12. https://doi.org/10.3390/s141019700

[136] A. Lymberis. 2003. Smart Wearable Systems for Personalised Health Management: Current R&D and Future Challenges. In *Proceedings of the 25th Annual International Conference of the IEEE EMBS.*

[137] Molly Mackinlay. 2013. Phases of Accuracy Diagnosis: (In) visibility of System Status in the Fitbit. *Intersect Stanford University Journals* 6, 2 (2013), 9.

[138] Magpi. 2016. *Big Data and Health.* Technical Magazine. Magpi.

[139] Emanuele Maiorana, Gabriel Emile Hine, and Patrizio Campisi. 2015. Hill-Climbing Attacks on Multibiometrics Recognition Systems. *IEEE Transactions on Information Forensics and Security* (2015). https://doi.org/10.1109/TIFS.2014.2384735

[140] Anindya Maiti, Murtuza Jadliwala, Jibo He, and Igor Bilogrevic. 2015. (Smart)Watch Your Taps: Side-Channel Keystroke Inference Attacks using Smartwatches. In *ISWC.*

[141] Ayodeji S. Makinde, Yaw Nkansah-Gyekye, and Loserian S. Laizer. 2014. Enhancing the Accuracy of Biometric Feature Extraction Fusion Using Gabor Filter and Mahalanobis Distance Algorithm. *International Journal of Computer Science and Information Security* 12, 7 (2014).

[142] Mohammed Mana, Mohammed Feham, and Boucif Amar Bensaber. 2011. Trust Key Management Scheme for Wireless Body Area Networks. *International Journal of Network Security* 12, 2 (2011), 8.

[143] S. S. Manivannan and E. Sathiyamoorthy. 2016. Preventing Health care web applications from session hijack attacks using session key authentication and distributed session ID. *ARPN Journal of Engineering and Applied Sciences* (2016).

[144] R. Manjusha and R. Ramachandran. 2015. Sharing Data in Cloud Based on Trust Attribute Based Encryption (TABE). *ARPN Journal of Engineering and Applied Sciences* 10, 9 (2015), 3. https://doi.org/10.5815/ijisa.2014.03.05

[145] Stevan Marinkovic, Emanuel Popovici, and Emil Jovanov. 2012. Improving Power Efficiency in WBAN Communication Using Wake Up Methods. In *International Conference on Wireless Mobile Communication and Healthcare.* Springer, 303–317. https://doi.org/10.1007/978-3-642-37893-5_34

[146] Thomas Martin, Michael Hsiao, Dong Ha, and Jayan Krishnaswami. 2004. Denial-of-Service Attacks on Battery-powered Mobile Computers. In *Second IEEE International Conference on Pervasive Computing and Communications.*

[147] Ignacio Martin-Diaz, Daniel Morinigo-Sotelo, Oscar Duque-Perez, and Rene De J. Romero-Troncoso. 2016. Advances in Classifier Evaluation: Novel Insights for an Electric Data-Driven Motor Diagnosis. *IEEE Access* 4 (2016), 14. https://doi.org/10.1109/ACCESS.2016.2622679

[148] Garima Mehta, Malay Kishore Dutta, and Pyung Soo Kim. 2016. A Secure Encryption Method for Biometric Templates Based on Chaotic Theory. *Transactions on Computational Science* XXVII (2016). https://doi.org/10.1007/978-3-662-50412-3_8

[149] Abhishek Mitra, Saurabh Bisht, and Vikas Ranjan. 2002. *Voice based Biometric Security System*. Student project report.

[150] Jeffrey Montes. 2015. *Validation and Reliability of the Hexoskin and FitBit Wearable BIO Collection Devices*. Master's thesis. UNLV.

[151] Vivian Genaro Motti and Kelly Caine. 2014. Human Factors Considerations in the Design of Wearable Devices. In *Proceedings of the Human Factors and Ergonomics Society 58th Annual Meeting*.

[152] Judith M. Myerson. 2012. *What Is New? Data Security Management*. AAuerbach Publications, CRC Press, LLC. CRC Press, LLC.

[153] Dellys Hachemi Nabil, Benatchba Karima, Koudil Mouloud, and Bouridane Ahmed. 2013. Threat models on biometri systems: A comparative study. In *Fourth International Conference on Computational Aspects of Social Networks*. https://doi.org/10.1109/CASoN.2012.6412400

[154] Abhishek Nagar, Karthik Nandakumar, and Anil K. Jain. 2010. Biometric Template Transformation: A Security Analysis. In *Proceedings of SPIE 7541, Media Forensics and Security II*. SPIE. https://doi.org/10.1117/12.839976

[155] Ani Nahapetian. 2016. Side-Channel Attacks on Mobile and Wearable Systems. In *13th IEEE Annual Consumer Communications & Networking Conference*.

[156] Ben Nassi, Alona Levy, Yuval Elovici, and Erez Shmueli. 2016. Handwritten Signature Verification Using Hand-Worn Devices. *arXiv* (2016). https://doi.org/arXiv:1612.06305

[157] Muhammad Naveed, Xiaoyong Zhou, Soteris Demetriou, XiaoFeng Wang, and Carl A. Gunter. 2014. Inside Job: Understanding and Mitigating the Threat to External Device Mis-Bonding on Android. *Internet Society* (2014).

[158] J. A. Nelder and R. Mead. 1965. A simplex method for function minimization. *Journal of Computation* (1965).

[159] Caitlin Newark. 2016. *Trends in Biometric Data Collections*. Technical Report. https://www.novetta.com/2016/03/trends-in-biometric-data-collections/

[160] James Newsome, Elaine Shi, Dawn Song, and Adrian Perrig. 2004. The Sybil Attack in Sensor Networks: Analysis & Defenses. In *Third International Symposium on Information Processing in Sensor Networks*. https://doi.org/10.1109/IPSN.2004.239019

[161] Zedong Nie, Yuhang Liu, Changjiang Duan, Zhongzhou Ruan, Jingzhen Li, and Lei Wang. 2015. Wearable Biometric Authentication Based on Human Body Communication. In *12th International Conference on Wearable and Implantable Body Sensor Networks*. https://doi.org/10.1109/BSN.2015.7299362

[162] Ifeoma U. Ohaeri, Michael Esifarienrhe, and Naison Gasela. 2005. Multimodal Biometrics as Attacks Measure in Biometric Systems. In *International Conference in Wireless Networks*.

[163] Adam Page, Siddharth Pramod, Tim Oates, and Tinoosh Mohsenin. 2015. An Ultra Low Power Feature Extraction and Classification System for Wearable Seizure Detection. In *37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. https://doi.org/10.1109/EMBC.2015.7320031

[164] Pascal Paillier. *Paillier Encryption and Signature Schemes*. PEM: Privacy-Enhanced Mail.

[165] Tom Parker, Gertjan Halkes, Maarten Bezemer, and Koen Langendoen. 2010. The ÎžMAC framework: redefining MAC protocols for Wireless Sensor Networks. *Wireless Networks* 16, 7 (2010), 16. https://doi.org/10.1007/s11276-010-0241-7

[166] Imtiaz Parvez, Mahdi Jamei, Aditya Sundararajan, and Arif I. Sarwat. 2014. RSS based Loop-free Compass Routing Protocol for Data Communication in Advanced Metering Infrastructure (AMI) of Smart Grid. In *IEEE Symposium Series on Computational Intelligence*. IEEE. https://doi.org/10.1109/CIASG.2014.7011570

[167] G. Peng, G. Zhou, D. T. Nguyen, X. Qi, Q. Yang, and S. Wang. 2017. Continuous Authentication With Touch Behavioral Biometrics and Voice on Wearable Glasses. *IEEE Transactions on Human-Machine Systems* 47, 3 (June 2017), 404–416. https://doi.org/10.1109/THMS.2016.2623562

[168] N. Poh, C. H. Chan, J. Kittler, Julian Fierrez, and Javier Galbally. 2015. Description of Metrics for the Evaluation of Biometric Performance. (March 2015). Retrieved March, 2017 from http://www.beat-eu.org/

[169] Drew Prindle. 2015. Kokoon EEG Headphones can detect when youâĂŹre in Deep Sleep, Trigger Lucid Dreams. (mar 2015). Retrieved March, 2017 from http://www.digitaltrends.com/cool-tech/kokoon-eeg-headphones/

[170] Mahmudur Rahman, Bogdan Carbunar, and Umut Topkara. 2014. Concise Paper: SensCrypt: A Secure Protocol for Managing Low Power Fitness Trackers. In *IEEE 2nd International Conference on Network Protocols*. https://doi.org/10.1109/ICNP.2014.38

[171] Mahmudur Rahman, Bogdan Carbunar, and Umut Topkara. 2016. Secure Management of Low Power Fitness Trackers. *IEEE Transactions on Mobile Computing* 15, 2 (2016). https://doi.org/10.1109/TMC.2015.2418774

[172] Mahmudur Rahman, Umut Topkara, and Bogdan Carbunar. 2015. Movee: Video Liveness Verification for Mobile Devices using Built-in Motion Sensors. *IEEE Transactions on Mobile Computing* (2015). https://doi.org/1109/TMC.2015.2456904

[173] Raghavendra Ramachandra and Christoph Busch. 2017. Presentation Attack Detection Methods for Face Recognition Systems: A Comprehensive Survey. *Comput. Surveys* 50, 8 (2017). https://doi.org/10.1145/3038924

[174] Christian Rathgeb and Andreas Uhl. 2011. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security* (2011). https://doi.org/10.1186/1687-417X-2011-3

[175] Abhimanyu Rathore. 2015. Wearable and Big Data: Potential Challenges, Potential Rewards. (Aug. 2015). Retrieved November 2017 from http://electronicsofthings.com/expert-opinion/wearable-and-big-data-potential-challenges-potential-rewards/

[176] Alvalapati Goutham Reddy, Ashok Kumar Das, Vanga Odelu, and Kee-Young Yoo. 2016. *An Enhanced Biometric Based Authentication with Key-Agreement Protocol for Multi-Server Architecture Based on Elliptic Curve Cryptography.* ECE Senior Capstone Project 2016 Tech Notes. PLoS One.

[177] Deloitte Technical Report. 2015. *Harnessing safety data from wearable devices.* Technical Report. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lshc-harnessing-safety-data-from-wearable-devices.pdf

[178] ABI Research. 2014. *Internet of Things vs. Internet of Everything: WhatâĂŹs the Difference?* ABI Research Technical Report. ABI Research.

[179] Injong Rhee, Ajit Warrier, Mahesh Aia, Jeongki Min, and Mihail L. Sichitiu. 2008. Z-MAC: A Hybrid MAC for Wireless Sensor Networks. *IEEE/ACM Transactions on Networking* 3, 7 (2008), 16. https://doi.org/10.1109/TNET.2007.900704

[180] Alejandro Riera, Stephen Dunne, Ivan Cester, and Giulio Ruffini. 2011. *STARFAST: a Wireless Wearable EEG/ECG Biometric System based on the ENOBIO Sensor.* Technical Report.

[181] Chris Roberts. 2006. *Biometric Attack Vectors and Defenses.* Danish Biometrics Technical Report. Danish Biometrics. Archived.

[182] Eric Douglas Romesburg. 2015. *Reduction of Physiological Metric Error due to Internal Cadence.* Patent. United States Patent Application Publication.

[183] Markus Schatten, Miroslav Baca, and Mirko Cubrilo. 2009. Towards a General Definition of Biometric Systems. *International Journal of Computer Science Issues (IJCSI)* 2 (2009), 7. https://doi.org/arxiv.org/pdf/0909.2365

[184] Stefan Schneegass, Youssef Oualil, and Andreas Bulling. 2016. SkullConduct: Biometric User Identification on Eyewear Computers using Bone Conduction through the Skull. In *CHI Conference on Human Factors in Computing Systems.* 1379–1384. https://doi.org/10.1145/2858036.2858152

[185] MirHojjat Seyedi, Behailu Kibret, Sravanreddy Salibindla, and Daniel T. H. Lai. 2015. An Overview of Intra-Body Communication Transceivers for Biomedical Applications. In *IGI Global.* IGI. https://doi.org/10.4018/978-1-4666-5888-2.ch045

[186] B. Shanthini and S. Swamynathan. 2012. A Novel Multimodal Biometric Fusion Technique for Security. In *International Conference on Information and Knowledge Management.* IACSIT Press.

[187] Hugo Silva, Andre Lourenco, Filipe Canento, Ana Fred, and Nuno Raposo. 2015. ECG Biometrics: Principles and Applications. In *Proceedings of the International Conference on the Bio-inspired Systems and Signal Processing.* 215–220. https://doi.org/10.5220/0004243202150220

[188] Vinay Singh and Rahul Sharma. 2013. Performance Analysis of Mac Protocols for WBAN on Varying Transmitted Output Power of Nodes. *International Journal of Computer Applications* 67, 7 (2013). https://doi.org/10.5120/11410-6743

[189] Lukas Smital, Clifton Haider, Pavel Leinveber, Pavel Jurak, Barry Gilbert, and David Holmes. 2016. Towards Real-Time QRS Feature Extraction for Wearable Monitors. In *38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society.* https://doi.org/10.1109/EMBC.2016.7591487

[190] Nicko Van Someren. 2015. *3 Tips for Securing Wearable Technology in the Work Place.* Review Article. Wearable Tech.

[191] Ctirad Sousedik and Christoph Busch. 2013. Presentation Attack Detection Methods for Fingerprint Recognition Systems: A Survey. *IET Biometrics* (2013). https://doi.org/10.1049/iet-bmt.2013.0020

[192] Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, and B.V.K. Vijaya Kumar. 1998. Biometric Encryption TM using Image Processing. In *Proceedings of SPIE*, Vol. 3314. San Jose, CA, 422–431. https://doi.org/10.1117/12.304705

[193] Denis Speicher. 2006. *Vulnerability Analysis of Biometric Systems using Attack Trees.* Master's thesis.

[194] Edmund Spinella. 2003. *Biometric Scanning Technologies: Finger, Facial and Retinal Scanning.* SANS Institute InfoSec Reading Room Report. SANS Institute.

[195] Edmund Spinella. 2004. *An Exploration of Voice Biometrics.* SANS Institute InfoSec Reading Room Report. SANS Institute.

[196] Alina Elena Stanciu, Lacramiora-Mihaela Nemtol, and Ilona Madalina Moise. 2012. Considerations regarding the spectral efficiency of orthogonal frequency division multiplexing. In *11th International Conference on Development and*

Application Systems.

[197] Aditya Sundararajan, Alexander Pons, and Arif Sarwat. 2014. A Generic Framework for EEG-Based Biometric Authentication. In *12th International Conference on Information Technology âĂŞ New Generations*. IEEE, 139–144. https://doi.org/10.1109/ITNG.2015.27

[198] Kamil Surmacz, Khalid Saeed, and Piotr Rapta. 2013. An improved algorithm for feature extraction from a fingerprint fuzzy image. *Optica Applicata* XLIII, 3 (2013). https://doi.org/10.5277/oa130311

[199] Yagiz Sutcu, Qiming Li, and Nasir Memon. 2007. Protecting Biometric Templates with Sketch: Theory and Practice. *IEEE Transactions on Information Forensics and Security* 2, 3 (2007).

[200] Yagiz Sutcu, Qiming Li, and Nasir Memon. 2007. *Security and Privacy in Biometrics* (1st. ed.). The name of the series one, Vol. 9. Springer-Verlag London, London, Chapter 4, 69–104. https://doi.org/10.1007/978-1-4471-5230-9_4

[201] Mihai T. Tarata. 2003. Mechanomyography versus Electromyography, in monitoring the muscular fatigue. (2003).

[202] Andrew Beng Jin Teoh and Jaihie Kim. 2015. *Error Correction Codes for Biometric Cryptosystem: An Overview.* ECE Senior Capstone Project 2016 Tech Notes. Yonsie University.

[203] K. M. S. Thotahewa. 2014. *MAC Protocols for UWB-Based WBAN Applications.* Springer. https://doi.org/10.1007/978-3-319-05287-8_2

[204] Zouheir Trabelsi, Mohamed Al Hemairy, and Mohammad M. Masud. 2014. Resilience of Fingerprint and Iris Readers against Common Denial of Service Attacks. In *World Congress on Computer Applications and Information Systems.* https://doi.org/0.1109/WCCAIS.2014.6916542

[205] Pim Tuyls, Anton H. M. Akkermans, Tom A. M. Kevenaar, Geert-Jan Schrijen, Asker M. Bazen, and Raymond N. J. Veldhuis. 2005. Pratical Biometric Authentication with Template Protection. In *International Conference on Audio- and Video-Based Biometric Person Authentication*, Vol. 92. Springer. https://doi.org/10.1007/11527923_45

[206] Umut Uludag, Sharath Pankanti, Salil Prabhakar, and Anil K. Jain. 2010. Biometric Cryptosystems: Issues and Challenges. In *Proceedings of the IEEE*, Vol. 92. IEEE.

[207] John Kelsey Bruce Schneier David Wagner and Chris Hall. 1998. Cryptanalytic attacks on Pseudorandom Number Generators. In *5th International Workshop on Fast Software Encryption.*

[208] Yujie Wang, Liudong Xing, and Honggang Wang. 2016. Reliability modeling of relay-assisted wireless body area networks. In *Annual Reliability and Maintainability Symposium.* https://doi.org/10.1109/RAMS.2016.7447976

[209] James L. Wayman. 1999. Error-Rate Equations for the General Biometric System. In *IEEE Robotics & Automation Magazine.* IEEE.

[210] J. Wei. 2014. How Wearables intersect with the Cloud and the Internet of Things: Considerations for the developers of wearables. *IEEE Consumer Electronics Magazine* 3, 3 (2014), 3. https://doi.org/10.1109/MCE.2014.231789

[211] Bruce R. Wilkins. 2014. *Wearable Technology and Its Associated Security Risk.* Technical Survey Report. ISACA.

[212] Meredydd Williams, Louise Axon, Jason R. C. Nurse, and Sadie Creese. 2016. Protecting User Data in Ubiquitous Computing: Towards Trustworthy Environments. In *IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI).* 6.

[213] Brad Wing. 2014. *Information Technology: American National Standard for Information Systems.* NIST SP-500-290 1.

[214] Fengyuan Xu, Zhengrui Qin, Chiu C. Tan, Baosheng Wang, and Qun Li. 2011. IMDGuard: Securing Implantable Medical Devices with the External Wearable Guardian. In *IEEE INFOCOM*. IEEE. https://doi.org/10.1109/ECRTS.2011.14

[215] Bian Yang, Christoph Busch, Koen de Groot, Haiyun Xu, and Raymond N. J. Veldhuis. 2012. Performance Evaluation of Fusing Protected Fingerprint Minutiae Templates on the Decision Level. *MDPI Sensors* (2012). https://doi.org/10.3390/s120505246

[216] Shenglin Yang and Ingrid Verbauwhede. 2010. Secure Iris Verification. In *IEEE International Conference on Acoustics, Speech and Signal Processing*, Vol. 2. SPIE. https://doi.org/10.1109/ICASSP.2007.366190

[217] Zamboni. 2013. Attacking Biometric Access Control Systems. (March 2013). Retrieved March, 2017 from https://www.defcon.org/images/defcon-13/dc13-presentations/DC_13-Zamboni.pdf

[218] William Zeller and Edward W. Felten. 2008. *Cross-Site Request Forgeries: Exploitation and Prevention.* Technical Report. Princeton University.

[219] Xuebing Zhou, Stephen D. Wolthusen, Christoph Busch, and Arjan Kuijper. 2009. Vulnerabilities of fuzzy vault schemes using biometric data with traces. In *Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing.* https://doi.org/10.1109/IIH-MSP.2009.237

[220] Ziuming Zhu, Song Han, Pei-Chi Huang, Aloysius K. Mok, and Deji Chen. 2011. MBStar: A Real-time Communication Protocol for Wireless Body Area Networks. In *Euromicro Conference on Real-Time Systems.*

[221] Thomas Guthrie Zimmerman. 1995. *Personal Area Networks (PAN): Near-Field Intra-Body Communication.* Master's thesis. Media Arts and Sciences.

Received ; revised ; accepted