Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

A survey on security and privacy issues in wearable health monitoring devices

Bonan Zhang [a,*], Chao Chen [a], Ickjai Lee [b], Kyungmi Lee [b], Kok-Leong Ong [a]

[a] School of Accounting, Information System and Supply Chain, RMIT University, Melbourne, 3000, VIC, Australia
[b] College of Science and Engineering, James Cook University, Townsville, 4811, QLD, Australia

ARTICLE INFO

Keywords:
Wearable devices
Security
Privacy
Survey
Biometric

ABSTRACT

Recent developments in mobile computing power and wireless communication speeds have significantly improved the efficiency of medical systems. This paper focuses on passive wearable sensor devices, which are integral to noninvasive monitoring of physiological data in healthcare observation. Beyond data collection, some wearables play an active role in patient treatment, underscoring the critical importance of protecting their security and privacy. Breach in these areas can severely affect patient health. However, the distinctive characteristics of wearable technologies introduce unique security and privacy challenges, including the potential for unauthorized access to sensitive location, medical, and physiological data. This review delves into the security and privacy concerns associated with wearable devices and proposes potential remedies. Its value lies in providing insights for researchers and manufacturers, aiming to advance the development of safer and more effective wearable medical technologies.

Contents

[*] Corresponding author.
E-mail addresses: bonan.zhang@rmit.edu.au (B. Zhang), chao.chen@rmit.edu.au (C. Chen), Ickjai@jcu.edu.au (I. Lee), joanne.lee@jcu.edu.au (K. Lee), kok-leong.ong2@rmit.edu.au (K.-L. Ong).

https://doi.org/10.1016/j.cose.2025.104453
Received 9 March 2024; Received in revised form 8 January 2025; Accepted 19 March 2025
Available online 28 March 2025

1. Introduction

The invention of wearable devices dates back to 1977, when wearable devices appeared as calculator watches (Mann, 1997). Many head-mounted or wrist-worn devices have also been developed and commercialized since then. However, their adoption has been mainly constrained by their high cost. Fitbit introduced its inaugural pedometer in 2010, featuring functionalities to monitor both steps and heart rate (Kaewkannate and Kim, 2016). Since then, wearable devices have been widely promoted through this inexpensive fitness bracelet and universal smartwatch. Wearable devices are now available for health checks, entertainment, training, and many others. While wearable technologies encompass a wide range of devices, including those that can administer medications or interact with implants, this paper specifically examines passive wearable sensor devices. These devices, which include smart watches, wristbands, smart glasses, smart jewelry, electronic clothing, and skin patches (Iqbal et al., 2021). These devices focus solely on monitoring health metrics such as heart rate and activity levels without direct intervention in medical treatment. Devices like the Apple Watch now offer users a wealth of applications such as taking vital signs, answering calls, NFC payments, navigation, and more. According to forecasts, the wearable device market could reach US$118.16 billion by 2028 (Research, 2018).

A current device that people may be more familiar with than wearable devices is the smartphone, which is currently near saturation in terms of penetration. Smartphones generally have more computing power and can offer more features than other general wearable devices. However, wearable devices have advantages that smartphones lack, along with irreplaceable functions in the medical field. The first is that wearable devices generally have a variety of built-in sensors, including acceleration, gyroscopes, infrared, and temperature sensors (Ates et al., 2022). These sensors allow wearable devices to measure the user's physical health, offering an opportunity to improve the quality of life. The second characteristic is 'wearable,' indicating that the user remains in constant contact with the device, thereby enabling ongoing monitoring of the user's physical health. Wearable devices have the capability to autonomously alert a physician or emergency responders when there is a significant alteration in the user's health status or if the user is in danger. If the device includes an integrated GPS sensor, it can deliver an exact location to rescue personnel, thereby ensuring the safety of the user. The final point is that wearable devices can guide the long-term treatment of patients. According to the World Health Organization, chronic diseases account for three quarters of all deaths worldwide and place a high economic burden on countries and societies (Who and Consultation, 2003). Hence, wearable devices can play an important role in the management of chronic diseases. For example, doctors can formulate personalized treatment plans for patients through telehealth consultations (Dinesen et al., 2016). These benefits of wearable devices have led to their widespread use in the medical field. Our survey will focus on these wearable devices that can be used in the medical field.

While the always-on capability of wearable devices undeniably contributes significantly to patient recovery and life safety, it simultaneously presents several security and privacy concerns. For example, some companies have banned employees from using Google glasses due to privacy concerns. This is due to the possibility that the glasses' front camera could be continuously active, potentially resulting in the inadvertent disclosure of confidential company information and the privacy of individuals. In addition, many wearable devices collect physiological information about a user for analysis. The data collected by the device may even include the biometric information of the user (Martin et al., 2000). Malicious individuals have the potential to distort these data or expose confidential details about the user (Yaqoob et al., 2019). In this paper, we restrict our security analysis to wearable sensor devices that do not actively intervene in medical treatments. Such devices primarily collect and transmit data, thus requiring security measures against unauthorized data access and ensuring data integrity, without the complications introduced by devices that deliver medications or alter the function of implanted devices. This survey focuses on the security and privacy issues currently faced by medical wearables and the solutions available. We also discuss possible future research directions for the next generation of wearable health monitoring devices in terms of security.

To our knowledge, this is the first survey on the security and privacy issues of wearable health monitoring devices. Some previous work has looked at particular aspects of wearable-related devices. Khan et al. (2020) provided an overview of current biometric applications and developments in wearable devices. Blasco et al. (2016) also focused on the different biometric technologies among the wearable devices. Some studies have focused on applications for specific scenarios, for example, health monitoring and prognosis recovery (Pantelopoulos and Bourbakis, 2009, 2008; Baig et al., 2013), gait recognition (Marsico and Mecca, 2019), and gesture recognition (Chen et al., 2020). Mosenia et al. (2017) presented the goals and challenges of designing wearable devices for medical use. Seneviratne et al. (2017) concentrated on the design and challenges of the wearable devices that consumers use every day. Shrestha and Saxena (2017)'s survey focused on all types of wearable devices, instead of medical wearables. The focus of the Pourbemany et al. (2023), Gomes et al. (2023) and Jin et al. (2022)'s survey is all on one point in the functionality of the wearable device and does not provide a comprehensive discussion of the

Table 1
Comparison among our survey and existing surveys.

Ref	Components of healthcare system	Focus on Wearable devices	Security and privacy goals	Attack Taxonomy	Solution Taxonomy	Existing Solutions
Khan et al. (2020)	◐	◐	◐	○	○	◐
Blasco et al. (2016)	◐	●	○	○	○	◐
Pantelopoulos and Bourbakis (2009)	●	●	◐	○	○	◐
Pantelopoulos and Bourbakis (2008)	●	●	○	○	○	◐
Baig et al. (2013)	●	◐	◐	○	○	◐
Marsico and Mecca (2019)	●	●	◐	○	◐	◐
Chen et al. (2020)	◐	◐	○	○	◐	◐
Mosenia et al. (2017)	●	●	◐	●	●	◐
Seneviratne et al. (2017)	◐	●	◐	○	●	◐
Shrestha and Saxena (2017)	◐	●	●	●	●	◐
Jin et al. (2022)	◐	●	◐	○	○	◐
Pourbemany et al. (2023)	●	●	○	○	○	○
Our survey	●	●	●	●	●	●

● = Complete information provided, ◐ = Partial information provided, ○ = No information provided.

security and privacy issues of the various features of the wearable device. In contrast, in this survey we focus on the current security and privacy challenges facing wearable health monitoring devices, existing solutions, and potential future research directions.

The purpose of this survey is to provide researchers with a comprehensive overview of security and privacy trends in wearable health monitoring devices, as well as future directions and challenges in the field. It will give the reader an appreciation of the field and the background to contribute to its development. Table 1 lists the main existing surveys in the field, clearly demonstrates a gap in the literature, and illustrates the unique contributions of this survey. The contributions of this work are listed below.

- First, we provide a detailed overview of existing medical wearables, including their classification and sensor composition;
- Second, we explore the current wearable devices' security and privacy needs and the current challenges;
- Finally, we synthesized our findings and share our view of the future research directions in the area of security and privacy for wearable devices.

The remainder of the paper is organized as follows. Section 2 introduces the preliminaries of the security and privacy issue in wearable health monitoring devices. In Section 3, we summarize the current security and privacy challenges of wearable devices. In Section 4, we introduce the recent security issue in wearable devices. In Section 5, we discuss the privacy issue in wearable devices. Section 6 provides the research challenges and future research directions in wearable health monitoring devices. Section 7 concludes our work.

2. Preliminaries and taxonomy

We first introduce three aspects of wearable health monitoring devices: the classification of wearable health monitoring devices, types of sensors, and communication methods. We also present the taxonomy of the literature reviewed in this section.

2.1. Types of wearable health monitoring devices

Research by Ehrich et al. (2020)'s points to a paradigm shift from hospital care to home care is now being promoted to improve hospital turnover and patient quality of life. Medical manufacturers are also shifting their research focus from stationary medical devices to portable devices and wearables. There are already many wearable health monitoring devices on the market to help patients with their daily monitoring. These devices can be classified according to where they are worn: wrist-worn, head-worn, smart clothing, and body patches.

Wrist-worn devices: These are currently the most popular wearable devices. The main devices in this category are smartwatches and wristbands. These devices generally contain two main functions: communication notification (for example, incoming calls, text messages, emails, and weather changes) and monitoring of physical signals and biomechanics information from the human body. Typically, these devices continuously monitor the user's heart rate, blood oxygen levels, blood pressure, and exercise history (Alugubelli et al., 2022). The Apple Watch can even generate basic ECG information from measurements and detect if the user is experiencing atrial fibrillation. These wrist devices can detect physiological signals from the human body, and they are also used as fitness tracking devices to record the user's daily life. The same equipment can also be used for the monitoring of rehabilitation training to guide patients in their rehabilitation (Spaccarotella et al., 2021).

Head-worn devices: Head-mounted devices refer to wearable devices worn on the head or neck. In the medical field, the three main categories are smart glasses, electroencephalogram (EEG) readers, and earbuds. Smart glasses monitor the user's status mainly through the camera on the glasses. Similarly to wrist devices, smart glasses can also monitor the user's movement. However, efforts are now being made to provide doctors with guidance during surgical procedures using smart glasses. An EEG reader can record electrical activity on the scalp in a way that has been shown to represent macroscopic activity beneath the surface layers of the brain. Analyzing EEG readings for abnormalities can be used to diagnose if a patient has epilepsy (Smith, 2005). Similarly, EEG reader can diagnose patients with sleep disorders, depth of anaesthesia, coma and brain death (Ortolani et al., 2002). EEG reader was once the primary method for diagnosing brain tumors, strokes, and other focal brain lesions (Tatum IV, 2021). The primary role of earbuds in the medical field is to help restore hearing in patients with hearing loss. Since brainwave electrical signals can also be collected in the human ear, there are also some devices that attach electrode pads to earbuds to monitor the patient's brainwaves (Nakamura et al., 2017).

Smart clothing devices: Smart clothing is generally achieved by attaching electronic systems to conventional garments (Barfield, 2015). Sensors for monitoring physiological parameters are integrated into the fabric, and the monitoring of physiological states is achieved by wearing it close to the body (Pandian et al., 2008). Smart clothing is mainly used in special scenarios such as battlefields, fires, and rescues. Smart clothing is almost indistinguishable from ordinary clothing when worn, but it can monitor the user's physiological state at all times. This is vital for personnel in special occupations such as soldiers, firefighters, and astronauts who work in extreme environments. In addition to monitoring the user's vital signs for normality, the user's current stress and fatigue levels can also be analyzed, such as from the user's heart rate and blood pressure (Zieniewicz et al., 2002). Smart clothing can alert users when their physical or mental state is not suitable to continue a task and subsequently to evacuate from these dangerous scenarios in time.

Body patches: Body patches can be used to monitor the physiological state of a user in specific parts of the body. Body patches are applied directly to the human skin and can provide more accurate measurements than the devices mentioned above. Currently, the body patch is used mainly to monitor the ECG signal of patients. The ECG data are obtained by sticking body patches to multiple parts of the body. Hence, it is more accurate than a single-position measurement. It plays a key role in preoperative and postoperative monitoring, dynamic surveillance, and monitoring of specific diseases in patients (Engineering, 2021). In addition to being used to monitor blood pressure and heart rate, by collecting sweat from the skin, the body patch can also monitor a patient's blood sugar, lactate, caffeine, and alcohol levels without invading the body (Sempionatto et al., 2021).

2.2. Classification of wearable sensors

For wearable health monitoring devices, the most important component is their associated sensors. Sensors work by converting the physical or chemical signals collected into data that can be processed by the system. Physiological monitoring of the patient is achieved by capturing these signals. This section categorizes sensors into four distinct dimensions, as depicted in Fig. 1. In this analysis, sensors are categorized according to signal type, signal source, and persistence. Table 2 presents a classification scheme for wearable sensors based on taxonomy.

Signal: The signals collected by wearable devices can be divided into two types: physical signals and chemical signals. Since wearable device monitoring is non-invasive, the signals collected are mainly physical signals. Chemical signals are obtained by analyzing the level of various chemicals in the patient's sweat. Physical signals can include light signals, electrical signals, sound signals, and others. The same types of physical signals can also be used in different locations in the body to monitor different physiological information (Cheng et al., 2021). For example, electrical signals can be used to monitor information from brain waves or to monitor muscle movement.

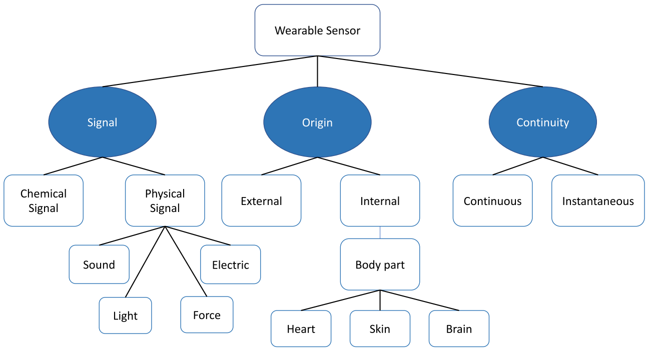

Fig. 1. Medical wearable sensors for monitoring.

Origin: Originally used to monitor the user's physiological state, there are two types: those generated internally by the user's body and external sources of information. Internal body origin refers to information generated by the patient's physiological activity such as heart rate and blood pressure. The remaining information sources are classified as external sources.

Body part: This part is classified according to the part of the body from which the sensor gets its signal. Depending on the functional requirements, it is worn on different parts of the body to obtain information. For example, it is possible to receive heartbeat data from the heart, sweat information from the skin, and brainwave information from the brain.

Continuity: There are two modes in which sensors are used for monitoring, one is to continuously read the signal for monitoring (e.g., ECG), and the other is to take transient measures (e.g., fingerprints). Only the first of these monitoring modes can be used to build continuous authentication systems.

2.3. Communication methods

A wide range of technologies are currently available to support communication in wearable health monitoring devices. They can be divided into short-range and long-range communication according to the communication distance. This subsection provides an overview of the relevant communication technologies available on wearable health monitoring devices.

2.3.1. Short-range communication technologies

Short-range communication is the main communication method used by wearable health monitoring devices. This type of communication allows for longer battery life and can effectively reduce the cost of the device (Ometov et al., 2021). The main mode of communication between devices is peer-to-peer communication. In a mobile wearable network, it communicates with the gateway via short-range technology. In this sub-section, we will introduce short-range communication technologies in the order of distance from short to long.

The communication technology with the shortest communication range is the near-field communication (NFC) system. This technology typically has a communication distance of up to 10 cm and communicates via a 13.56 Mhz frequency (Coskun et al., 2015). NFC communication is achieved between devices by inductive coupling between the transmitting and receiving devices. It is mainly used on wearable devices for payments and personal authentication.

Bluetooth technology, particularly its low-energy variant, is the predominant communication method in wearable devices. Serving as a short-range communication protocol designed for Personal Area Networks (PAN), it operates at a 2.4 GHz frequency. With its ability to facilitate interactions over distances up to 100 m, low-energy Bluetooth is a core technology that enables efficient connectivity for wearable

Table 2
Taxonomy-based wearable sensor classification.

Signal	Sensor	Origin	Body Part	Continuity
Light	PPG	□	Vascular	●
	Fingerprint Reader	□	Finger	○
	Camera	△	–	○
Force	Three-Axis Accelerometer	△	–	●
	Gyroscope	△	–	●
	Barometer	△	–	○
Electrical	Electrocardio-gram Sensor	□	Heart/Brain/Skin	●
Temperature	Temperature Sensors	□	Skin	○
Sound	Microphones	□ △	Respiratory	●
Location	GPS	□	–	●○
Chemical	Electrochemical Sensors	□	Skin	○

● = Continuous, ○ = Instantaneous, □ = Internal, △= External.

devices (Ferro and Potorti, 2005). Wearable devices primarily use Bluetooth to transmit collected data to devices such as smartphones.

In medical scenarios, there is often a need for centralized data collection of vital signs collected by various devices to enable a more accurate diagnosis. The construction of wireless sensor networks between wearable health monitoring devices is generally achieved through Zigbee networks (Frehill et al., 2007). Although Zigbee has a lower data processing rate compared to Bluetooth communication, it consumes less energy and can be used at a lower cost. However, the efficiency of Zigbee transmission in medical scenarios is already sufficient, and it also has short latency and high capacity, which is essential for real-time monitoring of multiple patients' vital signs.

The third major short-range communication technology is defined by the IEEE 802.11 standard and is also known as WiFi. This communication technology provides connectivity for mobile devices within a wireless local area network. Compared to the three previously described communication methods, it enables high-speed data transmission and is therefore mainly used to update equipment systems or upload data (Ometov et al., 2021).

2.3.2. Long-range communication technologies

Long distance communication tends to consume a lot of battery life, so this type of communication has not been promoted in wearable devices (Andres-Maldonado et al., 2017). However, long-range communication technology can remove the limitations of communication distances and expand the range of applications. Therefore some companies are also offering solutions for long distance communication in wearable devices (Chen et al., 2017). The current main approach is to integrate long-range communication via embedded Subscriber Identification Module (SIM) cards.

Current wearable devices often need to be connected to other devices to perform their full function. If long-range communication of wearable devices is achieved, the wearable device could be used as a standalone device. This real need is driving the trend for wearables to use long-range communication as a future development. The narrowband IoT and LTE machine-type communications (LTE-M) developed by the current 3GPP ecosystem (Andres-Maldonado et al., 2017) provide the conditions for long-range communication in wearable devices (Djapic et al., 2018). Both protocols have been optimized for communication energy consumption and complexity, while successfully reducing antenna size and cost.

2.4. Taxonomy of security and privacy

To give the reader an idea of the current security and privacy issues facing wearable health monitoring devices and to help them easily find the most relevant papers, we create a taxonomy of security and privacy issues for wearable health monitoring devices in Fig. 2. We have categorized the articles collected according to the areas they cover, the objectives they address, and the methods they use. In general, we note that there are two areas of focus among the articles: security and privacy issues. The articles investigating security can be further categorized into three parts: communication security, authentication, and integrity. Privacy issues can be further categorized as wither direct privacy breaches or indirect privacy breaches. For papers on the category of secure communication of wearable devices, we have divided the communication into two categories based on the object involved: communication with paired devices and communication with monitoring devices. For security authentication categories, we further divided the authentication into three types of authentication: knowledge-based, biometric-based, and possession-based. Integrity-related papers have been divided into two categories depending on their target audience: certifying the integrity of wearable devices and certifying the integrity of other devices through wearable devices. The classification of direct privacy breaches within privacy concerns can be further classified into two components: cloud server data management and device data management. Indirect privacy leaks can be further divided into three components: input inference, biometric inference, and behavioral inference.

3. Security and privacy challenges

In order to provide the reader an appreciation of the security issues faced by wearable health monitoring devices, we shall discuss this from two perspectives: the security and privacy needs of wearable health monitoring devices and then the security privacy challenges they face.

Security and privacy are two critical aspects to consider when designing a wearable medical device. These security and privacy requirements for wearable health monitoring devices are listed below.

3.1. Security requirements

Confidentiality, integrity and availability are the three key elements that make up device security. When designing a wearable device, it must adequately address these three elements. Specific information on these three requirements is as follows.

Confidentiality: Only legitimate users will be able to access the data recorded by a wearable device. Legitimate users include authenticated individuals, authenticated paired devices such as smartphones and computers, or authenticated online servers. For these legitimate users, the wearable device must authenticate their legitimacy and validity and ensure that the authentication process remains secure from attacker interference (Piciucco et al., 2021). In practice, wearable devices should ensure that their data is kept confidential, both on

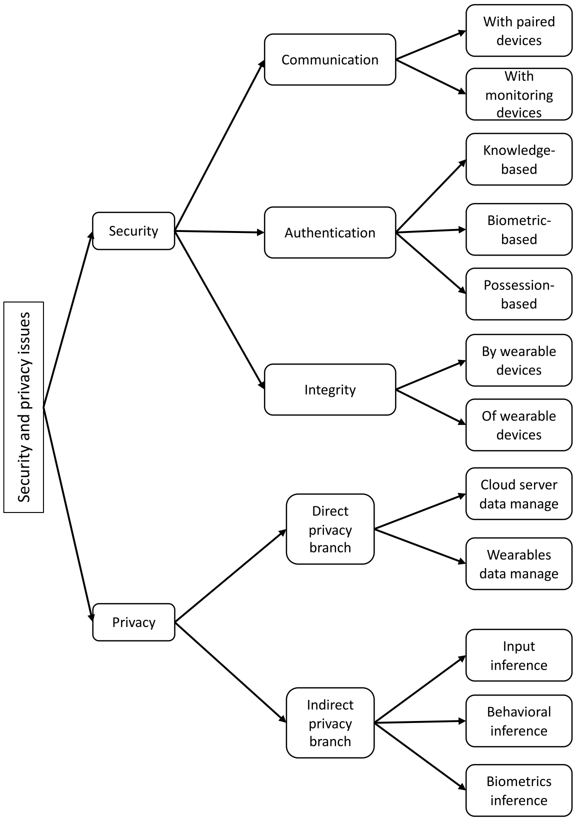

Fig. 2. Taxonomy of security and privacy in wearable health monitoring devices.

their own and when transmitted to other legitimate users (Li et al., 2011). Confidentiality is of paramount importance for wearable health monitoring devices. This is because the devices often collect sensitive physiological information about the patient. Patients expect wearable health monitoring devices to not only protect their privacy, but also strict rules and regulatory requirements for healthcare providers.

Integrity: Integrity is used primarily to ensure that the information has not been received for unauthorized modifications. These measures are used primarily to ensure the accuracy and integrity of medical data. On the other hand, integrity is also needed to prevent unintentional changes, such as data loss due to system failures (Rieback et al., 2006). The information recorded by the wearable, transmitted to other devices and the structure of the wearable should not be altered by unauthorized users (Ly and Jin, 2016; Clausing et al., 2015; Zhang et al., 2020c). In the case of wearable health monitoring devices, a lack of integrity can lead to doctors giving a wrong treatment plan that endangers a patient's life.

Availability: Availability requires the device to operate continuously and normally. In the case of wearable health monitoring devices, ensuring the availability of the device is relevant to the safety of patients' lives. Authorized users should be able to access the data recorded by the wearable at any time. The user should be able to transfer information to/from the wearable device. The wearable should also be resistant to any form of denial of service attack to ensure proper use of the device (Rathore et al., 2017). Wearable health monitoring devices should be resistant to battery drain attacks (Fiore et al., 2017), storage overflow attacks (Shrestha and Saxena, 2017) or communication channel interference attacks.

3.2. Security challenges

We discussed the security requirements when designing wearable health monitoring devices in the previous subsection. The challenges of wearable devices we face in practical design can be divided into three areas: communication security, authentication security, and integrity security. In the following subsections, we will cover each of these challenges.

3.2.1. Communication challenges

Wearable devices, given their limitations in resources and functionality, typically require collaboration with other devices. In order to perform as expected, these devices need to establish communication with other systems to carry out commands or transmit data acquired by sensors (David and Jeyachandran, 2016). As we have previously described, communication in wearable devices is mainly made possible by short-range communication technologies. Ensuring secure communication between wearable devices and other devices is essential for wearable devices to properly execute treatment protocols and protect patients' privacy. The confidentiality, integrity and availability of security requirements become vulnerable when the communication of the device is insecure (Li et al., 2015).

- Communication with paired devices: Due to the limitations of wearable devices, it is sometimes necessary to connect to other devices to perform patient monitoring tasks together. When a user wants to extend the functionality of their wearable device, they need to connect it to their existing device. When making the connection, a key pair will be established between the two devices. This process is also known as pairing (Wong et al., 2007). These may include pairing with smartphones, computers, monitors, and wearable devices in other locations on the patient's body, and are often located around the device, so communication is generally established via Bluetooth Low Energy or Zigbee (Dementyev et al., 2013). The purpose of this type of communication is to integrate patient information and to make a reasonable determination of the patient's current status (Zhang et al., 2014).
- Communication with monitoring equipment: After the wearable device has collected the patient's vital signs, the information should be uploaded to a doctor for analysis (Pantelopoulos and Bourbakis, 2009). In addition, in critical situations where the life of a patient is at stake, it is vital that the device immediately alerts paramedics for urgent care. In such scenarios, data gathered by the wearable device is transmitted to a smart mobile device, like a smartphone, through Bluetooth or alternative communication methods. The mobile device then forwards these data to a remote healthcare center via a cellular or WiFi network. This process allows healthcare professionals to monitor patients' health conditions and react quickly to any emergency, providing real-time intervention and support (Iqbal et al., 2021; Lins et al., 2023).

The first type of communication focuses on how to securely generate key pairs to protect communication. For devices that can be networked, pairing can be achieved by relying on a certificate authority to verify the identity of the device (Scarfone et al., 2008). For most wearable devices, however, there is no networking capability, so pairing key-pairs cannot be generated by this method. Traditional pairing is achieved by involving a human in the pairing process to prove the validity of the device, for example by entering a string of pairing codes displayed on one device into another (Du et al., 2019). This type of pairing authentication, achieved through human assistance, is not only cumbersome but also error prone. Furthermore, wearable devices often have small screens or no screens (Xu et al., 2017). This makes the pairing process challenging.

For the second type of communication system, more aspects need to be considered in the implementation. This is due to the involvement of several distinct devices in this mode of communication. The design of the encryption solution must take into account aspects such as lightness and scalability in order to adapt the system to a wide range of devices (Park et al., 2016).

3.2.2. Authentication challenges

For wearable devices, authentication is primarily used to confirm that the person or party who wishes to use the device is legitimate (Suh and Devadas, 2007). If the device does not authenticate securely a user, the information within the device can be leaked, causing a breach of confidentiality. There are several ways to authenticate a user. A classification based on the characteristics used for authentication can be divided into the following three categories.

- Authentication based on what you know: This type of authentication is based on what the user knows, e.g., pin, password, and contacts.
- Authentication based on what you have: This type of authentication is based on the device (e.g., smartphone, smartwatch, token) or program (e.g., app installed on the device) that the user has.
- Authentication based on what you are: This authenticates users by their own biometric characteristics. These biometric features include fingerprints, face, voice, brain waves, and gait.

Authentication provides an effective defense against device theft attacks and protects the privacy of the user. In this paper, we evaluate the performance of the different authentication methods on the basis of the evaluation criteria for the authentication methods proposed by Bonneau et al. (2012). This evaluation criterion assesses the authentication scheme based on availability, deployability, and security.

3.2.3. Integrity challenges

Device integrity is fundamental for wearable devices, as the effectiveness of all previously mentioned mitigation strategies relies on maintaining the device's integrity. Seneviratne et al. (2017). If the internal hardware has been damaged or modified, then any security measures built on it are ineffective. Therefore, it is necessary to confirm the integrity of the device before implementing a security defense policy. As medical wearables play an essential role in providing accurate patient data to healthcare providers, recent literature has begun to emphasize the importance of ensuring the integrity of data transmission from wearable devices (Banerjee et al., 2018). Depending on the usage scenario, it can be divided into verifying the integrity of information on wearable devices (Shebaro et al., 2012; Chinaei et al., 2021; Siddiqi et al., 2019; Ali et al., 2014; Wang and Liao, 2022) and verifying the integrity of other devices through wearable devices (Shrestha et al., 2020).

3.3. Privacy requirements

Depending on privacy information, privacy issues can be divided into device ID privacy, device log information privacy, wearer privacy, and bystander privacy. Specific information about these privacy concerns is as follows.

Device ID Privacy: Since the wearable device remains with the user, identifying the device's location can lead to a breach of the user's position. Zhang et al. (2020b). Wearable devices therefore need to be designed to ensure that they are not tracked by any unauthorized party. For wearable devices, persistent identifiers, such as RFID identifiers, Bluetooth device addresses, and MAC addresses, can lead to the device being identified and consequently reveal the user's location (Heinrich et al., 2021, 2022). Therefore, device information should be kept confidential (see Fig. 3). **Device Log or Measurement Privacy**: Due to the specific characteristics of wearable health monitoring devices, they collect a large amount of private and physiological information about the patient. Moreover, data including specifics of a patient's treatment can potentially be deduced from the log data of the wearable device (Siddiqi et al., 2019). Therefore, the measurement information and the access log information on the device should be accessible only by authorized users. It is also important to ensure that any information about sensitive activities is not extracted by unauthorized users (Das et al., 2016; Hemapriya et al., 2017).

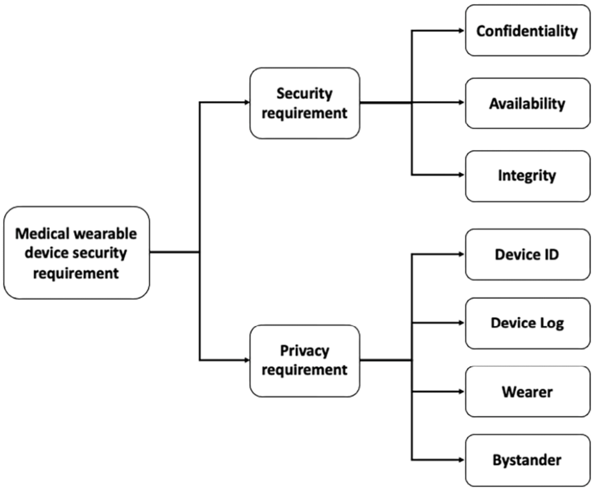

Fig. 3. Classification of wearable device security and privacy requirements.

Wearer Privacy: As wearable devices become more capable, they can record information about the user, such as name, address, medical history, location, lifestyle, and other information. For wearable health monitoring devices, the patient treatment process that they store is vital private information for the patient. So, a key focus of the design of mobile devices is to ensure that such private user information is not disclosed to unauthorized users (Liu and Li, 2018; Su et al., 2023; Ioannidou and Sklavos, 2021).

Bystander Privacy: Many wearable devices currently possess cameras, microphones, and various sensors. Consequently, the design of such devices must incorporate protective measures against malicious activities to prevent them from being used to identify bystanders or to obtain information about the lives of people in proximity (Gurrin et al., 2013). Bystanders may not be aware that their actions are being recorded, raising privacy issues in the social environment (Patidar et al., 2023).

3.4. Privacy challenges

In the case of wearable health monitoring devices, their various sensors can collect a lot of private information about the user. It is vital to ensure that this private information is not compromised. Depending on the content of the privacy breach, the privacy of wearable devices can be divided into two areas: direct privacy breaches and indirect privacy breaches.

3.4.1. Direct privacy breaches

One of the functions of medical wearables is to collect physiological information about the patient, so there is often a lot of information about the user's medical history, health status, location, and others on the device. The leakage of this privacy can have many implications on the user's life.

There have already been numerous incidents of privacy breaches caused by wearable devices. In 2011, the fitness tracking company Fitbit faced a class-action lawsuit for allegedly selling user data to advertisers without their consent (Actions, 2016). In 2018, the fitness tracking app Strava inadvertently exposed the locations of military bases and personnel worldwide. This happened because the app allowed users to track and share their exercise routes on social media, leading to the leakage of sensitive location information (Guardian, 2018). In 2021, a report revealed that data belonging to 61 million records of Fitbit and Apple devices were leaked. The breach occurred because their database was not password protected, resulting in the information being visible in plain text (Fowler, 2021). From these cases, we can conclude that in terms of data management, both the cloud database and the device itself must be protected to prevent direct privacy leaks.

For wearable health monitoring devices, the case data they collect needs to be accessible for both the patient and the doctor. To facilitate patient and doctor access to Personal Health Records (PHRs), many healthcare systems rely on cloud-based platforms to manage patient data (Srinivas et al., 2018; Wang et al., 2019). For these data stored in the cloud, designers need to consider two aspects: whether they can ensure that patient privacy is not compromised in the event of an attack on the database and how to design a system for accessing the data.

Another aspect of ensuring the privacy of wearable devices is ensuring that attackers cannot steal data through programmatic vulnerabilities. When dealing with data stored on a device, designers must contemplate two key aspects: the isolation of applications from one another (Hester et al., 2016), and the development of a data flow control system to safeguard private information (Lomotey et al., 2017).

3.4.2. Indirect privacy breaches

In contrast to direct privacy breaches, indirect privacy breaches mostly infer user privacy from information collected by sensors. We have previously described the large number of sensors that may be fitted to wearable devices. Significant user privacy information, including user habits, location, and input data, can be deduced from sensor information (Sridharan et al., 2019; Torre et al., 2016). Depending on the characteristics used for the inference, they can be divided into the following categories.

- Input inference: Most medical wearables are equipped with motion and sound sensors to monitor the physiological condition of the patient. Since a majority of these gadgets are worn on the hand, an examination of the sensor data enables researchers to deduce the user's input on other devices (Wang et al., 2016a).
- Behavioral Inference: An increasing number of wearable devices are now equipped with EEG sensors to collect the user's brain waves. The brain waves collected can be used for audio and video entertainment, input of information, and other operations. On the other hand, an attacker may also be able to deduce the current behavior of the user by analyzing their EEG (Zhao et al., 2017). The information collected by the wearable device can also infer the user's personality and interests (Sridharan et al., 2019).
- Biometric inference: It is very difficult to obtain biometric information from a person in real life. In the case of medical wearables, it has always been about collecting physiological information from the user for diagnostic purposes. Through examination of the physiological data of this user, an attacker could potentially deduce the user's biometric identifiers (Vhaduri and Poellabauer, 2019).

4. Security issue in wearable health monitoring devices

In the previous section, we have discussed how specific security challenges need to be addressed when designing wearable health monitoring devices. In this section, we detail the solutions currently available for these issues.

4.1. Communication issues

As we described in the previous section, the two main modes of communication for wearable health monitoring devices are with the paired device and with the monitoring device. For the first communication mode, we are mainly comparing the efficiency of key production between devices and the time required for authentication. The comparison between the different methods is shown in Table 3. For the second mode of communication, we compare different approaches in terms of ease of deployment and security. The comparison between the methods is shown in Table 4.

4.1.1. Communication with paired devices

In order to address the security of the pairing of wearable devices, a number of methods have been proposed in the literature that use surrounding information for pairing. This survey provides a systematic comparison of different pairing methods. All of these pairing methods can be divided into the following two categories.

- Environment based: When a user pairs a wearable device, the two devices should be close to each other, and the environment around the two devices should be similar. This type of approach envisages the use of information in the environment surrounding the device to create the key. LightTouch (Liang et al., 2018) relies on the ambient light sensor on the wearable device to establish a secure connection to the display. The method starts by placing the wearable's ambient light sensor close to the display a user want to connect to, which shows a picture. Based on the data sent to the screen from the ambient light sensor, the screen is able to determine the position of the wearable device. Based on the brightness data at that location, the display and the wearable device can generate a pair of keys for subsequent communication of the connection (Liang et al., 2018). Goodrich et al. (2006) propose a way to establish communication keys between devices via audio. This approach uses a text-to-speech (TTS) engine to enable communication connections between devices. The TTS engine converts the English sentence in the device's public key into speech and displays/renders the same sentence on the receiving device. This reliance on audio to generate keys is risky, and (Anand and Saxena, 2018) show that audio information can be captured from the vibrations of the transmitting audio device. They also propose an improvement: the vibrations can be effectively concealed by adding a noise vibration during pairing. The method, proposed by Jin et al. (2020), also generate key pairs by using the surrounding environment. This method generates keys by identifying the ambient RF noise around the environment. The design of their method is based on a pattern they discovered: although the RF noise power indicates at different parts of the body is different, they have the same trend.
- Human-based: Wearable devices are generally personal (i.e., not shared) so generating keys through the user's actions can also be effective in preventing eavesdropping attacks. This method is generally used to pair devices with each other by completing a few simple actions. Most of the existing methods are implemented with the help of motion sensors on wearable devices. Revadigar et al. (2017) propose to identify the user's gait (e.g., each person walks with a particular gait) through acceleration sensors on wearable devices and use the common feature of gait to generate encryption keys. In addition to the use of gait to generate keys, the generation of pairing keys from ECG information is also a recently proposed new method. Zhao et al. (2022) proposed an improved martingale randomness extraction (IMRE) algorithm, which exploits the tendency of inter-pulse intervals in ECG signals to kick off high entropy keys. This method has a very high pairing efficiency and very low energy consumption. Meanwhile, the method proposed by Li et al. (2017b) relies on Received Signal Strength (RSS) trajectory to help establish keys between two devices. By simply shaking or moving one of the devices, the user changes the RSS between the two devices. Furthermore, this trajectory of change in received signal strength should be similar for both devices, and both devices can construct an encryption key based on this trajectory. Based on a similar approach (Li et al., 2020) proposed a method for pairing between two devices via gyroscopes. The device generates a pairing key by collecting gyroscopic data in case the user presses a button or turns a knob. The pairing method can be done within seconds. Recently, Das et al. (2017) have also designed an authentication protocol that enables a wearable device to support authentication only with

Table 3
Comparing the performance of different wearable device pairing methods.

Reference	Sensor Tools	Key Length (bit)	Key generation (ms)	Success rate	Energy Consumption (mJ)	Key verification	Key generation rate (bits)
Revadigar et al. (2017)	Accelerometer	128	208.1		12.7713	0.0403	
Das et al. (2017)	Fingerprint scan	128					
Jin et al. (2020)	RF transceiver	128		96.8			138
Li et al. (2017b)	RF transceiver	128	610				210
Srinivas et al. (2018)	Networked equipment	160				36Th+1TME+Tcrt	
Li et al. (2020)	Gyroscope	128	501	97.8		3.2 s	10.3 14.8
Zhao et al. (2022)	electrodes	256	21.905	98.97	1.379	0.37	
Xu et al. (2017)	Accelerometer	128	4600	98.3	198.5	0.2	28

Table 4
Comparing the performance of different WBAN systems.

Reference	Fine-grained access control	Scalability	Flexibility	Forward secrecy	Backward secrecy	Lightweight	Confidentiality
He et al. (2013)	●	◐	●	●	●	◐	◐
He et al. (2016)	◐	●	○	●	●	◐	●
Li et al. (2017a)	○	◐	○	●	●	●	●
Arfaoui et al. (2020)	●	◐	●	●	●	◐	●
Shuai et al. (2019)	◐	●	○	●	○	●	◐
Das et al. (2017)	●	●	◐	●	●	●	●
Zhang et al. (2016)	●	●	○	●	○	◐	◐
Hathaliya et al. (2020)	●	●	●	●	●	○	◐
Yang et al. (2017)	●	●	○	○	○	●	◐
Di Pietro et al. (2014)	●	●	○	○	○	●	◐
Webber et al. (2023)	◐	●	○	○	○	●	●
Srinivas et al. (2018)	○	●	○	●	●	●	◐

● = offer benefit, ◐ = almost offer benefit, ○ = does not offer benefit.

that user's mobile terminal through biometrics. These identification methods tend to be easy to operate, but they have the disadvantage that none of them considers authentication between the wearable device and external parties.

The current trend for establishing keys between paired devices is to minimize human intervention (Goodrich et al., 2006; Anand and Saxena, 2018; Jin et al., 2020). The keys are established by using the sensors already present in the wearable device. Unfortunately, in a medical scenario, there is no guarantee that every wearable device in the patient will have these sensors. This poses difficulties for the promotion of these key generation methods. On the other hand, current methods do not yet meet the needs of healthcare scenarios in terms of key generation rate and authentication time. Therefore, future work is needed to optimize these key generation methods to make them more suitable for medical scenarios.

4.1.2. Communication with monitoring equipment

The methods we have described above are primarily used for the pairing process between wearable devices and between wearable and companion devices. A further necessary communication process for wearable health monitoring devices is to connect to the monitoring device. Due to the resource limitations of wearable devices, the primary requirement for this type of communication is a lightweight encryption scheme (Zhang et al., 2023; Zhao et al., 2020a). Several monitoring programs for remote patients have been developed in recent years. Due to the specificity of wearable health monitoring devices, in this paper, we evaluate the network system through the following seven aspects.

Fine-grained access control: A healthcare security system requires access control of patient data to ensure that private patient data is not available to unauthorized users. Within a healthcare system, there are a variety of roles, including doctors, patients, nurses, and others. The system must assign varying access rights to these distinct users (Chen et al., 2018).

Scalability: For the use of a system in hospitals, there are often multiple patients and multiple users who need to use the system simultaneously. The system needs to be able to operate efficiently with a large number of users at the same time (Lorincz et al., 2004).

Flexibility: Unexpected events sometimes inevitably occur during the patient's treatment. Access control policies for patient data should be able to be adapted to time, place, and special events. For example, when a patient requires emergency care, access should be provided to a doctor or nurse who is not on the access list. Providing flexibility in access control will ensure the safety of the patient's life (Lorincz et al., 2004).

Forward secrecy: If an attacker obtains the long-term key of the system at some point in the future, he will not be able to decrypt previous communication sessions (or forge an authentication key) using that key (Jablon, 2001). This is now mainly achieved through one-time hash chain technology (Shuai et al., 2019; He et al., 2013; Li et al., 2017a; Zhang et al., 2016). The second approach is to turn the key calculation into a computationally difficult problem. He et al. (2016), Hathaliya et al. (2020) implement forward encryption by converting the key calculation to a Diffie–Hellman problem (He et al., 2016; Hathaliya et al., 2020). A final way to achieve forward secrecy is to produce keys by combining long-term keys with ephemeral random nonces (Das et al., 2017).

Backward secrecy: If an attacker has the key to the current node, he will not be able to decrypt later encrypted data with that key (or forge an authentication key). The primary way to achieve this is to produce encryption/decryption keys by randomly selecting numbers on the web server at each round of key generation (He et al., 2013; Li et al., 2017a; Das et al., 2017). As with forward secrecy, backward secrecy can be implemented by combining a long-term key with ephemeral random nonces, making the computation of the long-term key a computationally difficult problem (He et al., 2016; Hathaliya et al., 2020).

Lightweight: As medical wearables are generally battery powered, the lifespan of these devices is highly dependent on battery power. On the other hand, busy medical schedules do not allow doctors to wait for the wearable to recharge when the device runs out of power. Medical wearable devices typically do not include powerful processors due to cost constraints. Consequently, the system must reduce the overhead associated with communication, encryption, decryption, and storage of the wearable (Imtiaz et al., 2014). In the event of an emergency, the wearable should be able to quickly provide patient information. This requires the encryption algorithms used on the device to be as fast as possible while still ensuring the security of the information. The lightweight of systems is now being achieved in two main ways: hand over complex calculations to devices with more computing power, such as mobile phones (Huang et al., 2015), and cloud-based servers (Srinivas et al., 2018). Similarly, He et al. (2016) and Hathaliya et al. (2020) also used this approach to achieve backward secrecy of the system. An adversary can constantly flood the Medical Sensor Networks (MSN) node with fake commands, thus exhausting the node's resources and making it unable to respond in a timely manner.

Confidentiality: To safeguard patient privacy, the system must maintain data confidentiality. Specifically, for wearables, the system should ensure that data remain confidential either on the wearable device itself or on the local server (Tanveer et al., 2022).

In order to be able to achieve these goals, a number of corresponding systems have been proposed. However, due to the limitations of the performance of the wearable device, each of these solutions has to balance security and usability. The solution proposed by He et al. (2013) is the first to secure the data transmission and access control system for Medical Sensor Networks. The system implements a key update mechanism between devices via a hash chain and protects signatures through a proxy. The system successfully achieves efficient and secure information transfer and fine-grained data access control. The system also achieves backward secrecy by combining long-term keys with random bytes. If the attacker obtains the current key of the node, it is also computationally difficult to obtain the solution to the long-term key. However, the use of the system consumes a large amount of computational resources, which limits its scalability.

In order to increase the scalability of the system, (Srinivas et al., 2018) proposed a cloud-based wearable device authentication scheme to achieve a lightweight system. Shifts a lot of computing work from the wearable device to the cloud to do it, thus easing the computing needs of the wearable device. And the scheme analyzes the security of the system through the Automated Validation of Internet Security Protocols and applications (AVISP) tool (Armando et al., 2005). The system provides effective defense against replay, man-in-the-middle, and impersonation attacks. However, the system does not address device stolen attacks. To address this issue, Das et al. (2017) also proposed a secure authentication protocol based on the environment of the wearable device. In this system, the wearable and mobile devices of the user can authenticate with each other and generate communication keys between these devices for secure communication. However, their systems are more challenging to deploy in real-world scenarios.

Shuai et al. (2019)'s approach also guarantee forward secrecy through a one-time hash chain technique. Furthermore, the method uses pseudonymous identity methods to provide user anonymity and resist asynchronous attacks. The authentication scheme designed by Li et al. (2017a) provides mutual authentication and achieves anonymity and unlinkable manner of the transmitted information. The scheme is also much less expensive in terms of storage requirements, computational cost, and energy consumption than other related solutions proposed previously. In 2016, He et al. (2016) built on their previous work to consider a particular situation: the transfer of information between users and other stakeholders, such as health centers. The solution allows two patients registered at different medical centers to authenticate in domains with matching symptoms and generate a session key for future secure communication. When a patient's device uploads the patient's physiological data, it is generally expected that only the healthcare professionals associated with the patient's treatment will be able to view the data. The scheme proposed by Arfaoui et al. (2020) takes this into account. The scheme they designed not only implements access control, but is also context-aware. With context-aware functionality, the system adaptively adjusts the security and privacy levels of authentication.

For such wireless network systems, they are also vulnerable to black hole attacks and cesspool attacks. Attackers do or disrupt normal communication and information transfer by creating one or more black hole nodes in the network (Di Pietro et al., 2014). To address this problem, the POS-MKC framework proposed by Webber et al. (2023). Using IDS to compute the intrusion metric by detecting the number of packets sent and received. Thus, it effectively detects the black hole attacking nodes and achieves secure transmission with minimum delay.

Table 5
Comparing the performance of different wearable device authentication methods.

Reference	Sensor and tools	Equal error rate	FAR	FRR	CIR	Time needed for recognition
Hutchins et al. (2018)	Touch sensor	7.2	<8.2	<10.2		1.7 s
Piciucco et al. (2021)	EDA and BVP sensor				98.58	30 s
Chauhan et al. (2016)	Touch sensor	3			97	2.74msc
Nakamura et al. (2017)	EEG sensor		0.9	12.8	98.3	60 s
Arias-Cabarcos et al. (2021)	EEG sensor	14.5	1.8	46		6 s
Vhaduri and Poellabauer (2019)	Accelerometer Photoelectric sensors	5	2	10	97	
Avola et al. (2024)	Accelerometer				98.82	
Nguyen and Memon (2018)	Touch sensor	1.3	0.98	5.3	94.7	2 s
Yan et al. (2019)	Analog-to-digital converter		2	1.1		5 s
Iwakiri and Murao (2023)	microphone	0.034				
Zhang et al. (2021)	magnetometer	0.05		6.9 9.7	96.3	1.5 s
Huh et al. (2023)	microphone	0.79	0.24	3.41		
Zeng et al. (2017)	inertial sensors		<2	<1	97	

Due to the resource constraints of the wearable devices, most methods cannot achieve cryptographic security while balancing the lightness of the system. It should be noted that some approaches do not consider implementing fine-grained access control, which is very important in healthcare scenarios. From Table 4 we can see that none of the methods now proposed for communication between wearables and monitoring devices meets all the needs of the medical scenario. Therefore, new systems for establishing connections need to be investigated in future work.

4.2. Authentication issues

As mentioned above, when evaluating authentication systems, we focus on the three main points: usability, deployability, and security. Usability looks at how easy the authentication method is for users to use and whether it can fulfill the need for efficient and accurate authentication. The main aspect of deployability considerations is whether the authentication method can be rolled out to a wide range of people and devices. Security considers the ability of the authentication method to resist various possible attacks. To allow a more visual comparison of the performance of the different methods in terms of authentication accuracy, Table 5 shows the performance gap between the different methods. A comparison of the various authentication methods on these three points is shown in Table 6.

4.2.1. Knowledge-based authentication

Currently, knowledge-based authentication stands as the predominant method in use. Its hallmark is its flexibility, which allows users to seamlessly adjust, supplement, or revoke their authentication details. This section delves into the application of existing knowledge-based verification techniques specific to wearable devices. For knowledge-based authentication methods, there are currently three main ways to achieve this.

Password: Users complete authentication by entering pre-set numbers or numbers and letters on a wearable device. The biggest advantage of this approach is that it does not require the wearable device to be configured with any hardware devices and is simple to implement. However, many studies have now shown that there are many limitations to using passwords as a method of authentication (Roth et al., 2004; Klein, 1990; Zhang et al., 2020a; Hatzivasilis et al., 2015). The use of text passwords, especially random passwords, is often complex to remember for the user. However, when easy-to-remember passwords are used, their passwords tend to have low-entropy properties. Using a dictionary attack on an average user's password tends to have a high success rate, and Wang et al. (2016b) demonstrate that an attacker has a 73% probability of guessing a user's password out of 100 guesses if the attacker has some information about the user of the device. On the other hand, as wearable devices generally have small or even no screens, users cannot make complex inputs through the device. Therefore it is challenging to use wearable devices to solve the problem of low entropy of user passwords by adding password policies. Also, users are susceptible to shoulder surfing or observation attacks when entering passwords (Zakaria et al., 2011).

Patterns: This authentication approach involves users drawing a predefined pattern on their wearable device for verification. A prime advantage of pattern-based authentication is its intuitive nature, which potentially allows faster access than passcodes. Moreover, this technique avoids the need for specialized hardware on the wearable. However, like password-based methods, it remains susceptible to shoulder

Table 6
Compare the usability, deployability and security standards of wearable authentication solutions.

Category	Paper	Memorywise-Effortless	Scalable-for-Users	Nothing-to-Carry	Physically-Effortless	Easy-to-Learn	Efficient-to-Use	Infrequent-Errors	Easy-Recovery-from-Loss	Accessible	Negligible-Cost-per-User	Mature	Non-Proprietary	Resilient-to-Physical-Observation	Resilient-to-Targeted-Impersonation	Resilient-to-Throttled-Guessing	Resilient-to-Unthrottled-Guessing	Resilient-to-Internal-Observation	Resilient-to-Leaks-from-Other-Verifiers	Resilient-to-Phishing	Resilient-to-Theft	No-Trusted-Third-Party	Requiring-Explicit-Consent
Knowledge-based	Hutchins et al. (2018) Beat-pin	◐	◐	●	●	○	●	◐	◐	○	◐	◐	●	○	●	●	◐	◐	●	◐	●	●	●
	Nakamura et al. (2017) EEG	●	●	◐	●	●	○	●	●	●	◐	◐	●	●	●	●	●	◐	◐	◐	●	●	●
	Arias-Cabarcos et al. (2021) EEG	●	◐	◐	●	●	◐	○	●	●	◐	○	●	●	●	●	●	◐	◐	●	●	●	●
	Nguyen and Memon (2018) Tap-pin	◐	◐	●	●	○	●	◐	◐	○	◐	◐	●	○	●	●	◐	◐	●	◐	●	●	●
Biometric-based	Piciucco et al. (2021) electrodermal	●	●	●	●	●	◐	●	●	◐	●	◐	●	●	●	●	●	◐	◐	◐	●	●	◐
	Chauhan et al. (2016) Gesture	●	●	●	●	●	●	●	●	◐	◐	◐	●	●	●	●	◐	◐	◐	◐	●	●	●
	Vhaduri and Poellabauer (2019) hybrid	●	●	●	●	●	○	●	●	●	●	◐	●	●	●	●	◐	◐	◐	◐	●	●	◐
	Zeng et al. (2017) Gait	●	●	◐	●	●	◐	●	●	○	◐	◐	●	○	●	●	●	◐	◐	◐	●	●	◐
	Biswas et al. (2019) PPG	●	●	◐	◐	●	◐	◐	●	○	◐	◐	●	○	●	●	●	◐	◐	◐	●	●	◐
	Huang et al. (2020) ECG	●	●	●	●	●	◐	●	●	●	●	◐	●	●	●	●	●	●	◐	◐	●	●	◐
Possession Based	Yan et al. (2019) TouchAuth	●	●	◐	●	●	●	●	●	●	◐	◐	●	●	●	●	●	●	●	●	◐	●	◐
	Miao et al. (2023) TouchKey	●	●	◐	●	●	●	●	●	●	◐	◐	●	●	●	●	●	●	●	●	◐	◐	◐
	Shrestha et al. (2024) Listening-Watch	●	◐	◐	●	●	◐	◐	●	●	◐	◐	●	●	●	●	●	●	●	●	◐	●	◐
	Karapanos et al. (2015) Sound-Proof	●	●	◐	●	●	●	●	●	●	◐	◐	●	●	●	●	●	●	●	●	◐	●	◐

● = offer benefit, ◐ = almost offer benefit, ○ = does not offer benefit.

surfing or observation attacks. Furthermore, the simplicity of stored patterns, constrained by potential drawing limitations, makes them relatively easy to predict (Khamis et al., 2016; Von Zezschwitz et al., 2013).

Voice or Sound Commands: Wearable devices achieve authentication by recognizing special speech or user commands (Shi et al., 2021). The method can also be combined with voice recognition to achieve two-factor authentication. The advantage of this method is that the user does not have to enter the password manually. This is particularly important for users who have limited mobility or who are engaged in specialized operations. However, since the microphone needs to receive the authentication information, the surrounding ambient noise can have an impact on the accuracy of the authentication. On the other hand, there is a risk of being recorded and mimicked if not combined with a voice recognition system. There is also the possibility of attacking the system through ultrasonic waves that cannot be heard by the human ear (Shi et al., 2021).

In the specific implementation of these methods, they require the help of different wearable device hardware for authentication. The study of this needs to be selected based on the hardware device it has for the product. We have categorized them into touch screen-based authentication, microphone-based authentication, touch sensor-based authentication, and brainwave-based authentication.

Touch screen based: Most existing authentication methods for wearable devices rely on touch screens. Depending on the chosen method, there are three primary ways of unlocking: PIN: Users authenticate by entering a 4–6 digit code set by them. Pattern PIN: Users draw a predetermined pattern within a 3 × 3 grid to unlock the device. Draw PIN: Users draw their PIN directly on the screen. This method validates based on the user's drawing habits and the accuracy of the PIN entered (Van Nguyen et al., 2017). As Nguyen and Memon (2017), these methods exhibit a low error rate during seated authentication. However, error rates spike when users authenticate while walking. Among these, the Draw PIN method, while more secure, has a longer authentication time and higher error rate, making it less practical for everyday device unlocking.

Microphone based: Voice-based PIN authentication is an alternative. Users verbally provide their set PIN code, and the system employs speech-to-text technology to match the spoken numbers with the stored PIN. This method is verified solely based on the correctness of the spoken number, without considering the identity of the speaker (Nguyen and Memon, 2017). Offering a higher level of convenience, this mode eliminates the need for a touch screen and facilitates easy unlocking, irrespective of the user's activity. Nevertheless, it is considered the least secure method of the four. External parties or nearby devices might intercept and document the user's voice during the authentication process, thus gaining access to the PIN code (Ren et al., 2021).

Touch sensor based: Traditional PIN code authentication, while straightforward and user-friendly, is susceptible to shoulder surfing attacks. Attackers can easily memorize the user's input. In response to these vulnerabilities, rhythm-based authentication methods for wearable devices have gained traction recently (Nguyen and Memon, 2018; Hutchins et al., 2018). This approach stands apart from fingerprint and facial recognition systems, which require advanced sensors; rhythm-based methods only require the device's touch sensor. The user first sets a familiar melody via the touch interface. For subsequent authentications, replaying this melody unlocks the device. Given that users tap the same area repeatedly, this method is less prone to thermal and smudge attacks compared to PIN-based systems (Hutchins et al., 2018).

Two notable rhythm-based authentication methods are Best-PIN (Hutchins et al., 2018) and TapMeIn Nguyen and Memon (2018). Both utilize melodies for authentication and boast high accuracy rates. However, they differ in their feature extraction: Best-PIN focuses on tap timing, intervals between taps, and relative intervals. In contrast, TapMeIn considers the pressure, size, and duration of each tap's commencement and release. Furthermore, TapMeIn has a more efficient enrollment process, requiring the user to input the melody three times, while Best-PIN requires seven repetitions for optimal accuracy. In general, TapMeIn outperforms Best-PIN in terms of both enrollment and authentication efficacy.

Brain wave based: As medical technology advances, innovative solutions that use user brain waves have emerged for authentication (Nakamura et al., 2017; Arias-Cabarcos et al., 2021). Numerous studies confirm the potential of EEG sensors in collecting brainwave signals for user authentication. This method necessitates users to recall specific memories, producing corresponding brainwaves, thereby categorizing it as knowledge-based authentication. However, medical-grade EEG equipment remains prohibitively expensive and difficult to distribute widely.

Nakamura et al. (2017) showcased that biometric authentication based on brainwaves can be achieved using consumer-grade EEG headsets. This method yielded a commendable accuracy rate (exceeding 98%) under the device's stipulated conditions. The authentication process involves capturing EEG signals when users rest with their eyes closed, which provides the most stable signals. However, this approach requires extended periods to obtain adequate EEG signals. In their experimental design, data from three 190-second sessions were gathered from participants to register authentication details. Additionally, each authentication procedure required a 10-second brainwave collection.

Arias-Cabarcos et al. (2021) devised an authentication framework grounded in a consumer-grade EEG sensor. Distinctively, their method authenticated users by discerning specific brain waves elicited upon encountering novel stimuli. The work of Arias-Cabarcos et al. (2023) further improves the accuracy of this type of authentication method by increasing the amount of data set. However, it still has an equal error rate of more than 7. 2%. Unfortunately, the method currently falls far short of the required certification accuracy.

Multi-Factor Authentication: Using only passwords as an authentication method for wearable devices is not secure, so it is now common to use multi-factor authentication to improve security. One of the authentication factors added can be another device, or the user's habits. A simple multi-factor authentication method is sending an authentication code to a smartphone or other wearable device, making that device a second factor in the authentication scheme. In general, using a smartphone as a second factor makes it easier for the user to view and copy the code, so wearable devices are often used in conjunction with smartphones.

Zhang et al. (2021) devised a multifactor authentication mechanism for password input. The security of this system is enhanced by a wrist-mounted magnetic strap. As users enter their password, the wearable device captures magnetic field information, which subsequently serves as gesture authentication for touch actions.

4.2.2. Biometric-based authentication

Biometric authentication for wearable devices stands out as the most user-centric method. Gradually, bioinformatics-based approaches are replacing knowledge-based authentication techniques. The primary benefit is that users are not burdened with the task of recalling or carrying specific items for successful authentication. This modality relies chiefly on the user's distinct physical or behavioral traits for differentiation. In the context of wearables, a significant advantage of biometric authentication is the array of built-in sensors that can effortlessly gather physiological data about the user, facilitating authentication. In this section, we explore the potential signal sources utilized by wearables and their respective authentication implementations.

Depending on the source of the biosignal, they can be classified in the following ways.

Electrocardiogram: The Electrocardiogram (ECG) stands as a frequently captured signal in medical settings. An ECG is obtained by attaching electrodes to the body of a person, recording electrical fluctuations arising from the heart's depolarization and repolarization cycles (Kumar and Clark, 2012). Fig. 4 shows a standard ECG cycle.

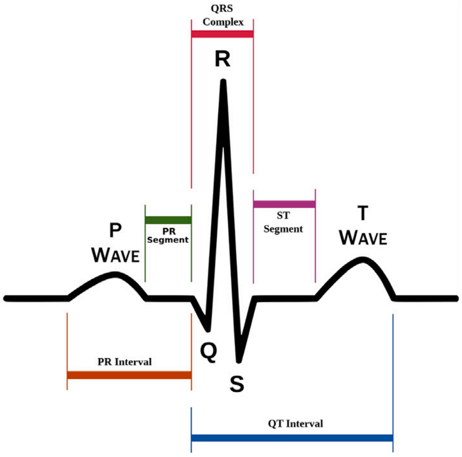

Fig. 4. An example of an ECG cycle.

Numerous cardiac anomalies alter the ECG pattern, establishing its importance in medical diagnosis (Lyakhov et al., 2021; Prabhakararao and Dandapat, 2020). ECG signals efficiently highlight various physiological attributes of the myocardium. Factors such as an individual's lifestyle, heart mass orientation, conductivity, and cardiac activation sequence lead to noticeable differences in ECG signals between individuals (Agrafioti et al., 2011).

In contrast to conventional biometric authentication techniques, ECG-based authentication offers several merits (Condon and Willatt, 2018; Labati et al., 2019). For starters, ECG signals are exclusively obtained from electrodes in direct contact with the human body. This means that unlike fingerprints or facial recognition, the ECG cannot be accessed by simply external observation, bolstering its resistance to spoofing attacks. Another benefit is its ability for in vivo detection. ECG signals are obtained exclusively from living individuals, which improves the resilience of the system against malicious threats (Labati et al., 2019). Furthermore, it uses dynamic biometric data instead of static data. Once biometric features, such as fingerprints, are compromised, their vulnerability persists. However, ECG authentication persistently provides novel samples, strengthening its protection against replay attacks. This adaptable characteristic also proves beneficial for ongoing authentication in wearable devices (Zhao et al., 2021).

Photoplethysmography: Photoplethysmography (PPG) stands as an optical technique used to measure both heart rate and oxygen saturation in users (Castaneda et al., 2018; Biswas et al., 2019). The method utilizes a light-emitting diode paired with a light sensor to capture the PPG signal. Its straightforward design and minimal components make it cost-effective, compact, and user-friendly. The process involves the diode emitting light into skin tissue, with a photodetector gauging the amount of light reflected back. As blood flow intensifies, there is a corresponding increase in the reflected light (Wang et al., 2013a). Previous research has indicated a striking similarity between ECG and PPG signals (Yathav et al., 2017), suggesting the potential of PPG-based authentication as a viable alternative to ECG-based methods.

Due to the ease of measuring PPG signals, there is currently a growing trend of articles on achieving biometric authentication based on PPG (Zhao et al., 2020b; Luque et al., 2018). However, the main limitation of PPG certification now is the lack of high-quality data sets (Li et al., 2023). Currently, there are no studies that demonstrate significant specificity between PPG signals in different individuals.

Gait: Gait authentication is achieved by collecting changes in the accelerometer and gyroscope on the wearable device when the user walks. These sensor data can be analyzed to authenticate the user by identifying the user's unique rhythm, gait length, and gait symmetry when walking (Sprager and Juric, 2015). And when the user starts walking, wearables located in different parts of the body will be able to collect different data, allowing multi-factor authentication.

Iris: Authentication through iris images has proven to be an excellent means of authentication. The images of human iris are highly stable and unique, and the theoretical probability of finding two identical iris is one in 10^{72} (Kumar and Passi, 2010). A prerequisite for iris authentication is the ability to take high-quality iris photos. The user needs to be at the right distance and point the camera in order to take an image that can be used for authentication (Thavalengal et al., 2015).

In the previous part, we have described the sources of biosignals that can be used for biometric authentication in wearable devices. In this section, we will detail the specific implementation of these schemes. It can be classified into heart-based, behavioral, and image-based approaches.

Heart-based authentication: Heart-based authentication primarily authenticates users by identifying unique features of their ECG or PPG signals. These signals are predominantly collected using electrodes or light-sensing elements integrated into wearable devices. Current authentication methods fall into two primary categories: distance-based techniques and machine-learning algorithms. Distance-based approaches predominantly function by determining the similarity or distance between a user's registered signals and incoming signals. Should the congruence between these signals exceed a set threshold, authentication is deemed successful (Arteaga-Falconi et al., 2015). Features available for comparison span wave positioning, amplitude, and spectral properties, among others (Abdeldayem and Bourlai, 2019). An inherent advantage of this methodology is its minimal consumption of computational resources and battery power per verification. The simplicity of implementation further enhances its appeal, making it adaptable on various mobile devices. However, a notable downside remains its relatively lower authentication accuracy.

On the other hand, current research-centric authentication algorithms predominantly use machine learning approaches. Alongside traditional machine-learning methods such as Random Forest (Asif et al., 2023) and SVM (Hejazi et al., 2016a), there is a growing trend towards validating models using deep neural networks (Rincon-Melchor et al., 2023; Prakash et al., 2023; Islam et al., 2022). Three dominant strategies emerge in feature extraction for machine learning model training: first, derived fiducial point characteristics from the time domain Kim et al. (2022); second, translated these into frequency domain attributes (Sun et al., 2022); and third, obtained features directly through deep neural networks (Srivastva et al., 2022; Asif et al., 2023). A notable contribution from (Huang et al., 2020) involved the use of a deep learning technique to distill distinctive representations of ECG features and discern their interaction, ultimately achieving commendable accuracy in off-person ECG recognition.

A method of authentication using SVM was proposed by Hejazi et al. (2016b). The method first uses the continuous wavelet transform to convert the ECG signal from the time domain to the time-frequency domain, thus providing both time and frequency information about the signal (Aguiar-Conraria and Soares, 2011). The method is used to train the SVM model by extracting autocorrelation features. The methodology achieved an average EER of less than 3 per cent using a simple model basis.

Convolutional neural networks have achieved very good results in the field of image processing. Currently, its application in the field of ECG recognition also has great promise. A recent study extracted features and enabled convolutional neural networks to be trained by using the Transformer (Vaswani et al., 2017) approach (Rincon-Melchor et al., 2023). An average performance of 99% accuracy was achieved with a very large set of datasets. Although it is not practical to configure this method for wearable devices, its superior performance may point the way to future developments.

Behavioral-based method: Authentication of this nature is predominantly based on the analysis of distinct user behaviors. Each individual exhibits unique operational or behavioral tendencies. Recognizing the nuances among these behaviors facilitates authentication. Within the realm of wearables, these behaviors manifest as gait, gestures, and other habits.

Among them, authentication through gait is a hot topic in current research. Now there are two main ways to realize the authentication method based on gait. The first is training with deep learning/machine learning models (Ntantogian et al., 2015; Gafurov et al., 2007a; Zeng et al., 2017). As there is currently no large amount of gait data available to train the model, the model is prone to poor performance outside of the training data set and lacks generalizability (O'Mahony et al., 2020). The second is identification through hand-made features (Avola et al., 2024). It uses the researcher's understanding of motion science to select the most useful features for recognizing gait to train the model. The advantage of this type of approach is that it does not require a large dataset to train a usable model.

However, since gait features are observable features, they are susceptible to impersonation/spoof attacks (Gafurov et al., 2007b). To solve the problem of easy imitation of gait features, the easiest way to improve the robustness of authentication is to introduce more authentication factors. It is by introducing biohash information as a second factor in authentication that the gaithashing method improves security (Ntantogian et al., 2015).

In addition to using gait, using the user's gestures is also an option. Chauhan et al. (2016) have implemented a scheme for the authentication of smart glasses by recognizing hand gestures. Smart glasses are usually equipped with a touchpad that the user can tap or swipe (forward, backward, or downward) to control the smart glasses. In the scheme of Chauhan et al. (2016), it is by recognizing these gestures on the touchpad that the user is authenticated. The method uses each touch's pressure, position, and duration as features for training using support vector machines with Gaussian radial basis function kernel. The method achieves a high accuracy rate in user identification. However, one drawback in their approach is that when training the machine learning algorithm, the real authentication information of other users is used as a negative sample and there is a risk of compromising the authentication information of other users. In addition to the user touching the touchpad directly to achieve gesture authentication, Huh et al. (2023) proposed a gesture authentication method that is better for the user. The user simply makes a fist or opens the palm of the hand, and the wrist-worn device plays a sound and collects it with a microphone. Due to the different structure of the wrists of different people, the sound collected will be significantly different. This allows for effective user authentication.

Multifactor authentication can also be achieved by monitoring other body metrics for wearable devices. The method devised by Vhaduri and Poellabauer (2019) is achieved using a combination of three biometric techniques: behavioral (steps), physiological (heart rate), and hybrid (calorie burn and metabolic equivalent of task). The method achieves an authentication accuracy rate of 93% when the user is sedentary and 90% when not sedentary. Piciucco et al. (2021) then successfully used Electrical Skin Activity (EDA) and Blood Volume Pulses (BVP) collected by the wearable device to identify the user. This method uses convolutional neural networks to extract discriminative features from the combined spectrograms of the collected data. The average correct recognition rate in the experiment was 98.58% if the test sample was guaranteed to last 30 s.

A common drawback of authentication methods that depend on acquiring physiological data is the prolonged registration time required (Vhaduri and Poellabauer, 2019; Piciucco et al., 2021). These methods often require that users interact with the device for a substantial period of time to collect sufficient physiological data to distinguish between different individuals. Similarly, for accurate user authentication, these systems require a longer data collection period.

Image-based method: This mode of authentication is now ubiquitously integrated into a variety of devices. The process relies primarily on sensors that capture distinctive user features, encompassing fingerprints, facial patterns, and the iris. Given the advancements in smart glasses technology, there is a growing interest in the feasibility of iris-based authentication for wearable devices (Lee et al., 2004). However, real-world implementation of iris authentication remains an active area of research. Ruiz-Albacete et al. (2008) have unveiled a method that mimics iris authentication using counterfeit images. In contrast, Wang et al. (2013b) introduced a technique to counteract these deceptive attempts to authenticate the iris, specifically designed for smart glasses.

4.2.3. Possession-based authentication

Possession-based authentication is also known as a token-based authentication method. This form of authentication is based on an object that the user has. This approach requires minimal user participation, enabling authentication as long as the user retains the correct item or device (Peltier and Peltier, 2016; Rittenhouse and Chaudhry, 2015). In this scenario, the wearable device is similar to a physical token, and the external device is unlocked by recognizing the wearable device worn by the user. Furthermore, for wearable devices, continuous implicit authentication can be used to ensure that the user of the device has not changed, providing better security than using other devices alone. The use of wearable devices as an authentication method provides better security for wearable devices than other devices alone by providing implicit continuous authentication to ensure that the device user has not changed.

A more straightforward implementation of this type of solution would be to store a certificate issued by a trusted certificate authority on the wearable device. In cases where authentication is necessary, the wearable transmits the certificate to the terminal for verification using an infrared link (Ullah et al., 2019).

TouchAUth is an authentication method that does not require certificates (Yan et al., 2019; Miao et al., 2023). The scheme is based on the fact that the induced Body Electric Potentials (iBEPs) of two proximity locations on the same human body are similar. When a user needs to unlock a smart device, they touch the device with the hand that is wearing the smartwatch, and it is unlocked. A similar solution to that used by TouchAUth is sound-proof, which achieves authentication based on the fact that the ambient sound around two approaching devices should be similar (Karapanos et al., 2015). Determine if a device can be unlocked by comparing the similarity of ambient sounds collected by the end device and the phone. However, the approach is vulnerable to passive "environmental guessing" and active "environmental manipulation" attacks. To address this problem, (Shrestha et al., 2024) proposed a way to perform authentication by generating random speech. When a user tries to log in, the authentication device generates a short random code and converts it into speech. If the wearable device's audio recording contains this code and is similar enough to the authentication device it can be authenticated.

4.3. Integrity issues

As integrity is critical to any device, many schemes have now been proposed to verify the integrity of wearable devices and to verify the integrity of other devices through wearable devices. In this sub-section, we summarize how these methods are implemented.

4.3.1. Verifying the integrity of wearable devices

Due to the resource limitations of wearable devices, it is often not possible to run complex detection programs on wearable devices. In order to be able to check the integrity of the equipment information, this is usually conducted with the help of other equipment. Shebaro et al. (2012) encode the information sent by the sensors using a lightweight Bloom filter and perform decoding and verification work at the base station. The method is effective in detecting packet loss attacks and faulty sensor nodes by dynamically adjusting the routing to avoid using these faulty nodes for communication.

Chinaei et al. (2021)'s proposed method of detecting integrity is then implemented via blockchain. Another currently mainstream method of achieving integrity is through blockchain. Due to its decentralized control and tamper-proof nature, blockchain is now widely used to develop trusted communication systems (Tschorsch and Scheuermann, 2016). Hossein builds a distributed platform to implement an on-demand authentication solution by leveraging the tamper-proof.

character of blockchain databases. For wearable health monitoring devices, hospitals can interact with connected devices for witnessing services. Ali et al. (2014) use a data proof protocol to ensure that the information passed by the device has not been modified. The protocol generates link fingerprints by exploiting the symmetrical spatio-temporal properties of the wireless channel. The fingerprint is complex for an attacker to forge and is unique to both communicating parties. This allows a third party to verify the transaction details at a later date.

4.3.2. Verifying the integrity through wearable devices

On the other hand, due to the easy portability of wearable devices, some studies have also used wearable devices to ensure the integrity of user input. IvoriWatch (Shrestha et al., 2020) is a method of verifying the integrity of user input by a user wearing a watch or wristband. The wearable device captures hand movements by capturing data input from the user and sends the collected data to a remote host. The remote host compares the correlation between the user's hand movements and the user's input. The user input will only be confirmed if it is sufficiently correlated.

5. Privacy issues in wearable health monitoring devices

In this section, we focus on the privacy issues raised on wearable health monitoring devices.

5.1. Direct privacy breach

Most direct privacy breaches for medical wearables are due to vulnerabilities in the data management system. Quite a lot of research has been conducted to improve device privacy security in terms of both cloud-based data management and wearable device data management. In this subsection, we will describe how each of these approaches is implemented.

5.1.1. Cloud server data management

Depending on the amount of data and equipment, current data management platforms can be divided into two categories: large-scale data management and small-scale equipment data management. For the former platform, privacy protection is currently achieved mainly through database access management. Yi et al. (2015)'s approach achieves the protection of patient privacy by separating the patient data collected by the device into three numbers and then storing them in separate data servers. As long as one of the data servers is not compromised, an attacker cannot gain access to patient information. Moreover, arbitrary database managers can provide data to medical personnel, but they have no way of knowing what the content of the data is. This method successfully ensures that insiders do not steal patient data. Wang et al. (2019)'s approach is also used to address the issue of patient privacy on cloud platforms. In their scheme a system was proposed to support fine-grained search authorization. Furthermore, the solution implements a hidden access policy to avoid attackers inferring user privacy through access rights. But these two methods may limit researchers if they need to analyze patient data. Yi et al. (2015)'s systems used to analyze patient data only include mean, correlation, variance and regression analysis, which may not be adequate for the analysis needs. Meanwhile, Wang et al. (2019)'s system can only perform simple single keyword searches or joint keyword searches, and data cannot be analyzed by combining it with machine learning. How to provide enough information for researchers to study while ensuring patient privacy and security is the direction of future research.

In addition to a cloud server for large-scale device data management, Poh et al. (2019) propose a protocol for smart home data management. The solution consists of two main components: the solution first guarantees the confidentiality of communication between devices by means of a lightweight authentication and key protocol. Secondly, to protect the user's privacy, the method implements a searchable encryption protocol that allows the user to perform cryptographic queries on the smart device. The focus of the solution is to ensure that the privacy of a small range of devices is not compromised. However, this protocol does not achieve protection of the privacy of user data in the smart hub setting.

Cloud server platforms can significantly enhance the capabilities of wearable health monitoring devices and aid in the accessibility of data for patients and healthcare practitioners (Yang et al., 2016). However, it also provides new ways for attackers to steal user data. Most of these cloud server data management solutions that we have described in this article secure the system at the expense of limiting functionality. Future research will need to find a balance between cloud server functionality and security.

5.1.2. Wearable device data management

Another aspect of ensuring the privacy of wearable devices is to ensure that attackers do not steal privacy through the device. By isolating applications on wearable devices from each other, the underlying system can be effectively protected from erroneous or malicious application code. The Hardin et al. (2018) solution achieves this with the help of a memory protection module. And their solution can be deployed using only ultralow-power microprocessors. In addition, the deployment of the solution does not have a significant impact on the battery life of the device. Fernandes et al. (2016)'s approach, on the other hand, is to ensure that user privacy is not compromised by more careful management of the application's data flows. When an application requests data that involves sensitive user data, the application needs to assert its data flow requirements and perform operations in accordance with its asserted data flow. Their approach effectively prevents applications from compromising user privacy through data flows, including implicit data flows. However, this framework also places a burden on developers who must be aware of what code is operating on sensitive data.

In terms of data management for wearable devices, most of the current approaches require new hardware to be added to the device or new requirements to be added when developing applications, which makes it very difficult to promote these methods. Therefore, new standards for application development and device design for wearable health monitoring devices are needed in the future to promote privacy protection of devices.

5.2. Indirect privacy breach

Indirect privacy breaches are mainly caused by sensors in wearable devices. In this subsection, we will describe what user privacy may be compromised by these sensor data leaks.

5.2.1. Input inference

Inferring user input is achieved mainly through the motion and sound sensors on the wearable device. In this subsection, we will describe each of these two methods.

Motion-based input inference: This part of the attack focuses on detecting the user's wrist movements to infer information such as passwords entered by the user on the keyboard. Previous research has demonstrated reasonably high inference accuracy of input information for various devices such as input on POS machines (Liu et al., 2015), QWERT keyboards (Liu et al., 2015; Wang et al., 2015), and virtual keyboards on mobile phones (Maiti et al., 2018) when accelerated sensor detection data is obtained.

Inferring the user's keystrokes is usually done in two steps. The first step is keystroke detection: to determine the start and end of each keystroke input; the second step is keystroke inference: keystroke inference is used to infer what the user has typed this time. The attacker generally uses the data from the acceleration sensor to analyze the start and end of keystrokes. Keystroke detection can also be assisted by using the microphone devices in the smartwatch (Liu et al., 2015). Keystroke inference is also generally achieved by using motion sensors. They were using the smartwatch to collect the trajectory of the user's hand to infer the user output. Predicting the user's input on the numeric keypad is generally performed by using machine learning algorithms (Liu et al., 2015; Maiti et al., 2018). Inferring input on the QWERT keyboard is much more difficult. This is because the smartwatch can only capture the trajectory of one of the user's hands, i.e. half of the keyboard's input is captured intelligently. However, an attacker can infer the words entered by the user using dictionary inference (Goodrich et al., 2006) or point cloud fitting in conjunction with a Bayesian model (Wang et al., 2015).

Audio-based input inference: This method uses each keystroke's start and end times and the interval between keystrokes to infer what was typed. Much work has been undertaken in the past to infer what the user is typing on the keyboard from the information collected by the microphone (Asonov and Agrawal, 2004; Halevi and Saxena, 2010, 2012). Most of this work was completed through the microphone on the PC. Previous research (Halevi and Saxena, 2010) has also shown that if the microphone is too far away from the input, the accuracy of its predictions will be significantly reduced. And this attack can also be combined with machine learning algorithms to achieve a higher character prediction accuracy (64%) (Halevi and Saxena, 2012).

On the other hand, capturing the vibrations of a smartphone during transmission to a medical device via a microphone could potentially be used to infer the encryption key (Kim et al., 2015). Halevi and Saxena (2010) also report that the auxiliary audio channel can be compromised by proximity eavesdropping. A pairing attack within a range of 3 ft was able to achieve a success rate of over 97%. Furthermore, the microphone data from the device may reveal private information about the user in addition to the user's private information as well as that of those around the user. This leakage is unconscious to the people around them, who may not know that their information may have been leaked.

Previous research (Eberz et al., 2018; Rushanan et al., 2014) has demonstrated that because wearable devices are worn on the user's body at all times and have multiple motion or sound sensors to detect user activity, there is a high probability of leakage of this data resulting in leakage of user input. However, many applications have access to these sensors and how to limit this privacy leakage is an issue that needs to be addressed in the future.

5.2.2. Behavioral inference

As mentioned in the previous section, EEG devices can detect the user's unique brainwaves to verify the user's identity. However, the EEG signals captured by such sensors can be misused by malicious agents, potentially compromising the user's privacy. Martinovic et al. (2012) demonstrate that the EEG information captured via inexpensive BCI devices also has the potential to leak private information about the user. The method they devised first required tricking a user using an EEG device into completing a cleverly designed classification game. In this game, several images are provided that may stimulate the user's memory. The captured brainwave information is used to determine which images are relevant to the user and deduce hidden information about the user. That hidden information may include bank card passwords, place of residence, and user contacts (Martinovic et al., 2012). However, their approach is still a long way from practical use. Firstly, there has to be a way to access the brainwave information collected by the BCI device, and secondly, the user has to be tricked into completing the game they have designed while wearing the device. Lastly, and most importantly, they did not achieve accurate prediction of the user's private information through this method. Their experiments used information entropy to measure user information leakage rate which was only 10%–20% of the total information, with a maximum value of approximately 43%.

Another method of stealing users' brainwaves to compromise their privacy, proposed by Xiao et al. (2019), is more complete. They first reverse-engineered the framework of a home EEG system, from which they identified flaws in the design and implementation of the system. Moreover, two easy-to-use PoC attacks have been designed through these flaws. An attacker can remotely access the user's brainwave data through a carefully designed program. On the other hand, an attacker can also steal the user's brainwave data directly by getting close to the victim. This solution solves the problem of the difficulty of physically accessing the user's brainwave data. Xiao et al. (2019) proposed a new joint recurrent convolutional neural network model to predict users' activities. By evaluating the model with real-world EEG data, the model achieves an accuracy of 70. 55% to infer user activity.

In addition to inferring what the user is thinking, how wearables can be used to infer a user's personality and mood has also been widely studied (Zufferey et al., 2023; Li et al., 2022). Information such as the wearer's personality and mood can be inferred to a certain extent from the information collected by the device such as the number of steps taken, heart rate, sleep time, and changes in battery level. This information could potentially be used to send more targeted adverts to the wearer and design marketing strategies.

With the continuous development of brainwave detection devices and body monitoring devices, more devices will enter people's daily life in the future, or help doctors detect the state of patients. How to filter the information collected by the devices so that the user's privacy is not compromised is a direction for future research.

5.2.3. Biometrics inference

In real-life scenarios, it would not be easy to obtain user biometric data in the target context. These systems often have well-established defense strategies (Eberz et al., 2018). However, an attacker can obtain the user's biometric data by tricking the user into using another system that uses the same type of biometrics. Such attacks are then referred to as cross-context attacks (Eberz et al., 2018), where experiments analyzed whether attackers were able to feature predictions of five biometric information – ECG, eye movements, mouse movements, touchscreen dynamics and gait – through such cross-contextual attacks. Their experiments show that such attacks against biometric information theft are feasible. These biometrics generally have particular predictable features. Cross-contextual attacks on eye movements, mouse movements, and touch screen input were easier among these five biometric features. Cross-context attacks on the ECG and gait are much more challenging to achieve.

There has not been much research into stealing biometric information from users via wearable devices for use in other scenarios. The current accuracy of the method is not yet very high. However, as the accuracy of device detection increases and machine learning algorithms develop, this method of stealing user biometric information will also become possible.

6. Research challenge and future direction

Due to the scarcity of healthcare resources, the use of wearable health monitoring devices to improve healthcare efficiency has become a main trend today. And with the emergence of the Internet of Things model, the widespread use of medical wearables has led to a number of threats and attacks on the security and privacy of individuals based on these devices. In recent years, the security and privacy concerns of wearable devices have gained a great deal of attention. However, we expect these issues to continue to be of concern due to the complexity of use scenarios, the variety of devices, and the immaturity of the solutions. For the medical sector, there are currently two challenges in the design of these devices. Firstly, these devices are unable to employ complex encryption systems because of their constrained resources, especially regarding computational power and energy capacity (Huang et al., 2015; Hester et al., 2016). Secondly, these measures should not disrupt the patient's treatment process. Physicians must have continuous access to the data collected by these devices and be able to provide medical assistance during emergencies without any hindrance (Chen et al., 2018). Unfortunately, current measures do not adequately address security/privacy threats to medical wearables. The information stored on medical wearables, such as health conditions, consultation records, or prescription records, also makes them a prime target for many adversaries. In this section, we discuss future research directions for medical wearables in order to ensure the security and privacy of healthcare systems.

Lack of targeted solutions: The potential vulnerabilities and attacker capabilities of wearable devices applied in medical systems may be very different compared to other domains. The majority of the existing solutions are designed for situations encountered by users in their everyday activities. However, these solutions often overlook the various conditions that can emerge during patient treatments (Yi et al., 2018). Furthermore, most of the research work has focused on a single aspect of the constituent healthcare systems. Combining different solutions in a real-world scenario can cause problems such as slow device response and mismatch between solutions. In future work, it will be necessary to design a solution specifically for use in medical scenarios with wearable devices.

Lack of standard communication protocols: Developing detailed communication standards for healthcare devices will help manufacturers design new devices with a basis for compliance. For wearable health monitoring devices, obtaining certification according to international standards is essential for entry into the medical market. Regrettably, these standards are currently oriented toward the development and design of risk assessment (Dickens and Cook, 2006). However, for wearable devices, which need to be used in conjunction with various other devices, the specific environment in which they are used is more complex than in a development environment. Inadequate software design has resulted in numerous security weaknesses and associated vulnerabilities, including SQL injection and buffer overflow. These vulnerabilities are linked to flaws in the communication protocol (Walter, 2018). This is why a set of communication standards for medical wearables should be developed as a future research direction, which is crucial for product developers. It will help developers propose a standard solution to various threats.

Lack of a lightweight universal platform: While certain wearable gadgets like smartwatches and smart glasses offer substantial computing capabilities, most wearable technology still suffers from limitations in terms of storage capacity and computational power. Hence, developing a wearable device platform requires a lightweight design. A lightweight system is crucial for ensuring the reliable operation of the device (Das et al., 2017; Coelho et al., 2021). Furthermore, the use of wearable health monitoring devices often requires a connection to multiple devices to work together. The manufacturers, application software, communication protocols and operating systems of these devices may all be different. Most of today's security solutions have been developed for a single product in response to existing threats. Therefore, most platforms are not generic and do not have a way of addressing a wide range of security issues.

Lack of an energy management system: Wearable devices are constrained by limited resources and energy. Engaging in repetitive and complex operations results in increased additional energy usage, thereby considerably shortening their usable time. Hussein et al. (2022). In developing security systems for wearable devices, it is essential to achieve a balance between energy consumption and energy demands to prolong the device's lifespan. Moreover, the device must be capable of withstanding various types of DoS attacks and ensure that energy is conserved effectively (Shrestha and Saxena, 2017).

Lack of zero-effort authentication: For users of medical wearables, the odds are that they will have limited mobility. To facilitate the authentication of these patients, the pursuit of zero-effort authentication on medical wearables becomes a future endeavor. In addition, the various sensors on these wearable devices make it possible to achieve zero-effort authentication. In our previous sections, we have described the attempts of many researchers to use various biometric characteristics such as brain waves, gait, heart rate, and other methods of authentication. However, most of these authentication methods take long to authenticate or require tedious operations (Arias-Cabarcos et al., 2021; Hejazi et al., 2016b; Luque et al., 2018). Therefore, future work is underway to improve the performance of these authentication methods to make these wearable medical devices more suitable for use in medical scenarios.

Lack of intrusion detection system: Since medical wearables not only hold confidential patient information but also play a significant role in patient care, they are increasingly becoming targets for attackers. These devices typically operate in interconnected networks, and the breach of one device can potentially affect others (Makhdoom et al., 2023). An intrusion detection system is therefore needed to detect the various possible attacks that a device may encounter. The system should proactively alert the patient or healthcare provider when the device is under attack. In future research, researchers should focus on developing a standard intrusion detection system for use in the medical field to secure devices.

Defending against side-channel attacks: The use of encryption technology can effectively secure the communications of wearable devices, thereby reducing privacy breaches. However, even if the device is encrypted, many users' privacy can still be compromised through the side channel. In earlier sections, we have explained the ways in which user privacy may be compromised by retrieving data from different sensors on the device (Maiti et al., 2018; Liu and Li, 2018). Data such as user input, passwords, and even biometrics can be inferred using these sensor data. This privacy leakage problem can be partially solved by reducing signal strength and adding noise. However, it is still a challenge to provide a generic solution to address the various side channel privacy leaks of devices.

Cloud server privacy protection: Storing patient data via cloud servers is increasingly becoming a common solution. For both patients and medical staff it is easy to view the patient's current status via the cloud server. In addition, the cloud server enables the wearable device to provide additional functionality, such as helping doctors visually analyze the patient's disease process. However, the use of cloud servers also brings with the risk of privacy breaches. As these data are often related to the privacy of the patient, the data should be encrypted before being stored. Although numerous query and computational techniques have been developed to safeguard the privacy of cloud servers, they might not be appropriate for resource-constrained devices like wearables (Yang et al., 2016; Wang et al., 2019). And most of these privacy query solutions designed for use on cloud platforms sacrifice the platform's analytics in order to keep data secure. This makes it difficult for healthcare professionals to analyze patients' data. Future research will therefore need to investigate how encryption schemes can be optimized to work on wearable devices. And there is a need to find a balance between security and functionality when it comes to querying data from cloud servers.

Robust design: For wearable health monitoring devices, it is vital to ensure the usability of the device. Many software or hardware defects will inevitably occur during the manufacture of equipment, and it is impossible to cover all faults through testing. This necessitates incorporating fault tolerance into the equipment to facilitate its ability to detect, diagnose, and rectify faults as they arise, while maintaining the functionality of the remaining equipment. Beyond hardware malfunctions, fault tolerance is also essential to ensure the device's operability in case of software errors (Albahri et al., 2019). On the other hand, these devices also need to provide easier access, authentication and operation modes in the event of an emergency to ensure that resuscitation is completed efficiently.

Lightweight remote testing: Ensuring the integrity of the device is vital to its security. For medical devices, without ensuring the integrity of the device, there is no guarantee that the correct treatment will be provided to the patient. While we have outlined several remote attestation schemes for verifying the integrity of wearables, only a small number are specifically designed to accommodate wearable devices with constrained resources (Shebaro et al., 2012; Chinaei et al., 2021). Therefore, it is necessary to design lightweight integrity verification and verification mechanisms for wearable devices in future work.

Machine learning and big data: In the healthcare field there is now a gradual promotion of the use of big data and machine learning algorithms to help healthcare providers in the diagnosis, treatment, and prognostic guidance of patients. By using these data big data analysis and machine learning model training can be performed. For wearable devices they are often involved in both data collection and model prediction. By attacking wearable devices it is possible to inject poison data or steal trained machine learning models. Previous work has proposed method to steal deep neural network models running on wearable devices via electromagnetic probes (Batina et al., 2019). Some recent work has proposed identifying flaws in machine learning in healthcare systems by adversarial machine learning attacks (Finlayson et al., 2019; Newaz et al., 2020). Therefore, in future research, it is necessary to ensure the integrity of the data collected by wearable devices and to prevent the theft of trained models.

Legislation: Current regulations for wearable health monitoring devices include mainly the European Union General Data Protection Regulation (GDPR) (GDPR, 2016) and the United States Health Insurance Portability and Accountability Act (HIPAA) (O'herrin et al., 2004). Both regulations primarily protect user privacy and security. They standardize the flow of healthcare information and mandate the protection of personal identity information within the medical and health insurance industries. The establishment of these regulations has effectively raised both patient and physician confidence about the use of these devices. In addition, studies have shown that these regulations have reduced the average level of user concern about privacy (Paul et al., 2020). However, it should be noted that when healthcare providers offer services online, information sharing can become complex. For example, regulatory issues may arise when the doctor providing the service and the patient are not in the same state or even the same country, thus prompting the need for new standardized laws regarding licensing, certification, and protection adapted to different circumstances

7. Conclusion

This study provides a comprehensive and integrated analysis of the literature on the safety aspects of wearable health monitoring devices. It can be seen that medical wearables offer increasingly complex and diverse functionality, and there is a trend to connect devices to networks to provide richer functionality. A side effect of these trends is that these devices will also face new security and privacy concerns. We have divided the literature into two categories, security issues and privacy issues, based on the categories of security problems. After reviewing recent research, we have suggested future directions for research and development to address the shortcomings of current security strategies. We believe that this survey will help future workers become familiar with these attack and defense strategies against wearable health monitoring devices.

CRediT authorship contribution statement

Bonan Zhang: Writing – review & editing, Writing – original draft. **Chao Chen:** Writing – review & editing, Supervision. **Ickjai Lee:** Writing – review & editing, Supervision. **Kyungmi Lee:** Writing – review & editing, Supervision. **Kok-Leong Ong:** Writing – review & editing, Supervision.

Declaration of competing interest

Declaration of Interest Statement: There are no potential conflicts of interest with this paper.

Data availability

No data was used for the research described in the article.

References

Abdeldayem, S.S., Bourlai, T., 2019. A novel approach for ECG-based human identification using spectral correlation and deep learning. IEEE Trans. Biom. Behav. Identity Sci. 2 (1), 1–14.

Actions, T.C., 2016. Fitbit sleep tracker class action settlement. URL https://topclassactions.com/lawsuit-settlements/closed-settlements/fitbit-sleep-tracker-class-action-settlement/.

Agrafioti, F., Gao, J., Hatzinakos, D., Yang, J., 2011. Heart biometrics: Theory, methods and applications. Biometrics 3 (199–216), 25.

Aguiar-Conraria, L., Soares, M.J., 2011. The Continuous Wavelet Transform: A Primer. Technical Report, NIPE-Universidade do Minho.

Albahri, O.S., Albahri, A.S., Zaidan, A., Zaidan, B., Alsalem, M., Mohsin, A.H., Mohammed, K., Alamoodi, A.H., Nidhal, S., Enaizan, O., et al., 2019. Fault-tolerant mhealth framework in the context of IoT-based real-time wearable health data sensors. IEEE Access 7, 50052–50080.

Ali, S.T., Sivaraman, V., Ostry, D., Tsudik, G., Jha, S., 2014. Securing first-hop data provenance for bodyworn devices using wireless link fingerprints. IEEE Trans. Inf. Forensics Secur. 9 (12), 2193–2204.

Alugubelli, N., Abuissa, H., Roka, A., 2022. Wearable devices for remote monitoring of heart rate and heart rate variability—what we know and what is coming. Sensors 22 (22), 8903.

Anand, S.A., Saxena, N., 2018. Noisy vibrational pairing of IoT devices. IEEE Trans. Dependable Secur. Comput. 16 (3), 530–545.

Andres-Maldonado, P., Ameigeiras, P., Prados-Garzon, J., Navarro-Ortiz, J., Lopez-Soler, J.M., 2017. Narrowband IoT data transmission procedures for massive machine-type communications. IEEE Netw. 31 (6), 8–15.

Arfaoui, A., Boudia, O.R.M., Kribeche, A., Senouci, S.-M., Hamdi, M., 2020. Context-aware access control and anonymous authentication in WBAN. Comput. Secur. 88, 101496.

Arias-Cabarcos, P., Fallahi, M., Habrich, T., Schulze, K., Becker, C., Strufe, T., 2023. Performance and usability evaluation of brainwave authentication techniques with consumer devices. ACM Trans. Priv. Secur. 26 (3), 1–36.

Arias-Cabarcos, P., Habrich, T., Becker, K., Becker, C., Strufe, T., 2021. Inexpensive brainwave authentication: new techniques and insights on user acceptance. In: 30th USENIX Security Symposium. USENIX Security 21, pp. 55–72.

Armando, A., Basin, D., Boichut, Y., Chevalier, Y., Compagna, L., Cuéllar, J., Drielsma, P.H., Héam, P.C., Kouchnarenko, O., Mantovani, J., et al., 2005. The AVISPA tool for the automated validation of internet security protocols and applications. In: International Conference on Computer Aided Verification. Springer, pp. 281–285.

Arteaga-Falconi, J.S., Al Osman, H., El Saddik, A., 2015. ECG authentication for mobile devices. IEEE Trans. Instrum. Meas. 65 (3), 591–600.

Asif, M.S., Faisal, M.S., Dar, M.N., Hamdi, M., Elmannai, H., Rizwan, A., Abbas, M., 2023. Hybrid deep learning and discrete wavelet transform-based ECG biometric recognition for arrhythmic patients and healthy controls. Sensors 23 (10), 4635.

Asonov, D., Agrawal, R., 2004. Keyboard acoustic emanations. In: IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004. IEEE, pp. 3–11.

Ates, H.C., Nguyen, P.Q., Gonzalez-Macia, L., Morales-Narváez, E., Güder, F., Collins, J.J., Dincer, C., 2022. End-to-end design of wearable sensors. Nat. Rev. Mater. 7 (11), 887–907.

Avola, D., Cinque, L., De Marsico, M., Fagioli, A., Foresti, G.L., Mancini, M., Mecca, A., 2024. Signal enhancement and efficient DTW-based comparison for wearable gait recognition. Comput. Secur. 137, 103643.

Baig, M.M., Gholamhosseini, H., Connolly, M.J., 2013. A comprehensive survey of wearable and wireless ECG monitoring systems for older adults. Med. Biol. Eng. Comput. 51 (5), 485–495.

Banerjee, S., Hemphill, T., Longstreet, P., 2018. Wearable devices and healthcare: Data sharing and privacy. Inf. Soc. 34 (1), 49–57.

Barfield, W., 2015. Fundamentals of Wearable Computers and Augmented Reality. CRC Press.

Batina, L., Bhasin, S., Jap, D., Picek, S., 2019. CSI NN: Reverse engineering of neural network architectures through electromagnetic side channel. In: 28th USENIX Security Symposium. USENIX Security 19, pp. 515–532.

Biswas, D., Everson, L., Liu, M., Panwar, M., Verhoef, B.E., Patki, S., Kim, C.H., Acharyya, A., Van Hoof, C., Konijnenburg, M., et al., 2019. CorNET: Deep learning framework for PPG-based heart rate estimation and biometric identification in ambulant environment. IEEE Trans. Biomed. Circuits Syst. 13 (2), 282–291.

Blasco, J., Chen, T.M., Tapiador, J., Peris-Lopez, P., 2016. A survey of wearable biometric recognition systems. ACM Comput. Surv. 49 (3), 1–35.

Bonneau, J., Herley, C., Van Oorschot, P.C., Stajano, F., 2012. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In: 2012 IEEE Symposium on Security and Privacy. IEEE, pp. 553–567.

Castaneda, D., Esparza, A., Ghamari, M., Soltanpur, C., Nazeran, H., 2018. A review on wearable photoplethysmography sensors and their potential future applications in health care. Int. J. Biosens. Bioelectron. 4 (4), 195.

Chauhan, J., Asghar, H.J., Mahanti, A., Kaafar, M.A., 2016. Gesture-based continuous authentication for wearable devices: The smart glasses use case. In: International Conference on Applied Cryptography and Network Security. Springer, pp. 648–665.

Chen, M., Ma, Y., Li, Y., Wu, D., Zhang, Y., Youn, C.H., 2017. Wearable 2.0: Enabling human-cloud integration in next generation healthcare systems. IEEE Commun. Mag. 55 (1), 54–61.

Chen, Y., Sun, W., Zhang, N., Zheng, Q., Lou, W., Hou, Y.T., 2018. Towards efficient fine-grained access control and trustworthy data processing for remote monitoring services in IoT. IEEE Trans. Inf. Forensics Secur. 14 (7), 1830–1842.

Chen, W., Yu, C., Tu, C., Lyu, Z., Tang, J., Ou, S., Fu, Y., Xue, Z., 2020. A survey on hand pose estimation with wearable sensors and computer-vision-based methods. Sensors 20 (4), 1074.

Cheng, Y., Wang, K., Xu, H., Li, T., Jin, Q., Cui, D., 2021. Recent developments in sensors for wearable device applications. Anal. Bioanal. Chem. 413 (24), 6037–6057.

Chinaei, M.H., Gharakheili, H.H., Sivaraman, V., 2021. Optimal witnessing of healthcare IoT data using blockchain logging contract. IEEE Internet Things J. 8 (12), 10117–10130.

Clausing, D.I.E., Schiefer, M., Lösche, U., Morgenstern, D.I.M., 2015. Security evaluation of nine fitness trackers. Indep. IT- Secur. Inst..

Coelho, Y.L., dos Santos, F.d.S., Frizera-Neto, A., Bastos-Filho, T.F., 2021. A lightweight framework for human activity recognition on wearable devices. IEEE Sensors J. 21 (21), 24471–24481.

Condon, A., Willatt, G., 2018. ECG biometrics: the heart of data-driven disruption? Biom. Technol. Today 2018 (1), 7–9.

Coskun, V., Ozdenizci, B., Ok, K., 2015. The survey on near field communication. Sensors 15 (6), 13348–13405.

Das, A.K., Pathak, P.H., Chuah, C.N., Mohapatra, P., 2016. Uncovering privacy leakage in BLE network traffic of wearable fitness trackers. In: Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications. pp. 99–104.

Das, A.K., Wazid, M., Kumar, N., Khan, M.K., Choo, K.K.R., Park, Y., 2017. Design of secure and lightweight authentication protocol for wearable devices environment. IEEE J. Biomed. Heal. Inform. 22 (4), 1310–1322.

David, D.S., Jeyachandran, A., 2016. A comprehensive survey of security mechanisms in healthcare applications. In: 2016 International Conference on Communication and Electronics Systems. ICCES, IEEE, pp. 1–6.

Dementyev, A., Hodges, S., Taylor, S., Smith, J., 2013. Power consumption analysis of bluetooth low energy, ZigBee and ANT sensor nodes in a cyclic sleep scenario. In: 2013 IEEE International Wireless Symposium. IWS, IEEE, pp. 1–4.

Di Pietro, R., Guarino, S., Verde, N.V., Domingo-Ferrer, J., 2014. Security in wireless ad-hoc networks–a survey. Comput. Commun. 51, 1–20.

Dickens, B., Cook, R.J., 2006. Legal and ethical issues in telemedicine and robotics. Int. J. Gynecol. Obs. 94 (1), 73–78.

Dinesen, B., Nonnecke, B., Lindeman, D., Toft, E., Kidholm, K., Jethwani, K., Young, H.M., Spindler, H., Oestergaard, C.U., Southard, J.A., et al., 2016. Personalized telehealth in the future: a global research agenda. J. Med. Internet Res. 18 (3), e53.

Djapic, R., Vivier, G., Zhen, B., Wang, J., Lee, J., Haiming, W., 2018. Wearables white paper.

Du, H., Wen, Q., Zhang, S., 2019. An efficient certificateless aggregate signature scheme without pairings for healthcare wireless sensor network. IEEE Access 7, 42683–42693.

Eberz, S., Lovisotto, G., Patane, A., Kwiatkowska, M., Lenders, V., Martinovic, I., 2018. When your fitness tracker betrays you: Quantifying the predictability of biometric features across contexts. In: 2018 IEEE Symposium on Security and Privacy. SP, IEEE, pp. 889–905.

Ehrich, J., Pettoello-Mantovani, M., Molloy, E., Kerbl, R., Vural, M., Lenton, S., publications team Jonathan North, O., Observatory, C.W.E., 2020. The challenges of adapting hospital care for children to changing needs in Europe. pp. 22–52.

Engineering, M., 2021. Wearable health patch technology. https://www.2mel.nl/wearable-health-patch/.

Fernandes, E., Paupore, J., Rahmati, A., Simionato, D., Conti, M., Prakash, A., 2016. {FlowFence}: Practical data protection for emerging {IoT} application frameworks. In: 25th USENIX Security Symposium. USENIX Security 16, pp. 531–548.

Ferro, E., Potorti, F., 2005. Bluetooth and wi-fi wireless protocols: a survey and a comparison. IEEE Wirel. Commun. 12 (1), 12–26.

Finlayson, S.G., Bowers, J.D., Ito, J., Zittrain, J.L., Beam, A.L., Kohane, I.S., 2019. Adversarial attacks on medical machine learning. Science 363 (6433), 1287–1289. http://dx.doi.org/10.1126/science.aaw4399, URL https://www.science.org/doi/abs/10.1126/science.aaw4399, arXiv:https://www.science.org/doi/pdf/10.1126/science.aaw4399.

Fiore, U., Castiglione, A., De Santis, A., Palmieri, F., 2017. Exploiting battery-drain vulnerabilities in mobile smart devices. IEEE Trans. Sustain. Comput. 2 (2), 90–99.

Fowler, J., 2021. Report: Fitness tracker data breach exposed 61 million records and user data online. URL https://www.websiteplanet.com/blog/gethealth-leak-report/.

Frehill, P., Chambers, D., Rotariu, C., 2007. Using zigbee to integrate medical devices. In: 2007 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE, pp. 6717–6720.

Gafurov, D., Snekkenes, E., Bours, P., 2007a. Gait authentication and identification using wearable accelerometer sensor. In: 2007 IEEE Workshop on Automatic Identification Advanced Technologies. IEEE, pp. 220–225.

Gafurov, D., Snekkenes, E., Bours, P., 2007b. Spoof attacks on gait authentication system. IEEE Trans. Inf. Forensics Secur. 2 (3), 491–502.

GDPR, G., 2016. General data protection regulation. 679, Regulation (EU).

Gomes, N., Pato, M., Lourenço, A.R., Datia, N., 2023. A survey on wearable sensors for mental health monitoring. Sensors 23 (3), 1330.

Goodrich, M.T., Sirivianos, M., Solis, J., Tsudik, G., Uzun, E., 2006. Loud and clear: Human-verifiable authentication based on audio. In: 26th IEEE International Conference on Distributed Computing Systems. ICDCS'06, IEEE, 10–10.

Guardian, T., 2018. Fitness tracking app gives away location of secret US army bases. URL https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

Gurrin, C., Qiu, Z., Hughes, M., Caprani, N., Doherty, A.R., Hodges, S.E., Smeaton, A.F., 2013. The smartphone as a platform for wearable cameras in health research. Am. J. Prev. Med. 44 (3), 308–313.

Halevi, T., Saxena, N., 2010. On pairing constrained wireless devices based on secrecy of auxiliary channels: The case of acoustic eavesdropping. In: Proceedings of the 17th ACM Conference on Computer and Communications Security. pp. 97–108.

Halevi, T., Saxena, N., 2012. A closer look at keyboard acoustic emanations: random passwords, typing styles and decoding techniques. In: Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. pp. 89–90.

Hardin, T., Scott, R., Proctor, P., Hester, J., Sorber, J., Kotz, D., 2018. Application memory isolation on ultra-low-power MCUs. In: 2018 USENIX Annual Technical Conference. USENIX ATC 18, pp. 127–132.

Hathaliya, J.J., Tanwar, S., Evans, R., 2020. Securing electronic healthcare records: A mobile-based biometric authentication approach. J. Inf. Secur. Appl. 53, 102528.

Hatzivasilis, G., Papaefstathiou, I., Manifavas, C., 2015. Password hashing competition-survey and benchmark. Cryptol. ePrint Arch..

He, D., Chan, S., Tang, S., 2013. A novel and lightweight system to secure wireless medical sensor networks. IEEE J. Biomed. Heal. Inform. 18 (1), 316–326.

He, D., Kumar, N., Wang, H., Wang, L., Choo, K.K.R., Vinel, A., 2016. A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network. IEEE Trans. Dependable Secur. Comput. 15 (4), 633–645.

Heinrich, A., Bittner, N., Hollick, M., 2022. Airguard-protecting android users from stalking attacks by apple find my devices. In: Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks. pp. 26–38.

Heinrich, A., Stute, M., Kornhuber, T., Hollick, M., 2021. Who can *find my* devices? Security and privacy of apple's crowd-sourced bluetooth location tracking system. Proc. Priv. Enhancing Technol. 2021 (3), 227–245. http://dx.doi.org/10.2478/popets-2021-0045, URL https://www.sciendo.com/article/10.2478/popets-2021-0045.

Hejazi, M., Al-Haddad, S.A.R., Singh, Y.P., Hashim, S.J., Aziz, A.F.A., 2016a. ECG biometric authentication based on non-fiducial approach using kernel methods. Digit. Signal Process. 52, 72–86.

Hejazi, M., Al-Haddad, S.A.R., Singh, Y.P., Hashim, S.J., Aziz, A.F.A., 2016b. ECG biometric authentication based on non-fiducial approach using kernel methods. Digit. Signal Process. 52, 72–86.

Hemapriya, D., Viswanath, P., Mithra, V., Nagalakshmi, S., Umarani, G., 2017. Wearable medical devices—Design challenges and issues. In: 2017 International Conference on Innovations in Green Energy and Healthcare Technologies. IGEHT, IEEE, pp. 1–6.

Hester, J., Peters, T., Yun, T., Peterson, R., Skinner, J., Golla, B., Storer, K., Hearndon, S., Freeman, K., Lord, S., et al., 2016. Amulet: An energy-efficient, multi-application wearable platform. In: Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM. pp. 216–229.

Huang, J., Badam, A., Chandra, R., Nightingale, E.B., 2015. {WearDrive}: Fast and {Energy – Efficient} storage for wearables. In: 2015 USENIX Annual Technical Conference. USENIX ATC 15, pp. 613–625.

Huang, Y., Yang, G., Wang, K., Liu, H., Yin, Y., 2020. Learning joint and specific patterns: A unified sparse representation for off-the-person ECG biometric recognition. IEEE Trans. Inf. Forensics Secur. 16, 147–160.

Huh, J.H., Shin, H., Kim, H., Cheon, E., Song, Y., Lee, C.H., Oakley, I., 2023. Wristacoustic: Through-wrist acoustic response based authentication for smartwatches. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 6 (4), 1–34.

Hussein, D., Bhat, G., Doppa, J.R., 2022. Adaptive energy management for self-sustainable wearables in mobile health. In: Proceedings of the AAAI Conference on Artificial Intelligence, vol. 36, (11), pp. 11935–11944.

Hutchins, B., Reddy, A., Jin, W., Zhou, M., Li, M., Yang, L., 2018. Beat-pin: A user authentication mechanism for wearable devices through secret beats. In: Proceedings of the 2018 on Asia Conference on Computer and Communications Security. pp. 101–115.

Imtiaz, S.A., Logesparan, L., Rodriguez-Villegas, E., 2014. Performance-power consumption tradeoff in wearable epilepsy monitoring systems. IEEE J. Biomed. Heal. Inform. 19 (3), 1019–1028.

Ioannidou, I., Sklavos, N., 2021. On general data protection regulation vulnerabilities and privacy issues, for wearable devices and fitness tracking applications. Cryptography 5 (4), 29.

Iqbal, S.M., Mahgoub, I., Du, E., Leavitt, M.A., Asghar, W., 2021. Advances in healthcare wearable devices. NPJ Flex. Electron. 5 (1), 9.

Islam, M.S., Alhichri, H., Bazi, Y., Ammour, N., Alajlan, N., Jomaa, R.M., 2022. Heartprint: A dataset of multisession ECG signal with long interval captured from fingers for biometric recognition. Data 7 (10), 141.

Iwakiri, S., Murao, K., 2023. User authentication method for wearable ring devices using active acoustic sensing. In: Proceedings of the 2023 ACM International Symposium on Wearable Computers. pp. 17–21.

Jablon, D., 2001. IEEE P1363 standard specifications for public-key cryptography. In: CTO Phoenix Technologies Treasurer, IEEE P1363 NIST Key Management Workshop.

Jin, X., Li, L., Dang, F., Chen, X., Liu, Y., 2022. A survey on edge computing for wearable technology. Digit. Signal Process. 125, 103146.

Jin, W., Li, M., Murali, S., Guo, L., 2020. Harnessing the ambient radio frequency noise for wearable device pairing. In: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. pp. 1135–1148.

Kaewkannate, K., Kim, S., 2016. A comparison of wearable fitness devices. BMC Public Health 16 (1), 1–16.

Karapanos, N., Marforio, C., Soriente, C., Capkun, S., 2015. {Sound – Proof}: Usable {Two – Factor} authentication based on ambient sound. In: 24th USENIX Security Symposium. USENIX Security 15, pp. 483–498.

Khamis, M., Alt, F., Hassib, M., von Zezschwitz, E., Hasholzner, R., Bulling, A., 2016. Gazetouchpass: Multimodal authentication using gaze and touch on mobile devices. In: Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems. pp. 2156–2164.

Khan, S., Parkinson, S., Grant, L., Liu, N., Mcguire, S., 2020. Biometric systems utilising health data from wearable devices: applications and future challenges in computer security. ACM Comput. Surv. 53 (4), 1–29.

Kim, Y., Lee, W.S., Raghunathan, V., Jha, N.K., Raghunathan, A., 2015. Vibration-based secure side channel for medical devices. In: 2015 52nd ACM/EDAC/IEEE Design Automation Conference. DAC, IEEE, pp. 1–6.

Kim, H., Phan, T.Q., Hong, W., Chun, S.Y., 2022. Physiology-based augmented deep neural network frameworks for ECG biometrics with short ECG pulses considering varying heart rates. Pattern Recognit. Lett. 156, 1–6.

Klein, D.V., 1990. Foiling the cracker: A survey of, and improvements to, password security. In: Proceedings of the 2nd USENIX Security Workshop. pp. 5–14.

Kumar, P., Clark, M.L., 2012. Kumar and Clark's Clinical Medicine E-Book. Elsevier Health Sciences.

Kumar, A., Passi, A., 2010. Comparison and combination of iris matchers for reliable personal authentication. Pattern Recognit. 43 (3), 1016–1026.

Labati, R.D., Muñoz, E., Piuri, V., Sassi, R., Scotti, F., 2019. Deep-ECG: Convolutional neural networks for ECG biometric recognition. Pattern Recognit. Lett. 126, 78–85.

Lee, J.J., Noh, S., Park, K.R., Kim, J., 2004. Iris recognition in wearable computer. In: International Conference on Biometric Authentication. Springer, pp. 475–483.

Li, L., Chen, C., Pan, L., Zhang, J., Xiang, Y., 2023. Sigd: A cross-session dataset for ppg-based user authentication in different demographic groups. In: 2023 International Joint Conference on Neural Networks. IJCNN, IEEE, pp. 1–8.

Li, Q., Ding, D., Conti, M., 2015. Brain-computer interface applications: Security and privacy challenges. In: 2015 IEEE Conference on Communications and Network Security. CNS, IEEE, pp. 663–666.

Li, J., He, Z., Cui, Y., Wang, C., Chen, C., Yu, C., Zhang, M., Liu, Y., Ma, S., 2022. Towards ubiquitous personalized music recommendation with smart bracelets. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 6 (3), 1–34.

Li, X., Ibrahim, M.H., Kumari, S., Sangaiah, A.K., Gupta, V., Choo, K.K.R., 2017a. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. Comput. Netw. 129, 429–443.

Li, Z., Pei, Q., Markwood, I., Liu, Y., Zhu, H., 2017b. Secret key establishment via RSS trajectory matching between wearable devices. IEEE Trans. Inf. Forensics Secur. 13 (3), 802–817.

Li, C., Raghunathan, A., Jha, N.K., 2011. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In: 2011 IEEE 13th International Conference on E-Health Networking, Applications and Services. IEEE, pp. 150–156.

Li, X., Zeng, Q., Luo, L., Luo, T., 2020. T2pair: Secure and usable pairing for heterogeneous iot devices. In: Proceedings of the 2020 Acm Sigsac Conference on Computer and Communications Security. pp. 309–323.

Liang, X., Peterson, R., Kotz, D., 2018. Securely connecting wearables to ambient displays with user intent. IEEE Trans. Dependable Secur. Comput. 17 (4), 676–690.

Lins, L.F.T.d., do Nascimento, E.G.C., da Silva Júnior, J.A., de Medeiros Fernandes, T.A.A., de Andrade, M.F., de Mesquita Andrade, C., 2023. Accuracy of wearable electronic device compared to manual and automatic methods of blood pressure determination. Med. Biol. Eng. Comput. 61 (10), 2627–2636.

Liu, Y., Li, Z., 2018. aleak: Privacy leakage through context-free wearable side-channel. In: IEEE INFOCOM 2018-IEEE Conference on Computer Communications. IEEE, pp. 1232–1240.

Liu, X., Zhou, Z., Diao, W., Li, Z., Zhang, K., 2015. When good becomes evil: Keystroke inference with smartwatch. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. pp. 1273–1285.

Lomotey, R.K., Pry, J., Sriramoju, S., 2017. Wearable IoT data stream traceability in a distributed health information system. Pervasive Mob. Comput. 40, 692–707.

Lorincz, K., Malan, D.J., Fulford-Jones, T.R., Nawoj, A., Clavel, A., Shnayder, V., Mainland, G., Welsh, M., Moulton, S., 2004. Sensor networks for emergency response: challenges and opportunities. IEEE Pervasive Comput. 3 (4), 16–23.

Luque, J., Cortes, G., Segura, C., Maravilla, A., Esteban, J., Fabregat, J., 2018. End-to-end photopleth ysmography (PPG) based biometric authentication by using convolutional neural networks. In: 2018 26th European Signal Processing Conference. EUSIPCO, IEEE, pp. 538–542.

Ly, K., Jin, Y., 2016. Security studies on wearable fitness trackers. In: 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE.

Lyakhov, P., Kiladze, M., Lyakhova, U., 2021. System for neural network determination of atrial fibrillation on ECG signals with wavelet-based preprocessing. Appl. Sci. 11 (16), 7213.

Maiti, A., Jadliwala, M., He, J., Bilogrevic, I., 2018. Side-channel inference attacks on mobile keypads using smartwatches. IEEE Trans. Mob. Comput. 17 (9), 2180–2194.

Makhdoom, I., Abolhasan, M., Franklin, D., Lipman, J., Zimmermann, C., Piccardi, M., Shariati, N., 2023. Detecting compromised IoT devices: Existing techniques, challenges, and a way forward. Comput. Secur. 132, 103384.

Mann, S., 1997. Wearable computing: A first step toward personal imaging. Computer 30 (2), 25–32.

Marsico, M.D., Mecca, A., 2019. A survey on gait recognition via wearable sensors. ACM Comput. Surv. 52 (4), 1–39.

Martin, T., Jovanov, E., Raskovic, D., 2000. Issues in wearable computing for medical monitoring applications: a case study of a wearable ECG monitoring device. In: Digest of Papers. Fourth International Symposium on Wearable Computers. IEEE, pp. 43–49.

Martinovic, I., Davies, D., Frank, M., Perito, D., Ros, T., Song, D., 2012. On the feasibility of {Side – Channel} attacks with {Brain – Computer} interfaces. In: 21st USENIX Security Symposium. USENIX Security 12, pp. 143–158.

Miao, Y., Gu, C., Yan, Z., Chau, S.Y., Tan, R., Lin, Q., Hu, W., He, S., Chen, J., 2023. Touchkey: Touch to generate symmetric keys by skin electric potentials induced by powerline radiation. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 7 (2), 1–21.

Mosenia, A., Sur-Kolay, S., Raghunathan, A., Jha, N.K., 2017. Wearable medical sensor-based system design: A survey. IEEE Trans. Multi- Scale Comput. Syst. 3 (2), 124–138.

Nakamura, T., Goverdovsky, V., Mandic, D.P., 2017. In-ear EEG biometrics for feasible and readily collectable real-world person authentication. IEEE Trans. Inf. Forensics Secur. 13 (3), 648–661.

Newaz, A.I., Haque, N.I., Sikder, A.K., Rahman, M.A., Uluagac, A.S., 2020. Adversarial attacks to machine learning-based smart healthcare systems. In: GLOBECOM 2020-2020 IEEE Global Communications Conference. IEEE, pp. 1–6.

Nguyen, T., Memon, N.D., 2017. Smartwatches locking methods: A comparative study. In: SOUPS.

Nguyen, T., Memon, N., 2018. Tap-based user authentication for smartwatches. Comput. Secur. 78, 174–186.

Ntantogian, C., Malliaros, S., Xenakis, C., 2015. Gaithashing: a two-factor authentication scheme based on gait features. Comput. Secur. 52, 17–32.

O'herrin, J.K., Fost, N., Kudsk, K.A., 2004. Health insurance portability accountability act (HIPAA) regulations: effect on medical record research. Ann. Surg. 239 (6), 772–778.

O'Mahony, N., Campbell, S., Carvalho, A., Harapanahalli, S., Hernandez, G.V., Krpalkova, L., Riordan, D., Walsh, J., 2020. Deep learning vs. traditional computer vision. In: Advances in Computer Vision: Proceedings of the 2019 Computer Vision Conference (CVC), Volume 1 1. Springer, pp. 128–144.

Ometov, A., Shubina, V., Klus, L., Skibińska, J., Saafi, S., Pascacio, P., Flueratoru, L., Gaibor, D.Q., Chukhno, N., Chukhno, O., et al., 2021. A survey on wearable technology: History, state-of-the-art and current challenges. Comput. Netw. 193, 108074.

Ortolani, O., Conti, A., Di Filippo, A., Adembri, C., Moraldi, E., Evangelisti, A., Maggini, M., Roberts, S., 2002. EEG signal processing in anaesthesia. Use of a neural network technique for monitoring depth of anaesthesia. Br. J. Anaesth. 88 (5), 644–648.

Pandian, P., Mohanavelu, K., Safeer, K., Kotresh, T., Shakunthala, D., Gopal, P., Padaki, V., 2008. Smart vest: Wearable multi-parameter remote physiological monitoring system. Med. Eng. Phys. 30 (4), 466–477.

Pantelopoulos, A., Bourbakis, N., 2008. A survey on wearable biosensor systems for health monitoring. In: 2008 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE, pp. 4887–4890.

Pantelopoulos, A., Bourbakis, N.G., 2009. A survey on wearable sensor-based systems for health monitoring and prognosis. IEEE Trans. Syst. Man, Cybern. Part C (Appl. Rev.) 40 (1), 1–12.

Park, E., Kim, K.J., Kwon, S.J., 2016. Understanding the emergence of wearable devices as next-generation tools for health communication. Inf. Technol. People 29 (4), 717–732.

Patidar, P., Goel, M., Agarwal, Y., 2023. VAX: Using existing video and audio-based activity recognition models to bootstrap privacy-sensitive sensors. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 7 (3), 1–24.

Paul, C., Scheibe, K., Nilakanta, S., 2020. Privacy concerns regarding wearable IoT devices: how it is influenced by GDPR?.

Peltier, T.R., Peltier, J., 2016. Complete Guide to CISM Certification. Auerbach Publications.

Piciucco, E., Di Lascio, E., Maiorana, E., Santini, S., Campisi, P., 2021. Biometric recognition using wearable devices in real-life settings. Pattern Recognit. Lett. 146, 260–266.

Poh, G.S., Gope, P., Ning, J., 2019. Privhome: Privacy-preserving authenticated communication in smart home environment. IEEE Trans. Dependable Secur. Comput. 18 (3), 1095–1107.

Pourbemany, J., Zhu, Y., Bettati, R., 2023. A survey of wearable devices pairing based on biometric signals. IEEE Access.

Prabhakararao, E., Dandapat, S., 2020. Myocardial infarction severity stages classification from ECG signals using attentional recurrent neural network. IEEE Sens. J. 20 (15), 8711–8720.

Prakash, A.J., Patro, K.K., Samantray, S., Pławiak, P., Hammad, M., 2023. A deep learning technique for biometric authentication using ECG beat template matching. Information 14 (2), 65.

Rathore, H., Mohamed, A., Al-Ali, A., Du, X., Guizani, M., 2017. A review of security challenges, attacks and resolutions for wireless medical devices. In: 2017 13th International Wireless Communications and Mobile Computing Conference. IWCMC, IEEE, pp. 1495–1501.

Ren, Y., Zheng, Z., Xu, S., Li, H., 2021. User identification leveraging whispered sound for wearable devices. IEEE Trans. Mob. Comput. 22 (3), 1841–1855.

Research, G.V., 2018. Wearable technology market size analysis report 2028. https://www.grandviewresearch.com/industry-analysis/wearable-technology-market.

Revadigar, G., Javali, C., Xu, W., Vasilakos, A.V., Hu, W., Jha, S., 2017. Accelerometer and fuzzy vault-based secure group key generation and sharing protocol for smart wearables. IEEE Trans. Inf. Forensics Secur. 12 (10), 2467–2482.

Rieback, M.R., Crispo, B., Tanenbaum, A.S., 2006. Is your cat infected with a computer virus? In: Fourth Annual IEEE International Conference on Pervasive Computing and Communications. PERCOM'06, IEEE, 10–pp.

Rincon-Melchor, V., Nakano-Miyatake, M., Juarez-Sandoval, O., Olivares-Mercado, J., Moreno-Saenz, J., Benitez-Garcia, G., 2023. Deep learning algorithm for the people identification using their ECG signals as a biometric parameter. In: 2023 46th International Conference on Telecommunications and Signal Processing. TSP, IEEE, pp. 154–159.

Rittenhouse, R., Chaudhry, J., 2015. A survey of alternative authentication methods. In: International Conference on Recent Advances in Computer Systems. Atlantis Press, pp. 179–182.

Roth, V., Richter, K., Freidinger, R., 2004. A PIN-entry method resilient against shoulder surfing. In: Proceedings of the 11th ACM Conference on Computer and Communications Security. pp. 236–245.

Ruiz-Albacete, V., Tome-Gonzalez, P., Alonso-Fernandez, F., Galbally, J., Fierrez, J., Ortega-Garcia, J., 2008. Direct attacks using fake images in iris verification. In: European Workshop on Biometrics and Identity Management. Springer, pp. 181–190.

Rushanan, M., Rubin, A.D., Kune, D.F., Swanson, C.M., 2014. Sok: Security and privacy in implantable medical devices and body area networks. In: 2014 IEEE Symposium on Security and Privacy. IEEE, pp. 524–539.

Scarfone, K., Padgette, J., et al., 2008. Guide to bluetooth security. NIST Spec. Publ. 800 (2008), 121.

Sempionatto, J.R., Lin, M., Yin, L., Pei, K., Sonsa-ard, T., de Loyola Silva, A.N., Khorshed, A.A., Zhang, F., Tostado, N., Xu, S., et al., 2021. An epidermal patch for the simultaneous monitoring of haemodynamic and metabolic biomarkers. Nat. Biomed. Eng. 5 (7), 737–748.

Seneviratne, S., Hu, Y., Nguyen, T., Lan, G., Khalifa, S., Thilakarathna, K., Hassan, M., Seneviratne, A., 2017. A survey of wearable devices and challenges. IEEE Commun. Surv. Tutor. 19 (4), 2573–2620.

Shebaro, B., Sultana, S., Reddy Gopavaram, S., Bertino, E., 2012. Demonstrating a lightweight data provenance for sensor networks. In: Proceedings of the 2012 ACM Conference on Computer and Communications Security. pp. 1022–1024.

Shi, C., Wang, Y., Chen, Y.J., Saxena, N., 2021. Authentication of voice commands by leveraging vibrations in wearables. IEEE Secur. Priv. 19 (6), 83–92.

Shrestha, P., Liu, Z., Saxena, N., 2020. Ivoriwatch: Exploring transparent integrity verification of remote user input leveraging wearables. In: Annual Computer Security Applications Conference. pp. 706–716.

Shrestha, P., Mahdad, A.T., Saxena, N., 2024. Sound-based two-factor authentication: Vulnerabilities and redesign. ACM Trans. Priv. Secur. 27 (1), 1–27.

Shrestha, P., Saxena, N., 2017. An offensive and defensive exposition of wearable computing. ACM Comput. Surv. 50 (6), 1–39.

Shuai, M., Liu, B., Yu, N., Xiong, L., 2019. Lightweight and secure three-factor authentication scheme for remote patient monitoring using on-body wireless networks. Secur. Commun. Netw. 2019.

Siddiqi, M., Ali, S.T., Sivaraman, V., 2019. Secure opportunistic contextual logging for wearable healthcare sensing devices. IEEE Trans. Dependable Secur. Comput. 18 (2), 753–764.

Smith, S.J., 2005. EEG in the diagnosis, classification, and management of patients with epilepsy. J. Neurol. Neurosurg. Psychiatry 76 (suppl 2), ii2–ii7.

Spaccarotella, C.A.M., Migliarino, S., Mongiardo, A., Sabatino, J., Santarpia, G., De Rosa, S., Curcio, A., Indolfi, C., 2021. Measurement of the QT interval using the apple watch. Sci. Rep. 11 (1), 10817.

Sprager, S., Juric, M.B., 2015. Inertial sensor-based gait recognition: A review. Sensors 15 (9), 22089–22127.

Sridharan, M., Bigham, J., Campbell, P.M., Phillips, C., Bodanese, E., 2019. Inferring micro-activities using wearable sensing for ADL recognition of home-care patients. IEEE J. Biomed. Heal. Inform. 24 (3), 747–759.

Srinivas, J., Das, A.K., Kumar, N., Rodrigues, J.J., 2018. Cloud centric authentication for wearable healthcare monitoring system. IEEE Trans. Dependable Secur. Comput. 17 (5), 942–956.

Srivastva, R., Singh, Y.N., Singh, A., 2022. Statistical independence of ECG for biometric authentication. Pattern Recognit. 127, 108640.

Su, Y., Li, Y., Cao, Z., 2023. Gait-based privacy protection for smart wearable devices. IEEE Internet Things J..

Suh, G.E., Devadas, S., 2007. Physical unclonable functions for device authentication and secret key generation. In: 2007 44th ACM/IEEE Design Automation Conference. IEEE, pp. 9–14.

Sun, L., Zhong, Z., Qu, Z., Xiong, N., 2022. Perae: an effective personalized AutoEncoder for ECG-based biometric in augmented reality system. IEEE J. Biomed. Heal. Inform. 26 (6), 2435–2446.

Tanveer, M., Ahmad, M., Nguyen, T.N., Abd El-Latif, A.A., et al., 2022. Resource-efficient authenticated data sharing mechanism for smart wearable systems. IEEE Trans. Netw. Sci. Eng. 10 (5), 2525–2536.

Tatum IV, W.O., 2021. Handbook of EEG Interpretation. Springer Publishing Company.

Thavalengal, S., Bigioi, P., Corcoran, P., 2015. Iris authentication in handheld devices-considerations for constraint-free acquisition. IEEE Trans. Consum. Electron. 61 (2), 245–253.

Torre, I., Koceva, F., Sanchez, O.R., Adorni, G., 2016. Fitness trackers and wearable devices: how to prevent inference risks? In: Proceedings of the 11th EAI International Conference on Body Area Networks. pp. 125–131.

Tschorsch, F., Scheuermann, B., 2016. Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutor. 18 (3), 2084–2123.

Ullah, I., Alomari, A., Ul Amin, N., Khan, M.A., Khattak, H., 2019. An energy efficient and formally secured certificate-based signcryption for wireless body area networks with the internet of things. Electronics 8 (10), 1171.

Van Nguyen, T., Sae-Bae, N., Memon, N., 2017. DRAW-A-PIN: Authentication using finger-drawn PIN on touch devices. Comput. Secur. 66, 115–128.

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A.N., Kaiser, Ł., Polosukhin, I., 2017. Attention is all you need. Adv. Neural Inf. Process. Syst. 30.

Vhaduri, S., Poellabauer, C., 2019. Multi-modal biometric-based implicit authentication of wearable device users. IEEE Trans. Inf. Forensics Secur. 14 (12), 3116–3125.

Von Zezschwitz, E., Dunphy, P., De Luca, A., 2013. Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices. In: Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services. pp. 261–270.

Walter, C.W., 2018. The Personal Fog: an Architecture for Limiting Wearable Security Vulnerabilities. The University of Tulsa.

Wang, C., Guo, X., Wang, Y., Chen, Y., Liu, B., 2016a. Friend or foe? Your wearable devices reveal your personal pin. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. pp. 189–200.

Wang, H., Lai, T.T.-T., Roy Choudhury, R., 2015. Mole: Motion leaks through smartwatch sensors. In: Proceedings of the 21st Annual International Conference on Mobile Computing and Networking. pp. 155–166.

Wang, C., Li, Z., Wei, X., 2013a. Monitoring heart and respiratory rates at radial artery based on PPG. Optik 124 (19), 3954–3956.

Wang, Y., Liao, T., 2022. Data integrity and causation analysis for wearable devices in 5G. In: 2022 IEEE International Conference on E-Health Networking, Application & Services (HealthCom). IEEE, pp. 142–148.

Wang, H., Ning, J., Huang, X., Wei, G., Poh, G.S., Liu, X., 2019. Secure fine-grained encrypted keyword search for e-healthcare cloud. IEEE Trans. Dependable Secur. Comput. 18 (3), 1307–1319.

Wang, T., Song, Z., Ma, J., Xiong, Y., Jie, Y., 2013b. An anti-fake iris authentication mechanism for smart glasses. In: 2013 3rd International Conference on Consumer Electronics, Communications and Networks. IEEE, pp. 84–87.

Wang, D., Zhang, Z., Wang, P., Yan, J., Huang, X., 2016b. Targeted online password guessing: An underestimated threat. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. pp. 1242–1254.

Webber, J.L., Arafa, A., Mehbodniya, A., Karupusamy, S., Shah, B., Dahiya, A.K., Kanani, P., 2023. An efficient intrusion detection framework for mitigating blackhole and sinkhole attacks in healthcare wireless sensor networks. Comput. Electr. Eng. 111, 108964.

Who, J., Consultation, F.E., 2003. Diet, nutrition and the prevention of chronic diseases. World Heal. Organ. Tech. Rep. Ser. 916 (i-viii), 1–149.

Wong, F.L., Stajano, F., Clulow, J., 2007. Repairing the bluetooth pairing protocol. In: Security Protocols: 13th International Workshop, Cambridge, UK, April 20-22, 2005, Revised Selected Papers 13. Springer, pp. 31–45.

Xiao, Y., Jia, Y., Cheng, X., Yu, J., Liang, Z., Tian, Z., 2019. I can see your brain: Investigating home-use electroencephalography system security. IEEE Internet Things J. 6 (4), 6681–6691.

Xu, W., Javali, C., Revadigar, G., Luo, C., Bergmann, N., Hu, W., 2017. Gait-key: A gait-based shared secret key generation protocol for wearable devices. ACM Trans. Sens. Netw. (TOSN) 13 (1), 1–27.

Yan, Z., Song, Q., Tan, R., Li, Y., Kong, A.W.K., 2019. Towards touch-to-access device authentication using induced body electric potentials. In: The 25th Annual International Conference on Mobile Computing and Networking. pp. 1–16.

Yang, Y., Liu, X., Deng, R.H., Li, Y., 2017. Lightweight sharable and traceable secure mobile health system. IEEE Trans. Dependable Secur. Comput. 17 (1), 78–91.

Yang, Z., Zhou, Q., Lei, L., Zheng, K., Xiang, W., 2016. An IoT-cloud based wearable ECG monitoring system for smart healthcare. J. Med. Syst. 40, 1–11.

Yaqoob, T., Abbas, H., Atiquzzaman, M., 2019. Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review. IEEE Commun. Surv. Tutor. 21 (4), 3723–3768.

Yathav, J., Bailur, A., Goyal, A., Abhinav, 2017. miBEAT based continuous and robust biometric identification system for s on-the-go applications. In: Proceedings of International Conference on Communication and Networks: ComNet 2016. Springer, pp. 269–275.

Yi, X., Bouguettaya, A., Georgakopoulos, D., Song, A., Willemson, J., 2015. Privacy protection for wireless medical sensor data. IEEE Trans. Dependable Secur. Comput. 13 (3), 369–380.

Yi, E.B., Maji, A., Bagchi, S., 2018. How reliable is my wearable: A fuzz testing-based study. In: 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. DSN, IEEE, pp. 410–417.

Zakaria, N.H., Griffiths, D., Brostoff, S., Yan, J., 2011. Shoulder surfing defence for recall-based graphical passwords. In: Proceedings of the Seventh Symposium on Usable Privacy and Security. pp. 1–12.

Zeng, Y., Pande, A., Zhu, J., Mohapatra, P., 2017. WearIA: Wearable device implicit authentication based on activity information. In: 2017 IEEE 18th International Symposium on a World of Wireless, Mobile and Multimedia Networks. WoWMoM, IEEE, pp. 1–9.

Zhang, T., Cheng, Z., Qin, Y., Li, Q., Shi, L., 2020a. Deep learning for password guessing and password strength evaluation, A survey. In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, pp. 1162–1166.

Zhang, Y., Han, D., Li, A., Zhang, L., Li, T., Zhang, Y., 2021. MagAuth: Secure and usable two-factor authentication with magnetic wrist wearables. IEEE Trans. Mob. Comput. 22 (1), 311–327.

Zhang, J., Liu, Y., Wu, D., Lou, S., Chen, B., Yu, S., 2023. VPFL: A verifiable privacy-preserving federated learning scheme for edge computing systems. Digit. Commun. Netw. 9 (4), 981–989.

Zhang, T., Lu, J., Hu, F., Hao, Q., 2014. Bluetooth low energy for wearable sensor-based healthcare systems. In: 2014 IEEE Healthcare Innovation Conference. HIC, IEEE, pp. 251–254.

Zhang, C., Shahriar, H., Riad, A.K., 2020b. Security and privacy analysis of wearable health device. In: 2020 IEEE 44th Annual Computers, Software, and Applications Conference. COMPSAC, IEEE, pp. 1767–1772.

Zhang, A., Wang, L., Ye, X., Lin, X., 2016. Light-weight and robust security-aware D2D-assist data transmission protocol for mobile-health systems. IEEE Trans. Inf. Forensics Secur. 12 (3), 662–675.

Zhang, J., Wu, D., Liu, C., Chen, B., 2020c. Defending poisoning attacks in federated learning via adversarial training method. In: Frontiers in Cyber Security: Third International Conference, FCS 2020, Tianjin, China, November 15–17, 2020, Proceedings 3. Springer, pp. 83–94.

Zhao, Y., Chen, J., Guo, Q., Teng, J., Wu, D., 2020a. Network anomaly detection using federated learning and transfer learning. In: International Conference on Security and Privacy in Digital Economy. Springer, pp. 219–231.

Zhao, G., Ge, Y., Shen, B., Wei, X., Wang, H., 2017. Emotion analysis for personality inference from EEG signals. IEEE Trans. Affect. Comput. 9 (3), 362–371.

Zhao, G., Jiang, Q., Liu, X., Ma, X., Zhang, N., Ma, J., 2022. Electrocardiogram based group device pairing for wearables. IEEE Trans. Mob. Comput..

Zhao, T., Wang, Y., Liu, J., Chen, Y., Cheng, J., Yu, J., 2020b. Trueheart: Continuous authentication on wrist-worn wearables using ppg-based biometrics. In: IEEE INFOCOM 2020-IEEE Conference on Computer Communications. IEEE, pp. 30–39.

Zhao, T., Wang, Y., Liu, J., Cheng, J., Chen, Y., Yu, J., 2021. Robust continuous authentication using cardiac biometrics from wrist-worn wearables. IEEE Internet Things J. 9 (12), 9542–9556.

Zieniewicz, M.J., Johnson, D.C., Wong, C., Flatt, J.D., 2002. The evolution of army wearable computers. IEEE Pervasive Comput. 1 (4), 30–40.

Zufferey, N., Humbert, M., Tavenard, R., Huguenin, K., 2023. Watch your watch: Inferring personality traits from wearable activity trackers. In: Proceedings of the USENIX Security Symposium (USENIX Security). p. 18.

Bonan Zhang is a Ph.D. student at RMIT. He received his bachelor's degree in software engineering from Sun Yat-Sen University, and his master's degree in computer science from University of Melbourne. His research interests include network security, biometric, healthcare system and machine learning.

Chao Chen (Member, IEEE) received the Ph.D. degree in computer science from Deakin University, Geelong, VIC, Australia, in 2017. He is currently a Senior Lecturer with the College of Business and Law, RMIT University, Melbourne, VIC, Australia. He is conducting research on applying advanced analytics to solve emerging cyber security issues, such as networks traffic classification, social spam detection, insider threat detection, and machine learning security, such as inference attacks on machine learning (ML) models.

Ickjai Lee recived PhD in 2002 from the School of Electrical Engineering and ComputerScience, University of Newcastle, in Australia. He is currently head of Information Technology school, James Cook University. He have been actively involved in working on broad areas of geoinformatics and intelligence informatics. His research interests include geospatial data mining, multiple classifiers, geospatial databases, conceptual spaces, Web 2.0, map segmentation, clustering, geo visualisation, internet of things, and Voronoi tessellations.

Kyungmi Lee received her PhD degree in Computer Science in 2007 from Griffith University, Australia. She started her academic career as a lecturer in School of Business and IT at Charles Sturt University, Australia and continued her academic pursuit after moving to James Cook University. She is an active researcher, and her research interests include machine learning, algorithm optimisation, neural networks, data mining, and applied artificial intelligence.

Kok-Leong Ong is a Professor of Business Analytics in the College of Business and Law, RMIT University. He is currently working on a range of analytics projects making data actionable through analytics-2-business translation, automation, and applications. His research focuses on analytics and machine learning translation into practice within different business verticals, and the development of new techniques as required to meet individual business needs.