Security and Privacy Concerns for Healthcare Wearable Devices and Emerging Alternative Approaches

Eleni Boumpa[1(✉)], Vasileios Tsoukas[1], Anargyros Gkogkidis[1], Georgios Spathoulas[2], and Athanasios Kakarountas[1]

[1] Intelligent Systems Laboratory, Department of Computer Science and Biomedical Informatics, University of Thessaly, Lamia, Greece
{eboumpa,vtsoukas,agkogkidis,kakarountas}@uth.gr
[2] Department of Information Security and Communication Technology, Norwegian University of Science and Technology (NTNU), Gjovik, Norway
georgios.spathoulas@ntnu.no

Abstract. The wide use of wearable devices rises a lot of concerns about the privacy and security of personal data that are collected and stored by such services. This concern is even higher when such data is produced by healthcare monitoring wearable devices and thus the impact of any data leakage is more significant. In this work a classification of the wearable devices used for healthcare monitoring is conducted, and the most prominent relevant privacy and security issues and concerns are presented. Furthermore, a brief review of alternative approaches that can eliminate most of such issues, including federated learning, homomorphic encryption, and tinyML, is presented. The aim of this work is to present the privacy and security concerns in healthcare monitoring wearable devices, as well as some solutions in hot topics about these issues.

Keywords: Privacy · Security · Wearable devices · Healthcare

1 Introduction

Wearable Devices (WDs) have already become an integral part of our lives. Research and development in relevant fields, such as the Internet of Things (IoT), Artificial Intelligence (AI), and Machine Learning (ML) continuously evolve, affecting WDs that in turn penetrate more and more in people's daily lives. The main fields of use of WDs can be generally classified as i) wellness and/or healthcare monitoring [1], ii) entertainment [2], and iii) gaming [3].

The field of WDs for healthcare monitoring is very interesting and promising from both research and industry points of view. Furthermore, the use of WDs for healthcare monitoring becomes more and more popular among users, as they can use them for various purposes, such as improving their wellness, reducing

X. Gao et al. (Eds.): MobiHealth 2021, LNICST 440, pp. 19–38, 2022.
https://doi.org/10.1007/978-3-031-06368-8_2

their stress, and monitoring their vital signals. A classification of the WDs for healthcare monitoring is proposed in [4]. As depicted in Fig. 1 the three main categories are i) e-textiles, ii) e-patches, and iii) accessories. While the last category could also be sub-classified as i) wrist-worn, ii) head-mounted, and iii) other WDs. It is observed that in the category of e-textiles, WDs mainly use smart fabric to monitor users' health. Many applications have been proposed, such as paper [5], which explores the pedestrians' safety via shoe-mounted inertial sensor. Also, the authors in [6] present a wearable accelerometer network for recognition of muscle activation in high-motion exercising.

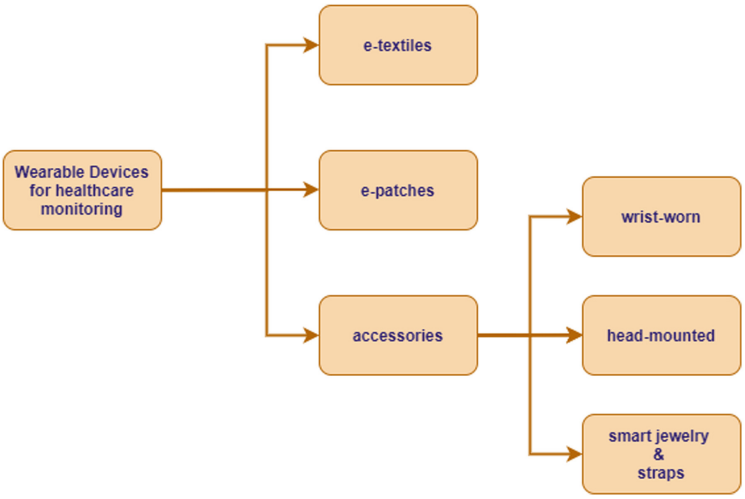

Fig. 1. The classification of WDs for healthcare monitoring as proposed by S. Seneviratne et al. [4].

The category of e-patches is the latest entry in WDs for healthcare monitoring. This category includes the sensor patches and the e-tattoo/e-skin. A research team [7] developed a patch for 24/7 health monitoring. The patch monitors electrocardiogram (ECG) and electroencephalogram (EEG) signals and transmits them in real-time, without intervening in people's daily life. An e-tattoo was proposed by Kim et al. [8]. The proposed wearable is an alcohol bio-sensing system for non-invasive alcohol monitoring via sweat.

The last category is further classified into three subcategories. The wrist-worn devices include smartwatches and wrist bands. A plethora of such WDs, that monitor users' activities and their vital signals, has been designed and produced both from research teams and the industry. A characteristic example of these WDs is presented in work [9], a smartwatch that monitors Cardiopulmonary Resuscitation (CPR). In the sub-category of head-mounted WDs, most common systems are smart eye-wear devices, such as Google Glass [10]. Many research teams have developed extensions and applications for Google Glass for healthcare

reasons, such as the authors in [11]. In this work, a real-time augmented-reality system for people suffering from color blindness has been proposed. Another type of devices that belongs in this sub-category is headsets/earbuds devices. Such a device was developed in [12], which regulates inflammation and treats rheumatoid arthritis by delivering electrical fields in the outer ear. Lastly, examples of devices that belong to the sub-category of other WDs are smart jewelry and straps. A ring [13] has been developed to monitor users' health conditions, while a custom-built microphone capturing different body vibrations from body surface has also been proposed in [14]. This WD captures and recognizes non-speech body sounds, helping in various health conditions, like respiratory physiology.

It is obvious that all WDs collect data to facilitate the services they offer, however healthcare WDs tend to monitor and collect data that are more frequently characterized as sensitive and confidential. Some characteristic examples of collected data from those WDs are location, quality of surrounding air, activity, movement, sleep, body temperature, heart rate, blood pressure, blood oxygen, and measuring cognitive functions [15]. Depending on the type and the context of each application, the confidentiality and/or the integrity of such data can be critical and thus leaking and/or tampering with those can induce high risks. This is both a big issue and a challenge for security and privacy researchers. The main focus of the present paper is to identify the highest security and privacy concerns with respect to healthcare WDs, enumerate corresponding threats, and propose alternative approaches that can significantly reduce the attack surface area of such systems.

The contribution of this work is to review the emerging approaches for securing WDs regarding healthcare applications. A classification of WDs used in healthcare monitoring is conducted, and a taxonomy of threats and attacks for these devices is presented. The main focus is to highlight the privacy concerns in sensitive healthcare information and suggest several emerging technologies as alternative possible solutions. The remainder of this paper is organized as follows: In Sect. 2 a brief review of privacy and security concerns in WDs is presented; Sect. 3 provides a classification of threats and attacks in the WDs; Sect. 4 reviews some related works about security and privacy in WDs; in Sect. 5 several solutions are presented about security and privacy in WDs; while Sect. 6 concludes the review's findings.

2 Privacy and Security Concerns in Wearable Devices

Statista's global consumer survey in 2021 estimated the number of WDs users per country. The survey reported that the users of WDs for the United Kingdom, United States, Sweden, China, and India were above 30% [16]. Only in Russia, consumers purchased four million WDs in the first nine months of 2021, while annual WDs sales increased by 400 thousand devices between the years 2019 and 2020 [17]. Moreover, in 2020 the market value of wearable medical devices in Latin America was around 665 million U.S dollars. In 2021, it is projected to amount to 777 million U.S dollars, and it is forecasted to skyrocket to a value

of 1.4 billion U.S dollars by the end of the year 2025 [18]. It is noticed that this data is being increasingly collected and processed to provide health monitoring and tracking [19]. Health-related data is identified as personal data and, more precisely, as sensitive data and the most confidential information among all types of personal data [20]. This data must be protected, transmitted only to trusted third parties, and securely stored [21]. The procedure of collecting, transmitting, and storing health-related data can raise many privacy and security concerns due to user behavior, attacks, and data breaches [22]. Furthermore, users are able to use several of those WDs to make payments, something that adds more security concerns to the aforementioned. In conclusion, the three main issues regarding security and privacy in health WDs are user behavior and perception, health-related data transfer, and data storage. A brief description follows of the aforementioned issues as they are presented in the literature [15,23,24].

2.1 User's Behavior

In 2020 a survey [25] showed that people in the fourth decade, or more, of their life, have less understanding of what sensitive data is and the importance of securing it. Another interesting finding was that many users chose not to use any authentication method to secure their devices, and the majority of them thought that they had no sensitive information stored in the devices. The users are prominent actors in the procedure of protecting their information regarding the way they use the device and protect it. Several studies revealed that users are not in a position to protect their devices due to a lack of knowledge or understanding [25–28] on how to achieve it. This raises the need for awareness campaigns and training especially to users aged 50+, on the importance of securing devices and protecting sensitive data. In 2018, a survey about the willingness to share wearable health device information among U.S. citizens 18+ years old was conducted by Statista. The results revealed that 90% of the respondents would share the information with their doctor. A 76-percentage answered that they would share data with a friend or family member, whereas almost 47% would share sensitive data with other communities or app users [29]. Another survey [23] revealed that users have a poor perception of danger and threats and cannot comprehend meanings such as security and privacy. Users tend to trust every application and wearable manufacturer with their sensitive data. The survey concludes with the conjecture that the user could possibly be the weakest link regarding security. Finally, a study [15] of 106 users, owning a health-related WD, showed that half of them were unaware of the need to protect their health information. Additionally, interviewees have a gap in knowledge about the privacy concerns associated with the data acquired by WDs.

2.2 Data Transfer

Most health-related WDs gather data and send it to the cloud for processing. The reason behind the need for transferring data to the cloud is due to the nature of the process data must go through. The high complexity of Deep Learning (DL)

algorithms and ML models requires more power and computational resources than those a small WD can provide. Moreover, most WDs collect health-related data such as heart rate, body temperature, oxygen saturation, blood pressure, and more, every few minutes or even while the user is asleep. This results in a vast amount of data that is impossible to store inside the device. WDs are configured to connect to other smart devices via Bluetooth or Wi-Fi. The data under transmission most of the time is not encrypted, and the devices under consideration have insufficient or even no wireless security mechanisms. Furthermore, when a user connects his/her private devices to work networks, may prove dangerous. WDs may act as a starting node that can open a network backdoor, due to device vulnerabilities in stealing corporate data. WDs are always connected to a network, intranet, internet, or a mesh network with other smart devices. Due to limited resources, computational power, and cost minimization requirement, WDs are not developed with security in mind. Hackers attempt to find their weakest and most vulnerable point in order to gain access or even alter data and manage the communication [30]. Moreover, despite the main advantages of bluetooth, this technology suffers from many threats and vulnerabilities with attacks such as Denial of Service (DoS), Man-in-the-middle (MITM), and eavesdropping attacks, or bluetooth-specific attacks such as bluesnarfing [31].

2.3 Data Storage

The third step of the data procedure, after capturing and transferring, is storing data in the cloud. Once data is stored in the cloud, the user does not have a clear image of how this data is manipulated and used. Additionally, this data may now be owned by the company that maintains the server and not the actual owner (the user), giving them the opportunity to use the data in ways they disclose in the user terms and agreement [32]. Two of the most common issues regarding data storage on the cloud are the DoS attacks, which could hinder data availability, and data breaches leading to sensitive information exposure. According to a study by WebsitePlanet and independent cybersecurity expert Jeremiah Fowler, over 61 million fitness tracker records from Apple and Fitbit were leaked in a data breach. The researchers determined that the data leak originated with GetHealth, a health and wellness startup that enables customers to consolidate their data from WDs, medical devices, and apps. The disclosed data belonged to users of WDs distributed around the world and included data such as their names, birth dates, weight, height, gender, and geographical location. There was no password or any cryptographic means to protect the database, and the content in plain text was easily recognizable. Fitbit was cited in more than 2,700 recordings, while Apple's Healthkit was mentioned more than 17,000 times. Additionally, researchers determined that the files included information of the location of the data on the storage medium, as well as a blueprint of the network's backend operations, making it an exceedingly simple target for attackers [33].

3 Threats and Attacks

In this section, a classification of the most common security threats and attacks is provided. Each threat is categorized in three different layers as mentioned above, about the user, data transfer, and data storage. Additionally, the impact, the likelihood for the attack, and its consequences to the triad of confidentiality-integrity-availability properties (CIA) are reported. Confidentiality is related to prohibiting access to information for unauthorized users, integrity ensures that the information is correct and unaltered, and availability guarantees that the information and/or service are always available.

Wearable Device: The first threat has to do with the device itself, and it belongs to the first layer, the user. The user may lose the device, or a malicious user could steal it. This threat has low to high impact, depending on the user; it is easy and highly possible to happen and can impact confidentiality and integrity.

Social Engineering: It also belongs in the first layer of the data procedure and involves attackers that attempt to gain the confidence of users to get the necessary information. In summary, social engineering is the skill of persuading others into disclosing sensitive information. Hackers may get information by impersonating other individuals through email, chat, or even in-person. The impact is moderate and could hinder confidentiality and integrity [34].

Brute Force Attack: This type of attack often happens as a subsequent step of previous attacks. The hacker must have physical access to the device and possibly some information about the user. What follows is many attempts based on trial and error to get access. The hacker can use an automated process with malicious software or enter random sequences of characters by hand. This type of attack could happen for access in the WD or access to the data storage infrastructure. The possibility for a successful attack can be identified as moderate, and the impact of the damage is high. This type of attack can hinder all three aspects of information security. A similar type of attack is dictionary attacks, where the attacker uses a list of the most common passwords [35–37].

Malware/Ransomware: Malicious software can be installed in the WD and access or alter sensitive information. This type of threat has a moderate impact; it is not that common and could hinder confidentiality and integrity [38]. Another similar attack is ransomware, in which the attacker uses software to encrypt the user's sensitive information and asks for a ransom to release the decryption key. A common type of attack with high impact that affects all three pillars of information security [39].

Denial of service (DoS): With this type of attack, the hacker attempts to bring a computer or network to a halt, rendering it unreachable to its authorized users. DoS attacks make this possible by flooding the target with traffic or by providing information that causes the target to crash. In all cases, the DoS attack denies

genuine users access to the service or system. DoS attacks may be classified into two broad categories: flooding services and crashing services. Flood attacks occur when the system gets an excessive amount of traffic that the server cannot buffer, leading it to slow down and finally cease operation. The most popular flood assaults are:

- *Buffer overflow* is the most used DoS attack. The goal is to send more traffic to a network address than the system's developers intended. Buffer overflow includes two other types of attacks, i) Internet Control Message Protocol (ICMP) and ii) Synchronization (SYN) flood. i) ICMP flood - takes advantage of any misconfiguration that may appear in network devices by delivering packets to every device on the targeted network, rather than just one. ii) SYN flood - initiates a request for connection with a server but never completes it. This process is repeated until all open ports are inundated with requests, and none are accessible to genuine users.
- *DoS attacks* are forming the second category, the crashing type, the attacks simply exploit flaws in the target system or service, causing it to crash. These attacks send input that exploits flaws in the target system, crashing or severely destabilizing it to the point where it cannot be accessed or utilized.
- *Distributed Denial of Service (DDoS)* assault is another category of DoS attacks. A DDoS happens when numerous systems coordinate a DoS attack on a single target. The critical distinction is that the victim is attacked simultaneously from several sites rather than being targeted from a single place.

In general, DoS attacks are common; it is an easy way to disrupt services due to automated software and may have a high impact on data storage by hindering their availability [40–43].

Rogue access point: A rogue access point is a threat deployed on a network without the consent of the network's owner. The attacker who controls the rogue access point may intercept personal and sensitive information transferred through the network. There are two categories of interception, active and passive. In the active interception, the attacker can receive the user's data, alter it, and then deliver the updated user data to the target endpoint. In the passive interception, the hacker may read the user's private information, but there is no possible way to alter the information for other malicious usages. This threat occurs in the second step of the data procedure, data transfer, it is not a common threat, and the impact is high, affecting the integrity and confidentiality [44–46].

Man in the middle attack: The man in the middle (MITM) is a kind of attack in which the attacker discreetly transmits and maybe modifies messages between two users who are under the impression that they are communicating directly with one another. A type of MITM attack is eavesdropping which is a real-time illegal interception of private communication between two parties. Another type of MITM attack is the replay attack, where the attacker intercepts the communication between users and then delays or resends messages. These attacks occur in data transfer. They are easy to perform, with a high impact on confidentiality and integrity [4,47–49].

SQL injection: Attackers insert SQL statements in input fields to gain access to private information, alter it or even delete it. An SQL injection attack could destroy a database or even a system. It is a common attack, easily achievable since the hacker only needs to type SQL statements, with high impact and affecting all three security information pillars [50,51].

In Table 1 a taxonomy of threats/attacks in the three layers of the user, the data transfer, and the data storage in WDs is depicted. The layer of the user is divided into two categories, that of the user and the device, as there are some differences in the attacks between them. Also, the CIA properties affected are pointed out for every threat/attack. Furthermore, the impact of each threat/attack, on a 3-grade scale (low, moderate, high), as well as the difficulty of every threat/attack, on a 3-grade scale (easy, medium, hard), are highlighted.

Table 1. Taxonomy of the threats and attacks in wearable devices.

Threat/Attack	User	Device	Data transfer	Data storage	Impact	Difficulty	Confidentiality	Integrity	Availability
Theft/Lost	●	○	○	○	Moderate	Easy	●	●	○
Social	●	○	○	○	Moderate	Medium	●	●	○
Brute	○	●	○	●	High	Medium	●	●	●
Guessing	○	●	○	●	High	Hard	●	●	●
Dictionary	○	●	○	●	High	Easy	●	●	●
Malware	○	●	○	●	Moderate	Medium	●	●	●
Ransomware	○	●	○	●	High	Medium	●	●	●
DoS	○	○	●	○	High	Easy	○	○	●
Rogue	○	○	●	○	High	Hard	●	●	○
MITM	○	○	●	○	High	Easy	●	●	○
Replay	○	○	●	○	High	Easy	●	●	○
Eavesdropping	○	○	●	○	High	Easy	●	●	○
SQL injection	○	○	○	●	High	Easy	●	●	●

4 Related Works

This section provides a brief review of previously accomplished works regarding the security and privacy issues in WDs. The works are reported in chronological order.

A brief review of security and privacy issues both in electronic healthcare records and wearable healthcare monitoring devices is explored in [52]. While these technologies provide many benefits for healthcare delivery to all the involved, such as patients, doctors, and familiars, some privacy and security issues, like data storage, data transfer, and data analysis rights, raise privacy and security concerns and are examined in this work.

Safavi and Shukur [53] proposed a privacy and security framework for WDs in healthcare. The developed framework can be embedded in every operating system for WDs, while it comprises ten principles for the WDs users' privacy protection.

From another point of view, Wang et al. [54] examined security concerns in WDs and suggested a multi-layered security architecture for WDs. The proposed architecture aims to prevent the system's security enemies from "breaking through" the security in all system layers. A security analysis of WDs is presented in [42]. After a brief review of the security and privacy attacks in WDs, the authors also evaluated three WDs to understand their security and privacy vulnerabilities. While the authors of work [55] conducted a survey about the lack of users' understanding regarding the security and privacy of wearable healthcare monitoring devices that they use. The respondents showed a poor understanding of threats about their recorded health data. Furthermore, the authors present a method to mitigate the results of users' security and privacy threats, through their education about this issue.

Seneviratne et al. [4] analyzed the communication security threats of WDs. They classified these threats, regarding network security, into three categories according to confidentiality, integrity, and availability. Furthermore, they presented some approaches that address these threats.

The authors of the paper [22] highlight the importance of the deployment of a framework for effective privacy, equity, and protection of users of wearable wellness and/or healthcare devices. This is a result of the fact that more and more people that live in the United States use wearable health monitoring devices. This issue raises one of the most challenging public health problems, which is a serious individual privacy concern. Also, the authors of the paper [56] conducted an ethical survey about the use of WDs in healthcare. The survey's results show that the users are concerned about their data and their usage of them from third parties. The aim of this work is to be proposed an ethical framework that considers users' privacy.

Finally, a discussion about the various privacy and security problems from the use of WDs is presented in [57]. Additionally, this work proposed both the adoption of different policies from the companies for their consumers' privacy issues and the awaken of users about the misuse of WDs and their data leakage.

5 Emerging Approaches

The model under which health monitoring service providers offer their services usually requires WDs to constantly collect health/medical-related data on the side of the user and transmit such data to their side to process for monitoring, prognosis, and/or prevention. When it comes to prognosis it is common for service providers to use ML models, which can either be user-specific or generic, to which such data is fed. While health related data is considered as very sensitive, the aforementioned model of processing set as prerequisites the transmission of such data to the service provider and the processing of that (potentially after integration with data of others), in order to produce models that will enable decision taking on the side of the user.

It is obvious that this increased flow of information from WDs to the service provider and vice versa, increases the risk of sensitive data leakage either

through cases of direct data breaches or even through cases of personal data inference from trained models [94,95]. In the present section an analysis of alternative approaches that enable the training of models in more privacy conscious workflows is presented. The emerging approaches of Federated Learning (FL), Homomorphic Encryption (HE), and Tiny Machine Learning (TinyML) have been employed to minimise data privacy issues in the last two steps of the data procedure in WDs, the data transfer and the data storage. A brief description of the aforementioned approaches and several applications of those in the field of healthcare monitoring are described in the rest of the Section.

5.1 Federated Learning

Federated Learning is an emerging technology with great scientific interest, especially in the field of healthcare [58–67]. With FL, participants are able to train ML models collaboratively by only exchanging parameters of trained models, instead of exchanging sensitive information for each participant. The approach enables the training of personalised models for each participant through a secure workflow. FL can also contribute to a better understanding of data and produced models. Additionally, FL reduces network bandwidth requirements as only parameters required for aggregation must be transmitted to the server. The technology can be classified into three main categories, horizontal FL, vertical FL, and federated transfer learning. In the first category, participants share different records of a data-set; in the second participants share different features of the same samples; and finally, in the third and last category, the participants attempt to transfer trained models between completely heterogeneous sets of data. Finally, FL can protect against known network and device attacks, while there are enhancements that ensure that no connected actor is malicious [68–72].

A team of researchers proposed FL4W [71], a FL system for WDs aiming at human activity recognition. The system's architecture is the classic client-server architecture, where the server orchestrates the devices in four different steps. In the first step devices are registered to the system. Then the server specifies the appropriate tasks and hyperparameters to broadcast to the WDs. The third step contains the local model training where every device uses data without uploading anything to the server. Finally, the parameter tables of the updated models are sent to the server, which aggregates the local models with federated averaging [73] algorithm.

FedHealth [74] is a framework for healthcare WDs. The framework utilizes the technology of FL and aims to achieve accurate personal healthcare without compromising privacy. Four different procedures are required to create intelligent WDs. To begin, a server-side cloud model is trained using publicly available data. This model is then distributed to all users, who may start training their own models using data from their devices. The user model may then be uploaded to the server to be used for the training of a new global model. It is worth mentioning that no user data or information are uploaded to the sever apart from the encrypted model parameters in this phase. The parameters are encrypted with HE, which is going to be discussed later on. Finally, any user may train

personalized models by combining the cloud model with his or her previous model and data. The system may update both the user and the cloud models concurrently in response to the latest user data. As a result, the more time a user spends with the service, the more tailored for the user the model may be. Finally, the future plans for the system are to be extended so it can be in a position to detect Parkinson's disease and developed in a way so it can be deployed in hospitals.

Finally, in work [75], an edge-based FL framework is being proposed. According to the authors, the system could aid healthcare practitioners by offering data-driven insights for illness diagnosis and prognosis by analyzing mobility levels and behaviors obtained from WDs. The suggested framework is organized into three modules: cloud, edge, and application. The cloud module will be administered by a model owner who will be responsible for coordinating different cloud-based duties such as patient registration, database maintenance, and model uploading. It consists of two primary components: a controller, which provides alerts when possibly updated global models become available, and a master aggregator, which uses techniques such as federated averaging. The global model is being trained using publicly accessible datasets so that users' sensitive information is safe. The edge module comprises three essential components: a FL server, a local-storage controller, and an aggregator. This module improves the overall training process by personalizing the models on each corresponding device. Finally, the application module enables the addition of any device capable of generating health-related data. In conclusion, the framework could be extended to support disease prevention, addiction and mental health tracking, and real-time health monitoring.

5.2 Homomorphic Encryption

Homomorphic Encryption is a technique that enables mathematical operations on encrypted data without requiring the decryption of such data. The outcome of the aforementioned actions is an encrypted result. The result in its decrypted form corresponds to the outcome of operations done on the raw data [76]. HE systems are classified into two broad types according to the sort of operations they support: HE and partially HE [77]. A system is identified as fully homomorphic if it exhibits both additive and multiplicative properties of homomorphism [78]. Although the first system was described in 1978, the first feasible fully homomorphic system was developed in 2009 [79]. While fully homomorphic schemes are believed to be safer than partially homomorphic schemes, they need much more computer resources and have a higher overhead. The somewhat HE schemes are a subcategory of the Fully Homomorphic Encryption (FHE) schemes. They include addition and multiplication, but only specific operations are permitted, and calculations are limited as the cipher-text size expands [80]. Partially homomorphic systems may allow just one type of operation at a time, either addition or multiplication and are identified as a more practicable option than fully homomorphic systems.

In work [81] the authors suggest a four-layer mobile healthcare network, which includes a WD part, a preprocessing section, a cloud server section, and a physician diagnostic portion. Then, three secure medical calculations are defined: the average heart rate, the identification of long QT syndrome, and the chi-square testing. To perform calculations on the ciphertext, the encryption of the health data is accomplished using FHE.

Using data acquired from WDs, a team [82] presented a smart responsive software that may advise in real-time patients, physicians, emergency teams, and carers. Depending on the patient's health, the relevant user will be notified to act as required and take care of the situation. To safeguard the private and sensitive information of patients undergoing treatment and care, they discuss a secure HE technique that will maintain data encryption throughout the data gathering, collecting, and processing stages.

Researchers in [83] presented a wireless sensor network for healthcare in which data is encrypted utilizing the technique of HE. The system ensures secure communication and data storage by dividing the original data into two or three portions. Additionally, the system enables forwarding nodes to transmit encrypted sensor data without decrypting it. As a consequence, even if a forwarding node is hacked, the attacker will be unable to eavesdrop on the data, providing far more privacy than older healthcare systems.

The authors of work [84] propose an end-to-end encrypted security architecture that enables safe data collection from embedded medical devices, protected processing on this data in a low-cost commodity cloud environment, and restricted delegation of access to this data to selected recipients. This solution capitalizes on recent advances in HE and Proxy Re-Encryption (PRE) to address the practical demands of a secure medical data architecture's data collection, processing, and dissemination. According to the authors this architecture reduces the cost of healthcare data systems by securely outsourcing computation to cloud computing environments, while also reducing vulnerabilities to some of the most pernicious security threats, such as insider attacks, and enabling additional cost savings through the use of lower-cost embedded medical devices.

In study [85] a privacy-preserving solution based on HE for preventing attackers from accessing medical plaintext data is suggested. Computations are spread to numerous edge virtual nodes and all arithmetic operations are masked, preventing untrusted cloud servers from knowing about the actions done on the encrypted patient data. Virtual edge nodes use cloud computing resources to perform computationally difficult mathematical operations, and minimize data transmission latency between devices and edge nodes. A comparison to prior research revealed that homomorphically encrypted data kept at the edge protects the privacy and integrity of the data.

A team in [86] proposed a privacy-preserving protocol for healthcare systems that makes use of WDs and implemented it on the Raspberry Pi, in order to determine the real efficiency of FHE over WDs. The authors developed the protocol using two FHE libraries, HElib and SEAL, on a Raspberry Pi, and a network simulator in order to quantify the computational and communication

costs associated with wireless body area networks. The results indicate that the protocol with SEAL has a lower communication overhead than the protocol with HElib. The protocol with SEAL has almost identical transmission costs to the simple protocol, which is the one that lacks encryption. SEAL was able to do more homomorphic operations per unit of plaintext than HElib. As a result, Helib, which is faster, is well suited for applications requiring low time complexity, while SEAL is well suited for applications requiring a large number of homomorphic operations.

5.3 Tiny Machine Learning

Tiny Machine Learning is one of the fastest-growing domains, attracting increased attention from the healthcare sector. TinyML is a hardware-software hybrid that allows ML models and DL algorithms to be deployed on small, reasonably inexpensive, and power-efficient devices. These devices will pave the way for new services and technologies that do not require costly and energy-intensive Graphics Processing Units (GPUs) or cloud systems that are constrained by significant restrictions with respect to security, latency, and bandwidth. A typical TinyML workflow is composed of three major phases. The first step is to train the ML model on a workstation with sufficient processing capability. Following that, the model is optimized through using model reduction methods such as pruning and quantization. Finally, the refined TinyML model is ready to be implemented in the healthcare WDs in the last stage [87–89]. ML on device is a helpful step in preventing consumers from losing or leaking data and from waiting for results due to latency and load difficulties. WDs will be used to gather, analyze, and extract data. This data is not communicated to other devices or servers, resulting in safer and more private devices. Additionally, microcontrollers are considered to be ultra-low-power devices. They typically operate in less than one mWatt and can deliver machine intelligence for the cost of a battery. TinyML may be the field that revolutionizes how we see healthcare applications today by introducing several new devices and apps that the whole healthcare research community may use. Wearable gadgets for health monitoring and prevention seem to have the highest promise for TinyML applications. They will provide real-time analysis and possible alerts without requiring data transmission or significant computational power, resulting in autonomous, intelligent, safe, and efficient devices in the form factor of a wristwatch or earwear.

The authors in [90] created a wrist device that monitors vital indicators such as body temperature, breathing pattern, and blood oxygen saturation in order to aid in the prioritization of COVID-19 patients in the emergency room. The neural network that evaluates respiration operates locally on the WD, preventing data transfer to the cloud, using TinyML technology, and protecting the privacy of patient-sensitive information.

The work [91] discusses the fields of AI, low-power wide-area network and TinyML for new safe and intelligent WDs. The research demonstrates the unique properties of these cutting-edge paradigms, concluding that the future generation of WDs will enable a broad range of fresh services and applications.

In another study [92], TinyML is recommended for customized home healthcare with the goal of assisting patients in rehabilitation, patients with chronic and acute diseases, but also caregivers' physical and emotional well-being during times of extreme stress, such as the COVID-19 pandemic.

To conclude, in [93] proposed a novel TinyML framework for healthcare is capable of the following: 1) selection or customization of ML models, 2) enhancing optimization for improved decision making, and (3) learning and adapting for improved performance. Additionally, the system will be sufficient to support a variety of e-health applications, including symptom tracking, hygiene monitoring, body scanning, and mental health.

Finally, in Table 2 a taxonomy of the aforementioned applications of emerging approaches is presented. Also, the system's type (framework, network, model, scheme, protocol, and device), as well as the Technology Readiness Lever (TRL) of each work is depicted.

Table 2. Taxonomy of the emerging approaches for security and privacy issues.

Work	Type	Federated learning	Homomorphic encryption	TinyML	TRL
[71]	Framework	●	○	○	5
[74]	Framework	●	●	○	5
[75]	Framework	●	○	○	1
[81]	Network	○	●	○	3
[82]	Model	○	●	○	3
[83]	Network	○	●	○	2
[84]	Framework	○	●	○	2
[85]	Scheme	○	●	○	2
[86]	Protocol	○	●	○	4
[90]	Device	○	○	●	6
[91]	Device	○	○	●	5
[92]	Device	○	○	●	1
[93]	Framework	○	○	●	1

6 Conclusion

This work aims to provide a brief literature review on wearable healthcare devices. However, the wide use of these devices, especially for healthcare purposes, arises several concerns about data privacy and security. The security threats and attacks that wearable devices are exposed to were identified and categorized, while the corresponding impact and difficulty were assessed. Also, the confidentiality, integrity, and availability effect of each threat has been highlighted. Furthermore, the existing emerging approaches for processing data collected in multiple WDs that strengthen security and privacy, like Federated

Learning, Homomorphic Encryption and TinyML are reviewed. A taxonomy of the proposed emerging approaches for security and privacy issues is presented. Overall, the review provides to the researchers an evaluation on security and privacy issues concerning the healthcare wearable devices that are quite common to our daily life.

References

1. Lu, L., et al.: Wearable health devices in health care: narrative systematic review. JMIR Mhealth Uhealth **8**(11), e18907 (2020)
2. Olson, J.S., Redkar, S.: A survey of wearable sensor networks in health and entertainment. MOJ Appl. Bionics Biomech. **2**(5), 280–287 (2018)
3. Future Marketing Insights. https://www.futuremarketinsights.com/reports/wearable-gaming-technology-market. Accessed 21 Oct 2021
4. Seneviratne, S., et al.: A survey of wearable devices and challenges. IEEE Commun. Surv. Tutorials **19**(4), 2573–2620 (2017)
5. Jain, S., Borgiattino, C., Ren, Y., Gruteser, M., Chen, Y., Chiasserini, C.F.: Lookup: enabling pedestrian safety services via shoe sensing. In: Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services, pp. 257–271 (2015)
6. Mokaya, F., Lucas, R., Noh, H.Y., Zhang, P.: Myovibe: vibration based wearable muscle activation detection in high mobility exercises. In: Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing, pp. 27–38 (2015)
7. ILLINOIS.EDU. https://news.illinois.edu/view/6367/233722. Accessed 21 Oct 2021
8. Kim, J., et al.: Noninvasive alcohol monitoring using a wearable tattoo-based iontophoretic-biosensing system. Acs Sens. **1**(8), 1011–1019 (2016)
9. Gruenerbl, A., Pirkl, G., Monger, E., Gobbi, M., Lukowicz, P.: Smart-watch life saver: smart-watch interactive-feedback system for improving bystander CPR. In: Proceedings of the 2015 ACM International Symposium on Wearable Computers, pp. 19–26 (2015)
10. Google Glass. https://www.google.com/glass/start/. Accessed 21 Oct 2021
11. Tanuwidjaja, E., et al.: Chroma: a wearable augmented-reality solution for color blindness. In: Proceedings of the 2014 ACM international joint conference on pervasive and ubiquitous computing, pp. 799–810 (2014)
12. Nēsos - Treat diseases by harnessing the power of the brain to regulate immune function.https://nesos.com. Accessed 21 Oct 2021
13. Ōura ring: accurate health information accessible to everyone.https://ouraring.com. Accessed 21 Oct 2021
14. Rahman, T., et al.: BodyBeat: a mobile system for sensing non-speech body sounds. In: MobiSys, vol. 14, no. 10.1145, pp. 2–594 (2014)
15. Cilliers, L.: Wearable devices in healthcare: privacy and information security issues. Health Inf. Manag. J. **49**(2–3), 150–156 (2020)
16. Wearable device usage 2021. (n.d.). Statista. https://www.statista.com/forecasts/1101110/wearables-devices-usage-in-selected-countries. Accessed 22 Oct 2021
17. Wearables sales volume in Russia 2021. (n.d.). Statista. https://www.statista.com/statistics/1243485/number-of-wearables-sold-in-russia/. Accessed 22 Oct 2021

18. Wearable medical devices market Latin America 2025. (n.d.). Statista. https://www.statista.com/statistics/800329/wearable-medical-devices-market-value-latin-america/. Accessed 22 Oct 2021
19. Khan, S., Parkinson, S., Grant, L., Liu, N., McGuire, S.: Biometric systems utilising health data from wearable devices: applications and future challenges in computer security. ACM Comput. Surv. (CSUR) **53**(4), 1–29 (2020)
20. Mehraeen, E., Ghazisaeedi, M., Farzi, J., Mirshekari, S.: Security challenges in healthcare cloud computing: a systematic. Glob. J. Health Sci. **9**(3) (2017)
21. Celdrán, A.H., et al.: PROTECTOR: towards the protection of sensitive data in Europe and the US. Comput. Netw. **181**, 107448 (2020)
22. Montgomery, K., Chester, J., Kopp, K.: Health wearables: ensuring fairness, preventing discrimination, and promoting equity in an emerging Internet-of-Things environment. J. Inf. Policy **8**, 34–77 (2018)
23. Bellekens, X.J., Nieradzinska, K., Bellekens, A., Seeam, P., Hamilton, A.W., Seeam, A.: A study on situational awareness security and privacy of wearable health monitoring devices. Int. J. Cyber Situational Aware. **1**(1), 74–96 (2016)
24. Els, F., Cilliers, L.: Improving the information security of personal electronic health records to protect a patient's health information. In: 2017 Conference on Information Communication Technology and Society (ICTAS), pp. 1–6. IEEE (2017)
25. Tsoukas, V., Gkogkidis, A., Kakarountas, A.: A survey on mobile user perceptions of sensitive data and authentication methods. In: 24th Pan-Hellenic Conference on Informatics, pp. 346–349 (2020)
26. Cilliers, L., Viljoen, K.L.A., Chinyamurindi, W.T.: A study on students' acceptance of mobile phone use to seek health information in South Africa. Health Inf. Manag. J. **47**(2), 59–69 (2018)
27. Wiercioch, A., Teufel, S., Teufel, B.: The authentication dilemma. J. Commun. **13**(8), 443–449 (2018)
28. Cherapau, I., Muslukhov, I., Asanka, N., Beznosov, K.: On the impact of touch id on iphone passcodes. In: Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), pp. 257–276 (2015)
29. Sharing of wearable health device data U.S. 2018. (n.d.). Statista. https://www.statista.com/statistics/829472/wearable-health-data-sharing-willingness-us-adults/. Accessed 22 Oct 2021
30. Siboni, S., Shabtai, A., Tippenhauer, N.O., Lee, J., Elovici, Y.: Advanced security testbed framework for wearable IoT devices. ACM Trans. Internet Technol. (TOIT) **16**(4), 1–25 (2016)
31. Shah, K.T.: Privacy and Security Issues of Wearables in Healthcare (Doctoral dissertation, Flinders University, College of Science and Engineering.) (2019)
32. Piwek, L., Ellis, D.A., Andrews, S., Joinson, A.: The rise of consumer health wearables: promises and barriers. PLoS Med. **13**(2), e1001953 (2016)
33. 61 M Fitbit, Apple Users Had Data Exposed in Wearable Device Data Breach. Healthitsecurity. https://healthitsecurity.com/news/61m-fitbit-apple-users-had-data-exposed-in-wearable-device-data-breach. Accessed 22 Oct 2021
34. Schlöglhofer, R., Sametinger, J.: Secure and usable authentication on mobile devices. In: Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia, pp. 257–262 (2014)
35. Clarke, N.: Transparent User Authentication: Biometrics. Springer Science & Business Media, RFID and behavioural profiling (2011)

36. Bellovin, S.M., Merritt, M.: Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise. In: Proceedings of the 1st ACM Conference on Computer and Communications Security, pp. 244–250 (1993)
37. Conrad, E., Misenar, S., Feldman, J.: Eleventh Hour CISSP®: Study Guide. Syngress (2016)
38. Bada, M., von Solms, B.: A Cybersecurity Guide for Using Fitness Devices (2021). arXiv preprint http://arxiv.org/abs/2105.02933
39. Garmin: the latest wearable attacked by ransomware and a controversial ransom. Panda Security Mediacenter (2020). https://www.pandasecurity.com/en/mediacenter/adaptive-defense/garmin-ransomware-attack/. Accessed 22 Oct 2021
40. What is a denial of service attack (Dos)? (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos. Accessed 23 Oct 2021
41. Arış, A., Oktuğ, S.F., Yalçın, S.B.Ö.: Internet-of-things security: denial of service attacks. In: 2015 23nd Signal Processing and Communications Applications Conference (SIU), pp. 903–906. IEEE (2015)
42. Ching, K.W., Singh, M.M.: Wearable technology devices security and privacy vulnerability analysis. Int. J. Netw. Secur. Appl. **8**(3), 19–30 (2016)
43. Hale, M.L., Lotfy, K., Gamble, R.F., Walter, C., Lin, J.: Developing a platform to evaluate and assess the security of wearable devices. Digit. Commun. Netw. **5**(3), 147–159 (2019)
44. Forensic analysis and security. Security Today. https://securitytoday.com/articles/2018/05/01/forensic-analysis-and-security.aspx. Accessed 23 Oct 2021
45. Secure Wi-Fi For Healthcare Applications. Aruba Network (n.d.). https://www.arubanetworks.com/assets/wp/WP_Healthcare_WLAN.pdf. Accessed 23 Oct 2021
46. Rai, S., Chukwuma, P., Cozart, R.: Security and Auditing of Smart Devices: Managing Proliferation of Confidential Data on Corporate and BYOD Devices. Auerbach Publications, Boca Raton (2016)
47. Melamed, T.: An active man-in-the-middle attack on bluetooth smart devices. Safety and Security Studies, vol 15 (2018)
48. Bluetooth bug opens devices to man-in-the-middle attacks. https://threatpost.com/bluetooth-bug-mitm-attacks/159124/. Accessed 23 Oct 2021
49. Hajian, R., ZakeriKia, S., Erfani, S.H., Mirabi, M.: SHAPARAK: scalable healthcare authentication protocol with attack-resilience and anonymous key-agreement. Comput. Netw. **183**, 107567 (2020)
50. Zhang, C., Shahriar, H., Riad, A.K.: Security and privacy analysis of wearable health device. In: 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 1767–1772. IEEE (2020)
51. Chen, K., et al.: Internet-of-things security and vulnerabilities: taxonomy, challenges, and practice. J. Hardware Syst. Secur. **2**(2), 97–110 (2018). https://doi.org/10.1007/s41635-017-0029-7
52. Meingast, M., Roosta, T., Sastry, S.: Security and privacy issues with health care information technology. In: 2006 International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 5453–5458. IEEE (2006)
53. Safavi, S., Shukur, Z.: Conceptual privacy framework for health information on wearable device. PLoS One **9**(12), e114306 (2014)
54. Wang, S., Bie, R., Zhao, F., Zhang, N., Cheng, X., Choi, H.A.: Security in wearable communications. IEEE Netw. **30**(5), 61–67 (2016)

55. Bellekens, X., Hamilton, A., Seeam, P., Nieradzinska, K., Franssen, Q., Seeam, A.: Pervasive eHealth services a security and privacy risk awareness survey. In: 2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA), pp. 1–4. IEEE (2016)
56. Anaya, L.S., Alsadoon, A., Costadopoulos, N., Prasad, P.W.C.: Ethical implications of user perceptions of wearable devices. Sci. Eng. Ethics **24**(1), 1–28 (2018). https://doi.org/10.1007/s11948-017-9872-8
57. Alrababah, Z.: Privacy and Security of Wearable Devices (2020)
58. Liu, J.C., Goetz, J., Sen, S., Tewari, A.: Learning from others without sacrificing privacy: simulation comparing centralized and federated machine learning on mobile health data. JMIR Mhealth Uhealth **9**(3), e23728 (2021)
59. Rieke, N., et al.: The future of digital health with federated learning. NPJ Digit. Med. **3**(1), 1–7 (2020)
60. Huang, L., Shea, A.L., Qian, H., Masurkar, A., Deng, H., Liu, D.: Patient clustering improves efficiency of federated machine learning to predict mortality and hospital stay time using distributed electronic medical records. J. Biomed. Inf. **99**, 103291 (2019)
61. Lee, J., Sun, J., Wang, F., Wang, S., Jun, C.H., Jiang, X.: Privacy-preserving patient similarity learning in a federated environment: development and analysis. JMIR Med. Inf. **6**(2), e7744 (2018)
62. Brisimi, T.S., Chen, R., Mela, T., Olshevsky, A., Paschalidis, I.C., Shi, W.: Federated learning of predictive models from federated electronic health records. Int. J. Med. Inf. **112**, 59–67 (2018)
63. Sheller, M.J., Reina, G.A., Edwards, B., Martin, J., Bakas, S.: Multi-institutional deep learning modeling without sharing patient data: a feasibility study on brain tumor segmentation. In: Crimi, A., Bakas, S., Kuijf, H., Keyvan, F., Reyes, M., van Walsum, T. (eds.) BrainLes 2018. LNCS, vol. 11383, pp. 92–104. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-11723-8_9
64. Farhad, A., Woolley, S., Andras, P.: Federated learning for AI to improve patient care using wearable and IoMT sensors. In: 2021 IEEE 9th International Conference on Healthcare Informatics (ICHI), pp. 434–434. IEEE (2021)
65. Li, W., et al.: Privacy-preserving federated brain tumour segmentation. In: Suk, H.-I., Liu, M., Yan, P., Lian, C. (eds.) MLMI 2019. LNCS, vol. 11861, pp. 133–141. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-32692-0_16
66. Fang, L., et al.: Bayesian inference federated learning for heart rate prediction. In: Ye, J., O'Grady, M.J., Civitarese, G., Yordanova, K. (eds.) MobiHealth 2020. LNICST, vol. 362, pp. 116–130. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-70569-5_8
67. Xiao, Z., Xu, X., Xing, H., Song, F., Wang, X., Zhao, B.: A federated learning system with enhanced feature extraction for human activity recognition. Knowl. Based Syst. **229**, 107338 (2021)
68. Xu, J., Glicksberg, B.S., Su, C., Walker, P., Bian, J., Wang, F.: Federated learning for healthcare informatics. J. Healthc. Inf. Res. **5**(1), 1–19 (2021). https://doi.org/10.1007/s41666-020-00082-4
69. Li, T., Sahu, A.K., Talwalkar, A., Smith, V.: Federated learning: challenges, methods, and future directions. IEEE Signal Process. Mag. **37**(3), 50–60 (2020)
70. Hao, M., et al.: Efficient and privacy-enhanced federated learning for industrial artificial intelligence. IEEE Trans. Industr. Inf. **16**(10), 6532–6542 (2019)
71. He, X., Su, X., Chen, Y., Hui, P.: Federated learning on wearable devices: demo abstract. In: Proceedings of the 18th Conference on Embedded Networked Sensor Systems, pp. 613–614 (2020)

72. Yang, Q., Liu, Y., Chen, T., Tong, Y.: Federated machine learning: concept and applications. ACM Trans. Intell. Syst. Technol. (TIST) **10**(2), 1–19 (2019)
73. McMahan, B., Moore, E., Ramage, D., Hampson, S., yArcas, B.A.: Communication-efficient learning of deep networks from decentralized data. In: Artificial intelligence and statistics, pp. 1273–1282. PMLR (2017)
74. Chen, Y., Qin, X., Wang, J., Yu, C., Gao, W.: Fedhealth: a federated transfer learning framework for wearable healthcare. IEEE Intell. Syst. **35**(4), 83–93 (2020)
75. Hakak, S., Ray, S., Khan, W.Z., Scheme, E.: A framework for edge-assisted healthcare data analytics using federated learning. In: 2020 IEEE International Conference on Big Data (Big Data), pp. 3423–3427. IEEE (2020)
76. Yi, X., Paulet, R., Bertino, E.: Homomorphic encryption. In: Homomorphic Encryption and Applications. SCS, pp. 27–46. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-12229-8_2
77. El Makkaoui, K., Beni-Hssane, A., Ezzati, A.: Cloud-ElGamal and fast cloud-RSA homomorphic schemes for protecting data confidentiality in cloud computing. Int. J. Digit. Crime Forensics (IJDCF) **11**(3), 90–102 (2019)
78. Biksham, V., Vasumathi, D.: Homomorphic encryption techniques for securing data in cloud computing: a survey. Int. J. Comput. Appl. **975**, 8887 (2017)
79. Gentry, C.: A Fully Homomorphic Encryption Scheme. Stanford university, California (2009)
80. Sathya, S.S., Vepakomma, P., Raskar, R., Ramachandra, R., Bhattacharya, S.: A review of homomorphic encryption libraries for secure computation (2018). arXiv preprint http://arxiv.org/abs/1812.02428
81. Sun, X., Zhang, P., Sookhak, M., Yu, J., Xie, W.: Utilizing fully homomorphic encryption to implement secure medical computation in smart cities. Pers. Ubiquit. Comput. **21**(5), 831–839 (2017). https://doi.org/10.1007/s00779-017-1056-7
82. Farooqui, M., et al.: Improving mental healthcare using a human centered internet of things model and embedding homomorphic encryption scheme for cloud security. J. Comput. Theor. Nanosci. **16**(5–6), 1806–1812 (2019)
83. Wang, X., Zhang, Z.: Data division scheme based on homomorphic encryption in WSNs for health care. J. Med. Syst. **39**(12), 1–7 (2015). https://doi.org/10.1007/s10916-015-0340-1
84. Rohloff, K., Polyakov, Y.: An end-to-end security architecture to collect, process and share wearable medical device data. In: 2015 17th International Conference on E-health Networking, Application & Services (HealthCom), pp. 615–620. IEEE (2015)
85. Salim, M.M., Kim, I., Doniyor, U., Lee, C., Park, J.H.: Homomorphic encryption based privacy-preservation for IoMT. Appl. Sci. **11**(18), 8757 (2021)
86. Prasitsupparote, A., Watanabe, Y., Shikata, J.: Implementation and analysis of fully homomorphic encryption in wearable devices. In: The Fourth International Conference on Information Security and Digital Forensics. The Society of Digital Information and Wireless Communications, pp. 1–14 (2018)
87. David, R., et al.: TensorFlow lite micro: embedded machine learning for TinyML systems. Proc. Mach. Learn. Syst. **3**, 800–811 (2021)
88. Gorospe, J., Mulero, R., Arbelaitz, O., Muguerza, J., Antón, M.Á.: A generalization performance study using deep learning networks in embedded systems. Sensors **21**(4), 1031 (2021)
89. Han, S., Pool, J., Tran, J., Dally, W.J.: Learning both weights and connections for efficient neural networks (2015). arXiv preprint http://arxiv.org/abs1506.02626

90. Fyntanidou, B., et al.: IoT-based smart triage of Covid-19 suspicious cases in the Emergency Department. In: 2020 IEEE Globecom Workshops (GC Wkshps), pp. 1–6. IEEE (2020)
91. Sanchez-Iborra, R.: LPWAN and embedded machine learning as enablers for the next generation of wearable devices. Sensors **21**(15), 5218 (2021)
92. Yamanoor, S., Yamanoor, N.S.: Position paper: low-cost solutions for home-based healthcare. In: 2021 International Conference on Communication Systems & NETworkS (COMSNETS), pp. 709–714. IEEE (2021)
93. Padhi, P.K., Charrua-Santos, F.: 6G enabled tactile internet and cognitive internet of healthcare everything: towards a theoretical framework. Appl. Syst. Innov. **4**(3), 66 (2021)
94. Papernot, N., McDaniel, P., Sinha, A., Wellman, M.P.: SoK: security and privacy in machine learning. IEEE Eur. Symp. Secur. Priv. (EuroS&P) **2018**, 399–414 (2018). https://doi.org/10.1109/EuroSP.2018.00035
95. Yeom, S., Giacomelli, I., Fredrikson, M., Jha, S.: Privacy risk in machine learning: analyzing the connection to overfitting. In: 2018 IEEE 31st Computer Security Foundations Symposium (CSF), pp. 268–282 (2018). https://doi.org/10.1109/CSF.2018.00027