cryptography

MDPI

Article

On General Data Protection Regulation Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications

Irene Ioannidou * and Nicolas Sklavos

SCYTALE Group, Computer Engineering and Informatics Department, University of Patras, 26504 Patras, Greece; nsklavos@upatras.gr
* Correspondence: eioannidou@upatras.gr

Abstract: Individual users' sensitive information, such as heart rate, calories burned, or even sleep patterns, are casually tracked by smart wearable devices to be further processed or exchanged, utilizing the ubiquitous capabilities of Internet of Things (IoT) technologies. This work aims to explore the existing literature on various data privacy concerns, posed by the use of wearable devices, and experimentally analyze the data exchanged through mobile applications, in order to identify the underlying privacy and security risks. Emulating a man-in-the-middle attack scenario, five different commercial fitness tracking bands are examined, in order to test and analyze all data transmitted by each vendor's suggested applications. The amount of personal data collected, processed, and transmitted for advertising purposes was significant and, in some cases, highly affected the network's total overhead. Some of the applications examined requested access for sensitive data driven device functionalities, such as messaging, phone calling, audio recording, and camera usage, without any clear or specific reason stated by their privacy policy. This paper concludes by listing the most critical aspects in terms of privacy and security concerning some of the most popular commercial fitness tracking applications.

Keywords: confidentiality; general data protection regulation (GDPR); Internet of Things (IoT); personal data; privacy; smart devices

Citation: Ioannidou, I.; Sklavos, N. On General Data Protection Regulation Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications. *Cryptography* **2021**, *5*, 29. https://doi.org/10.3390/cryptography5040029

Academic Editors: Seyit A. Camtepe and Josef Pieprzyk

Received: 13 July 2021
Accepted: 7 October 2021
Published: 18 October 2021

1. Introduction

As the demand for consumer wearables, including smart bands and fitness trackers, is rising, serious concerns over data privacy and security issues are coming into the spotlight. Despite the extensive interaction, users are rarely aware of when and what data are shared on the internet, by their smart devices, as well as completely unaware of the fact that their data being stored and resold is a common practice. Personal data are a digital, easy to resell, product, and users seem to be in agreement with the idea that all their internet activity is constantly being monitored. For advertisers, data collected in such large quantities, enables targeting the right audience, in the right place, at the right time, with the right message. This brings to the surface considerable data protection risks. Creating huge volumes of data makes data management one of the most critical challenges for IoT infrastructures. As fragmentation across the many IoT actors grows, so does the importance of data laws, regulations, and policies [1]. The legal framework of General Data Protection Regulation (GDPR) entered into force in 2016 after passing the European Parliament, and, as of May 25 2018, all organizations are required to be compliant. Privacy and data protection have always been a priority for the European Union's law policy, thus the European Commission began adjusting its policies, to gradually develop the GDPR framework (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on

26 June 2021)). In order to protect privacy and establish consent from a data subject in every case, it includes strict rules on the basis of the following seven principles:

- Purpose limitation;
- Data minimization;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality;
- Accountability.

The EU-GDPR supports all legal process activities in order to create a balanced and simplified regulatory environment, for both European Union businesses and citizens. An important aspect of the new regulation is the way personal data is defined, being considered as a person's valuable asset. The new legislation is on track with technological advancements, such as Internet of Things (IoT) and Big Data paradigms, for which data collection and analysis are of the utmost importance. It aims to cover all aspects, by strongly considering technical terms, such as the internet protocol (IP) addresses, location data, and other attributes, that can be used to identify an individual. Protecting fundamental human rights and ensuring citizens' privacy in a holistic way has always been a driving force for the legal frameworks developed by the associated European Union's committees and GDPR is considered the most priority in all means for those rights when it comes to the digital world. In order to keep pace with the technological advancements that are rapidly adopted by citizens globally, the European Union acted decisively and rigorously over the most important issues uncovered by the IoT era, including the ubiquitous privacy challenges of the casual wearables' usage.

Modern wearable devices are tiny, inexpensive, consume little power, and offer continuous monitoring and measurement of the users' physical and physiological status. Referring to miniaturized electronic devices that are incorporated into different types of accessories and clothing, "wearables" can be attached to the user's body and collect a great amount of helpful but often sensitive information [2]. The various and innovative opportunities that wearable technology offers, led to the quick and global adoption of smart devices and tracking bands by the general population, as well as by many manufacturing companies that use wearables as hands-free guidance tools in order to improve productivity [3]. As hardware components become smaller and power sources become more efficient, the development of multifunctional wearable devices has emerged into a significant consumer market, which is expected to reach USD 150 billion by 2027, with a compound annual growth rate of 20.5% since 2020 [4].

In this work, we focus on smartwatches and fitness trackers that are the most popular due to mobility and connectivity capabilities [5]. Smartwatches and fitness wristbands are continuously connected to each user's mobile device and use a large variety of sensors and modules, including microphones, GPS trackers, accelerometers, cameras, and more, in order to ease the access to data and offer important information, alerts, or even recommendations to them [6]. Although usage of such devices has spread widely as a part of everyday lifestyle, and aims to improve individuals' wellbeing, it entails several personal data privacy concerns [7]. New practices, paradigms, and technologies are raising the questions that this study focuses on answering:

1. Is data privacy and security established for the popular wearable devices in the new, GDPR, era?
2. What are the privacy risks that users may encounter using fitness tracking applications, smart devices, and wearable technology?

In order to answer the above questions, an overview of past research on security and privacy vulnerability issues, as well as real time analysis of the data transmitted by wearable devices, through widely used fitness tracking applications, was required. By monitoring such apps and comparing the results with the literature's findings, potential risks, as well as their severity, can be identified and addressed in the future, in order to

enhance security and ensure privacy. In order to answer the above research questions, privacy and security issues were examined for the activity tracking applications: Xiaomi Mi Fit, Samsung Health, Shenzhen, FitPro, Huawei Health, and Sony Lifelog. Through a man-in-the-middle attack, data collected by the above applications were monitored and further examined. These devices were selected due to their popularity, as well as the variety of existing research on them. For instance, Xiaomi Mi band and the associated application Mi Fit has been examined and was characterized as a "secure by design" device, although many weaknesses have been found in the Mi Fit Software [8]. Huawei Health has also been a matter of research [9] and although some advertising packets were found to be transmitted to third party providers, the fact that Huawei Watch is using the number comparison mode, one of the Bluetooth pairing modes, results in the inability to passive eavesdrop, making it impossible to intercept network traffic between the device and the application.

For the purpose of this study, all the hardware access requests granted were recorded, listed, and evaluated according to the potential risks and vulnerabilities stated in the literature [10–12]. Vulnerability is defined as a weakness that can be exploited by one or more threats or a flaw in a system's design, implementation, or operation and management that could be exploited. Data collected and stored in IoT devices may hold sensitive information, bringing to the surface security threats and known exploits of current IoT infrastructures [13]. As networked devices grow more common, so are cyber-attacks. The fundamental right to digital privacy is defined by the General Data Protection Regulation (GDPR), which brings the users' concerns over sensitive data to the surface and aims to act as an opportunity to ensure trust in the new technological era. The regulation affects any company or organization that processes data of citizens based in Europe and is focusing on the protection of any person's sensitive data. Despite being under research and discussion for a long time [14], privacy and security issues related to wearable devices and mobile technologies are a constantly transforming field, which is still current and open to research worldwide. As the adoption of wearable devices expands constantly, the number of devices connected on IoT is rising, together with the data exchanged by them. Since the data recorded may vary from fitness activity statistics to sensitive health records [15], ensuring users about security is more crucial than ever.

2. Personal Data and Privacy in the GDPR Era

Personal data are defined as all the information concerning a living natural person, who has been identified or can be identified both directly and indirectly. Common personal data examples are a person's name, age, occupation, genetic, mental, economic, cultural, or social identity, relationship status, location, racial origin, religion, political or philosophical views, and health information. Each one of the above-mentioned personal data types, is handled differently and is subject to different legal framework [16], thus GDPR is strongly considering topics around the use of the most sensitive ones.

Sensitive personal data include racial or ethnic origin, political views, religious or philosophical beliefs, membership in organizations, health information, social security and personal preferences, and criminal prosecution information. Privacy refers to all the parameters concerning a natural person's private life and is of broad sense, while the term "personal data" focuses on the specific parameters that can be used to identify an individual through the processing of finite information. Personal data may be used in order to control, monitor, evaluate, classify, manage, provide, serve, or protect public interest or the service of a superior legal interest. This information and its processing have certain quality characteristics and are subject to restrictions. These do not apply in the case of privacy which is considered as a permanent situation. A noticeable distinction is underlying on the existence of three elements:

1. The concept of processing;
2. The concept of storing; and
3. The concept of purpose.

These elements are crucial for the discrimination between personal data breaches and privacy compromising. The term "processing" covers a wide range of operations performed on data, either manually or by automated means. It includes the collection, registration, organization, structure, adaptation or alteration, retrieval, usage, disclosure by transmission, dissemination or any other form of disposal, association or combination of personal data. The General Regulation on Data Protection (GDPR) applies to both full and partial processing of personal data.

What is important about the EU-GDPR, is the fact that it applies to all companies and entities established in the European Union that process personal data as part of their activities, regardless of the location that the data are processed, as well as to any companies established outside the European Union, monitoring the individual users' behavior in the European Union. Although the legal framework applies to all the stated companies, small and medium sized enterprises that do not process data as their main activity, are not due to some obligations, such as the appointment of a data protection officer (DPO). Additionally, companies that do not specifically target their services or goods to individuals in the European Union, are not subject to the rules of GDPR.

Since smart devices and social networking platforms have become part of everyday life globally, sharing of personal data has become a prerequisite for the use of most digital applications and services. Following the new technological trends, users share sensitive personal data, including their biometric features, as the cost of easier access through their mobile devices and personal computers. Sensitive personal data, such as phone number, address, bank accounts, IP, VAT, and ID card numbers, are used to complete a profile, with behavioral data, consumer preferences, political beliefs, spatial and temporal choices, or even biometric or biochemical characteristics which are collected and must somehow be protected and secured. Although, users are becoming more concerned towards any electronic transaction that requires disclosure of their personal information, there are many cases of companies offering services under vague policies.

As in real world incidents, where privacy and security may be considered as inviolable principles, online privacy issues are of the exact same importance. However, when it comes to online networks, the process of collecting personal information is not always obvious. In most cases, the collection of personal data is performed "quietly", based on the user's traces left behind, utilizing background mechanisms whose existence and functionality is often ignored or not fully understood by the user.

In this context, concerns are raised over the process of creating user profiles (profiling) by companies, in order to explore consumer needs and adapt advertising marketing to these preferences. In most cases, this is completed by systematically recording and collecting information about the users. This way, although services and applications may be provided free of charge, in fact, data gathered by users' activity is becoming the real currency, usually to be later bought by third party companies. Although the above, advertising, strategies may not be directly of harm to the user, being able to construct and reveal their identity or even gaining access to specific device functionalities (phone calling, SMS reading, GPS tracking, recording, etc.) and its content (photos, videos, contact list, messages, etc.), without prior notice or approval, is considered as a clear privacy violation.

The published work [17], proposes a specific target user can be recognized just by processing the walking data collected by their smartphone's accelerometer and gyroscope signals. This is just to highlight the privacy and security issues that are arising, especially in cases of user profiling and sensitive personal data reselling to third parties, for marketing purposes [18]. At company and enterprise level, adhering to protection measures can be considered as a compliance indicator but does not guarantee compliance. In order to address all GDPR requirements, organizations processing such data, must follow privacy by design practices and utilize the proper control and information tools to confirm the legitimate interest of the data controller, as well as the unambiguous consents of individuals.

When it comes to wearable computing, data privacy is the most critical and challenging concern [19], as the collected data can be targeted by cyber attackers and has the potential of exposing users' sensitive information at risk [20]. Every modern smartphone is equipped with and using Bluetooth and Wi-Fi modules, which are required for the connection between fitness tracking devices and their applications, but still suffer a variety of vulnerabilities themselves [21], thus there is a high chance that users' sensitive data might be leaked without permission. As research indicates (Table 1), potential risks vary between devices, concluding that there is no health or activity tracking application that can be considered as fully secure [22]. Sensitive data are considered as one of the most valuable products in the modern, Internet of Things era, since it might lead to financial and legal consequences for the user [23], bringing the importance of security and privacy to the surface.

Table 1. Comparative table of research on wearables concerning privacy and security issues.

Study	Method	Findings
Fereidooni et al.	MITM attack targeting 17 different fitness trackers' associated applications	Only 5 out of 17 devices take minor measures to protect data integrity.
Clausing and Schiefer	MITM attack targeting 7 fitness trackers on Android and Apple Watch	User can be identified by accelerometer and gyroscope signals of walking data.
Zhang and Liang	MITM attack targeting 4 different smart wristbands and a smart watch	Identified Replay, MITM, brute-force and DoS attack vulnerabilities on Bluetooth Low Energy based smart wristbands.
Goyal, Dragoni, and Spognardi	MITM attack targeting Jawbone UP Move and Fitbit Charge fitness trackers	Vulnerabilities through Bluetooth and Wi-Fi networks in Fitbit and Jabone wristbands.
Ho, Novick, and Yeung	MITM in 43 different fitness tracking applications	12 out of 43 were found to be sharing a huge amount of information to 76 different third parties

3. The New Era of Wearable Internet of Things

The popularity of smart devices combined with paradigms, such as cloud computing and Big Data, have sparked a whole new era of Internet of Things, providing a solid framework for the interconnectivity of smart devices, including wearable sensors and smartphones, through cloud computing [24]. IoT is defined by the International Telecommunication Union (ITU) as the global infrastructure that enables advanced services to interconnect things based on interoperable information and communication technologies [25]. It involves data acquisition, storage, and processing technologies for embedded systems, applied to different aspects of everyday life and manufacturing as well, from commercial smart phones and wearables, to smart homes, smart greenhouses, and smart factories [26].

Recent research in the field of wearable devices formed the new and rapidly emerging field of wearable IoT (WIoT). This new sector includes wearable computing and communicating devices that usually contain accelerometers, gyroscopes, or pressure sensors, used for both diagnostic and monitoring purposes. Wearable devices are designed and developed as a big part of IoT, since they use sensors and facilitate communication in order to assist users by providing real-time access to the recorded information. Smart glasses, virtual reality headsets, as well as smart clothes are included in the range of WIoT. WIoT can be defined as the technological infrastructure that interconnects wearable sensors, to

enable monitoring human factors including health, wellness, behaviors, and other data to enhance quality of life. Embedded motion sensors may be used to track different data, from body activity, such as walking habits and heart pace [27], to tremors and disease symptoms [28].

3.1. Sensors

Sensors are devices producing data that can simplify real-time decision making and actuate independent action and policies [29]. Sensors that are widely used for commercial smart devices, such as wearables and smart phones, are the accelerometer and the gyroscope, which are based in micro electrical and mechanical systems (MEMSs). MEMS technology mimics conventional electrical and mechanical systems at a micro scale. Although MEMS have been a topic of both industrial and academic research for many years, there is still ongoing research on improvements and modifications [30]. As the terms define, accelerometers are used to measure an object's acceleration, whereas gyroscopes measure angular velocity. Since the first proposal of uniaxial accelerometer sensors for motion tracking by Veltink and Boom in 1996, a plethora of clinical studies has been conducted, considering health and activity tracking applications as well.

The measurement of human movement (motion tracking) has several useful applications in sports, medical, and other branches of studies. Such applications include fall risk assessment, quantifying sports exercise, studying people habits, and monitoring the elderly. Wearable trackers are becoming increasingly popular for two main reasons. They can be used to motivate the user during the daily workout, while providing automatic activity measurement information through a smart phone [31]. To accurately observe motion of the human body, 3-axis accelerometers, magnetometers, and gyroscopes sensors obtain data, each for a specific purpose [32], allowing the user that wears the sensors to become fully aware of their daily activity and life habits.

Sensors may be used for human activity recognition in the ubiquitous computing domain as well [33]. Auxiliary sensors, such as gyroscopes and magnetometers, can be combined with accelerometers to increase motion tracking accuracy. Combining these three sensors, in most cases, leads to 9 degrees of freedom (9DoF). Applying sensors for clinical purposes, such as gait motion, gravity sensitive accelerometers are used. These accelerometers estimate the tilt angles between the gravity vector and the sensor's axes. Nowadays, the most commonly used integrated sensors, providing accurate data with 9DoF, are accelerometers, gyroscopes, and magnetometers [33]. Accuracy is achieved by combining a set of tri-axial accelerometers, tri-axial gyroscopes, and a magnetometer to estimate and monitor human motion.

Currently, most of wrist-worn health and activity trackers operate in the conventional 2.45 GHz industrial, scientific, and medical (ISM) frequency band [34]. The majority of the wearable wireless sensor platforms use a commercial radio and antenna and require a large scale for their implementation. Although, the 2.45 GHz band has many advantages, such as the higher data rate and worldwide standards compatibility, it has become highly crowded, damping the communication reliability. An alternative to the crowded 2.45 GHz band, used for IoT applications, is the sub-GHz band. The most popular sub-GHz bands are 433 MHz for Asia, 868 MHz for Europe, and 915 MHz for USA.

3.2. Cloud Based IoT, Data Privacy and Encryption

With the introduction of Cloud-based IoT architectures, a series of security and privacy requirements to ensure the safety of data, including identity and location privacy, have been introduced. The user's sensitive data have to be protected so as to not disclose any living habits. To establish a secure cloud based IoT environment, input, output, and function privacy must be achieved. Attackers need to be prevented from extracting private data and mitigate packet forwarding attacks as well. Forward and backward security is also important so that new users can only decipher encrypted messages after joining the cluster and revoked users cannot decipher encrypted messages after leaving [35]. Currently,

there are some architectures proposed with the technical specifications, currently there is no standard architecture that is suitable for global IoT. There are several connectivity, processing, media monitoring, and storage management issues to be addressed. All the IoT functional blocks incorporate efficient IoT, with the role of IoT gateways being crucial in communication, as they allow connectivity between IoT servers and IoT devices and applications. Thus, specifying IoT security schemes and protocols is mandatory, together with the users' capability for optionally deciding which one to use each time [36].

Although wearable devices have a great potential as a part of the interconnected IoT, due to their capabilities of tracking individuals seamlessly and personalizing health and wellness recommendations, they also adopt many of the network, software and hardware vulnerabilities. Researchers have already conducted classification of IoT attacks and various architectures have been proposed for authentication and access control [37], as well as to secure IoT communications [38]. Common IoT vulnerabilities and threats include distributed denial of service (DDOS) and attacks concerning integrity of data such as data modification attacks [39]. All modern IoT cryptographic models and security schemes are based on widely adopted privacy standards through encryption algorithms.

The advanced encryption standard (AES) is mostly used to ensure confidentiality, while the asymmetric algorithm RSA serves for asymmetric encryption, key management and digital signatures. As secure hash functions, SHA standards are used combined with Diffie–Hellman (DH) and elliptic curve cryptography (ECC) to provide privacy based in asymmetric cryptography [36]. Special interest has been attracted by researchers on the security schemes of combined mode as well, mostly because it supports encryption and authentication [40], which are crucial in the case of minimized, embedded, and portable devices. Overall, current research is focused on optimal ciphers, and encryption algorithms are under investigation, based on the available resources of distinct IoT devices.

4. Security and Privacy Vulnerability Issues in Fitness Tracking Devices

Potential vulnerabilities of popular wearable fitness trackers, as well as the different methodologies to address them, recently are being discussed extensively by researchers, especially in Europe, due to the adoption of GDPR [16,40–42]. As more connected devices are introduced and used to monitor individual users' physical activities, IoT is rapidly expanding and the quantity, as well as the quality, of security risks for personal data leakage is increasing. Securing devices and developing trusted networks has become a key topic of research [43]. Major privacy and security implications regarding the usage of wearable fitness tracking devices have been explored, on hardware [44], firmware [45] and software [46] level, as well as by societal scope [47], indicating information disclosure, subtle data collection and social media connectivity as the most critical concerns for wearable users [41].

The key security threats concerning fitness trackers and smartwatches can be categorized as hardware, software, and network sided. Unlike smartwatches, activity trackers are less powerful in terms of computational processing. This makes them more dependent on the device they are connected to and most of the time they work under the operating system of the user's handheld portable device, inheriting its potential exploits as well. Thus, the vulnerability research can be more focused to the different network attacks and addressed under the wider view of the increasing IoT security challenges, such as user authentication issues. Almost all fitness and activity trackers use Bluetooth, ANT radio, cellular data, and Wi-Fi networks for connectivity purposes. Although the protocols and communications standards used may differ, IoT is open to any available state of the art protocol, covering range to the maximum possible [48].

Utilizing the popular features that social networking platforms are offering, these smart devices are often used to motivate users by connecting them online and allowing them to share their activity. Processing the collected geodata (location and ground elevation), those devices create a better user-dependent experience by delivering to them custom personal or community goals [49]. However, as it is proposed in [50], the same

geodata may be used in order to launch malicious attacks on location privacy, such as location prediction using the activity history, borough prediction based in city knowledge and city prediction with no prior knowledge at all. A tool for analysis was developed in [51], and a user-based study was conducted, on the privacy risks that arise by exposing the collected data by fitness applications in social networks. The tool aimed to increase awareness and expose complex risks, such as the possibility of social security number extraction, by combining data recorded by fitness devices and shared in social networks. Another research [52] reported the limitations of users' knowledge and awareness on the consequences of location sharing (retrieved by wearable devices and processed by fitness apps) through social networks. In other cases [53], sharing information about the user's spatiotemporal mobility patterns may be enough to reveal sensitive information, such as their home location.

As previously conducted empirical analysis has indicated, many popular Android applications do not have a privacy policy [54]. As another research [55] reported, 12 widely used activity tracking applications, were found to be sharing a huge amount of information about the device and the user to 76 different third parties. That information included the device's model, screen size, language, and, in some cases, sensitive user information such as gender, geo-location, running routes, sleeping patterns, or even eating habits. It is by no doubt that activity and health tracking applications collect and manage sensitive data by design [56], therefore the security and privacy requirements defined by data protection laws, such as the General Data Protection Regulation (GDPR) in the EU, as well as security issues from a technological point of view have to be researched.

5. Proposed Work: Experimental Environment and Analysis

In order to identify the existence of such threats on commercial, widely used activity tracking applications, an experimental environment was developed and utilized. Its main scores were to reveal the quality and quantity of information that is accessed and tracked by fitness tracking applications, in wearable devices, with or without the user's consent.

5.1. Experimental Environment

For the purposes of this work, five fitness tracking applications were examined, suggested by the vendor, each different commercial, widely used, fitness band. Those smart devices and the version of the suggested software that was monitored are given in Table 2 below.

Table 2. Smart wearable devices, vendor's recommended application and version examined.

Wearable Device	Application	Version
Xiaomi Mi Smart Band 4	Mi Fit	4.6.5
Samsung Galaxy Watch Active 2	Samsung Health	6.12.3.001
OEM M4-LH716	FitPro	1.5.2
Huawei Honor Band 5	Huawei Health	10.1.1.312
Sony SWR10	Lifelog	4.0.A.0.34

The main aim of the experimental environment was to emulate a man-in-the-middle attack scenario, at already illustrated in detail in Figure 1, in order to reveal all data transmitted by each application tested. All the applications were installed on a handheld android device Xiaomi Redmi Note 6 Pro, MIUI Global 11.0.4, Android 9 (PKQ1.180904.001) to be later monitored using the application "Lumen Privacy Monitor", version 2.2.2, as a tool to conduct the experimental analysis [57].

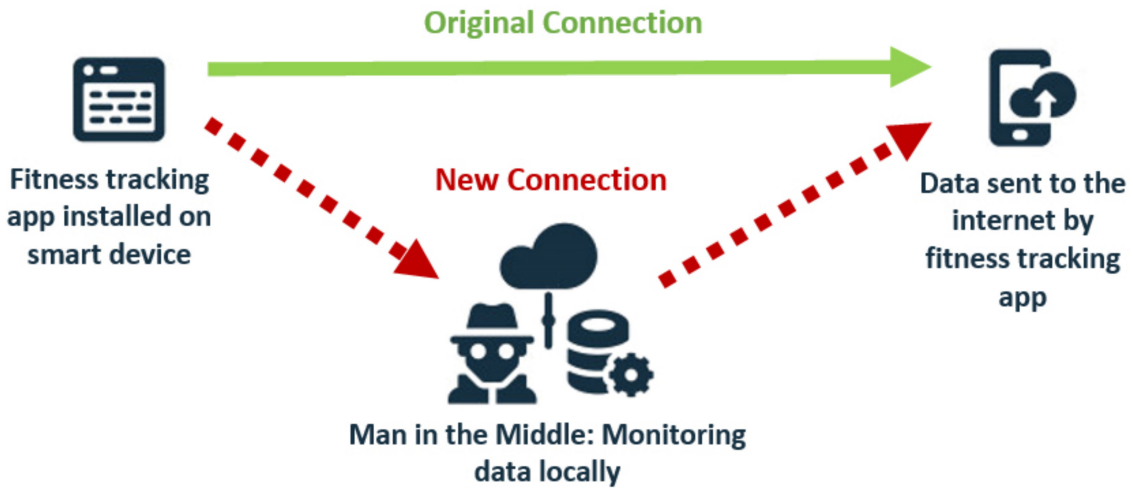

Figure 1. Data interception through man-in the middle attack on Android applications.

Android operating systems use the UID to set up a kernel-level application sandbox, not being able to perform any operations outside it. Since the sandbox is in the kernel, this security model extends to both native code and OS applications. The kernel enforces security between applications and the system at the process level through assigning user and group IDs to them. By default, applications cannot interact with each other and have restricted access to the OS. The sandbox is based on UNIX-style user separation of processes and file permissions. Any installed application that does not have the appropriate default user privileges is prevented from acting malicious (e.g., download software or read another application's data without permission). The permissions needed by the application in order to access protected parts of the system or other applications are declared in its AndroidManifext XML file, at the root of the project source set. This file is required and describes essential information about the application and its components. Permissions are requested by the applications either during installation, and the AndroidManifest file, or during run-time. Depending on their potential to harm the system and the user, permissions might be classified as of low, mid, or high risk.

Lumen follows the above classification and is currently available only for Android devices, requiring Android version above 4.2. It includes a user-friendly interface, allowing easy access to information about the already installed smart-hone applications. This information includes active connections, which data are being shared, as well as the percentage of traffic spent for advertising and tracking purposes. The main interface displays the three tabs (a) Flows, (b) Leaks, and (c) Apps, as shown in the following Figure 2.

Apps: Displays all applications monitored by Lumen, including a detailed report option. Through this interface, the user may view the number of trackers and the overhead caused by the connections each application tried to establish, leaks and traffic overview, and the requested permissions list, including risk assessments for each permission.

Leaks: Lists personal or device information leaked by each application.

Traffic: Leveraging Android's VPN permission, Lumen captures, analyzes and displays an overview of the network traffic, including encrypted flows, locally on the device and in user-space. It includes information about different connections (including HTTPS), bandwidth, and the overhead caused by that ads and analytics scripts.

"Lumen Privacy Monitor" tool, reads encrypted traffic and is able to determine privacy leaks inflicted by the application. It is developed as part of the Haystack Project by independent academic researchers at Berkeley and IMDEA Networks and has been used by researchers, as indicated by the corresponding literature review [16,58]. Some applications leak information to external servers, as well as to advertising networks or other online tracking services that monetize metadata, "Lumen" generates reports about the traffic patterns and the private data collected. It supports TLS interception for the real

time identification of applications that leak sensitive information over encrypted traffic. It enables finding and reporting of applications that leak private data over the network, as well as third-party organizations collecting them. In a man-in-the-middle-attack, the intruder redirects traffic between the user and the communication gateway. The common way to hijack is by signaling out a Wi-Fi network using a combination of techniques known as ARP spoofing and SSL stripping. The secure socket layer (SSL) header and hypertext transfer protocol (HTTP) packet generated at the application layer (Layer 7 on OSI model) of a computer are attached to the data being transferred for security.

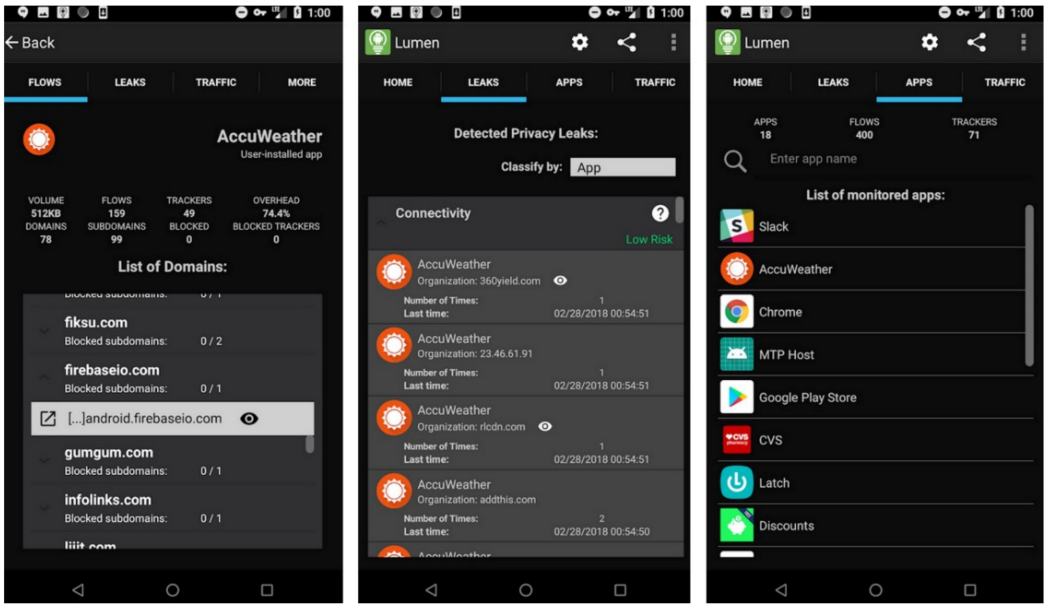

Figure 2. Lumen Privacy Monitor: Flows, Leaks and Apps interfaces.

Lumen runs locally on the user's device as a middleware between applications and the network interface in order to intercept traffic, being able emulate a "Man-In-The-Middle-Attack" (Figure 2) and detect leaks including software and hardware identifiers such as the Android ID, a permanent 64 bit long randomly generated number, and the Google Advertising ID, a unique 32 character anonymous string format universally unique identifier (UUID). Lumen takes advantage of Android's VPN permission to route transmitted packets through a process running in user-space, implementing a simplified layer-3/4 network stack. Running locally on the phone, its observes crucial application context, device status, user-related information and network traffic associated with user activities and intercepts encrypted traffic via local TLS proxy. Combining the above information allows Lumen to detect privacy leaks and provide unprecedented visibility for characterizing mobile traffic and performance security.

5.2. Experimental Results and Analysis

We evaluated five different fitness tracking wearable devices' recommended applications, using Lumen Privacy Monitor as a tool to emulate a forced man-in-the-middle attack, in order to examine underlying tracking activity, privacy leaks, permissions access, and the total communication overhead caused by advertisements, analytics scripts, and connections. Each one of the devices and applications was used for one year time, (equal to 52 weeks' time), and finally the results were expanded and scaled to one week level, in order the related comparisons to be more understandable, and the data volume was equally divided by the factor of total weeks 52 (equal to one year's time).

All five applications collect location and personal identifiers and connect via Bluetooth without any authentication. Higher number of trackers and overhead indicates greater amounts of data collected from users, thus lower privacy. As the number of permissions

required increases, higher are the chances that security is compromised, and the user's information and data control may be easily accessed by a third person. Network, as captured by Lumen, is shown in Figure 3.

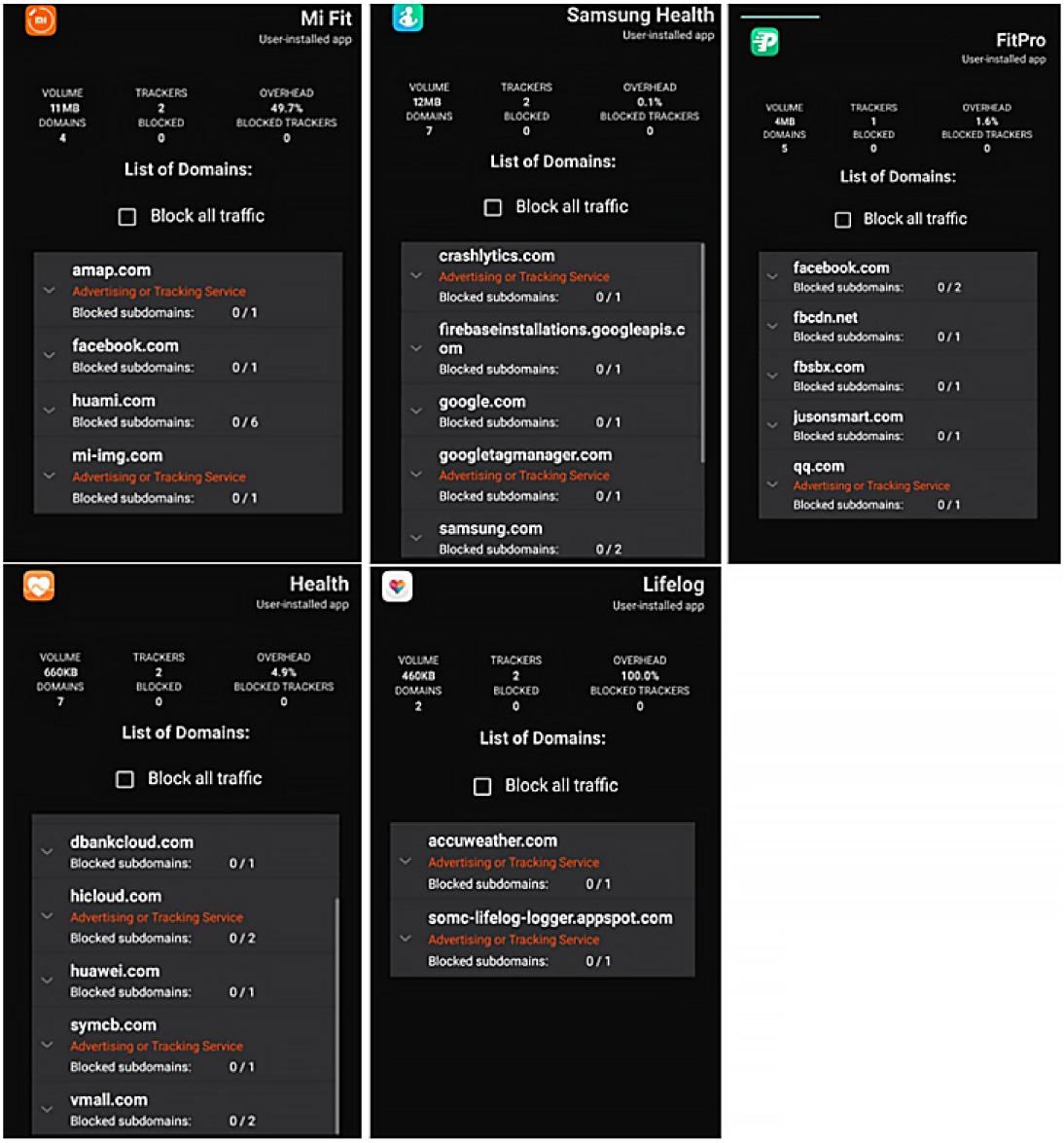

Figure 3. Traffic monitoring results for each activity tracking application.

The domains can be identified by the "Lumen Privacy Monitor" tool, as advertising or tracking services while the rest of them may be further investigated using external and online tools, aiming to analyze user data from trackers. As an example, we refer the one offered by "whotracks.me", for the domain "samsung.com", which was listed by "Lumen Privacy Monitor", on the Samsung Health app (Figure 4). As the listed results indicate (Table 3), all the fitness tracking applications examined, are using such services, although the total network overhead is not immediately affected depending on the number of the domains. For example, in the case of Sony Lifelog app, although only 2 tracking domains were found, and the data volume is low (460 kb), the total network overhead was 100%, highlighting a large amount of resources used in the network (e.g., bandwidth, energy, memory, time).

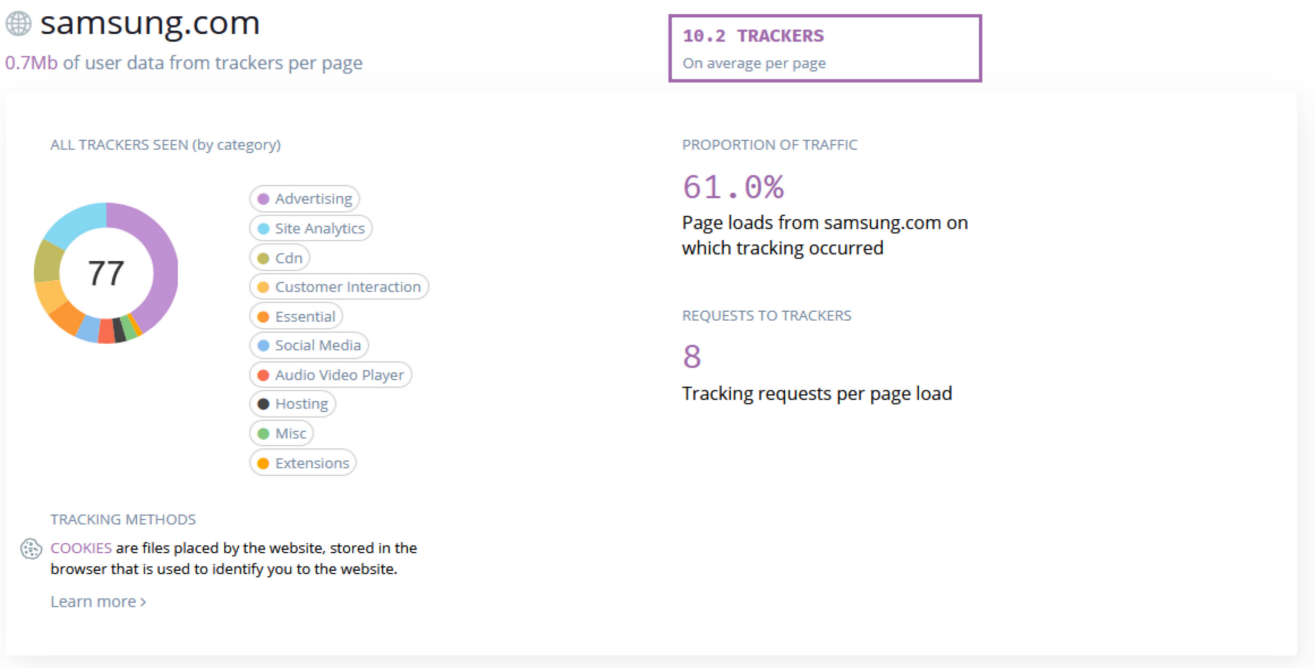

Figure 4. Tracker analysis results.

Table 3. Protocol statistics results for each activity tracking application (Data projected per week).

Application	Volume	Flows	Trackers	Overhead
Xiaomi Mi Fit	11 Mb	235	2	49.7%
Samsung Health	12 Mb	54	2	0.1%
FitPro	4 Mb	29	1	1.6%
Huawei Health	660 Kb	25	2	4.9%
Lifelog	460 Kb	10	2	100%

According to the experiment's results, presented in Table 4, in Huawei Health application, two privacy leaks were detected (connectivity settings and build fingerprint). Although both of the detected leaks are classified as low risk by Lumen, when combined with other leaked data, they can reveal a lot of information about the users' id and behavior. All of the applications make use of at least one advertising tracker, which in some cases highly impacts the total network overhead (Sony Lifelog and Huawei Health). As indicated by the domains' list, Samsung Health uses Google Analytics, while Xiaomi Mi Fit and Shenzhen FitPro use Facebook Analytics.

Table 4. Privacy and security indicators analysis per application.

Wearable Device	Number of Trackers	Number of Domains (of Which Advertising or Tracking Services)	Overhead (%)	Leaks
Xiaomi Mi Fit	2	4 (2)	49.7	0
Samsung Health	2	7 (2)	0.1	0
FitPro	1	5 (1)	1.6	0
Huawei Health	2	7 (2)	4.9	2 (Low Risk)
Lifelog	2	2 (2)	100	0

As previously mentioned, the requested permissions, Lumen's results, are separated into high, medium, and low risk level threats. Experimental results for the different categories of risks are visualized as shown in Figure 2. Figure 5 presents the number of high risk permissions requested per app. These permissions include geolocation data access, internal and external phone storage (read and write permissions as well), device state read, permission, phone call dialing and answering, access to the list of accounts in device's accounts service, audio recording access and camera access. Medium risk levels include pairing through Bluetooth, accessing network state and notification policy and more functionalities, such as vibrating, alarm setting, and modifying audio settings. The most critical 13 high risk threats monitored, are given in Table 5.

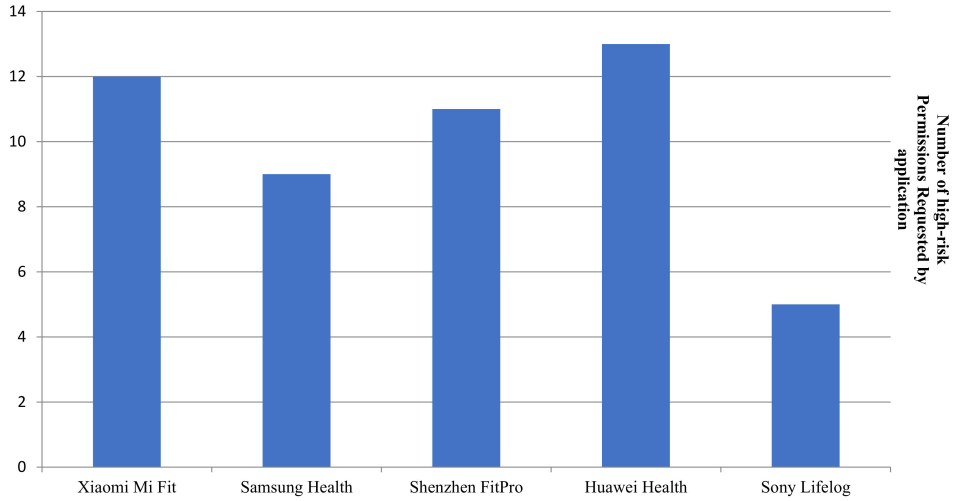

Figure 5. Number of permissions requested, classified as high-risk by Lumen, per application.

Table 5. High-risk access permission requests by application.

Requested Permission	Xiaomi Mi Fit	Samsung Health	Shenzhen FitPro	Huawei Health	Sony Lifelog
Approximate Location	✓	✓	✓	✓	✓
Precise Location	✓	✓	✓	✓	✓
Body Sensors (e.g., heart-rate)		✓			
Camera	✓	✓	✓	✓	✓
Record Audio (by phone's microphone)			✓	✓	
External Storage Read	✓	✓	✓	✓	✓
External Storage Write	✓	✓	✓	✓	
Phone State Read (phone number, cellular network, status of ongoing calls and list of phone accounts)	✓	✓	✓	✓	
Phone Calls Dial	✓			✓	
Phone Call Answer	✓			✓	
Outgoing Calls Process (allows call redirect and call abortion)	✓			✓	
List of accounts (device's accounts service)	✓	✓		✓	
Phone Contacts Read	✓	✓	✓	✓	
Call Log Read	✓		✓	✓	
SMS Read			✓		
SMS Receive			✓		

6. Discussion

Although in all applications' privacy policies collecting data for user experience enhancement purposes is clearly stated, the reasons behind granting permissions over camera control, audio recording, or even SMS access and phone calls are still vague. There is no doubt that users have to be totally aware before granting access to device modules that may leak sensitive personal data. In order to be considered as secure and GDPR compliant, privacy and security must be addressed by design and activity tracking applications must ensure the following principles:

Unlinkability: All personal data collected should be anonymous and never combined with other information that may be used to reveal the user's identity.

Transparency: Data processing should be completed only under the applications', clearly stated and specific, purpose. Users' whose data are being processed must be fully aware of the tracking before, after, as well as at the moment it is happening.

Intervenability: Users should constantly have the option of applying corrective measures or even fully withdrawing their consent of granting permission to data accessing and processing.

The above principles are critical when it comes to accessing information by embedded sensors, such as cameras and microphones, since they can be used to capture data concerning not only the individual user, but their surroundings as well. The experimental results, showcasing the many different permissions granted to the applications, combined with the results of the literature review conducted, raise serious issues on the users' data privacy. There is a high risk that sensitive or confidential data might leak without the users' consent. Even secondary device modules that do not require special user permissions, such as gyroscopes and accelerometers, might be utilized as a medium to eavesdrop conversations without consent [59] or, when combined, reveal sensitive health states, such as having a seizure [60].

Advertising trackers were reported in all of the devices, but only 2 out of the 5 devices reported high overhead (Mi Fit: 49.7%, Lifelog: 100%). An overhead of that high percentage means that higher number of resources will being used. This indicates the potential waste of bandwidth, memory, and energy as well. Since energy consumption is considered one of the most significant factors in IoT, overhead should never negatively impact sensors and communications. What has also to be mentioned, is that the number of trackers is not related to the overhead outcome. Although all the measured applications embed 1 to 2 trackers, the overhead differs greatly.

As the reported traffic and flows of all thee five applications indicate, there is no application ensuring sensitive user data disclosure. Considering both the literature and this work's experimental results, sharing user data with subsidiaries and third parties by commercial applications does not seem to be the exception, but rather the norm. Although all the examined applications required the user's approval in order to be granted permission to the functions and data of the device, the number of permissions required.

Although, according to the tracking domains, the applications examined collect information in order to deliver an optimized experience through customized recommendations and targeted advertising, requiring access to sensitive data and specific device functionalities, such as the camera or the phone calls dialing, is considered as a high risk and might strongly affect users' trust. Commercial applications may not intend to harm the device they are installed on, but third-party applications might potentially exploit vulnerabilities. Of course, access to device information, such as location, is reasoned for all fitness tracking applications, since it is required to record and optimize data delivered to the user. However, as shown in Table 5, requests for information regarding the smartphone's state (asked by 4 out of 5 applications), record audio using microphone (Shenzhen FitPro and Huawei Health), dial and answer phone calls (Xiaomi Mi Fit and Huawei Health), or even read and send messages (Shenzhen FitPro), raise concerns about data privacy inconsistencies.

At this point it has to be noted that, privacy inconsistencies are not necessarily violations of the law, since privacy requirements are self-defined standards derived from

laws and regulations, such as the above discussed EU-GDPR. Such frameworks enable steeper penalties for privacy compliance violations, forcing developers to follow "privacy by design". Although only two data leaks are detected, both in only one of the five examined applications, concerns are raised over the use of personal data for advertising purposes without the user's consent. Additionally, in some of the examined applications, questionable access permissions for the device's hardware functionalities (such as recording audio or dialing phone calls) are granted, without clear reasoning in their privacy policy statement. During application installation, all five applications requested the user's agreement on their privacy policy and clearly stated that they collect anonymous data, thus following the first privacy principle of unlinkability. However, considering the above access requests, the transparency principle is at stake. As for intervenability, it may be established using third party applications such as Lumen or the proposed research application PriADA [61], in order to manage and adapt information, as well as to limit or permanently deny data sharing.

As a matter of fact, software and privacy policies are frequently updated, meaning that the above results might differ depending on the current version. Thus, further and continuous research must be conducted. The examined applications might also be investigated using network traffic simulation tools [62]. Lumen states that it can analyze both encrypted and non-encrypted flow, analysis and evaluation utilizing other tools and environments, in order to find and analyze exceptions, is recommended as a topic of further research. Such scenarios can include software, such as mitmproxy, Jpcap library, TI SmartRF Packet Sniffer, or Wireshark, in order to track encrypted and non-encrypted network traffic, and compare results. This study examined a finite and limited number of activity tracking applications. Following research may focus on the monitoring of even more applications, as well as comparing the results between different smartphone devices or even different operating systems. Establishing secure network communications is also important in the IoT context and as encryption methods are further researched and new schemes are proposed, their adoption by manufacturers is crucial, in order to provide a secure environment. For instance, ensuring privacy for users' sensitive data, might include image encryption achieved through the synchronization of chaotic artificial neurons [63] or authenticated Hash functions with chaotic maps [64].

What has to be mentioned, considering the limitations of this research, is that the experimental scenario of this study, was oriented on testing, using the same Android device. Since the results might vary between different devices, operating systems, or even their versions, further, in-depth, research needs to be carried out, in order to identify any other underlying privacy risks, both on software and hardware level of commercial activity and fitness trackers. Further research might also focus detecting and highlighting such issues, in order to purpose resolving actions, as well as to encounter personal data breaches and cases of General Data Protection Regulation (GDPR) infringement.

7. Conclusions

Wearable devices, like any other computing device, are part of the IoT and fragile pieces of technology, adopting the vulnerabilities of the network and the devices they are connected to. WIoT is mainly based on the ability to improve everyday lifestyle, by collecting and analyzing great amounts of sensitive data, such as health records. Locational privacy issues may be addressed by enabling fitness devices and connecting them to smartphones, only when needed. Data reliability has to be ensured, and providers need to clearly discourage the exposition of sensitive data, such as biographical material, to third parties. Information transmission should, by any means, be encrypted and users always have the legal right to be informed and open to evaluate practices that could potentially lead to personal information being exposed to unauthorized parties.

As a main outcome of this work, high-risk security and privacy issues concerning data collected by commercial activity trackers were addressed. A background study on privacy and security was conducted, and an experimental environment using Lumen Monitor

tracking is utilized, to examine network traffic for underlying risks. The experimental analysis, combined with the results of previews research (Table 1), highlight the user privacy implications arising by fitness trackers usage. Thus, this work contributes to the ongoing research on vulnerabilities and security issues in popular fitness tracking applications, by demonstrating a step-by-step approach to detect privacy leaks, as well as stating a clear definition for the fundamental principles of designing GDPR compliant mobile applications. There is no doubt that security issues in wearable technology are still present and as the volume of data transmitted by devices is increasing, so are the privacy risks. Protecting personal data is a critical challenge for smart devices and IoT systems and should be a primary concern of both software and hardware design and development.

Author Contributions: I.I. and N.S., have contributed to: methodology, research, software, hardware, testbed, validation, results analysis, investigation, resources, writing—review and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: All of the reported data are included in the manuscript.

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

Abbreviations

Abbreviation	Full Form	Definition
9DoF	9 Degrees of Freedom	The process of capturing nine different types of orientation or motion related data.
GDPR	General Data Protection Regulation	The European legal framework setting guidelines for the collection and processing of personal information from individuals.
IoT	Internet of Things	A system of interrelated, internet -connected objects, able to collect and transfer data over a wireless network.
MEMS	Micro Electrical and Mechanical System	Miniaturized devices and structures that are made using the techniques of microfabrication.
MITM attack	Man-in-the-Middle Attack	Active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them.
OS	Operating System	System software managing hardware and software resources, and providing common services for applications.
TLS	Transport Layer Security	A security protocol providing privacy and data integrity for Internet communications.
UUID	Universally Unique Identifier	A 128-bit label used for information in computer systems.
WIoT	Wearable Internet of Things	A sub-category of IoT electronic devices that can be embedded in clothing worn as accessories.

References

1. Hadzovic, S.; Mrdovic, S.; Radonjic, M. Identification of IoT Actors. *Sensors* **2021**, *21*, 2093. [CrossRef]
2. Lee, J.; Kim, D.; Ryoo, H.-Y.; Shin, B.-S. Sustainable Wearables: Wearable Technology for Enhancing the Quality of Human Life. *Sustainability* **2016**, *8*, 466. [CrossRef]
3. Yang, H.; Kumara, S.; Bukkapatnam, S.T.; Tsung, F. The internet of things for smart manufacturing: A review. *IISE Trans.* **2019**, *51*, 1190–1216. [CrossRef]

4. Hayward, J.; Chansin, J.; Zervos, H. Wearable Technology 2018–2028: Markets, Players, Forecasts. Available online: http://www.idtechex.com/research/reports/wearabletechnology-2017-2027-markets-players-forecasts-000536.asp (accessed on 26 June 2021).
5. Kaewkannate, K.; Kim, S. A comparison of wearable fitness devices. *BMC Public Health* **2016**, *16*, 433. [CrossRef] [PubMed]
6. Muñiz, R.; Díaz, J.; Martínez, J.; Nuño, F.; Bobes, J.; García-Portilla, M.; Sáiz, P. A Smart Band for Automatic Supervision of Restrained Patients in a Hospital Environment. *Sensors* **2020**, *20*, 5211. [CrossRef] [PubMed]
7. Fereidooni, H.; Frassetto, T.; Miettinen, M.; Sadeghi, A.-R.; Conti, M. Fitness Trackers: Fit for Health but Unfit for Security and Privacy. In Proceedings of the 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), Philadelphia, PA, USA, 17–19 July 2017; pp. 19–24. [CrossRef]
8. Clausing, E.; Schiefer, M. *Internet of Things Security Evaluation of 7 Fitness Trackers on Android and the Apple Watch*; AV-TEST—The Independent IT-Security Institute: Magdeburg, Germany, 2016.
9. Zhang, Q.; Liang, Z. Security analysis of bluetooth low energy based smart wristbands. In Proceedings of the 2017 2nd International Conference on Frontiers of Sensors Technologies (ICFST), Shenzhen, China, 14–16 April 2017. [CrossRef]
10. Cusack, B.; Bryce, A.; Ward, G.; Mod, S. Assessment of security vulnerabilities in wearable devices. In Proceedings of the 15th Australian Information Security Management Conference, Perth, WA, Australia, 5–6 December 2017.
11. Langone, M.; Setola, R.; Lopez, J. Cybersecurity of Wearable Devices: An Experimental Analysis and a Vulnerability Assessment Method. In Proceedings of the 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), Turin, Italy, 4–8 July 2017.
12. Shiaeles, S.; Kolokotronis, N.; Bellini, E. IoT Vulnerability Data Crawling and Analysis. In Proceedings of the 2019 IEEE World Congress on Services (SERVICES), Milan, Italy, 8–13 July 2019.
13. Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and Security: Challenges and Solutions. *Appl. Sci.* **2020**, *10*, 4102. [CrossRef]
14. Warren, S.; Brandeis, L. The Right to Privacy. Available online: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (accessed on 26 June 2021).
15. Li, H.; Sun, G.; Li, Y.; Yang, R. Wearable Wireless Physiological Monitoring System Based on Multi-Sensor. *Electronics* **2021**, *10*, 986. [CrossRef]
16. Kalapodi, A.; Sklavos, N. The Concerns of Personal Data Privacy, on Calling and Messaging, Networking Applications. In *Communications in Computer and Information Science*; Springer: Singapore, 2021; pp. 275–289. [CrossRef]
17. Gadaleta, M.; Rossi, M. IDNet: Smartphone-based gait recognition with convolutional neural networks. *Pattern Recognit.* **2018**, *74*, 25–37. [CrossRef]
18. Hasan, O.; Habegger, B.; Brunie, L.; Bennani, N.; Damiani, E. A Discussion of Privacy Challenges in User Profiling with Big Data Techniques: The EEXCESS Use Case. In Proceedings of the IEEE International Congress on Big Data 2013, Santa Clara, CA, USA, 27 June–2 July 2013; pp. 25–30. [CrossRef]
19. Starner, T. The challenges of wearable computing: Part 1. *IEEE Micro* **2001**, *21*, 44–52. [CrossRef]
20. Mnjama, J.; Foster, G.; Irwin, B. A privacy and security threat assessment framework for consumer health wearables. In Proceedings of the 2017 Information Security for South Africa (ISSA), Johannesburg, South Africa, 16–17 August 2017; pp. 66–73. [CrossRef]
21. Goyal, R.; Dragoni, N.; Spognardi, A. Mind the tracker you wear. In Proceedings of the 31st Annual ACM Symposium on Applied Computing, Pisa, Italy, 4–8 April 2016. [CrossRef]
22. Braghin, C.; Cimato, S.; Della Libera, A. Are mHealth Apps Secure? A Case Study. In Proceedings of the 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 23–27 July 2018. [CrossRef]
23. Barcena, M.; Wueest, C.; Lay, H. How Safe Is Your Quantified Self? 2014. Available online: https://www.symantec.com/content/dam/symantec/docs/white-papers/how-safe-is-your-quantified-self-en.pdf (accessed on 27 August 2021).
24. Viel, F.; Silva, L.A.; Valderi Leithardt, R.Q.; Zeferino, C.A. Internet of Things: Concepts, Architectures and Technologies. In Proceedings of the 2018 13th IEEE International Conference on Industry Applications (INDUSCON), Sao Paulo, Brazil, 12–14 November 2018. [CrossRef]
25. Garrity, J. Harnessing the Internet of Things for Global Development. *SSRN Electron. J.* **2015**. [CrossRef]
26. Huh, J.-H. Implementation of lightweight intrusion detection model for security of smart green house and vertical farm. *Int. J. Distrib. Sens. Netw.* **2018**, *14*, 155014771876763. [CrossRef]
27. Ioannidou, I. Revolutionizing Sports Science through Information Technology: IoT, Augmented and Virtual Reality Applications. In Proceedings of the 1st International Interdisciplinary Conference on the Theme of "Sports and Art": Scientific and Artistic Dialogue, Ioannina, Greece, 5–7 April 2019. [CrossRef]
28. Ullah, F.; Haq, H.U.; Khan, J.; Safeer, A.A.; Asif, U.; Lee, S. Wearable IoTs and Geo-Fencing Based Framework for COVID-19 Remote Patient Health Monitoring and Quarantine Management to Control the Pandemic. *Electronics* **2021**, *10*, 2035. [CrossRef]
29. Rahman, A.; Asyhari, A.T. The Emergence of Internet of Things (IoT): Connecting Anything, Anywhere. *Computers* **2019**, *8*, 40. [CrossRef]
30. Rybarczyk, D. Application of the MEMS Accelerometer as the Position Sensor in Linear Electrohydraulic Drive. *Sensors* **2021**, *21*, 1479. [CrossRef]

31. Asimakopoulos, S.; Asimakopoulos, G.; Spillers, F. Motivation and User Engagement in Fitness Tracking: Heuristics for Mobile Healthcare Wearables. *Informatics* **2017**, *4*, 5. [CrossRef]
32. Becerra, V.; Perales, F.J.; Roca, M.; Buades, J.M.; Miró-Julià, M. A Wireless Hand Grip Device for Motion and Force Analysis. *Appl. Sci.* **2021**, *11*, 6036. [CrossRef]
33. Lima, W.S.; Souto, E.; El-Khatib, K.; Jalali, R.; Gama, J. Human Activity Recognition Using Inertial Sensors in a Smartphone: An Overview. *Sensors* **2019**, *19*, 3213. [CrossRef] [PubMed]
34. Kumar, S.; Buckley, J.L.; Barton, J.; Pigeon, M.; Newberry, R.; Rodencal, M.; Hajzeraj, A.; Hannon, T.; Rogers, K.; Casey, D.; et al. A Wristwatch-Based Wireless Sensor Platform for IoT Health Monitoring Applications. *Sensors* **2020**, *20*, 1675. [CrossRef] [PubMed]
35. Saraiva, D.A.F.; Leithardt, V.R.Q.; De Paula, D.; Mendes, A.S.; González, G.V.; Crocker, P. PRISEC: Comparison of Symmetric Key Algorithms for IoT Devices. *Sensors* **2019**, *19*, 4312. [CrossRef] [PubMed]
36. Sklavos, N.; Zaharakis, I.D. Cryptography and Security in Internet of Things (IoTs): Models, Schemes, and Implementations. In Proceedings of the 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Larnaca, Cyprus, 21–23 November 2016. [CrossRef]
37. Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet Things J.* **2017**, *4*, 1250–1258. [CrossRef]
38. Sadique, K.M.; Rahmani, R.; Johannesson, P. IMSC-EIoTD: Identity Management and Secure Communication for Edge IoT Devices. *Sensors* **2020**, *20*, 6546. [CrossRef]
39. Kumar, N.; Madhuri, J.; ChanneGowda, M. Review on security and privacy concerns in Internet of Things. In Proceedings of the 2017 International Conference on IoT and Application (ICIOT), Nagapattinam, India, 19–20 May 2017. [CrossRef]
40. Cilliers, L. Wearable devices in healthcare: Privacy and information security issues. *Health Inf. Manag. J.* **2020**, *49*, 150–156. [CrossRef]
41. Ching, K.W.; Singh, M.M. Wearable Technology Devices Security and Privacy Vulnerability Analysis. *Int. J. Netw. Secur. Its Appl.* **2016**, *8*, 19–30. [CrossRef]
42. Yan, T.; Lu, Y.; Zhang, N. Privacy Disclosure from Wearable Devices. In Proceedings of the 2015 Workshop on Privacy-Aware Mobile Computing, Hangzhou, China, 22 June 2015. [CrossRef]
43. Sklavos, N.; Zaharakis, I.D.; Kameas, A.; Kalapodi, A. Security & Trusted Devices in the Context of Internet of Things (IoT). In Proceedings of the 2017 Euromicro Conference on Digital System Design (DSD), Vienna, Austria, 30 August–1 September 2017; pp. 502–509. [CrossRef]
44. Mendoza, F.A.; Alonso, L.; López, A.M.; Cabarcos, D.D.S.A.P.A. Assessment of Fitness Tracker Security: A Case of Study. *Proceedings* **2018**, *2*, 1235. [CrossRef]
45. Rieck, J. Attacks on fitness trackers revisited: A case-study of unfit firmware security. *arXiv* **2016**, arXiv:1604.03313.
46. Saha, R.; Sarkar, S.; Datta, S.K. Balancing security & sharing of fitness trackers' data. In Proceedings of the 2017 1st International Conference on Electronics, Materials Engineering and Nano-Technology (IEMENTech), Kolkata, India, 28–29 April 2017; pp. 1–6. [CrossRef]
47. Torre, I.; Koceva, F.; Sanchez, O.R.; Adorni, G. A framework for personal data protection in the IoT. In Proceedings of the 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, Spain, 5–7 December 2016. [CrossRef]
48. Adat, V.; Gupta, B.B. Security in Internet of Things: Issues, challenges, taxonomy, and architecture. *Telecommun. Syst.* **2018**, *67*, 423–441. [CrossRef]
49. 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.* **2019**, *5*, 147–159. [CrossRef]
50. Meteriz, U.; Yildiran, N.F.; Kim, J.; Mohaisen, D. Understanding the Potential Risks of Sharing Elevation Information on Fitness Applications. In Proceedings of the 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), Singapore, 29 November–1 December 2020. [CrossRef]
51. Aktypi, A.; Nurse, J.; Goldsmith, M. Unwinding Ariadne's Identity Thread. In Proceedings of the 2017 on Multimedia Privacy and Security, Dallas, TX, USA, 30 October 2017. [CrossRef]
52. Alrayes, F.; Abdelmoty, A. Towards Location Privacy Awareness on Geo-Social Networks. In Proceedings of the 2016 10th International Conference on Next Generation Mobile Applications, Security and Technologies (NGMAST), Cardiff, UK, 24–26 August 2016. [CrossRef]
53. Singhal, S.; Neustaedter, C.; Schiphorst, T.; Tang, A.; Patra, A.; Pan, R. You are Being Watched. In Proceedings of the CHI Conference Extended Abstracts on Human Factors in Computing Systems, San Jose, CA, USA, 7–12 May 2016. [CrossRef]
54. Rowan, M.; Dehlinger, J. A Privacy Policy Comparison of Health and Fitness Related Mobile Applications. *Procedia Comput. Sci.* **2014**, *37*, 348–355. [CrossRef]
55. Ho, J.J.; Novick, S.; Yeung, C. A snapshot of data sharing by select health and fitness apps. In Proceedings of the Seminar on Privacy Implications of Consumer Generated and Controlled Health Data, Washington, DC, USA, 7 May 2014.
56. Bikos, A.N.; Sklavos, N. The Future of Privacy and Trust on the Internet of Things (IoT) for Healthcare: Concepts, Challenges, and Security Threat Mitigations. In *Book Recent Advances in Security, Privacy, and Trust for Internet of Things (IoT) and Cyber-Physical Systems (CPS)*; Li, K.-C., Brij, B., Gupta, B.B., Agrawal, D.P., Eds.; CRC-Press: Boca Raton, FL, USA, 2020; pp. 63–90.

57. Lumen Privacy Monitor | ICSI. Available online: https://www.icsi.berkeley.edu/icsi/projects/networking/haystack (accessed on 26 June 2021).
58. Razaghpanah, A.; Nithyanand, R.; Vallina-Rodriguez, N.; Sundaresan, S.; Allman, M.; Kreibich, C.; Gill, P. Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem. In Proceedings of the 2018 Network and Distributed System Security Symposium, San Diego, CA, USA, 18–21 February 2018. [CrossRef]
59. Michalevsky, Y.; Boneh, D. Gyrophone: Recognizing Speech from Gyroscope Signals. In Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, 20–22 August 2014; pp. 1053–1067.
60. Raij, A.; Ghosh, A.; Kumar, S.; Srivastava, M. Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. In Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems—CHI'11, Vancouver, BC, Canada, 7–12 May 2011. [CrossRef]
61. Lopes, H.; Pires, I.M.; Blas, H.S.S.; García-Ovejero, R.; Leithardt, V. PriADA: Management and Adaptation of Information Based on Data Privacy in Public Environments. *Computers* **2020**, *9*, 77. [CrossRef]
62. Prevezanos, I.; Tselios, C.; Angelou, A.; McGrath, M.; Mekuria, R.; Tsogkas, V.; Tsolis, G. Evaluating Hammer Network Traffic Simulator: System Benchmarking and Testbed Integration. In Proceedings of the GLOBECOM 2017—2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017. [CrossRef]
63. González-Zapata, A.M.; Tlelo-Cuautle, E.; Cruz-Vega, I.; León-Salas, W.D. Synchronization of chaotic artificial neurons and its application to secure image transmission under MQTT for IoT protocol. *Nonlinear Dyn.* **2021**, *104*, 4581–4600. [CrossRef]
64. De la Fraga, L.G.; Mancillas-López, C.; Tlelo-Cuautle, E. Designing an authenticated Hash function with a 2D chaotic map. *Nonlinear Dyn.* **2021**, *104*, 4569–4580. [CrossRef]