sensors

MDPI

Article

A Novel Privacy Preservation and Quantification Methodology for Implementing Home-Care-Oriented Movement Analysis Systems

Pablo Aqueveque [1], Britam Gómez [1], Patricia A. H. Williams [2] and Zheng Li [3,*]

[1] Electrical Engineering Department, Universidad de Concepción, Concepción 4070409, Chile; pablo.aqueveque@biomedica.udec.cl (P.A.); britam.gomez@biomedica.udec.cl (B.G.)
[2] College of Science and Engineering, Flinders University, Adelaide, SA 5042, Australia; trish.williams@flinders.edu.au
[3] Department of Computer Science, Universidad de Concepción, Concepción 4070409, Chile
* Correspondence: imlizheng@gmail.com

Abstract: Human movement is generally evaluated through both observations and clinical assessment scales to identify the state and deterioration of a patient's motor control. Lately, technological systems for human motion analysis have been used in clinics to identify abnormal movement states, while they generally suffer from privacy challenges and concerns especially at home or in remote places. This paper presents a novel privacy preservation and quantification methodology that imitates the forgetting process of human memory to protect privacy in patient-centric healthcare. The privacy preservation principle of this methodology is to change the traditional data analytic routines into a distributed and disposable form (i.e., DnD) so as to naturally minimise the disclosure of patients' health data. To help judge the efficacy of DnD-based privacy preservation, the researchers further developed a risk-driven privacy quantification framework to supplement the existing privacy quantification techniques. To facilitate validating the methodology, this research also involves a home-care-oriented movement analysis system that comprises a single inertial measurement sensor and a mobile application. The system can acquire personal information, raw data of movements and indexes to evaluate the risk of falls and gait at homes. Moreover, the researchers conducted a technological appreciation survey of 16 health professionals to help understand the perception of this research. The survey obtains positive feedback regarding the movement analysis system and the proposed methodology as suitable for home-care scenarios.

Keywords: movement analysis; inertial movement units; risk of falls; gait analysis; privacy preservation; privacy quantification; privacy risks; patient-centric healthcare

Citation: Aqueveque, P.; Gómez, B.; Williams, P.A.H.; Li, Z. A Novel Privacy Preservation and Quantification Methodology for Implementing Home-Care-Oriented Movement Analysis Systems. *Sensors* **2022**, *22*, 4677. https://doi.org/10.3390/s22134677

Academic Editors: Michael Vassallo, Hongnian Yu, Yanhong Liu and Arif Reza Anwary

Received: 29 April 2022
Accepted: 16 June 2022
Published: 21 June 2022

1. Introduction

The healthcare industry's digital transformation can be traced back to the development of computer engineering and information and communication technologies (ICT) in the 1950s [1]. Driven by the revolutionary development of modern computing devices, i.e., from large mainframes to small chips that can be embedded in wearable objects and sensors, healthcare is experiencing a rapid evolution in the use of Internet of Things (IoT) [2]. As such, it has been predicted that healthcare provisioning will transform from the current hospital-centred approach, first to the hospital-home-balanced hybrid model in the 2020s, and subsequently to a primarily home-centred model in the 2030s [3–5]. Compared to the traditional healthcare delivery model and hospital-oriented systems, the emerging personalised paradigm has been identified as able to improve preventive healthcare by increasing people's awareness of, and involvement in, the management and maintenance of their health [6].

A typical use case of the home-centred healthcare model is the individuals' movement analyses. In clinical movement analysis, health professionals not only need observations but also test different bio-mechanical aspects to assess the state and deterioration of a patient's motor control over various activities [7,8]. In recent years, high-technological systems have been employed for the bio-mechanical evaluation of movement, such as high-resolution camera-based systems, pressure mats, electromyography systems and balance platforms. Those systems can help characterise or predict the gait quality, risk of falls, comorbidities, balance and the patient dependence [9–14].

When implementing movement analysis systems in the home environments, there are inevitable privacy challenges and concerns. In fact, it has been identified that privacy is specifically critical in the home-based and/or wearable systems [6,15]. Several exploratory studies indicate that the main concerns about the privacy when using wearable systems include: the lack of control over the collected and shared information, unexpected disclosure of the user identification, and the misuse of the collected data [16,17]. Thus, many wearable systems have incorporated hardware/software solutions to protect privacy, such as using audio-visual feedback [18], physical and gesture switches to stop recording [19], using identification masking when information is being shared [20], and using machine learning algorithms to remove sensitive information automatically [21]. However, most of these solutions allow only to control the information to be masked or to decide when it is sent or recorded, while they do not allow users to repeatedly choose what, how, with whom, and when to store, process and transmit data in a consistent methodology.

Driven by such a gap, we have developed a novel methodology that enabled a distributed and disposable approach (DnD) to exclude patients' sensitive information from health data analytics. Recall that a methodology refers to "an organised set of principles which guide action in trying to 'manage' (in the broad sense) real-world problem situations" [22]. In the DnD-applicable cases, we advocate for *forgetting while analysing* as an intrinsic privacy preserving principle in patient-centric healthcare. As such, raw data with sensitive information will be immediately "forgotten" (neither stored nor transmitted) after their usage in the owner-side analytic, which imitates the natural forgetting process of human memory. Based on our proof-of-concept development and application of DnD within the home-care scenarios [23], this research further reinforces the theoretical foundation of DnD. Firstly, we have enriched DnD-friendly data analytic methods and followed the open method principle to share the method details [24]. Secondly, to help judge the efficacy of DnD (and other privacy-preserving techniques), we have developed an innovative privacy quantification framework based on fuzzy logic and privacy risk analysis. By quantitatively distinguishing between the privacy levels/risks within different data analytical scenarios, this methodology can conveniently and appropriately integrate the existing privacy preservation techniques, even if they focus on the minor and unusual aspects of privacy rather than addressing the essential aspects [25].

To verify the practical effectiveness and efficiency of our methodology, we also developed a home-care-oriented movement analysis system based on a wearable magneto-inertial measurement unit (MIMU). Technically, the MIMU sends raw data (tri-axial acceleration, tri-axial angular velocity, and tri-dimensional orientations) to a mobile platform to calculate clinical assessment scales for analysing the risk of falls and the gait quality [26,27]. The advances in movement analysis algorithms and device miniaturization make this system a low-cost and easy-to-use alternative to those high-technological systems of specialised laboratories for the bio-mechanical analysis of movement [28]. By introducing the movement analysis system together with our privacy preserving methodology to several local patient-centric healthcare projects, we have received positive feedback from the domain professionals.

Based on our local validation, we claim that this research particularly contributes to the remote healthcare for elderly people. According to the WHO, population ageing is happening and accelerating unprecedentedly [29]. The estimation is that the global number of people aged 60 years and older will increase to 1.4 billion by 2030 and 2.1 billion

by 2050 [29]. It is known that human ageing inevitably increases the risk of disability, dependence, and a number of comorbidities. In addition, many seniors could stay lonely and isolated especially in developing countries, which further increases the aforementioned risks. Therefore, it will be significantly valuable and helpful to offer home-care-oriented monitoring services to those elderly individuals, while this research can conveniently be applied and/or adapted to those multi-purpose daily activity monitoring systems.

The remainder of this paper is organised as follows. Section 2 briefly explains DnD-based privacy preservation and mainly introduces the newly developed privacy quantification framework. To facilitate applying DnD, a set of DnD-friendly data analytic methods are detailed in Section 3. Section 4 describes a home-care-oriented movement analysis system for validating our privacy preservation and quantification methodology. Section 5 demonstrates how we can apply DnD and the privacy quantification framework to the home-care scenarios, especially for caring elderly people. Section 6 draws conclusions and discusses our future work.

2. Privacy Preservation and Quantification for Implementing Movement Analysis Systems for Home Care

As mentioned earlier, the home-based healthcare provisioning inevitably involves more privacy risks than the hospital mode does. To address the privacy concerns when implementing movement analysis systems for home care, we introduce a novel privacy-preserving methodology that includes a DnD approach to privacy preservation and a privacy quantification framework.

2.1. DnD-Based Privacy Preservation

Paralleling the digital transformation of healthcare, privacy issues inevitably arise as a major concern in the healthcare ecosystem [25]. These issues are apparent, specifically in the IoT-based patient-centric context [6] and in the big data era [15]. Patients' privacy can be breached generally by the leakage of their health data, as the leakage may expose sensitive medical histories and other private information [30]. As a result, it has been reported that health data leakage can not only incur huge monetary losses but also cause significant negative impacts on individuals and the society [31]. Despite the decades of effort in digital healthcare system development, privacy studies investigating the exploitation of big healthcare data are still at an early stage. People expect government regulations and trusted organisations to mitigate privacy problems [6], yet the current legal frameworks have lagged behind the development of technologies and the business of big data analytics [32]. Although there exist sophisticated techniques of privacy preservation, these are generally inadequate for the emerging big data era [25], focusing on minor and unusual aspects of privacy rather than addressing the essential aspects.

Driven by the privacy concerns together with the IoT characteristics (i.e., the generally limited compute, storage and network resources of IoT devices), we have proposed a DnD approach to privacy preservation [23]. The DnD approach is developed based on the following intuitive and straightforward consensus:

- The less data/information we share, the less privacy risks we take.
- The less data/information we store, the less privacy risks we take.

It should be noted that DnD is not intended to replace the existing privacy-preserving mechanisms but to provide an additional layer to suitable techniques to further enhance the privacy-preserving effects. For example, the differential privacy preservation mechanism [33] matches one of the DnD scenarios where the raw data are excluded (or removed) from the analytical results. The discussion about, and the development of, DnD have been elaborated in our earlier work [23]. To avoid duplication, we do not repeat them in this paper. Instead, we directly show the application of DnD in Section 5.1, while this paper mainly describes our newly developed privacy quantification framework in the following subsection.

2.2. Risk-Driven Privacy Quantification Framework

The development of the DnD corresponds to a common concern around the linguistic variable "privacy risk"; i.e., the more health data people disclose (store or transmit to the outside world), the higher privacy risks people take. It is clear that estimating privacy risk degrees is more straightforward than directly estimating privacy levels in human discussions. Therefore, this research uses privacy risks as a bridge to investigate privacy quantification. Considering the subjective and imprecise descriptions on privacy risk degrees in natural language, this research uses fuzzy logic to grade the fuzzy set of linguistic terms of privacy risk (e.g., from "extremely low" to "extremely high"). Specifically, given the generally positive proportional relationship between data disclosure and privacy risk, the Sigmoidal ("s-shaped") Membership function [34] is used to represent the gradual transition between those linguistic terms, as shown in Equation (1).

$$\texttt{sig}(x; s, p) = \frac{1}{1 + e^{-(x-p)/s}}, \qquad 1 \leq s \leq 10, \quad 0 < x, p < 100 \tag{1}$$

where the membership function $\texttt{sig}(x; s, p)$ delivers the privacy risk degree between 0.0 and 1.0 when x percent of data are disclosed; p indicates the environment's (or data context's) objective privacy sensitivity, which can be adjusted as the inflection point when reaching the privacy risk degree 0.5; and s represents the user's subjective privacy sensitivity from 1 to 10, which can be obtained through questionnaires case by case. Within a particular environment, the higher the privacy sensitivity, the faster the privacy risk increases along with the data disclosure. For a single person, higher privacy sensitivity implies less tolerance in disclosing personal data and thus brings higher privacy risks to him/her even when disclosing a small amount of data. By assuming the privacy sensitivities are 10 and 8 in two different data contexts, respectively, and the inflection points are correspondingly at 30% and 50% of data disclosure, we demonstrate two concrete fuzzy membership functions for estimating and measuring privacy risks, as illustrated in Figure 1.

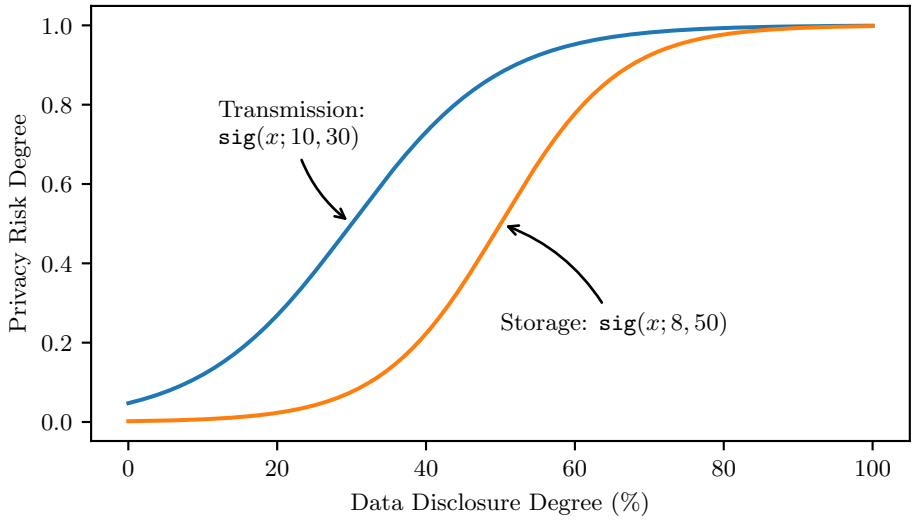

Figure 1. Two potential fuzzy membership functions for estimating and measuring privacy risks in different data contexts. (See their explanation and usage in Section 5.3.)

Given a specific degree of privacy risk, we implement privacy quantification by taking advantage of the negative proportional relationship between privacy risk and privacy level, as defined in Equation (2).

$$\mathscr{P} = 1 - \texttt{sig}(x; s, p) \tag{2}$$

where $\mathscr{P}$ represents the quantified privacy, and it can also be explained as the confidence in privacy preservation within a particular situation. Such a definition fits in the common sense: fewer privacy risks usually imply a better privacy environment with higher privacy levels.

Since different privacy risks exist in different data contexts (e.g., data storage and data transmission), the risk analysis and privacy quantification need to be conducted independently in each context. By treating independent data contexts as orthogonal privacy dimensions, we formulate a generic privacy quantification framework into Equation (3).

$$\mathbb{P} = \prod_{k=1}^{m} \mathscr{P}_k \tag{3}$$

where $\mathbb{P}$ represents the combined confidence in privacy preservation across m data contexts with respect to their individual privacy levels $\mathscr{P}_1$, $\mathscr{P}_2$..., and $\mathscr{P}_m$. As mentioned previously, the current version of DnD takes into account privacy only in data storage and data transmission. As such, the privacy quantification under DnD can be generalised as $\mathbb{P}_{DnD} = \mathscr{P}_{storage} \times \mathscr{P}_{transmission}$. The detailed implementations are exemplified together with a case study in Section 5.3.

2.3. Comparison against the Existing Privacy Quantification Approaches

In addition to qualitative discussions, privacy quantification is often needed to measure the privacy levels in different environments or situations (e.g., before and after applying privacy-enhancing technologies) in order to compare and judge the effectiveness and efficiency of different privacy-preserving techniques [35]. In other words, privacy quantification also plays a crucial role in privacy preservation. Here, we briefly and critically review four de facto approaches to privacy quantification to help justify the development of our privacy quantification framework.

- The **Information–Theoretic Approach** takes advantage of the inherent connection between privacy and information from a mathematical perspective, and it quantifies privacy by measuring the amount of information lost by users or the amount of information gained by attackers after data disclosure. Intuitively, the smaller the attacker's gain or the user's loss of information, the higher the privacy level. Based on the matured information theory, this approach has widely been discussed in academia. However, the sophisticated mathematical basis of this approach makes it hard to adapt to the diverse industrial needs [36], and it demonstrates the large gap between mathematical and natural languages when conducting empirical studies. For example, the concept "entropy" seems particularly difficult for normal people (e.g., patients) to understand and use in practical communications.
- The **Uncertainty-Based Approach** integrates an uncertainty data model into a privacy model, so as to quantify privacy with regard to the degree of uncertainty at which the private data can be inferred [37]. The quantification logic is that the higher the degree of uncertainty (e.g., achieved by a privacy preserving technique), the better the privacy in the protected data. Nevertheless, it has been identified that uncertain information-based guesses can still be correct, and consequently, privacy breaches may still occur even under highly uncertain circumstances [35].
- The **Input–Output Similarity-based Approach** utilises the similarity or diversity between the original data and the processed (or queried) data to quantify privacy, and it is primarily related to the anonymisation techniques in the database domain [38]. In this way, high privacy can usually be reflected by low similarity or high diversity between the input and output of data processing. This approach focuses on the data changes without considering the data disclosure environment; however, this will overestimate the privacy levels in some cases. For example, regular patterns in the anonymised data would still affect privacy if attackers were equipped with relevant background knowledge.
- The **Output–Output Indistinguishability-Based Approach** quantifies privacy by measuring the degree of obfuscation between the output data from different (while linked

or relevant) data processing events [39]. Accordingly, the harder it is to identify the relevance between related processing outcomes, the higher the privacy. It is clear that the privacy quantification here requires at least a pair of output datasets, and thus, this approach is not suitable to help understand the privacy levels within standalone patient-centric events.

To address the major concerns in the existing privacy quantification approaches, this research focuses on the linguistically easy-to-understand "privacy risk" and investigates fuzzy reasoning to encode human knowledge or common sense into numerical privacy recognitions, as demonstrated in Section 5.3. In particular, compared with the information–theoretic approach, the fuzzy-logic basis can make privacy risk-driven solutions easily adaptable to various data contexts via natural-language discussions. Compared with the input–output similarity-based approach, this research takes into account not only the data disclosure but also the influences from the environment and the patient.

3. DnD-Friendly Data Analytic Methods

We have identified that running statistics and streaming algorithms [40] are particularly suitable for DnD analytics. Unlike traditional methods that require preparing full data sets and correspondingly require large memory/storage spaces, both running analytics and streaming algorithms employ a recursive approach to the analytic computation without necessarily storing any historical data. Thus, these methods can be more efficient and lightweight than their traditional counterparts, especially in the real-time analytic situations. More importantly, the recursion feature matches the disposable fashion advocated by DnD for privacy preservation by avoiding storing and summing up all the data in the brute-force way.

The current stage of the research primarily uses "running analytical" methods for the development of DnD. The performance benefits of using running analytics have been noted over several decades [41]. Nevertheless, the implementations of running analytics are minimal [42,43] except for a couple of simple cases (i.e., running average and running variance). Even in the simple case of the running variance, there exist inconsistent implementations that either violate the spirit of recursion or lack arithmetic proofs. For example, the implementation in [44] is based on data accumulation, while "it is not obvious that the method is correct even in exact arithmetic" in [45].

To address the issues in the use of running analytics, we have investigated and shared the details of the typical running analytic methods employed in this research, including running min, max, average, sample standard deviation, and skewness. In fact, making analytic methods openly available has been identified as a higher-level strategy over open-source tools and open-access data for improving the repeatability, replicability, and reproducibility of scientific work [24]. It is noteworthy that some other analytic methods (e.g., Coefficient of Variance) can directly be implemented based on these typical ones. Furthermore, we have taken into account not only the arithmetic correctness but also the computation efficiency (e.g., avoiding the repeated calculations of intermediate results) through this research. As justified in [24], the shared formulas together with their detailed proofs (the detailed proofs of the methods specified in Section 3.1 are published in a separate paper [46]) can significantly facilitate the improvement and/or modification of those methods, for example, when uneven time intervals need to be considered in data analytics.

3.1. An Extendable Suite of Analytic Methods for Implementing DnD

According to our recent projects, the following statistical methods are most commonly used in the home-care scenarios.

3.1.1. Running Min and Running Max

Both minimum and maximum thresholds of many health indicators (e.g., blood pressure and heart beat rate) are useful to generate early warnings in patient-centric

healthcare systems. For example, the value of oxygen saturation (SpO2) below 90% has been used for asymptomatic patients to detect COVID-19 infection [47]. Thus, running min and running max are defined as two simple while crucial analytic methods in this work, as shown in Equations (4) and (5).

$$min_{n+1} = \texttt{min}(min_n, x_{n+1}), \qquad min_0 = 0 \tag{4}$$

$$max_{n+1} = \texttt{max}(max_n, x_{n+1}), \qquad max_0 = 0 \tag{5}$$

where min_n and max_n, respectively, indicate the minimum and maximum values within a series of data $x_1, x_2, ..., x_n$. After the new value x_{n+1} joins the data series, the functions $\texttt{min}()$ and $\texttt{max}()$ will make comparisons and return the new minimum and maximum values min_{n+1} and max_{n+1}.

3.1.2. Running Average

In medical examination reports, average measurement results with respect to various indicators are widely used to reflect a patient's health status. When conducting DnD analytics, the running average can be calculated by Equation (6).

$$\mu_{n+1} = \mu_n + \frac{x_{n+1} - \mu_n}{n+1}, \qquad \mu_0 = 0,\ n > 0 \tag{6}$$

where μ_{n+1} indicates the arithmetic average of $n+1$ values after the new value x_{n+1} joins the data series.

3.1.3. Running Sample Standard Deviation

The measure of standard deviation is commonly used to quantify how far a set of data spreads out from its average value. To facilitate the corresponding programming, this research highlights the recursive calculation of sample variance, as shown in Equation (7).

$$\begin{cases} \mathbb{V}_{n+1} = \mathbb{V}_n + (x_{n+1} - \mu_{n+1})(x_{n+1} - \mu_n) \\ \sigma^2_{n+1} = \dfrac{\mathbb{V}_{n+1}}{n}, \qquad \mathbb{V}_0 = \mathbb{V}_1 = 0,\ n > 1 \end{cases} \tag{7}$$

where σ^2_{n+1} represents the unbiased estimator for the sample variance, after the new value x_{n+1} joins the data series. σ_{n+1} is then the corresponding standard deviation. In particular, the sample variance σ^2_n is defined as a proportional function of the auxiliary variable $\mathbb{V}_n$ that can be calculated in a recursive way, while $\mathbb{V}_n$ essentially carries the crucial information of the second Central Moment, i.e., $\sum_{i=1}^{n}(x_i - \mu_n)^2$.

3.1.4. Running Sample Skewness

When focusing on the value space of a series of random data, skewness measures or estimates the symmetry of the data's distribution by comparing to the corresponding normal distribution. The recursive calculation formula of sample skewness is given by Equation (8).

$$\begin{cases} \mathbb{S}_{n+1} = \mathbb{S}_n - 3 \cdot (\mu_{n+1} - \mu_n) \cdot \mathbb{V}_n + (\mathbb{V}_{n+1} - \mathbb{V}_n)[x_{n+1} - \mu_{n+1} - (\mu_{n+1} - \mu_n)] \\ S_{n+1} = \dfrac{(n+1) \cdot \mathbb{S}_{n+1}}{n \cdot (n-1) \cdot \sigma^3_{n+1}}, \qquad \mathbb{S}_0 = \mathbb{S}_1 = \mathbb{S}_2 = 0,\ n > 2 \end{cases} \tag{8}$$

where S_{n+1} indicates the sample skewness of $n+1$ values, after the new value x_{n+1} joins the data series. In particular, S_n is defined as a proportional function of the auxiliary variable $\mathbb{S}_n$ that can be calculated in a recursive fashion, while $\mathbb{S}_n$ essentially carries the crucial information of the third Central Moment, i.e., $\sum_{i=1}^{n}(x_i - \mu_n)^3$.

It should also be noted that we have intentionally prepared these equation forms for improving algorithm efficiency. When implementing these analytic methods, practitioners can employ temporary variables to reuse suitable intermediate results to minimise computational workloads and to speed up programs. For example, $(\mu_{n+1} - \mu_n)$ and $(\mathbb{V}_{n+1} - \mathbb{V}_n)$ in Equation (8) can directly be obtained from the intermediate results in Equations (6) and (7).

4. A Wearable Movement Analysis System for Home Care

To facilitate validating our privacy preservation and quantification methodology, we further developed a wearable movement analysis system. The developed system consists of a wireless sensor for movement analysis and a mobile application that controls, receives and processes the raw data from the wireless sensor, incorporating clinical tests for the evaluation of fall risk and gait quality.

4.1. Electronic Sensor to Monitor Human Movement

We design an magneto-inertial measurement unit (MIMU) using a BNO055 sensor from Bosh Sensortec. This MIMU has a three-axis accelerometer, a three-axis gyroscope, and a three-axis magnetometer, as well as an internal processor capable of merging the inertial and magnetic data using an extended Kalman filter to deliver the orientation in quaternions.

The inertial and magnetic variables are measured at a sample frequency of 100 Hz using a STM32 32-bit microcontroller with an ARM Cortex-M4 processor. The raw data are sent to a mobile app over a Bluetooth 5.0 link. We use a 3.7 V, 1200 mAh LiPo battery to power the entire system, which gives the sensor up to 30 hours for continuous measurements.

A simplified block diagram and electronic PCB design of the sensor are shown in Figure 2.

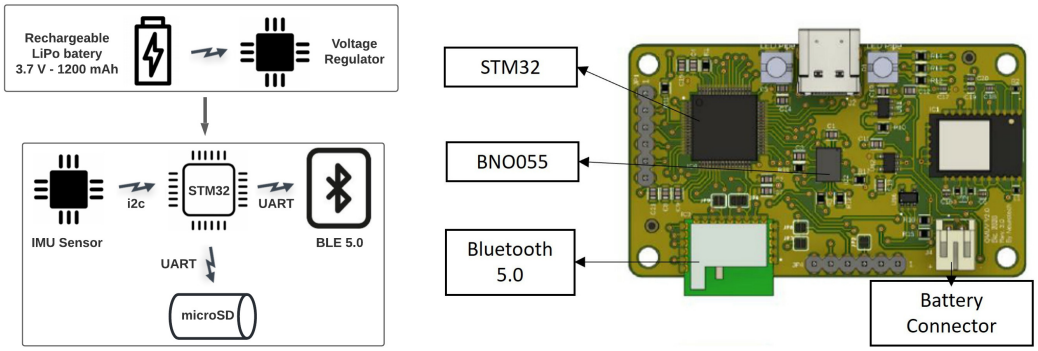

Figure 2. General electronic scheme and electronic PCB design of the implemented motion sensor.

To acquire significant movement information from the patients using a single measurement unit, we locate the MIMU on the lower back (L3–L5) using a 50 mm wide hook and loop elastic band with an adjustable design (see Figure 3). The final developed sensor has a weight of 104 g and a size of 95 × 75 × 20 mm.

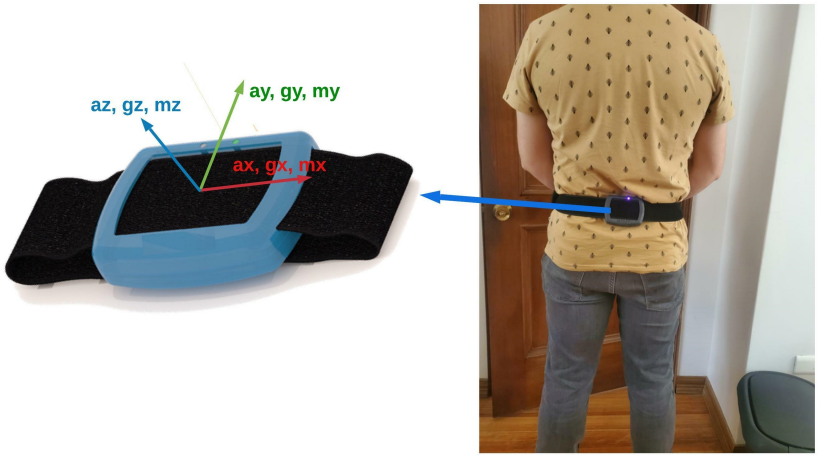

Figure 3. Sensor location for human movement analysis. The sensor is located to deliver their positive measurements in movements according to the axis.

The implemented sensor can measure static and dynamic movement information with low error in applications where the drift and noise produced by this sensor are negligible for human movement analysis purposes (see Table 1).

Table 1. Results for the static and dynamic evaluation of the sensor. Static evaluations where performed over 140 min of continuous measurement.

Sensor	Axis/Orientation	RMS	Drift	Offset	Dynamic Error
Acelerometer	X	0.0011 G	-	0.013 G	-
	Y	0.0011 G	-	0.033 G	-
	Z	0.0014 G	-	0.150 G	-
Gyroscope	X	1.12°/s	-	-	-
	Y	1.42°/s	-	-	-
	Z	1.41°/s	-	-	-
Euler	Yaw	-	0	-	$0.25 \pm 0.36°$
	Pitch	-	$2.88 \times 10^{-6}°/s$	-	$0.47 \pm 0.53°$
	Roll	-	$1.60 \times 10^{-5}°/s$	-	$-0.74 \pm 1.92°$

4.2. Mobile App for Motion Analysis

The measurement platform is a mobile application that communicates with the wireless movement sensor using Bluetooth 5.0.

The mobile app incorporates two algorithms developed and validated previously by the research team of this work. The first assess the risk of falls through the segmentation of the instrumented Timed Up & Go test (iTUG) [26], and the second is used for the analysis of gait through the instrumented 10 m walking test (iT10M) [27] (see Figure 4).

Figure 4. Mobile app implemented for home-care human movement analysis. Note that there are both tests for risk of falls and gait analysis. (**A**) Home menu to select the assessment test. (**B**) iTUG automatic results. (**C**) iT10M automatic results.

The mobile app communicates with an application programming interface (API) to manage the database where the user's pre-selected data are stored. We implemented an API using the PHP framework Lumen Laravel version 5.8. This API contains all the information related to the user sessions, the list of subjects, the raw signals (accelerations, angular velocities, and orientations), and the movement parameters extracted from each instrumented assessment scale.

4.2.1. Instrumentation of the Timed Up & Go Test

Although the iTUG is relatively new. Different authors indicate that the phases to be measured in the iTUG test are: (a) Standing, (b) Go walking, (c) 3 m mark turning, (d) Back walking, (e) Turn before sitting, and (f) Sitting (see Figure 5).

The automatic identification, segmentation, and analysis of the phases of the iTUG can increase its predictive value for the risk of falls. This approach produces a segmented evaluation regarding the phases in which the subjects present significant difficulties. We proposed an algorithm to automatically segment each phase of the iTUG using inertial data (accelerations and angular velocities) and orientation data (quaternions) [26]. Those algorithms allow us to extract of temporal indexes such as the duration of each iTUG phase and mobility parameters. The parameters we evaluate are the acceleration profile during standing and sitting, velocity profile during standing, sitting, and turning, steps during walking and trunk inclination during sitting and standing phases. Table 2 summarises the information that can be obtained using the proposed system.

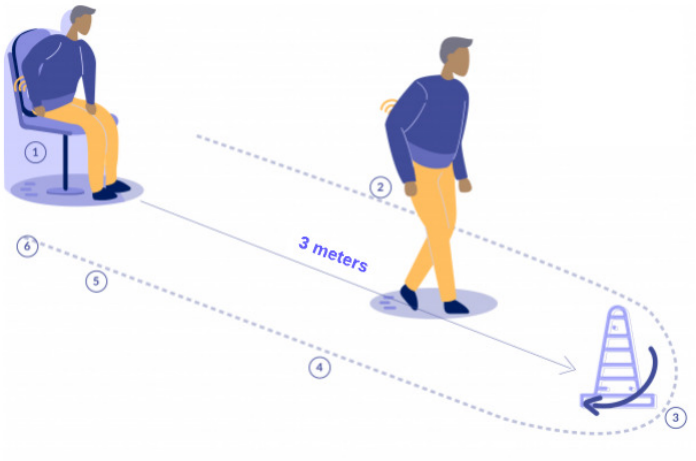

Figure 5. iTUG test with each phase segmented: (1) Standing, (2) Go walking, (3) 3 m mark turning, (4) Return walking, (5) Turn before sitting, and (6) Sitting. Note that the sensor is located on the lower-back of the person.

Table 2. Available information in the proposed movement analysis system by the iTUG for risk of falls evaluation.

Personal Data	Raw Data	Movement Indexes
• Name • Date of birth • Address • Phone number • Gender • Height • Weight • Email • Health history	• Tri-axial accelerations (m/s^2) • Tri-axial angular velocities (degrees/s) • Normalized quaternion orientations	• Risk of falling (Normal, Risk, High Risk) • Test duration (s) • Standing duration (s) • Sitting duration (s) • Walking duration (s) • Turning duration (s) • Pre-sitting turning duration (s) • Standing max acceleration (m/s^2) • Sitting max acceleration (m/s^2) • Maximum inclination during standing (degrees) • Maximum inclination during sitting (degrees) • Number of steps during walking • Angular velocity during turning (degrees/s) • Angular velocity during pre-sitting turning (degrees/s)

4.2.2. Instrumentation of the 10-m Walking Test

The iT10M is a clinical test used to evaluate the patient's gait from the performance of the walk in a predetermined distance of 10 m. In addition, the walking speed is measured and correlated with the patient's level of independence (see Figure 6). The instrumentation of this test allows estimating gait parameters with a single sensor located on the lower-back of the patient using a wearable alternative.

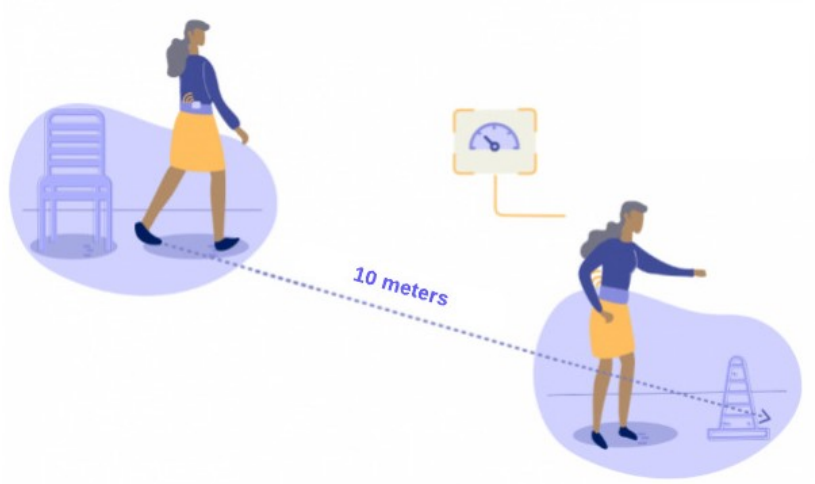

Figure 6. iT10M test. Note the sensor is located on the lower-back of the person.

The algorithm for gait analysis used and validated by the research team [27] allows processing the tri-axial accelerometry signals from the lower back. During the execution of the gait test, these data permit identifying the events of initial contact and final contact of each foot and, in this way, identifying the main gait events. With such data, it is possible to extract the spatio-temporal parameters of the gait cycle from each limb: Cadence (step/min), step time (s), stride time (s), double support time (s), single support time (s), swing phase duration (%), stance duration (%), step length (m), and stride length (m). Table 3 summarises the information that can be obtained using the proposed system.

Table 3. Available information in the proposed movement analysis system by the instrumentation of the iT10M for gait analysis.

Personal Data	Raw Data	Movement Parameters
• Name • Date of birth • Address • Phone number • Gender • Height • Weight • Email • Health history	• Tri-axial accelerations (m/s^2)	• Functional mobility • Walking speed (m/s) • Cadence (step/min) • Step time (s) • Stride time (s) • Double support time (s) • Single support time (s) • Swing phase duration (%) • Stance duration (%) • Step length (m) • Stride length (m) • Gait symmetry

5. Applying DnD to the Proposed Movement Analysis System for Home Care

Based on the aforementioned wearable movement analysis system (cf. Section 4), this research keeps developing and validating our DnD-based methodology and fosters a home-care project on multi-purpose daily activity monitoring and analytics. In particular, three main purposes of this home-care project are (1) establishing new indicators of individual health by monitoring a population's everyday activities, (2) measuring individual health by monitoring an individual's one-day activities, and (3) detecting/predicting individual accidents by monitoring an individual's real-time activities. As a matter of fact, it has been identified that dynamic factors such as physical activities should be considered alongside the static indicators (e.g., body mass index) to better reflect a person's health status [48].

Benefiting from our developed devices and trial studies, we are able and ready to monitor and identify a wide range of human activities. In particular, the DnD-friendly analytic methods formulated in Equations (4)–(7) have been extensively used in our current

monitoring trials (e.g., for real-time statistics of standing, sitting, and walking duration). Although monitoring the skewness of those indicators has not been implemented in our current work, we still report on this analytic method (i.e., Equation (8)) for the purpose of making this paper self-contained. By obtaining these parameters and indexes from a large of healthy people, we will further be able to create standard indicators and in turn use them for individuals' health measurement and fall risk detection.

5.1. DnD-Based Privacy Preserving Monitoring and Analytics of Daily Activities

The DnD approach advocates intrinsic privacy preservation by controlling data sharing and storing. The current implementation of DnD is to relieve the privacy risks in patient-centric monitoring and analytics of daily activities. For the convenience of discussion, we assume that the remote home-care from a hospital is based on a two-tier healthcare network, as shown in Figure 7.

At the home side of the healthcare network, the patient-centric data can be controllable across three storage levels and four transmission levels, respectively, as distinguished in Table 4. Specifically, it is suggested to retain locally either no data, analytic result, or raw data; and allow users to transfer either no data, regular handshakes, analytic result, or raw data to healthcare professionals. Correspondingly, the case study distinguishes between DnD-applicable scenarios and traditional analytics scenarios, as briefly explained below.

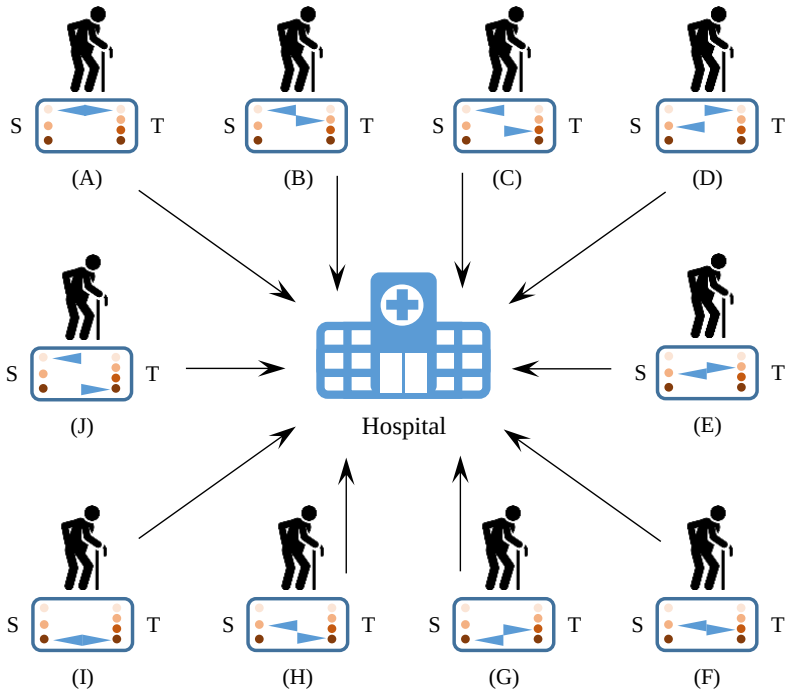

Figure 7. Different daily activity monitoring scenarios in the simplified healthcare network. In particular, *S* indicates user control policies for data storage, while *T* indicates user control policies for data transmission. (A) Store nothing and transmit nothing. (B) Store nothing and transmit regular handshakes and/or occasional notifications. (C) Store nothing and transmit analytic result. (D) Store analytic result and transmit nothing. (E) Store analytic result and transmit regular handshakes and/or occasional notifications. (F) Both store and transmit analytic result. (G) Store raw data and transmit analytic result. (H) Store analytic result and transmit raw data. (I) Both store and transmit raw data. (J) Store nothing and transmit raw data.

The DnD-applicable scenarios are proposed to be suitable for implementing DnD when we can forget the raw data immediately, such as:

- Scenario (A): Store nothing and transmit nothing. In this scenario, the collected raw data and the analytical result of a user's daily activities are neither saved by the user

nor shared with the others. Technically, we can follow the moving-window and/or the running statistical methods to continuously summarise the user's daily activities. The summary can be viewed at any time on a user-side monitor, while the present values will automatically vanish (or be updated) when the user refreshes the summary another time. In fact, this has been a common self-monitoring practice at home, e.g., tracking steps and heart rate from a smart watch.

- Scenario (B): Store nothing and transmit regular handshakes and/or occasional notifications. On top of Scenario (A), this scenario allows the hospital (who supervises the home care) to receive some basic information from the user at home. The regular handshakes may indicate the proper running status of the home-based daily activity monitoring system. The occasional notifications can be different shortcut codes that represent various predefined alerts. Once particular alerts are triggered, the user will receive professional interventions from the hospital. For example, if a fall is predicted or detected, the responsible professional will be notified and the remote camera will automatically be connected under the user's pre-granted permission to further decide whether or not to send an ambulance.
- Scenario (C): Store nothing and transmit analytic result. Depending on the user's control, the statistical summaries of a user's daily activities can be transmitted to the hospital either automatically or manually on a daily basis. By treating the hospital as a trusted third party (TTP), the user can let the hospital maintain his/her activity-related health profile instead of saving the daily summaries locally. Note that the mechanism of occasional notifications is enabled by default in this scenario. It is also worth mentioning that the user's living habit will not be disclosed in those overall summaries, because the detailed time series of the activity indicators and parameters are not recorded at all.
- Scenario (D): Store analytic result and transmit nothing. Similar to Scenario (A), here, the user also self-monitors the daily activities at home. Furthermore, in contrast with Scenario (C), the user is responsible for maintaining the activity-related health profile for himself/herself. Given the full control over the local data, the user can freely remove the historical summaries of daily activities, for example, to save storage space. On the other hand, since the hospital receives nothing, no professional intervention will be involved in this scenario.
- Scenario (E): Store analytic result and transmit regular handshakes and/or occasional notifications. This scenario obtains combinatory benefits from Scenarios (B) and (D). By saving the daily summaries, the user can maintain his/her activity-related health profile locally. By notifying the hospital with predefined alerts, the user will receive remote checkup or on-site care when abnormal activities are predicted or detected.
- Scenario (F): Both store and transmit analytic result. This scenario makes redundant collections of the statistical summary of a user's daily activities. As a result, the in-home system and the hospital both keep a copy of the user's activity-related health profile. From the user's perspective, this can be for the purpose of backing up or self-tracing the historical records of the summarized daily activities.

In contrast, the traditional analytic scenarios indicate the situations in which we need to store and/or transmit original sensor signals, such as:

- Scenario (G): Store raw data and transmit analytic result. By continuously recording and accumulating the original sensor signals with timestamps, this scenario may enable daily activity mining for a user via his/her in-home system. However, similar to Scenario (C), the statistical summaries of daily activities will be sent to the hospital only without being saved locally.
- Scenario (H): Store analytic result and transmit raw data. On the contrary of Scenario (G), here, the original sensor signals are directly relayed by the in-home system to the hospital, while the statistical summaries of daily activities are saved by the user only. In this case, by centralising different people's raw data together, the hospital as a TTP will be able to mine regular patterns of daily activities for a particular population.

- Scenario (I): Both store and transmit raw data. This scenario makes redundant collections of the original sensor signals of a user's daily activities. This may be useful for the user to conduct short-term daily activity analytics and for the hospital to conduct long-term and population daily activity analytics.
- Scenario (J): Store nothing and transmit raw data. By doing nothing locally but relaying the original sensor signals of a user's daily activities to the hospital, this scenario matches the situations of real-time and remote monitoring in the context of healthcare provisioning [49].

As the Figure 8 scheme shows, the mobile application summarises all the scenarios and controls the information flow.

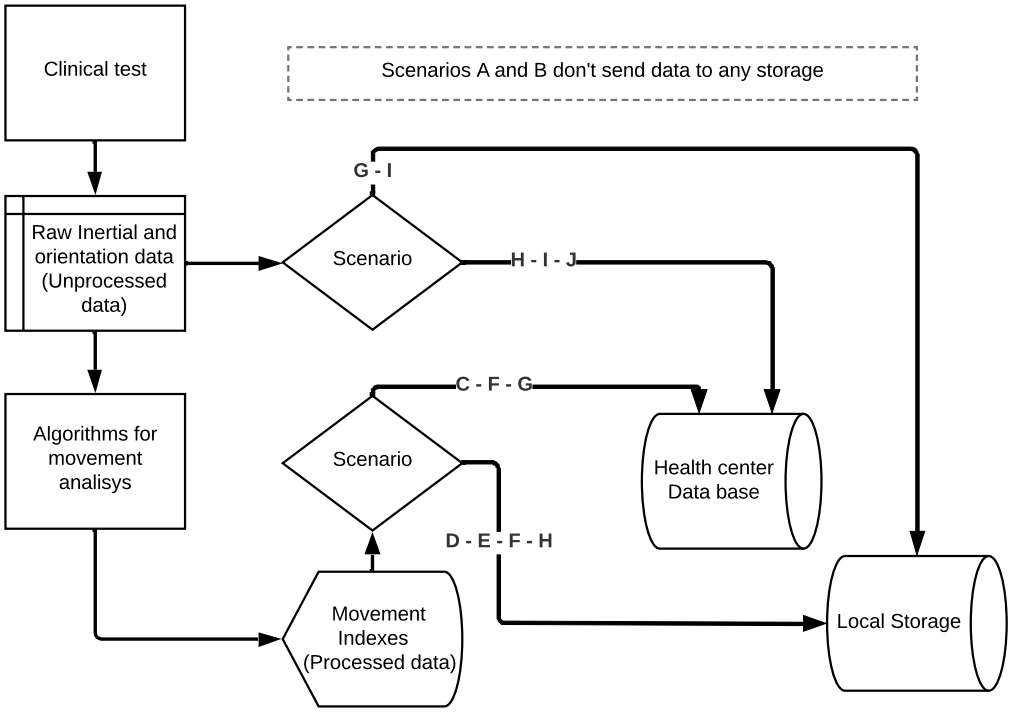

Figure 8. Information flow management depending the scenario selected on the mobile application.

5.2. Technical Implementation and Discussion

To accelerate the project progress, this research has implemented the DnD mechanism into a hybrid microservice system by reusing the software modules from the device-oriented trial studies and by using our previous microservice templates [50] for new functionality development. The whole solution logic is described in Algorithm 1.

The wearable devices send sensor signals to the software system of the local broker via Bluetooth 5.0 up to a maximum distance of 20 m without risk of occlusion. In terms of the mobile application, the user can select in a configuration screen his default privacy scenario and, also, can select his preference each time a clinical test is performed. In practice, the broker can further pass on the raw data to a user-side computer to facilitate local analytics. Given the structured switch-case decision tree, as shown in in Algorithm 1, it is convenient to distinguish between different scenarios and to conduct corresponding analytics. For example, we keep counting the elapsed time a patient spends in sitting, follow Equation (6) to calculate the running average of the patient's inclination angle when standing up, and follow Equation (7) to calculate the running standard deviation of the patient's walking speed, without necessarily waiting until finishing a whole-day measurement. Note that the measurable parameters and indices are specified in Section 4.

Algorithm 1 Solution to daily activity analytics

Input: Continuous signal data S from the wearable devices.
Output: Daily activity analytic results AR.

▷ Firstly, according to the user-controlled policy, try DnD-applicable analysis and also accumulate the raw data.
$D \leftarrow \emptyset$ ▷ D represents the raw data set.
for each $s \in S$ **do**
  ▷ Decompose each signal s into a tuple of meaningful information pieces $(d_1, d_2, d_3...)$.
  $(d_1, d_2, d_3...) \leftarrow s$
  if DnD-applicable **then**
    ▷ Applying DnD analytic methods (cf. Section 3.1) and continuously updating the analytic results AR.
    $AR \leftarrow \text{DND}(d_1, d_2, d_3...)$
  end if
  ▷ Optional raw data accumulation (also depending on the predefined policy).
  $D \leftarrow D \cup (d_1, d_2, d_3...)$
end for
▷ Secondly, if the user-controlled policy does not indicate any DnD-applicable scenario, then the analytic results AR will be empty, which means the offline analytics will be expected based on the accumulated raw data D.
if AR is NULL **then** ▷ Not in DnD-applicable scenarios.
  $AR \leftarrow \text{OFFLINEANALYTICS}(D)$
end if
▷ Thirdly, the post-analysis activities will be triggered according to the predefined policy.
switch *policy* **do** ▷ Given predefined policies.
  case *Store nothing* and *transmit analytic result*
    $D \leftarrow \emptyset$ ▷ Erase raw data locally.
    `send`(AR)
  case *Store analytic result* and *transmit nothing*
    $D \leftarrow \emptyset$ ▷ Erase raw data locally.
    `save`(AR)
  case *Store raw data* and *transmit analytic result*
    `save`(D)
    `send`(AR)
  case *Store nothing* and *transmit raw data*
    `send`(D)
    $D \leftarrow \emptyset$ ▷ Erase raw data locally.
  case *Others*
    ▷ More cases can be involved according to different policies.
return AR

5.3. Privacy Quantification in Different Scenarios of Daily Activity Analytics

Although the aforementioned scenarios of daily activity analytics can be informatively explained via natural-language descriptions, it is not straightforward for users to easily understand and compare the privacy levels between different scenarios. To facilitate privacy recognition and comparison, the developed risk-driven privacy quantification framework (cf. Section 2.2) was applied to this case study, which in turn validates the framework's efficacy in practice. In particular, the framework distinguishes between users' privacy sensitivity about data storage and about data transmission. Given the truth that the stored data are still at the user side, the sensitivity scale is assumed to be $s = 8$ for data storage privacy. In contrast, since users will lose control of the data after transmission, the highest sensitivity scale (i.e., $s = 10$) is set for data transmission privacy. For the similar reason, we set the inflection points to be $p = 50$ and $p = 30$ for more-controllable data storage and less-controllable data transmission, respectively, and using the equation system

(9) to quantify the privacy in DnD-based daily activity analytics. It should be noted that these parameter settings can conveniently be adjusted on a case-by-case basis as long as their justifications are consistent in/for the same data analytic project (e.g., daily activity analytics in this work).

$$\begin{cases} \mathscr{P}_{storage} = 1 - \mathtt{sig}(x; 8, 50) \\ \mathscr{P}_{transmission} = 1 - \mathtt{sig}(x; 10, 30) \\ \mathbb{P}_{DnD} = \mathscr{P}_{storage} \times \mathscr{P}_{transmission} \end{cases} \tag{9}$$

When it comes to the degree of data disclosure, further assumptions for the two cases of Regular Handshakes and Analytic Result are made, respectively. In the former case, although the regular handshake signals do not include any activity data, they may have carried some basic and predefined user information, e.g., the patient's identification at least. Therefore, it is aggressively assumed that 10% of personal data can be exposed by the handshake signals. In the latter case, although analytic results have abstracted original data into high-level summaries and interpretations, it is still possible to reveal some raw data details. In fact, recovering information from data summaries has been formally defined as an inverse problem [51]. Moreover, there is no doubt that the more analytic methods are employed together, the more original information could be revealed from the analytic results. For the purpose of demonstration, we fix the data disclosure degree in our case study's analytic results to be 30% of the entire raw data. Then, the privacy in different scenarios of daily activity analytics can be quantified as shown in Table 4.

It should be noted that the single-dimensional privacy can directly be recognised as 1 if disclosing zero percent of data (i.e., storing/transmitting nothing), or as 0 if disclosing 100% of data (i.e., storing/transmitting raw data), without necessarily using Equation (2) to calculate. In addition, Scenario (—) in Table 4 indicates the situations that are only for theoretical discussions here, because it makes little sense to keep all the data while not utilising them at all.

Table 4. Quantified Privacy in Different Scenarios of Daily Activity Analytics.

Privacy Dimension with respect to Data Storage	Privacy Dimension with respect to Data Transmission			
	Nothing to Transmit (0% disclosure)	**Regular Handshakes** (10% disclosure)	**Analytic Result** (30% disclosure)	**Raw Data** (100% disclosure)
Nothing to Store (0% disclosure)	Scenario (A): 1	Scenario (B): 0.881	Scenario (C): 0.5	Scenario (J): 0
Analytic Results (30% disclosure)	Scenario (D): 0.924	Scenario (E): 0.814	Scenario (F): 0.462	Scenario (H): 0
Raw Data (100% disclosure)	* Scenario (—): 0	* Scenario (—): 0	Scenario (G): 0	Scenario (I): 0

* Impractical scenarios for theoretical discussions only.

5.4. Technological Appreciation Survey

To know the health-domain professionals' perception of our technological proposal and methodology for privacy preservation, an anonymous survey of five questions was answered by 16 health professionals (3 medical technologists, 2 nurses, 1 psychiatrist, and 10 physiotherapists). All the 16 health professionals have experience using the movement analysis sensor and did not participate in any instance prior to the development and validation of the proposed technology. In addition, before answering the survey, users had to read and sign the informed consent, which was approved by the Biosecurity, Bioethical and Ethical Committee of the University of Concepción (Number 3180551). The result is presented in Table 5. Regarding whether the proposed technological system for the analysis of human movement is beneficial, 13 health professionals answered "Agree" or "Totally Agree". At the same time, two indicated "Neither Agree or Disagree", and one indicated that it did not seem helpful, although the proposed tool is of interest. Regarding whether

the privacy preservation proposal is useful for clinical applications, all 16 respondents indicated "Agree" or "Totally Agree". On whether the proposed method was considered good enough to maintain the privacy of patient information, 15 responded "Agree" or "Totally Agree" while one indicated "Disagree". About if the proposed methodology has advantages over other existing methods to preserve the information privacy, 12 declared "Agree" or "Totally Agree", while four answered "Neither Agree or Disagree". Finally, on whether they would like to see this privacy preservation methodology in other systems or technologies, 15 responded "Agree" or "Totally Agree", while one indicated "Neither Agree or Disagree". The results of this survey suggest that the proposed methodology has a high potential from the point of view of professionals in the health area.

Table 5. Technological appreciation survey.

Item	Strongly Disagree	Disagree	Neither Agree Nor Disagree	Agree	Totally Agree
(1) Are you satisfied with the proposed clinical human motion analysis system?	1	–	2	6	7
(2) Do you consider this privacy-preserving methodology helpful for clinical applications?	–	–	–	10	6
(3) Is the proposed privacy preservation methodology good enough to ensure the privacy of patient information?	–	1	–	9	6
(4) To the best of your knowledge, do you think the proposed privacy-preserving methodology has advantages over other known methods?	–	–	4	6	6
(5) Would you like to see the proposed privacy preservation methodology in other technologies or clinical applications?	–	–	1	6	9

6. Conclusions and Future Work

This paper presents a novel privacy preservation and quantification methodology for addressing privacy concerns in the home-care environments. In brief, this methodology advocates less sharing and less storing (i.e., DnD) to naturally reduce the significant privacy risks in data transmission and storage. When it comes to less sharing, data distribution has already been identified privacy-friendly for reducing data transmission and increasing user control. As for less storing, we argue to obey the decay theory to "forget" original data after their usage so as to avoid unexpected data leaks even from their owners. In practice, a home-based patient can choose which information he/she wants to share with health professionals according to their mutually agreed private scheme. Moreover, a risk-driven privacy quantification framework can be used not only to help judge the efficacy of DnD-based privacy preservation but also to better satisfy the diverse needs of privacy measurement. As the major contribution of this research, our proposed methodology essentially offers a generic approach to scoping a unified landscape for investigating privacy-friendly home-care systems. By including more data-processing dimensions and by analysing more privacy risks, this methodology will become more and more applicable to guide both the research and engineering of privacy preservation in the home-care environments.

To facilitate validating the proposed methodology, we also developed a movement analysis system for home-based fall risk evaluation and gait monitoring, using a single inertial measurement unit and a mobile analytics app. The custom platform contains algorithms developed and validated for the instrumentation of the iTUG and the iT10M

test. The system allows collecting the precise raw data in-home from the wireless movement measurement sensor and processing the collected data to obtain mobility indexes. This in-home evaluation can be done without attending a health centre or using high-technological systems for movement analysis. Thus, we also consider this movement analysis system as our contribution of this research, as it demonstrates the implementation of a lightweight home-care system, in addition to the validation of our methodology.

By introducing our work to several home-care-oriented projects, we have consulted the local professionals and received mostly positive feedback about our privacy preservation and quantification solution. On one hand, this strengthens our confidence that such a distributed and disposable principle will suit more home-care and particularly one-off healthcare scenarios. On the other hand, we realise that our methodology still suffers from some limitations at this current stage. Particularly, the effect of DnD's privacy preservation largely depends on the application scenarios. For example, we can expect the best privacy-preserving effect only when the raw data are neither stored nor transmitted. Although DnD is compatible with the existing privacy preserving mechanisms, there is still a lack of guidelines for integrating other techniques into DnD to satisfy the needs of mixed home-care scenarios. Therefore, in our future work, we plan firstly to explore new DnD-applicable home-care opportunities and make broader impacts in practice. Secondly, following the fundamental privacy principle (i.e., data minimisation [32]), we plan to combine DnD with the existing privacy preserving mechanisms. By giving DnD the highest priority, DnD will be able to work with and facilitate the implementations of other privacy-preserving techniques.

Author Contributions: Conceptualization, P.A., P.A.H.W. and Z.L.; methodology, P.A. and Z.L.; software, P.A., B.G. and Z.L.; validation, P.A., B.G. and Z.L.; formal analysis, B.G. and Z.L.; investigation, P.A., B.G., P.A.H.W. and Z.L.; resources, P.A. and Z.L.; data curation, B.G. and Z.L.; writing—original draft preparation, P.A., B.G., P.A.H.W. and Z.L.; writing—review and editing, P.A., B.G., P.A.H.W. and Z.L.; visualization, P.A., B.G., P.A.H.W. and Z.L.; supervision, P.A. and Z.L.; project administration, P.A. and Z.L.; funding acquisition, P.A. and Z.L. All authors contributed equally to this work. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported in part by Chilean National Research and Development Agency (ANID, Chile) under Grant FONDECYT Iniciación 11180905 and FONDEQUIP EQM150114.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and approved by the Ethics Committee of Universidad de Concepcion, Number 3180551.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

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

References

1. Sewell, J.P. Computer Development and Health Care Information Systems 1950 to Present. In *Informatics and Nursing: Opportunities and Challenges*, 5th ed.; LWW: Philadelphia, PA, USA, 2015; Chapter 1.
2. Martínez-Caro, E.; Cegarra-Navarro, J.G.; García-Pérez, A.; Fait, M. Healthcare Service Evolution Towards the Internet of Things: An End-user Perspective. *Technol. Forecast. Soc. Chang.* **2018**, *136*, 268–276. [CrossRef]
3. Rahmani, A.M.; Thanigaivelan, N.K.; Gia, T.N.; Granados, J.; Negash, B.; Liljeberg, P.; Tenhunen, H. Smart e-Health Gateway: Bringing Intelligence to Internet-of-Things Based Ubiquitous Healthcare Systems. In Proceedings of the 12th Annual IEEE Consumer Communications and Networking Conference (CCNC 2015), Las Vegas, NV, USA, 9–12 January 2015; pp. 826–834.
4. Thota, C.; Sundarasekar, R.; Manogaran, G.; Varatharajan, R.; Priyan, M.K. Centralized Fog Computing Security Platform for IoT and Cloud in Healthcare System. In *Exploring the Convergence of Big Data and the Internet of Things*; Prasad, A.K., Ed.; IGI Global: Hershey, PA, USA, 2018; Chapter 11, pp. 141–154.
5. Zhuang, Y.; Sheets, L.R.; Chen, Y.W.; Shae, Z.Y.; Tsai, J.J.; Shyu, C.R. A Patient-Centric Health Information Exchange Framework Using Blockchain Technology. *IEEE J. Biomed. Health. Inf.* **2020**, *24*, 2169–2176. [CrossRef] [PubMed]
6. Perera, C.; Ranjan, R.; Wang, L.; Khan, S.U.; Zomaya, A.Y. Big Data Privacy in the Internet of Things Era. *IT Prof.* **2015**, *17*, 32–39. [CrossRef]
7. Shirley Ryan—Abilitylab. Available online: https://www.sralab.org/ (accessed on 19 July 2021).

8. Park, S.H. Tools for assessing fall risk in the elderly: A systematic review and meta-analysis. *Aging Clin. Exp. Res.* **2018**, *30*, 1–16. [CrossRef] [PubMed]
9. Herssens, N.; van Criekinge, T.; Saeys, W.; Truijen, S.; Vereeck, L.; Van Rompaey, V.; Hallemans, A. An investigation of the spatio-temporal parameters of gait and margins of stability throughout adulthood. *J. R. Soc. Interface* **2020**, *17*, 20200194. [CrossRef]
10. Cebolla, E.C.; Rodacki, A.L.; Bento, P.C. Balance, gait, functionality and strength: comparison between elderly fallers and non-fallers. *Braz. J. Phys. Ther.* **2015**, *19*, 146–151. [CrossRef]
11. Kwon, M.S.; Kwon, Y.R.; Park, Y.S.; Kim, J.W. Comparison of gait patterns in elderly fallers and non-fallers. *Technol. Health Care* **2018**, *26*, 427–436. [CrossRef]
12. Schniepp, R.; Huppert, A.; Decker, J.; Schenkel, F.; Schlick, C.; Rasoul, A.; Dieterich, M.; Brandt, T.; Jahn, K.; Wuehr, M. Fall prediction in neurological gait disorders: Differential contributions from clinical assessment, gait analysis, and daily-life mobility monitoring. *J. Neurol.* **2021**, *268*, 1–14. [CrossRef]
13. Newstead, A.H.; Walden, G.J.; Gitter, A.J. Gait variables differentiating fallers from nonfallers. *J. Geriatr. Phys. Ther.* **2007**, *30*, 93–101. [CrossRef]
14. König, N.; Taylor, W.; Armbrecht, G.; Dietzel, R.; Singh, N. Identification of functional parameters for the classification of older female fallers and prediction of 'first-time'fallers. *J. R. Soc. Interface* **2014**, *11*, 20140353. [CrossRef]
15. Patil, H.K.; Seshadri, R. Big Data Security and Privacy Issues in Healthcare. In Proceedings of the 2014 IEEE International Congress on Big Data (IEEE BigData 2014), Anchorage, AK, USA, 27 June–2 July 2014; pp. 762–765.
16. Kapoor, V.; Singh, R.; Reddy, R.; Churi, P. Privacy issues in wearable technology: An intrinsic review. In Proceedings of the International Conference on Innovative Computing & Communications (ICICC 2020), New Delhi, India, 2 April 2020; pp. 1–7.
17. Motti, V.G.; Caine, K. Users' privacy concerns about wearables. In Proceedings of the 19th International Conference on Financial Cryptography and Data Security (FC2015), San Juan, Puerto Rico, 26-30 January 2015; pp. 231–244.
18. Ashok, A.; Nguyen, V.; Gruteser, M.; Mandayam, N.; Yuan, W.; Dana, K. Do not share! Invisible light beacons for signaling preferences to privacy-respecting cameras. In Proceedings of the 1st ACM MobiCom Workshop on Visible Light Communication Systems (VLCS 2014), Maui, HI, USA, 7 September 2014; pp. 39–44.
19. Denning, T.; Dehlawi, Z.; Kohno, T. In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies. In Proceedings of the 2014 SIGCHI Conference on Human Factors in Computing Systems (CHI 2014), Toronto, ON, Canada, 26 April–1 May, 2014; pp. 2377–2386.
20. Kravets, R.; Tuncay, G.S.; Sundaram, H. For your eyes only. In Proceedings of the 6th International Workshop on Mobile Cloud Computing and Services (MCS 2015), Paris, France, 11 September 2015; pp. 28–35.
21. Mathur, A.; Lane, N.D.; Bhattacharya, S.; Boran, A.; Forlivesi, C.; Kawsar, F. Deepeye: Resource efficient local execution of multiple deep vision models using wearable commodity hardware. In Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys 2017), Niagara Falls, NY, USA, 19-23 June 2017; pp. 68–81.
22. Li, Z.; O'Brien, L.; Kihl, M. DoKnowMe: Towards a Domain Knowledge-driven Methodology for Performance Evaluation. *ACM Sigmetrics Perform. Eval. Rev.* **2016**, *43*, 23–32. [CrossRef]
23. Li, Z.; Pino, E.J. D&D: A Distributed and Disposable Approach to Privacy Preserving Data Analytics in User-Centric Healthcare. In Proceedings of the 12th IEEE International Conference on Service-Oriented Computing and Applications (SOCA2019), Kaohsiung, Taiwan, 18–21 November 2019; pp. 176–183.
24. Li, Z.; Li, X.; Li, B. In Method We Trust: Towards an Open Method Kit for Characterizing Spot Cloud Service Pricing. In Proceedings of the 12th IEEE International Conference on Cloud Computing (CLOUD 2019), Milan, Italy, 8–13 July 2019; pp. 470–474.
25. Lu, R.; Zhu, H.; Liu, X.; Liu, J.K.; Shao, J. Toward Efficient and Privacy-preserving Computing in Big Data Era. *IEEE Netw.* **2014**, *28*, 46–50. [CrossRef]
26. Ortega-Bastidas, P.; Aqueveque, P.; Gómez, B.; Saavedra, F.; de-la Cuerda, R.C. Use of a Single Wireless IMU for the Segmentation and Automatic Analysis of Activities Performed in the 3-m Timed Up & Go Test. *Sensors* **2019**, *19*, 1647.
27. Aqueveque, P.; Gómez, B.; Saavedra, F.; Canales, C.; Contreras, S.; Ortega-Bastidas, P.; Cano-de-la Cuerda, R. Validation of a portable system for spatial-temporal gait parameters based on a single inertial measurement unit and a mobile application. *Eur. J. Transl. Myol.* **2020**, *30*, 9002. [CrossRef]
28. Rehman, R.Z.U.; Zhou, Y.; Del Din, S.; Alcock, L.; Hansen, C.; Guan, Y.; Hortobágyi, T.; Maetzler, W.; Rochester, L.; Lamoth, C.J. Gait analysis with wearables can accurately classify fallers from non-fallers: A step toward better management of neurological disorders. *Sensors* **2020**, *20*, 6992. [CrossRef]
29. World Health Organization. Health Topics: Ageing. Available online: https://www.who.int/health-topics/ (accessed on 23 November 2021).
30. Grubb, B. Thousands of Medical Histories Exposed in Data Breach. Available online: https://www.smh.com.au/business/companies/thousands-of-medical-histories-exposed-in-data-breach-20190807-p52euq.html (accessed on 22 September 2021).
31. Iyengar, A.; Kundu, A.; Pallis, G. Healthcare Informatics and Privacy. *IEEE Internet Comput.* **2018**, *22*, 29–31. [CrossRef]
32. Tene, O.; Polonetsky, J. Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern J. Technol. Intellect. Prop.* **2013**, *11*, 1.

33. Feng, X.; Zhang, C. Local differential privacy for unbalanced multivariate nominal attributes. *Hum.-Centric Comput. Inf. Sci.* **2020**, *10*, 25. [CrossRef]
34. Du, K.L.; Swamy, M.N.S. Introduction to Fuzzy Sets and Logic. In *Neural Networks and Statistical Learning*; Springer: London, UK, 2019; Chapter 26, pp. 769–801.
35. Wagner, I.; Eckhoff, D. Technical Privacy Metrics: A Systematic Survey. *ACM Comput. Surv.* **2018**, *51*, 57. [CrossRef]
36. Zhang, Z.; Lu, Z.; Tian, Y. Data Privacy Quantification and De-identification Model Based on Information Theory. In Proceedings of the 2019 International Conference on Networking and Network Applications (NaNA 2019), Daegu, Korea, 10–13 October 2019; pp. 213–222.
37. Dasgupta, A.; Kosara, R.; Chen, M. Guess Me If You Can: A Visual Uncertainty Model for Transparent Evaluation of Disclosure Risks in Privacy-Preserving Data Visualization. In Proceedings of the 16th IEEE Symposium on Visualization for Cyber Security (VizSec 2019), Vancouver, BC, Canada, 23–23 October 2019; pp. 1–10.
38. Miche, Y.; Ren, W.; Oliver, I.; Holtmanns, S.; Lendasse, A. A Framework for Privacy Quantification: Measuring the Impact of Privacy Techniques Through Mutual Information, Distance Mapping, and Machine Learning. *Cogn. Comput.* **2019**, *11*, 241–261. [CrossRef]
39. Petit, A.; Cerqueus, T.; Boutet, A.; Mokhtar, S.B.; Coquil, D.; Brunie, L.; Kosch, H. SimAttack: Private Web Search under Fire. *J. Internet Serv. Appl.* **2016**, *7*, 2. [CrossRef]
40. Navaz, A.N.; Harous, S.; Serhani, M.A.; Taleb, I. Real-Time Data Streaming Algorithms and Processing Technologies: A Survey. In Proceedings of the 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, 11–12 December 2019; pp. 246–250.
41. Henry, C.G.; Williams, R.R. Real-time Recursive Estimation of Statistical Parameters. *Anal. Chim. Acta* **1991**, *242*, 17–23. [CrossRef]
42. MathWorks. Moving Skewness and Moving Kurtosis. Available online: https://www.mathworks.com/matlabcentral/answers/426189-moving-skewness-and-moving-kurtosis (accessed on 2 June 2022).
43. Stackoverflow. How to calculate moving/running/rolling arbitrary function (e.g. kurtosis & skewness) using NumPy/SciPy? Available online: https://stackoverflow.com/questions/57133324/how-to-calculate-moving-running-rolling-arbitrary-function-e-g-kurtosis (accessed on 2 June 2022).
44. Faithfull, W. Recursive Statistics for Data Streams. Available online: https://faithfull.me/recursive-statistics-for-data-streams (accessed on 2 June 2022).
45. Cook, J.D. Accurately Computing Running Variance. Available online: https://www.johndcook.com/blog/standard_deviation/ (accessed on 2 June 2022).
46. Li, Z.; Galdames-Retamal, J. On IoT-Friendly Skewness Monitoring for Skewness-Aware Online Edge Learning. *Appl. Sci.* **2021**, *11*, 7461. [CrossRef]
47. Rao, P. Pulse Oximeters for COVID-19: What Oxygen Saturation Levels can Tell You about SARS-CoV-2 Infection. Available online: https://www.firstpost.com/health/pulse-oximeters-for-covid-19-what-oxygen-saturation-levels-can-tell-you-about-sars-cov-2-infection-8722451.html (accessed on 2 June 2022).
48. Coulman, K.; Toran, S.S. Body Mass Index May Not Be the Best Indicator of Our Health—How Can We Improve It? Available online: https://theconversation.com/body-mass-index-may-not-be-the-best-indicator-of-our-health-how-can-we-improve-it-143155 (accessed on 12 January 2022).
49. Albahri, O.S.; Zaidan, A.A.; Zaidan, B.B.; Hashim, M.; Albahri, A.S.; Alsalem, M.A. Real-Time Remote Health-Monitoring Systems in a Medical Centre: A Review of the Provision of Healthcare Services-Based Body Sensor Information, Open Challenges and Methodological Aspects. *J. Med Syst.* **2018**, *42*, 164. [CrossRef]
50. Li, Z.; Seco, D.; Rodríguez, A.E.S. Microservice-Oriented Platform for Internet of Big Data Analytics: A Proof of Concept. *Sensors* **2019**, *19*, 1134. [CrossRef]
51. Faloutsos, C.; Jagadish, H.V.; Sidiropoulos, N.D. Recovering Information from Summary Data. In *Proceedings of the 23rd VLDB Conference (VLDB 1997)*; VLDB Endowment Inc.: Athens, Greece, 1997; pp. 36–45.