data

MDPI

Article

Survey of Decentralized Solutions with Mobile Devices for User Location Tracking, Proximity Detection, and Contact Tracing in the COVID-19 Era

Viktoriia Shubina [1,2,*], Sylvia Holcer [3,4], Michael Gould [3] and Elena Simona Lohan [1]

[1] Faculty of Information Technology and Communication Sciences, Tampere University, Korkeakoulunkatu 1, 33720 Tampere, Finland; elena-simona.lohan@tuni.fi

[2] Faculty of Automatic Control and Computers, University "Politehnica" of Bucharest, Splaiul Independenței 313, 060042 Bucharest, Romania

[3] Institute of New Imaging Technologies, Universitat Jaume I, Avda. Sos Baynat, 12071 Castellón de la Plana, Spain; holcers@uji.es (S.H.); gould@uji.es (M.G.)

[4] Faculty of Electrical Engineering and Communication, Brno University of Technology, Technická 3058/10, 616 00 Brno, Czechia

* Correspondence: viktoriia.shubina@tuni.fi

Received: 31 July 2020; Accepted: 21 September 2020; Published: 23 September 2020

check for updates

Abstract: Some of the recent developments in data science for worldwide disease control have involved research of large-scale feasibility and usefulness of digital contact tracing, user location tracking, and proximity detection on users' mobile devices or wearables. A centralized solution relying on collecting and storing user traces and location information on a central server can provide more accurate and timely actions than a decentralized solution in combating viral outbreaks, such as COVID-19. However, centralized solutions are more prone to privacy breaches and privacy attacks by malevolent third parties than decentralized solutions, storing the information in a distributed manner among wireless networks. Thus, it is of timely relevance to identify and summarize the existing privacy-preserving solutions, focusing on decentralized methods, and analyzing them in the context of mobile device-based localization and tracking, contact tracing, and proximity detection. Wearables and other mobile Internet of Things devices are of particular interest in our study, as not only privacy, but also energy-efficiency, targets are becoming more and more critical to the end-users. This paper provides a comprehensive survey of user location-tracking, proximity-detection, and digital contact-tracing solutions in the literature from the past two decades, analyses their advantages and drawbacks concerning centralized and decentralized solutions, and presents the authors' thoughts on future research directions in this timely research field.

Keywords: Internet of Things (IoT) mobile devices; wearables; location estimation; user tracking; proximity detection; contact tracing; decentralized architectures; blockchain; Received Signal Strength (RSS); Bluetooth Low Energy (BLE); COVID-19

1. Introduction and Motivation

In recent months, humanity has been fighting a new and global threat, namely, the spreading and infectiousness of a new virus, Severe acute respiratory syndrome coronavirus 2 (SARS-COV-2), triggering a life-threatening disease for some people. The disease is known under the name of Coronavirus infectious disease 2019 (COVID-19) and can possibly create long-term complications, as stated in [1]. Medical and non-medical teams worldwide are looking actively for solutions to combat, mitigate, and slow the spreading of SARS-COV-2. Various forms of digital data for COVID-19 disease control have already been published, such as the raw measurements on various environmental factors from [2] or the geostatistical data of locations where COVID-19 tests were taken in the US [3], and the importance of data sharing has been already emphasized in the research literature, e.g., in [4].

Generally speaking, a *contact tracing* refers to the ability to identify, track, and inform the past contacts (within a predefined time window, corresponding to the most likely contagious period of a disease) of an infectious person, in order to manage any further spread of disease. Recent studies ascertained the start of this most likely contagious period as around three days before the onset of symptoms [5]. Once contact is identified, the person could be asked to self-isolate for safety measures.

Contact tracing can be done manually or digitally. A manual contact-tracing solution involves authorized personnel such as police forces or healthcare workers to identify the contacts of a person detected positive with COVID-19 or to identify the places visited by such a person during his/her period of being infectious. A *digital contact-tracing* procedure relies on technology, such as mobile devices and wearables carried by a person, or on visual cameras within commuting halls and shopping places, in order to identify persons that shared a particular space at a specific time, under the knowledge that infectious people also visited such timestamped locations [6].

Fully automated digital contact-tracing procedures are challenging to implement, because of various technological, medical, and ethical reasons that will be discussed in this paper. No such fully automated digital processes currently exist, to the best of the authors' knowledge. Semi-automatic digital methods combine some form of human-in-the-loop procedures and automatic procedures. Examples of human-in-the-loop actions are (i) a person voluntarily installing a COVID-19 contact-tracing application on his/her mobile device, (ii) a healthcare worker performing a COVID-19 test and confirming a positive result to an affected person, or (iii) a positive-confirmed person acknowledging in the pre-installed application on own device the results of the positive test and the most likely period of infectiousness. Examples of automatic actions are (i) a mobile application keeping track of encountered persons during a certain time window and possibly sending the anonymized IDs and timestamps to a server, (ii) a device-to-cloud protocol regularly interacting with a cloud/centralized server to determine if and when any of the encountered persons became infectious, etc.

Currently, there are more than 50 contact-tracing applications used in more than 30 countries worldwide to help in fighting the spread of COVID-19 and trying to tackle this infectious disease better than existing manual solutions. We have collected a list of these applications in a living database available in open access[1], to be regularly updated by the authors.

Figure 1 shows the number and geographic distribution of contact-tracing applications, according to the authors' searches and corresponding to the situation in July 2020. These applications referred to in Figure 1 originated in a particular country based on the location of their developers (e.g., three contact-tracing applications developed in France), but they typically can be used by any person, independently of his/her/their country of origin. Most of the existing digital contact-tracing apps are governmental applications and are supported by recent versions of Android phones, and in some cases, by modern versions of phones with iOS. A supplementary material with the full details of contact-tracing applications per country is also provided in open access by the authors (see footnote 1).

The large-scale adoption of wireless contact-tracing applications is currently hindered by the public's lack of trust in the privacy levels guaranteed by such applications; by the skepticism of the effectiveness of such an application to prevent the disease; and by the additional, sometimes non-negligible, power consumption of such an app running on a mobile device or user's wearable.

A recent study [7] showed that the highest adoption rate at present of a contact-tracing application in a country has been of only 38% in Ireland, which is still far from the desirable threshold value of

[1] Supplementary material provided by the authors in open access, with digital contact-tracing apps worldwide, https://sites.tuni.fi/survey-of-digital-solutions/.

60%. This value is considered necessary [7,8] to ensure a minimum critical mass for an automated or semi-automated digital contact-tracing application to become useful in disease prevention.

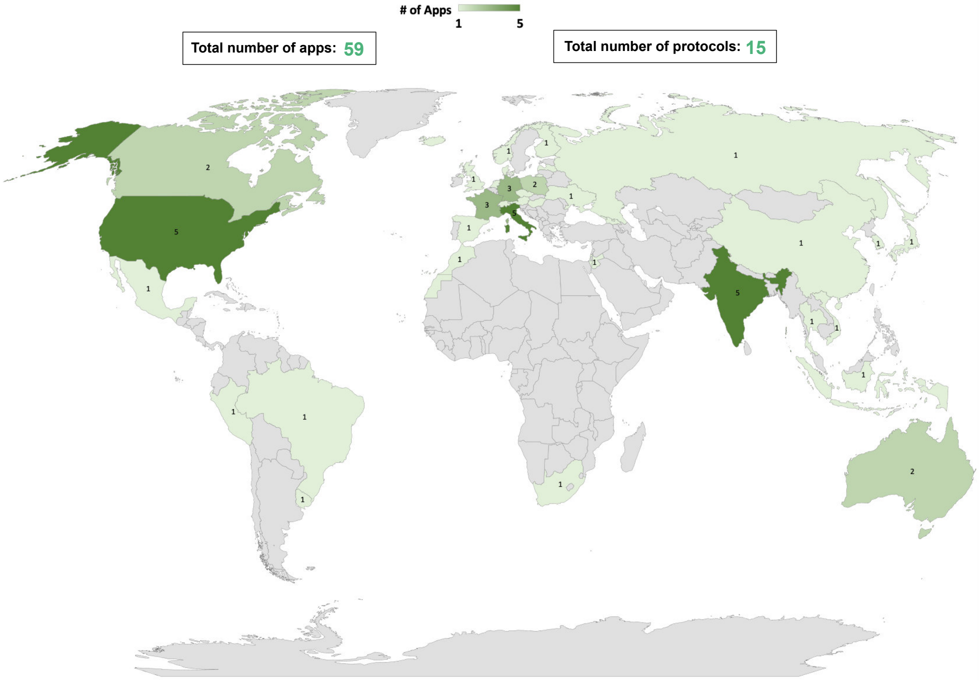

Figure 1. Worldwide distribution of current COVID-19 digital contract tracing applications, according to their country of origin (as of September 2020). We would like to point out that this map does not reflect the countries of use of a certain application or the percentage of the population adopting a certain app; it is to emphasize that efforts worldwide are dedicated to the creating of digital contact-tracing apps.

Considering that infectious diseases tend to spread exponentially, containment is an efficient means of slowing down the spread: the procedure is currently known under the term "Flattening the Curve" [9]. Due to the developed functionalities of modern smartphones (e.g., Bluetooth-based proximity tracing and location-based tracking) and the high adoption rate among users worldwide, mobile digital apps enable a mode of tracing backward one's contact history. Besides, digital solutions allow the interested institutions (e.g., health service providers, border control authorities, etc.) to determine if any person crossed paths with someone who tested positive for the COVID-19 within the epidemiologically relevant period (e.g., 3 days before the onset of symptoms [5] and up to 14 days after the onset of symptoms or from the test day).

Assuming the target of a high adoption rate of technological approaches worldwide, the privacy-versus-accuracy trade-off appears in line with the privacy-utility trade-off. The authors of [10] estimated the privacy risks for carriers, users, non-users, and local businesses.

Highly related to contact tracing, but less studied in the context of disease control, are the solutions for user location tracking and proximity detection. Both are reviewed in detail in our paper, and their connection to the contact-tracing solutions and possible usefulness towards disease control will be investigated. Our paper's contribution is three-fold:

- We offer a comprehensive review of user location tracking, proximity detection, and wireless contact-tracing solutions, by also explaining the underlying principles and technologies for such solutions.
- We address the issue of decentralization, as opposed to centralized approaches; discuss both centralized and decentralized approaches in terms of architectures and protocols; and summarize the advantages and challenges of a decentralized approach versus a centralized approach.

- We discuss the technical and privacy-related challenges in digital contact-tracing applications and present our ideas on open research questions and the way forward.

The remainder of the paper is organized as follows. Section 2 introduces the terminology and concepts addressed in this paper; Section 3 compares our work with other surveys from the literature and explains the progress beyond the state-of-the-art; Section 4 offers a comprehensive review of user location tracking, proximity detection, and wireless contact-tracing methods from the literature and discuss their applicability in the context of COVID-19 mitigation and prevention; Section 5 describes the decentralization idea and discusses several decentralized protocols for contact tracing, as well as their advantages and disadvantages compared to a centralized approach; the users' perception of the usefulness of decentralized architectures based on a web survey created by the authors is also presented in Section 5; Section 6 discusses various privacy-preserving techniques, while Section 7 focuses on energy-efficient solutions; Section 8 discusses the challenges to overcome towards a large-scale adoption of wireless contact-tracing apps; and Section 9 presents the conclusions.

2. Terminology and Conceptual Definitions

Decentralization is one of the key aspects of cybersecurity solutions in the wireless world of today [11–13]. Decentralization refers to the situation where the available information is split into pieces and stored in various parts (mobile agents, edge computing centers, etc.) of a network instead of storing everything on a central server; in addition, no single entity has full control or the complete information. Decentralization often goes hand in hand with some forms of anonymization of the data to be stored and processed, and with the time limitation on how long the data is to be stored. In decentralized architecture, no participant in the wireless communication chain has full information, neither can one infer comprehensive information about the other participants in the network based on the partial information one possesses.

Decentralization as a method to increase wireless security has been discussed, for example, in [14] (in the cryptocurrency context), in [15] (in the context of payment-channel transactions), or in [16] (for the inter-domain routing security). Decentralization, in the context of user location tracking, has also been addressed to a large extent in the last decade as a measure to offer increased privacy to the user. For example, the authors of [17] proposed a decentralized registry model for Location-Based Services (LBSs) by introducing several local servers (today called edge servers) in order to support dynamic discovery and routing between nodes. In 2014, the authors of [18] proposed a two-level cache mechanism with a decentralized architecture to protect users' mobility traces' privacy. More recently, in 2017, the authors of [19] proposed a peer-to-peer (P2P) decentralized model for increased location privacy of users. The model in [19] likewise showed a lower data retrieval time than the centralized architectures.

The concept of decentralized architectures has become increasingly important recently in the context of digital contact tracing used to cope with the global COVID-19 pandemic and to be able to identify how the contagious virus circulates within the population. As recently published research works in in the journal Nature show, there are multiple ways to tackle the spread of the virus, and decentralized privacy-preserving contact tracing is one of the most promising measures [20].

Related to the decentralization concept, *blockchain* methodologies also have permeated recent research on user localization [21,22]. A blockchain refers to cryptographically encrypted and decentralized registers (or ledgers) that maintain a continuously growing list of ordered data blocks. The main differences with the traditional decentralized protocols are the presence of the encryption and the total absence of a trusted central authority. Blockchain solutions for contact tracing have been recently addressed in [23], where the authors proposed that digitally signed pairwise encounters between mobile devices are stored in a distributed ledger and then some form of machine learning algorithms, such as deep learning networks, are used to identify the close social contacts.

The use of *data science* in the medical domain and for disease control is also a rather established paradigm, with data science solutions already proposed for the classification of vital human signs in order to monitor chronic diseases [24], to identify genetic diseases through probabilistic models [25], to build visualization systems for infectious disease outbreaks and spreads [26], and to handle missing data in healthcare big data [27].

Machine learning approaches, as a subcategory of data science, have been recently proposed for forecasting the future of COVID-19 [28]. An exponential smoothing algorithm was found to give the most accurate results, while the classical Support Vector Machines (SVM) gave the worst performance among the considered algorithms. The results were, however, limited to about two months of data and the authors pointed out that more research is needed for accurate real-time predictions.

Additional terms used in this paper, such as *user location tracking*, *proximity detection*, and *contact tracing*, are further addressed in detail in Section 4. The acronyms used in the paper are listed in the Section 9.

3. Added Value of Our Survey Compared to the State-Of-The-Art

An at-a-glance comparison of our survey with other surveys in the existing literature can be found in Table 1. Moreover, a living document presenting a dataset of contact-tracing applications worldwide, including a brief description of each application from available public data is accessible online, see footnote 1.

Table 1. Existing surveys in the literature and comparison with our survey; ✓= topic addressed; ✗ = topic not addressed.

Authors	Addressing Contact-Tracing Solutions	Addressing Proximity-Detection Solutions	Addressing User Location-Tracking Solutions	Addressing Privacy Protocols	Addressing Energy Efficiency
Li and Guo	✓	✗	✗	✗	✗
Bolic et al.	✓	✓	✗	✗	✗
Ye et al.	✗	✗	✓	✗	✓
Chen et al.	✓	✗	✓	✗	✓
Kaptchuk et al.	✓	✗	✓	✓	✗
Li et al.	✓	✗	✓	✓	✗
Ahmed et al.	✓	✗	✓	✓	✓
Martin et al.	✓	✓	✗	✓	✗
Nasajpour et al.	✗	✓	✗	✗	✗
Sun et al.	✓	✗	✗	✓	✗
Hernández-Orallo et al.	✓	✗	✗	✗	✗
Reichert et al.	✓	✗	✗	✓	✗
Braithwaite et al.	✓	✗	✗	✗	✗
Our survey	✓	✓	✓	✓	✓

In the related research presented in [29], the authors reviewed three data regulations (the European Union (EU) General Data Protection Regulation (GDPR), the approach released by the EU for efficient contact-tracing apps, and the EU guidelines on the use of location data in the COVID-19 outbreak) with respect to contact-tracing solutions as well as four technology protocols, namely, the Privacy-Preserving Proximity Tracing (PEPP-PT), Decentralized Privacy-Preserving Proximity Tracing (DP-PPT), the Apple/Google decentralized COVID-19 contact-tracing protocol, and a government-run contact-tracing technology. In addition, the authors in [29] also discussed 10 contact-tracing apps, six of them based on Bluetooth Low Energy (BLE) technology, one based on Quick Response code (QR code) scanning, two based on Global Positioning System (GPS), and one hybrid with GPS, BLE, and Wireless Fidelity (Wi-Fi). No user location or proximity-detection technologies were addressed in [29]. Seven out of 10 discussed apps in [29] used centralized protocols, the other three used decentralized solutions.

The focus in [30] was on proximity-detection approaches, based on Radio Frequency Identification (RFID) technology. The proximity-detection applications are mostly discussed in the context of object detection, rather than person-to-person proximity detection, but there is also a small part dedicated to the tracking of human interactions. The solution proposed in [30] would work in the context of contact tracing indoors if people were to carry RFID tags with them, and an RFID reader would be present in each room. The system proposed in [30] is unlikely to work well outdoors, and it would be quite expensive due to the need for a large infrastructure of RFID readers.

The authors of [31] studied a solution with barometer and accelerometer sensors to improve the energy efficiency of location trackers compared to GPS-based localization. However, no contact-tracing or proximity-detection aspects were discussed in [31].

In [32], solutions based on Artificial Intelligence (AI) were surveyed as measures to fight COVID-19. While the paper's main focus is on AI methods for the diagnosis, virology, pathogenesis, and COVID-19 treatment, there is also a small discussion related to AI usages in the patient route tracking and contact tracing. Data privacy was mentioned in the challenges section in [32], but no solutions were overviewed.

A survey on users' willingness to adopt a contact tracing or user tracking application was presented in [33]. The accuracy of the contact-tracing application was found to be the significant influencer towards the willingness of the app's adoption, followed by the privacy specification of the application. Of 789 respondents to the survey (all Americans), 85% expressed their willingness to adopt a COVID-19 contact-tracing app if it is accurate enough, 73% expressed their willingness to adopt it if it is private enough, and 88% expressed their willingness to adopt it if it is both accurate and private enough. The authors have found privacy aspects in [33] to be a significant factor in the mass adoption of a mobile app.

The authors of [34] addressed centralized-versus-decentralized approaches in the context of contact tracing and user location tracking based on a web survey with 244 respondents from the USA, selected from Amazon's crowdsourcing platform, MTurk. Six contact-tracing and/or location-tracking apps were selected, three of them with centralized architectures and three of them with decentralized architectures, and the survey participants were asked about their willingness to install any of those apps, as well as about their perceived trade-offs in terms of the applications' privacy and usefulness. The work in [34] is not yet peer-reviewed. The authors' findings were somewhat exceptional and confronted the general view, in the sense that they found that centralized contact tracing seemed to be preferred at the national/USA level rather than decentralized approaches.

The work in [35] is another study that has not yet been peer-reviewed, also discussing centralized-versus-decentralized architectures in contact-tracing and user location-tracking apps, with a particular focus on the security and privacy of such applications. Several possible attacks during wireless device tracking were reviewed, and examples of current apps based on centralized, decentralized, as well as hybrid architectures were given. The paper's best strength, in the authors' opinion, is their comparative table of 15 COVID-19 contact-tracing apps in terms of their robustness to various wireless attacks. Battery usage was also briefly addressed in [35], with the conclusion that the apps running in the background are less power-hungry than apps that run on the foreground decentralized apps and could save more battery than centralized ones by having less frequent needs of exchanging data with a central server.

In [36], a study recently published on arXiv, the authors surveyed different frameworks and mobile apps for digital contact tracing, with a particular focus on the privacy of various solutions. Twelve protocols, with eight of them supporting decentralized architectures, were overviewed, and some specific attacks of user privacy, as well as possible countermeasures, were also discussed. According to the work in [36], the most downloaded contact-tracing apps (as of July 2020) are the Corona-warn-app from Germany and Immuni from Italy, with both of more than one million downloads from Google play. Both are using the Google/Apple Exposure Notification (GAEN) decentralized protocol.

The study in [37] focused on Internet of Things (IoT) technologies at large and on their role in pandemics, by covering wearables, drones, and robots with e-health monitoring and/or proximity-detection functionalities. AI-based monitoring is seen as an important future step towards digital IoT-based solutions for solving different problems during the COVID-19 era, such as sickness prevention, health monitoring, tele-working, using social robots to reduce mental strain, etc.

The work in [38] is another recently published survey on arXiv with a focus on privacy of the digital contact-tracing apps.

The authors of [39] focused on smartphone-based contact-tracing technologies, and in particular, on stochastic and deterministic models of the spread of infectious diseases.

In [40], a survey of automatic contact-tracing apps was done, and security and privacy aspects were addressed in detail. Various cryptographic-based methods, such as homomorphic encryption and secure multi-party computation, were also addressed.

A very recent study [41] provided a systematic literature review on automated and semi-automated digital-tracing solutions. The authors first identified 4033 records in existing literature related to the contact-tracing solutions; then, they selected a subset of 110 papers as the most relevant works, and finally analyzed qualitatively a further subgroup of 15 articles among them. Their conclusions point out that the effectiveness of a digital contact-tracing method depends on the number of persons using such a digital app and the timeliness of the intervention, such as self-quarantine measures. They also found that manual contact-tracing solutions were reported in the literature to be more effective than digital contact-tracing solutions and that very few such comparisons exist. Privacy aspects were pointed out as being important, but outside the scope of the study in [41].

In distinction to all the surveys mentioned above, our survey jointly addresses contact tracing, proximity detection, and user location tracking; points out how different methods, not used yet in the context of contact tracing, could also be adapted in this context; and addresses both privacy and energy efficiency issues. Moreover, the main focus on our survey is on decentralized architectures, which were found in the majority of studies dedicated to digital contact tracing so far (see, e.g., in [33–36,38]) to be the most promising architectures in terms of a good trade-off between user-privacy preservation and accuracy of the contact tracing.

We would also like to emphasize the fact that this is a highly dynamic research field at the time of this paper's writing, and therefore some of the new and related research might not have been fully captured in Table 1, as this table reflects the situation at the beginning of September 2020.A survey on users' willingness to adopt a contact tracing or user tracking application was presented in [33]. The accuracy of the contact-tracing application was found to be the significant influencer towards the willingness of the app's adoption, followed by the privacy specification of the application. Of 789 respondents to the survey (all Americans), 85% expressed their willingness to adopt a COVID-19 contact-tracing app if it is accurate enough, 73% expressed their willingness to adopt it if it is private enough, and 88% expressed their willingness to adopt it if it is both accurate and private enough. The authors have found privacy aspects in [33] to be a significant factor in the mass adoption of a mobile app.

4. Wireless Location Technologies for User Location Tracking, Proximity Detection, and Contact Tracing

The following section surveys the leading solutions found in the literature so far for the location tracking, proximity detection, and contact tracing, and it gives a classification of wireless connectivity solutions, according to four criteria.

4.1. Classification of Wireless Connectivity Solutions

In order to design a wireless application for contact tracing, proximity detection, or/and user location tracking, one needs first to understand what kind of wireless technologies are currently available and what design constraints are essential, such as energy efficiency, spectrum availability, or low-cost low-power constraints. A top-level classification of wireless connectivity solutions is provided in Figure 2, where four main categories were identified by the authors:

1. *Cellular versus non-cellular* connectivity solutions: cellular solutions refer to the wireless communication techniques where a large geographical area is split into smaller cells, and each cell is served by a base station or an access node; the connectivity between base stations can be ensured either in a wireless manner or via optical fiber, and there is typically a centralized server/operator to maintain and control the whole cellular network. Examples or cellular technologies are Fourth-generation cellular systems (4G) or Long-Term Evolution (of cellular systems) (LTE) and Fifth-generation cellular systems (5G). Extensive surveys of cellular network connectivity solutions can be found, for example, in [42] (focus on localization aspects in cellular networks), [43] (focus on mobility models in cellular networks), or [44] (focus on green communications with cellular networks). The non-cellular solutions do not rely on the geographical division into cells and can operate both in an ad hoc/decentralized manner and in an infrastructure/centralized manner. Two of the most encountered solutions of non-cellular connectivity are BLE and Wi-Fi connectivity. To the best of the Authors' knowledge, cellular solutions have not been much investigated yet in the context of digital contact tracing, but this can change shortly with the advent of powerful 5G-based positioning technologies [45–47]. 5G-based positioning is addressed in more detail in Section 4.2. Examples of non-cellular wireless technologies are BLE, Wi-Fi, ZigBee, RFID, Long Range access (LoRa), NarrowBand Internet of Things (NB-IoT), etc. A good survey of non-cellular technologies can be found in [48]. The most used wireless technology for digital contact tracing at present is the BLE technology, due to its widespread on mobile devices and relative low-power consumption.
2. *Licensed versus non-licensed frequency bands*: a licensed band is a frequency band where wireless transmission is only allowed for operators having purchased a license; for example, traditionally, cellular operators have designated licensed frequency bands to operate. Unlicensed bands are the Industrial, Scientific, and Medical (ISM) bands as well as frequencies not yet allocated in the spectrum (e.g., some millimeter-wave frequencies and Terahertz (THz) frequencies). Interoperability issues between licensed and non-licensed spectra and cellular versus non-cellular communications have been addressed, for example, in [49]. A wireless tracking or contact-tracing solution relying on licensed bands would require the participation of operators having access to such licensed bands. Therefore, it is likely to be a centralized solution. Decentralized solutions in licensed bands are not available at the present moment to the best of the authors' knowledge.
3. *Mass-market versus high-end* connectivity solutions: a mass-market solution typically has low cost, low energy/power consumption, and it is affordable to the mass-market consumers. High-end connectivity solutions such as those relying on Augmented Reality (AR), Virtual Reality (VR), or Mixed Reality (XR) and, sometimes, on machine learning, are unlikely to become relevant promptly in the context of contact tracing and user tracking, as they aim at a narrow or niche market. They are unlikely to be adopted on a large scale (usually due to high costs). A good review of low-end, middle-end, and high-end IoT devices can be found in [50].
4. *Long-range versus short-range* connectivity: long-range connectivity such as cellular solutions and some IoT solutions refer to coverage ranges of several hundreds of meters to few or tens of km [48]. Short-to-medium range connectivity typically refers to ranges of up to a few tens of meters. On one hand, in terms of user tracking, proximity detection, and contact tracing, a short coverage area could mean a better accuracy of the distance estimates between any two users. On the other hand, if a user needs to connect to a server to upload or download data related to its own location,

a long-range connectivity solution is typically needed to be present on the user device. Relevant reviews of long-range connectivity solutions are provided in [48,51], where the focus is on IoT solutions. Short-range communications are reviewed in multiple studies, such as [52] with focus on near-field communications, [53] with focus on Bluetooth and BLE, then the study in [54] with focus on Ultra Wide Band (UWB) communications, and [48] with focus on general IoT solutions.

Additional studies on wireless connectivity and positioning solutions can be found, for example, in [55]. In the study, existing IoT domain technologies were classified via operating frequency bands, protocols versus enablers, range-based classification (i.e., short-, medium- and long-range operated solutions), data rates (low vs. high rates), and power-range classification (e.g., low-power vs. high-power operation).

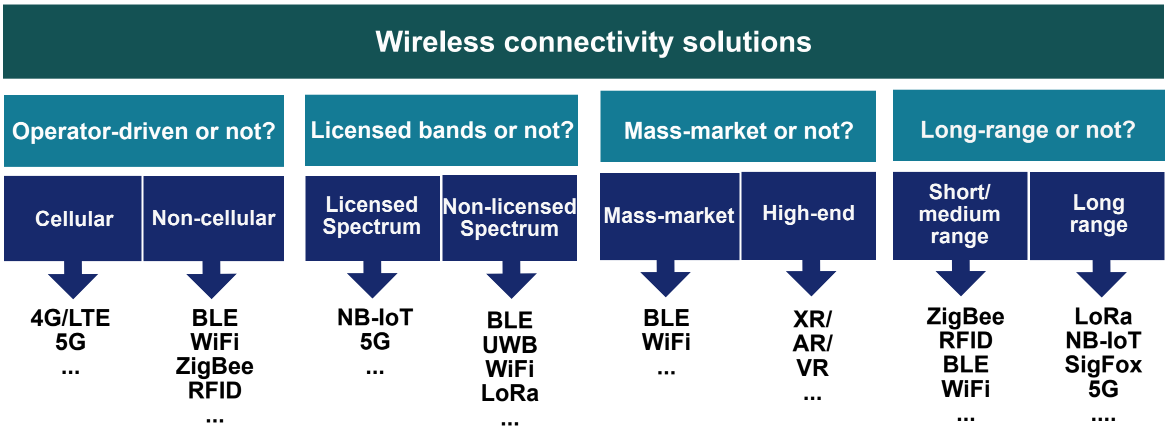

Figure 2. Classification of wireless connectivity solutions.

4.2. User Location Tracking

User location tracking is by no means a recent research field, and it has been intensively studied for more than two decades, since the advent of Global Navigation Satellite System (GNSS). User *location tracking* refers to wireless solutions able to estimate a user location with certain accuracy (in 2D or 3D dimensions) and also to allocate a timestamp to each location estimate, i.e., the continuous location estimates plus the time stamps form a user tracking solution. Location tracking is a domain with many potential implementation/application areas, and contact tracing based on user location is only one area [56,57].

The upper plot in Figure 3 illustrates a user-tracking scenario and gives examples of applications where user tracking could be applicable, such as increased security at country borders, workforce tracking, asset tracking market, etc.

There are many ways in which a device or user location can be computed, and the main location-related measurements are shown in Table 2, together with a qualitative estimate on their location accuracy capabilities. Received Signal Strength (RSS)-based localization relies on measuring the received signal power (or strength) from any kind of wireless signal able to be identified at a receiver. That is to say that, RSS measurements are not limited to a certain technology, but RSS can be measured from virtually any wireless signal, such as BLE, Wi-Fi, cellular, NB-IoT, LoRa, etc. The RSS is then converted into a distance or range measurement, by assuming a certain path-loss model, for example, as in Equation (1):

$$RSS[dB] = P_T[1m] - 10nlog_{10}(d) + \eta, \tag{1}$$

where RSS is the received power (in dB), P_T is the transmit power at 1 m away from the transmitter (also in dB), n is a path-loss coefficient with typical values between 1 and 10 (with $n = 2$ corresponding to a free space-loss propagation), d is the distance between the transmitter and the receiver (namely the distance between 2 users), and *eta* is a random variable, typically modeled as Gaussian distributed with zero mean and a shadowing standard deviation σ_η of the order of 4–10 dB [58].

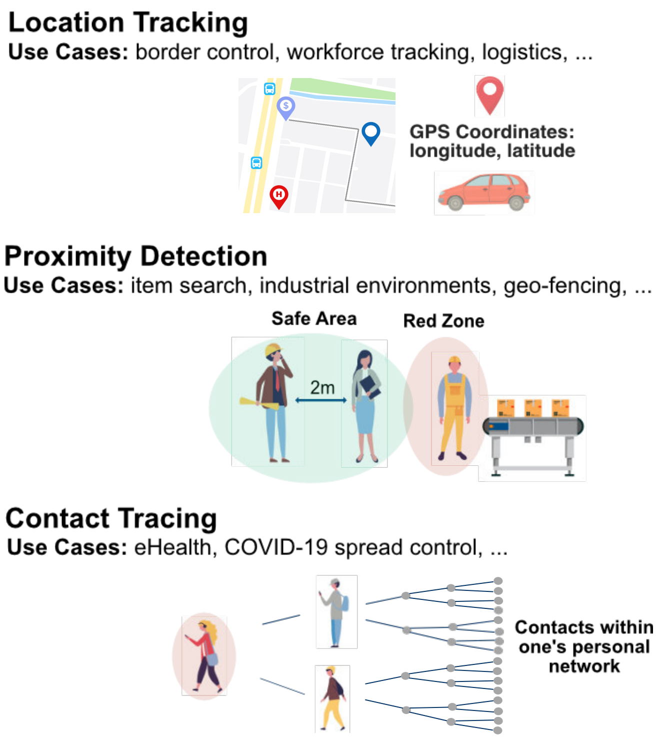
Location Tracking
Use Cases: border control, workforce tracking, logistics, ...
GPS Coordinates: longitude, latitude
Proximity Detection
Use Cases: item search, industrial environments, geo-fencing, ...
Safe Area
Red Zone
2m
Contact Tracing
Use Cases: eHealth, COVID-19 spread control, ...
Contacts within one's personal network

Figure 3. Illustration of scenarios for location tracking (upper plot), proximity detection (middle plot), and contact tracing (lower plot).

FingerPrinting (FP) is another possible method for localization, and it is again not limited to any particular technology, but it can be used broadly with any electromagnetic or non-electromagnetic (e.g., sound, light, etc.) signal [59]. FP-based estimation relies on two phases: (i) a training phase where fingerprints with location labels are collected from a certain space or geographical area and saved into a training database and (ii) an estimation phase where new measurements without any location labels are matched (or 'fingerprinted') with the data stored in the training database. The matching can be based on various Machine Learning (ML) approaches. The most commonly used fingerprinting algorithm is the k-Nearest Neighbours (kNN) algorithm [60]. FP methods have been addressed in detail in [59], a book dedicated to all aspects involved in FP-based positioning, navigation, and user tracking.

Time-based approaches such as Time of Arrival (TOA), Round Trip Time (RTT), and Time Difference of Arrival (TDOA) rely on the time–distance relationship of an electromagnetic wave, namely,

$$d = (t_R - t_T) * c, \tag{2}$$

where d is the distance between a transmitter and a receiver, c is the speed of light (if the signal is an electromagnetic signal), t_R is the time when the signal is received at the receiver, and t_T is the transmitter time. Receivers and transmitters need to be synchronized in a classical TOA approach. Alternatively, a wireless device can measure the so-called RTT, i.e., the time of the signal to reach a neighbour device found at distance d and to return to the original device. In such case,

$$d = rtt * c/2, \tag{3}$$

where rtt is the measured RTT. Yet another possibility used in user localization and mobile device tracking is for a receiver to compute the differences in the time of arrival from two reference transmitters, i.e., the TDOA. In this way, it is enough that the two transmitters are synchronized, as the receiver clock will not appear in the TDOA measurements. One significant aspect of timing-based measurements is that they are not easy to use in decentralized approaches. They typically require a centralized server to coordinate various reference transmitters, with respect to which a receiver computes its range or position.

Angle-based measurements such as Direction of Arrival (DOA), Angle of Arrival (AOA), or Angle of Departure (AOD) can also be used to estimate the user location, based on the idea that there are certain geometric dependencies between the horizontal (azimuth) and vertical (elevation) angles of the direction of signal propagation between a transmitter and a receiver and the distance d between a transmitter and a receiver. Extensive overviews of RSS, time-based, and angle-based location-related measurements can be found, for example, in [55,61]. Rarer, but possible measurements to be used in location estimation are also Frequency Difference of Arrival (FDOA) and Phase of Arrival (POA) measurements, as well as any hybrid combination between all the above-mentioned methods, such as RSS and TOA, TDOA and AOA, etc.

Among all the techniques mentioned in Table 2, RSS-based measurements are the most suitable for a decentralized architecture.

Table 2. Comparison of main user location-tracking mechanisms and their associated location-related measurements.

Method	Location-Related Measurement	Accuracy	Ref.
RSS	Range	◔	[55,58,62,63]
FP	Fingerprints	◑	[59,64,65]
TOA/ RTT	Range	◕	[55,62,66,67]
TDOA	Range difference	◕	[62,68,69]
DOA/AOA /AOD	Bearing	◑	[62,70]
FDOA	Doppler	◑	[71]
POA	Phase	◑	[61,62]
Hybrids	Range, phase, bearing, ...	◕	[72–74]

◔—Low; ◑—Medium; ◕—High.

5G-based user location studies are becoming more numerous, with applications in various areas such as smart city, logistics, automated vehicles, etc. [45–47]. To the best of the authors' knowledge, 5G-based positioning has not yet been addressed in the context of COVID-19 disease control, but 5G technology is an up-and-coming technology for providing ubiquitous location information, especially in a distributed manner [75]. This can be done, for example, by exploiting the cooperation among the mobile user devices, such as smartphones, smartwatches, and other IoT devices. Unlike most other cellular and non-cellular solutions relying, to some extent, on RSS measurements to compute the user location, 5G positioning is typically fully relying on a combination of TOA/TDOA and AOA measurements. By astutely combining time and angular information, 5G networks can achieve sub-m accuracy in the location estimation [76–78]. The high bandwidths available at mm-wave carrier frequencies, where most of the future 5G systems will operate, ensure this increased positioning accuracy compared to cm-wave solutions. Two potential challenges towards the adoption of 5G positioning as digital contact-tracing technologies are the reduced privacy level—as 5G-based positioning is typically implemented in a centralized approach—as well as the high-power requirements—as most 5G devices are requiring frequent battery recharges and are known to be still quite power-hungry [79].

Table 3 summarizes the most comprehensive surveys (to the best of the authors' knowledge) in the current literature regarding user location tracking solutions. Such studies were mostly written before COVID-19 emergency, and therefore the disease control mechanisms are not addressed in there. In the last column of Table 3, we present our view of how such studies can be relevant in COVID-19 disease control through digital methods. We point out some of the most suitable solutions investigated so far, and these can be further used to better manage and control infectious diseases.

Table 3. Comprehensive studies on **user location-tracking** solutions in the literature.

Reference	Main Findings	Relevance for COVID-19
[80]	A comprehensive survey on cellular and non-cellular positioning methods; high-accuracy simultaneous location and mapping solutions.	While contact tracing is not explicitly addressed here, centralized contact-tracing solutions can benefit from the reported high-accuracy localization solutions.
[42]	A thorough overview of cellular-based localization techniques, including sensor-aided and Assisted GNSS solutions.	Might be relevant for centralized contract tracing solutions with operators' collaboration, but sufficient accuracy can be achieved only with high-power/high energy-consumption solutions such as assisted GNSS and 5G.
[62]	A survey on indoor user-tracking solutions with pros and cons of each solution; challenges in indoor localization are also addressed in detail.	RSS-based localization solutions were typically found more energy efficient than TOA/AOA-based solutions; also Visible Light Communications (VLC)-based localization was emphasized as having both good accuracy and low energy consumption and might be a good future candidate for COVID-19 contact tracing.
[81]	Another survey on indoor user-tracking solutions with focus on RSS and FP solutions.	The application is not relevant for COVID-19 control.
[45,82]	Comprehensive surveys on 5G positioning methods.	Particular topic was not yet studied in COVID-19 context, but has high potential of high accuracy for user location both indoors and outdoors.

Table 4. Comprehensive studies on **proximity-detection** solutions in the literature.

Ref.	Main Findings	Relevance for COVID-19
[83]	Proximity detection via ZigBee of two devices equipped with ZigBee chipsets and using RSS.	Only objects placed at maximum 20 cm from each other were studied in [83], but the detection results higher than 96% are promising and zigBee ranges can go to several meters, thus making ZigBee a potential useful candidate for COVID-19 contact tracing.
[84]	A privacy-preserving protocol for proximity detection for any range measurements (RSS, TOA, etc.).	Rather high latencies (order of tens of ms) can hinder a good real-time implementation.
[85]	Proximity detection via BLE RSS and compressed sensing to deal with incomplete observations.	Very promising approach also in the COVID-19 contact-tracing context, even if not studied for this purpose in [85]; detection probabilities up to 90% for sub-m distances.
[86]	RFID-based proximity detection with ambient backscattering.	A digital contact tracing with such solution would require a centralized server, many RFID readers and people equipped with passive RFID tags; such solution would be quite expensive and impractical.

Table 4. *Cont.*

Ref.	Main Findings	Relevance for COVID-19
[87]	Wi-Fi RSS-based proximity detection between two mobile phones.	Promising approach as experiments in [87] showed 90% accuracy for distances below 2 m and 100% accuracy for distances below 3 m.
[88]	A sociometric sensor capable of detecting proximity, movement, and verbal interaction between people via Wi-Fi RSS, Inertial Measurement Unit (IMU), and sound sensor.	Another promising solution with proximity detection of 90% up to a distance of 3 m and having the ability to also detect verbal interactions; however it is an expensive and high-power solution.
[89]	Magnetic field-based proximity detection.	It requires centralized architectures and it has rather moderate accuracy.
[90]	Infrastructure-less proximity detection between users based on public web cameras.	Might provide a low-cost solution for the users, but it requires public webcams as well as protocols to identify the users; user privacy cannot be ensured.
[91]	MIT SafePaths is an open source location sharing app relying on BLE and GPS; it relies on Private Automated Contact Tracing (PACT) decentralized protocol.	It has already been proposed as a contact-tracing app, but its usefulness is still to be tested at large scales.

4.3. Proximity Detection

According to the World Health Organization (WHO), *proximity detection* in the context of COVID-19 utilizes the location-based (GPS) or Bluetooth technology to detect and trace the movements of individuals to distinguish people who may have been exposed to an contagious virus [92]. The risk of exposure to COVID-19 depends on the probability of coming into close (e.g., less than 2 m) or frequent contact with people who may be infected. However, proximity by itself is not a complete assessment of exposure, as exposure may vary independently of proximity, such as being in an enclosed area, a location separated by walls, or in an open-air space.

For IoT systems, it is vital to have reliable hardware and to predict a user's position in the area with high accuracy in order to be able to differentiate between individuals in a small space. Proximity detection in conjunction with Bayesian filtering aims to perform high accuracy positioning [93,94]. Another example of high-resolution beacon-based proximity detection for dense areas is described in [95].

In [96], the authors described a COVID-19 related proximity-detection approach and the efficacy of such approach.

Proximity-detection tools can be categorized as either centralized or decentralized, meaning that contact history can either be processed centrally, typically by a health authority, or by individual devices. Privacy concerns about the disclosure of personal data need to be addressed before using such tools.

The middle plot in Figure 3 illustrates a proximity-detection scenario (e.g., learning whether two users are in close vicinity) and gives examples of applications where proximity detection can be used.

A proximity-based privacy-preserving approach with use of smartwatch was described in [97]. The experiments in [98] indicated that in ideal settings, when all RSS measurements are available, a direct estimation provides the best proximity detection and lowest complexity among the studied solutions. Moreover, the context has a more significant effect on the resulting distance estimate matrix than the network localization approach.

Traditionally, the term for proximity detection has been mostly used for the detection of inanimate objects, such as a lost item in a smart house or a food item on a shelf of a warehouse. When used in the context of infectious disease control, user proximity detection is often studied in the context of contact tracing (see Section 4.4). Table 4 outlines the most comprehensive surveys (to the best of the authors' knowledge) in the current literature regarding proximity-detection solutions and discusses their relevance for COVID-19. Most of the proximity-tracing solutions have been developed in the pre-COVID-19 era, and therefore their usefulness as contact-tracing methods is still to be proved. For example, ZigBee-based and magnetic-field based solutions have not yet been implemented or tested for infectious diseases contact tracing. Furthermore, Wi-Fi-based solutions are currently estimated to be too power-hungry for a large-scale implementation on mobile user devices.

4.4. Contact Tracing

In general, *contact tracing* is the process of defining the chain of connections with individuals within one's personal network. Tracing and recognizing infected people, testing them with further isolation measures in case of positive test results, and tracing their interactions with other contacts aim to mitigate the spread of the virus. Contact tracing is mostly used in the eHealth domain and acts as a preventive measure in spreading diseases such as tuberculosis, Ebola, and recent infections (e.g., COVID-19). The objectives of contact tracing are (i) to identify the transmission routes of the virus, (ii) to notify individuals who possibly crossed paths with a user tested positive, (iii) to provide further recommendations on how to treat the infection, and (iv) to get the insights on the epidemiological results within certain areas.

A theoretical approach using both percolation and message passing techniques, to the role of contact tracing, in mitigating a pandemic spread is shown in [99].

A vast majority of the COVID-19 applications pursue the goal of location/proximity-based contact tracing. As stated in [29], contact-tracing applications rely on multiple technologies (e.g., GPS, QR code, and BLE), use various architectures and technology protocols.

The lower plot in Figure 3 illustrates a digital contact-tracing scenario where the purpose of the app installed on a wearable or a mobile phone is to detect which users are in close proximity to oneself (e.g., at maximum 2 m distance), for how long, and at which particular times, in such a way that, when one of the neighbors becomes infected with COVID-19, the other users found in the vicinity during the infectiousness period can receive alerts on their mobile devices and can take protective measures for own health and social health (e.g., self-quarantine, performing a COVID-19 test, taking prevention drugs if/when available, etc.)

Table 5 summarizes the most comprehensive surveys (to the best of the authors' knowledge) in the current literature regarding contact-tracing solutions and discusses their relevance for COVID-19, including potential challenges.

Table 5. Studies on **contact-tracing** solutions in the literature.

Ref.	Main Findings	Relevance for COVID-19
[29]	Existing privacy challenges related to the use of Static IDs and possible data linkage issues. Different BLE signal intensity at the ISM bands, multipath interference and spatial blockage between devices in BLE-based contact tracing.	The survey provides a systematic mapping of global status for contact-tracing applications deployed worldwide. The authors perform a qualitative analysis and compare the amounts of active users for particular applications. No single solution is emphasized as the way to go ahead.
[100]	Models of calibration and proximity accuracy with BLE RSS measurements.	BLE found as the best solutions nowadays for proximity detection; UWB suggested as future solution on smart phones.
[101]	Magnetometer-based contact tracing.	Requires a centralized architecture and it needs a large number of magnetic field samples for reliable results.
[102]	Efficient Privacy-Preserving Contact Tracing (EPIC) privacy-preserving protocol for any RSS-based contact tracing.	It relies on centralized server with encrypted information for better privacy protection; trustable servers are a must in such approaches.

Table 5. *Cont.*

Ref.	Main Findings	Relevance for COVID-19
[103]	Decentralized Privacy-Preserving Proximity Tracing (another abbreviation for DP-PPT) (DP-3T) protocol based on BLE RSS.	This is one of the most popular contact-tracing protocols nowadays, as it relies on a decentralized architecture and it is also the source of inspiration for GAEN protocol.
[104]	GAEN Exposure notification solution, supported by iOS and Android devices and relying on BLE RSS measurements.	Apps relying on GAEN protocol are currently the most downloaded mobile apps according to [36,38] and are the most promising to be widely adopted at long-term, due to their multi-device support, ease-of-installation, and decentralized architectures.
[38]	ROBust and privacy-presERving proximity Tracing (ROBERT) is developed by PRIVATICS team from Fraunhofer Institute and INRIA as an open source hybrid (decentralized plus some robust centralized features) protocol using BLE; DESIRE is a similar protocol as ROBERT developed by INRIA researchers.	Still in the research phase; aims at collaboration between various governments towards a cross-country adoption.

4.5. Comparative Summary

A comparative summary of underlying wireless technologies suitable for user location tracking, proximity detection, and/or contact tracing is shown in Table 6.

BLE is a wireless personal area network technology; in comparison to Classic Bluetooth, BLE is intended to provide a reduced power consumption and cost by operating at a similar communication range. This short-range technology, currently operating at ranges of up to a few hundred meters, is known as one of the most suitable for smartphones, which can provide proximity information useful for contact tracing. By using the BLE wireless radio signals for proximity information, users equipped with BLE-enabled devices can be notified if they were possibly infected.

Zigbee is a technology characterized as a low data rate solution, with low-power consumption, so-called close proximity Wireless Personal Area Network (WPAN). Zigbee is promising to be of lower cost in comparison with close rivals, for example, BLE or the popular technology as Wi-Fi [55]. However, probably due to lower data rates than BLE, ZigBee has not significantly penetrated the consumer market yet, and it is mostly used in industrial environments.

Wi-Fi is a low-to-moderate range wireless technology, supported by a wide variety of devices, e.g., personal computers, smartphones, cars, household appliances, wearable devices, and drones. Wi-Fi is usually operating at the 2.4 gigahertz and 5 gigahertz radio band, but recent Wi-Fi standards have expanded the spectrum to mm-wave carrier frequencies too. The carrier bands dedicated to this technology operate well in the Line-of-Sight (LOS) circumstances. However, walls or other obstructions can reduce the Wi-Fi coverage range significantly, but this also helps minimize the appearing interference between multiple networks located in close proximity densely populated areas. In the field of positioning, Wi-Fi signals were compared with BLE signals for example in [58].

UWB is a technology similar to Wi-Fi or BLE that can operate at a deficient energy level for short-range, high bandwidth communications across a large division of the radio spectrum. Due to the short pulse width and specific frequency range, UWB devices can transmit data correctly with minimal noise interference. This technology delivers a cm-level accuracy is used for improving the precision of localization on wearable devices and the latest mobile phones.

RFID is often seen as the father of all IoT. This solution refers to a technology whereby a reader captures digital data encoded in tags or smart labels via radio waves. RFID tags' data can be read outside the LOS, which is a strong advantage if the technology is used to determine the position of the human or an asset indoors. Nevertheless, RFID solutions are expensive and power-hungry, and they are unlikely to be selected for large-scale user tracking, proximity detection, or contact tracing, being most useful in small-scale scenarios, such as a hospital or a clinic, a warehouse, or a smart home.

Table 6. A survey of wireless technologies used for user location tracking and/or contact tracing on portable devices, including wearables.

Technology	Location-Tracking Capabilities	Contact-Tracing Capabilities	Proximity-Detection Capabilities	Examples of Wearables or Mobile Apps	Examples of Used Protocols
BLE	◑	◕	◕	EasyBand [105] Accent wristband [106] BLE-enabled device [103,104] TraceTogether app [39]	Cloud/ centralized [105,106] DP-3T [103] Google/Apple [104] EPIC [102]
ZigBee	◔	◑	◑	TelosB motes [107]	N/A
Wi-Fi	◑	◕	◕	VR headsets [108]	Cloud/ centralized EPIC [102]
UWB	◕	◑	◑	UWB Sensors [109]	N/A
RFID	◑	◑	◑	Wearable with RFID [110]	Cloud/ centralized [111]
GNSS	◕	◑	◔	Sports wearables for football player tracking [112] Comarch LifeWristband [113]	Cloud/ centralized
LoRa	◔	◑	◔	MoKo wearables [114]	Cloud/ centralized
VLC/Li-Fi	◔	◑	◑	VLC for wearable patient monitoring [115]	Cloud/ centralized
Acoustic/ Sound	◔	◔	◔	Acoustic localization via smartphone [116]	Cloud/ centralized
Infrared (IR) /LED	◔	◑	◑	LED-based positioning [117]	Cloud/ centralized
Magnetic sensors	◑	◔	◔	Smartphone with magnetometer [101]	Cloud/ centralized
Images/ Webcams	◑	◔	◔	Pedestrian proximity detection via webcams [90]	Cloud/ centralized
5G	◑	◑	◑	A 5G-based positioning testbed by Ericsson [118]	Cloud/ centralized

◔—Low; ◑—Medium; ◕—High.

GNSS systems refer to a constellation of satellites providing signals from space that transmit positioning and timing data to receivers. The receivers then utilize this data to define user locations using the time signals transmitted along a line of sight by radio from satellites. Examples of current GNSS include Galileo developed by the EU, the USA's NAVSTAR GPS, Global'naya Navigatsionnaya Sputnikovaya Sistema (GLONASS) originated in Russia, and China's BeiDou Navigation Satellite System. In the context of contact tracing, GNSS solutions are power-hungry and operate most effectively outdoors. Therefore, they are also less suitable than BLE for large-scale scalable apps.

LoRa is a long-range wireless technology, operating in unlicensed spectrum and using a chirp spread spectrum technology. LoRa allows low-power transmissions over long ranges such as more than 10 km for IoT devices. Devices equipped with LoRa are equipped geo-location sensing capabilities applied for trilaterating devices' positions, however the location accuracy provided by standalone LoRa solutions at the present is rather poor, in the order of few tens of meters. LoRa is a good candidate for long-range connectivity to the cloud, as a lower-power alternative to cellular connectivity.

Passive solutions such as GNSS and magnetic sensors are not adequate in stand-alone modes for contact tracing, as they would require additional wireless connectivity support for data exchange between wearables. They can be however used in conjunction with other wireless technologies, such as BLE or Wi-Fi. VLC or Light Fidelity (Li-Fi) solution requires LOS propagation between the two users and their accuracy is heavily affected by the body posture, orientation, hand movements, etc.

4.6. Open Access Datasets

This section obtained a summary of open access datasets from the available literature related to user location tracking, proximity detection, and/or contact tracing. They are summarized in Table 7.

Table 7. Summary of main open-datasets currently available for user location-tracking, proximity-detection, and/or contact-tracing studies.

Ref.	Main Purpose	Positioning Accuracy	Energy Consumption	Tested Deployment	Requirements
[119]	User location and tracking based on BLE RSS	◑	◔	Mixed Indoors/ Outdoors	Centralized architecture based on existing BLE infrastructure
[120]	Contact-tracing tool for livestock disease control	N/A	◕	Outdoor livestock movements extracted from Swedish Board of Agriculture	Relies on GPS-based location tracking
[121,122]	Contact tracing, proximity detection, and co-presence detection	◕	◑	Student campus	Uses existing infrastructure such as various mobile sensors, e.g., magnetometer, accelerometer, and WiFi networks
[123]	Contact-tracing calibration data for BlueTrace protocol	N/A	◔	Mixed Indoors/ Outdoors	Centralized architecture based on BLE
[124]	BLE-based dataset and software for user positioning and proximity detection	◑	◔	Indoors	Centralized architecture based on BLE
[125]	BLE and UWB data for calibration in user tracking	N/A	◑	Indoors	Centralized architecture based on BLE and UWB
[126]	BLE and Wi-Fi data for user location and tracking	◕	◕	Indoors	Centralized architecture based on BLE and Wi-Fi
[127]	UWB data for user location and tracking	◕	◕	Indoors	LOS between anchors and tags

◔—Low; ◑—Medium; ◕—High.

Some of the data available in these datasets were manually collected in indoor or outdoor scenarios, some have been collected from livestock-based on GPS chipsets carried on by the animals, and some provide computer-generated data. To the best of our knowledge, none of them have been investigated in the context of COVID-19 disease control. Still, the availability of such open access datasets could facilitate future studies in this timely research area. The main difference between the datasets focusing on user tracking and those focusing on proximity detection or contact tracing bases on the knowledge that the absolute user location is not needed in the proximity detection and contact tracing cases, and only a relative location, such as distance between two users or co-presence in the same room, is enough. Typically, the datasets meant for user tracking can also be used for proximity-detection and contact-tracing studies, as they contain additional information such as the absolute user locations, but the reverse is not usually true; when only the relative distance between users is stored, there might be not enough information for accurate user tracking.

4.7. Mathematical Models for Digital Contact Tracing

Mathematical models for digital contact tracing are still limited in modern literature, although this is also a very suitable and speedy progressing research domain. Practical examples of recently published works concerning mathematical modeling of infectious disease control through contact tracing are published in [5,39].

The authors of [128] provide a mathematical modeling approach discussing the topic of the COVID-19 contact-tracing efficacy. The results show the effect of contact-tracing programs with patterns of two states in the US. As a consequence, the study highlights the importance of early contact-tracing deployment. It shows that such first restriction measures have an opportunity to reduce the number of hospitalizations significantly and decrease the cumulative mortality rate. However, the authors figured out the efficiency of a belated application. They confirmed that disease control measures taken with a delay caused a decrease of total mortality by a factor of up to 38.1% in Florida and created a sparse reduction of ~5.6% in Michigan.

The authors of [129] claim that under an assumption of the test-and-trace coverage at 80% rate and the strictly followed time of 24 h from sample collection to quarantine measures, a digital contact-tracing app can decrease secondary contamination by 26% compared to the situation when no contact tracing is used.

Additional valuable knowledge feeding more astute models is related to the infectiousness window, as currently it is estimated to be from at least three days from the onset of early symptoms until at least 10 days after the first symptoms appear, according to [5,130].

The authors in [131] offer a stochastic model for trace-and-isolate strategy. They state that such a trace-and-isolate strategy could generally control the COVID-19 transmission within three months, but there are also scenarios (e.g., high number of asymptomatic transmissions) under which a trace-and-isolate strategy alone is insufficient and must be supplemented with further interventions, such as mass testing.

Table 8 lists the main open access repositories found in relation to mathematical models of infectious diseases, such as various datasets and software, but not related to contact tracing, proximity detection, or user tracking. The open access data listed in Table 8 was used for example for studying the transmission dynamics of COVID-19 [132] or for modeling the duration when a person is likely to be infectious for the others [133], etc.

Table 8. Additional open access datasets or software for mathematical modeling of the infectious diseases' spread, such as COVID-19.

Ref.	Characteristics
[132]	Dataset for the estimation of COVID-19 transmission dynamics; dataset collected in Tunisia during Feb-May 2020.
[133]	R-based software for modeling the periods of "infectiousness" of infected persons of generic infectious diseases.
[134]	A collection of links to more than 30 datasets for COVID-19 data analysis.
[135]	a limited dataset with various indicators, such as COVID-19 fatality rates, number of hospital beds, emergency investment in healthcare, etc.
[136]	A set of 100 computed tomography scans from 40 COVID-19 patients.
[137]	20 audio samples of coughs with 10 of them coming from COVID-19-positive patients.
[138]	Images with chest scans and clinical data from COVID-19-positive patients, collected by University of Arkansas for Medical Sciences.
[139]	A dataset with location information extracted from tweets related to the COVID-19 pandemic.

5. Decentralization Concept

5.1. Decentralized versus Centralized Architectures

There are multiple opinions on the distributed and decentralized architectures regarding their tendency to be more privacy-preserving than centralized architectures. The main difference between a decentralized and a centralized architecture is the amount of information stored on a cloud server and the place of the decision-making process. Centralized solutions tend to store a lot/all information on one cloud server. In contrast, decentralized architectures store pieces of information at each node, and only a minimal and necessary amount of information is kept at each node. Moreover, the decision-making process (e.g., computing the likelihood of being infected) is done at the server side in centralized architectures and on user devices in a decentralized architecture. In addition, there is also a difference in the data ownership between the centralized and decentralized architectures (the data remain the property of the user in decentralized approaches versus data are transferred with partial or full usage rights to the server in centralized approaches). The centralized application's efficiency is the primary benefit of using a centralized approach, especially when the centralized server is a trusted entity. Efficiency refers to the fact that data can be collected from all users using a certain contact-tracing app. Governments and health provider units can access such data for an efficient health monitoring of people in a certain area using that particular app. In a centralized scenario, the possible breaches in one's data's security and privacy can be seen as a drawback if an attacker could get access to the cloud server or if the cloud server is an untrustable entity. For the aim of updating applications with centralized architectures and storing the information privately and securely, the concept of differential privacy was introduced and deployed in some cases [140,141].

Figure 4 illustrates the comparison of a centralized and decentralized architecture for a contact-tracing application.

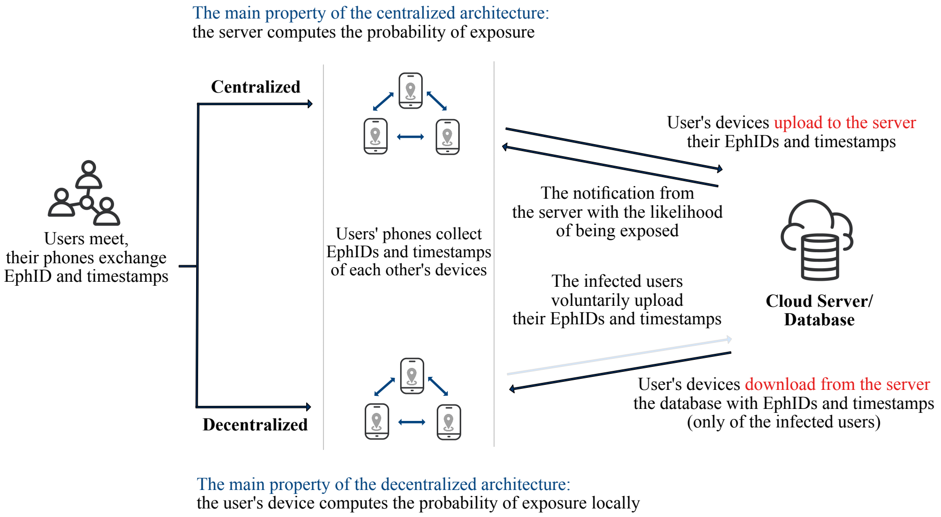
The main property of the centralized architecture:
the server computes the probability of exposure
Centralized
Users meet,
their phones exchange
EphID and timestamps
Users' phones collect
EphIDs and timestamps
of each other's devices
User's devices upload to the server
their EphIDs and timestamps
The notification from
the server with the likelihood
of being exposed
The infected users
voluntarily upload
their EphIDs and timestamps
Cloud Server/
Database
User's devices download from the server
the database with EphIDs and timestamps
(only of the infected users)
Decentralized
The main property of the decentralized architecture:
the user's device computes the probability of exposure locally

Figure 4. Centralized versus decentralized architectures in contact-tracing apps.

Clearly, the inputs in both architectures are typically the same: there is an algorithm in the considered app that is able to compute the distance between two users, using some available wireless signal, such as BLE or Wi-Fi (see also Figure 3) and some available measurements, such as RSS or RTT (see also Table 6). If the estimated distance is below a certain threshold (e.g., 2 m), the users' device exchange some Ephemeral ID (EphID) and timestamps between them for the duration over which the devices are at a close distance to each other. Exceptions to such app inputs occur when distance estimates occur at the server-side (in centralized approaches), in which case additional information (such as RSS, GPS, or magnetic field intensity measurements) is sent to the server together with the EphID and timestamps. After this distance-based exchange of EphID and timestamps between users, the centralized and decentralized approaches start to differ. In a centralized case, all users regularly upload the data (e.g., EphID and timestamps, and possibly additional measurements) to a cloud server. Infected users voluntarily inform the server that they have become infected (by using, for example, an authorization from a health service provider to avoid fake reports). The server is the unit that computes the likelihood of getting infected and sends an exposure notification to each user deemed highly likely to have been infected. In a decentralized approach, only infected users voluntarily upload their information (i.e., own EphID and timestamps stored over the past 14 days or so) to the server and the server broadcast the following information to all other users equipped with the corresponding app on their mobile devices. Own mobile device computes the likelihood to become infected and creates an exposure notification for the user. Sometimes these exposure notifications are also sent to the cloud server to collect statistics, for example.

Edge computing [93], as a concept, provides local computation and aggregation, and therefore such a paradigm is used to minimize response time and save the bandwidth.

One of the principal challenges related to digital contact tracing is related to the privacy of information that is collected from each user. The report consolidated and stored, and the choice application architecture (centralized or decentralized) delimit data privacy. Furthermore, some studies of the digital contact-tracing domain analyzed that the anonymity and security requirements of personal data cannot be confirmed, despite the solutions built and managed by authorized institutions, and that specific user profiles can be traced backward in rare cases [38,40].

As another factor related to the privacy concerns, there is the subject of surveillance: a noteworthy amount of personal data in a centralized governmental database could introduce a dangerous example on the way authorities are capable of 'spying' on individual behavior. Therefore, the central matter relates to some inclination of temporary measures, supported by an emergency, to be normalized and enlarged indefinitely.

The following example illustrates several consequences of implementing a centralized model for contract tracing. People's health records are private matters and having them publicly available can have many negative consequences. These may include a business owner losing customers, being denied service, or being socially ostracized, leading to emotional or physical harm. This has recently occurred in some cases in South Korea, which made its contact-tracing information available publicly. Local health authorities published anonymized location data of those infected with COVID-19, so that anyone could see if they have been to those areas at those given times and risked being infected as well. The agencies claimed they would only publish those areas where it was known that the infected person was not wearing a mask or came into close contact with others. In [142], the privacy of the data of 970 confirmed COVID-19 patients was analyzed, and the authors found that 70% of the time it was possible to deduce where the person worked or lived. Moreover, in 48% of the cases, social relationships with others were also identified. A BBC report [143] stated that many patients were verbally abused online by strangers which caused states of sleep deprivation and depression. It goes on to say that the stigma of contracting the virus is potentially very dangerous as people might be afraid to get tested, which can lead to more spreading.

5.2. Centralized versus Decentralized Protocols

Figure 5 illustrates the idea of a centralized protocol for a contact-tracing application. The app notifies users of a possible meeting with a contagious patient through a common Cloud Server/Database that aggregates all the information within the particular software ecosystem. This approach compromises privacy, yet has the benefit of human-in-the-loop inspections and health authority verification. Meanwhile, the back-end server processes pseudonymous personal data and enables the possibility of being re-identified. When a user has been confirmed positive for infection, the patient is invited to upload their history of contact logs to the central reporting server. With the users' consent, the health authority issues a key authorizing the upload. Thus, in this scenario, all users in contact with the patient receive notifications about the possibility of being exposed to the virus and get the instructions regarding their further actions.

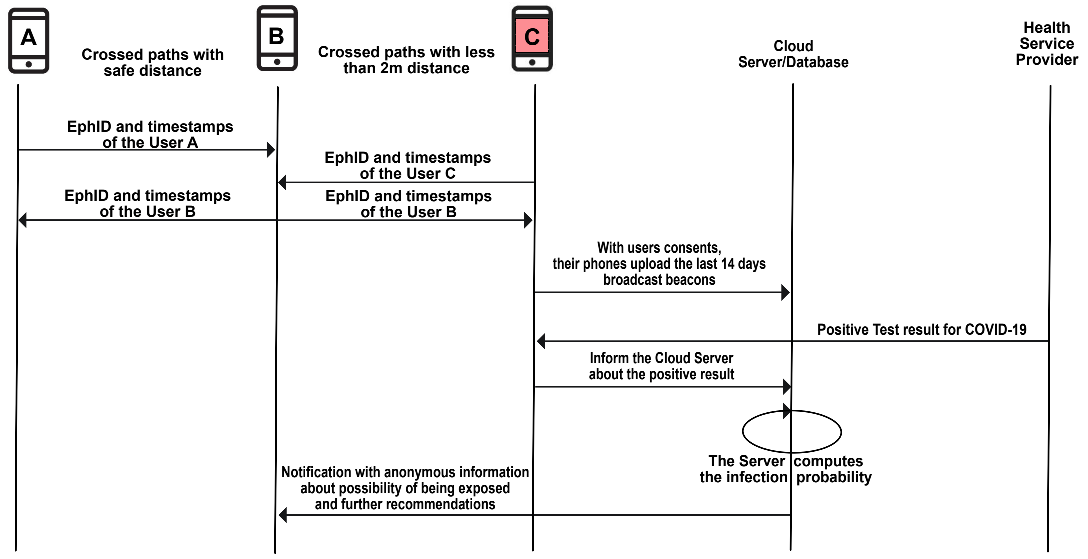
A
Crossed paths with safe distance
B
Crossed paths with less than 2m distance
C
Cloud Server/Database
Health Service Provider
EphID and timestamps of the User A
EphID and timestamps of the User C
EphID and timestamps of the User B
EphID and timestamps of the User B
With users consents, their phones upload the last 14 days broadcast beacons
Positive Test result for COVID-19
Inform the Cloud Server about the positive result
The Server computes the infection probability
Notification with anonymous information about possibility of being exposed and further recommendations

Figure 5. Centralized Protocol Scheme.

Table 9 lists the main centralized protocols for digital solutions to cope with COVID-19, their main strengths, and their challenges towards a mass adoption in the authors' view.

BlueTrace [144] is a Privacy-Preserving Cross-Border Contact-Tracing application available as open source on GitHub and developed by a Government Technology Agency in Singapore.

EPIC [102] protocol relies on BLE or Wi-Fi RSS measurements stored via encrypted form on a centralized server. EPIC is still in research phase and it is yet to be implemented and deployed to the best of the authors' knowledge.

PEPP-PT is a centralized privacy-preserving protocol developed by a multinational and multidisciplinary team from European countries, with the goal to be available as open source (on GitHub there is currently only its documentation available, as well as some samples for Android devices. As in EPIC, privacy is ensured through temporary user IDs and server encryption.

TraceSecure [145] is an extension of TraceTogether application with an additional cryptographic encryption at the server side for better privacy preservation. Two privacy-preserving protocols are proposed in [145]. Due to the additional cryptographic stage, a huge storage space (i.e., 230 GB) is required at the server side; also delays are of the order of several seconds. The TraceSecure protocol is still in the research phase and it has yet to be implemented.

TraceTogether [146] is another centralized app developed by the Singapore Government, in which nearby devices exchange BLE-based tokens and these tokens are continuously sent to a central server. Thus, the server has full information about users IDs and their contacts and the privacy preservation is weak.

Table 9. A list of main **centralized** protocols in contact tracing, proximity detection, and user tracking (as of September 2020).

Protocol Name	Strengths	Challenges
BlueTrace [144]	Open source; it does not collect location data; users mobile phones are collected only temporarily; it relies on temporary user IDs for users registrations and proximity detection.	It has some limitations on iOS devices; it is sensitive to replay/relay attacks.
EPIC [102]	It aims at a high level of privacy with a centralized approach.	In research phase; not yet implemented for real-field testing.
PEPP-PT [147]	Joint effort of several teams in Europe; meant to be available as open source for Android and iOS devices; user location data not collected.	Moderate robustness to privacy and security attacks.
TraceSecure [145]	More secure than TraceTogether.	In research phase; not yet implemented for real-field testing; high overheads at server side.
TraceTogether [146]	Minimal infrastructure needed as it relies on BLE RSS data.	Low privacy preservation.

Figure 6 illustrates the idea of a decentralized protocol for a contact-tracing application. For safety reasons, decentralized protocols function based on the EphID concept, semi-random rotating series that uniquely identify users. In a situation where two users cross their paths at a distance below a predefined threshold, they exchange EphIDs and store them locally on their devices. Typically, distance estimates are done based on BLE RSS measurements as most smartphones and wearables nowadays are equipped with BLE chipsets. Good BLE-based positioning studies, accompanied by open access datasets, can be found for example in [119,124]. The BLE signal must be continuously on, and sometimes this puts a significant extra burden on the life duration of the device battery. Methods to enhance energy efficiency are described in Section 7. Afterward, once a user tests positive for infection, a report is sent voluntarily to a central server (e.g., a cloud server). Each user device within the software ecosystem downloads regularly (e.g., once a day) the reports from the server, and the device individually checks their local contact logs for a match with the (EphID, timestamps) pairs contained in the downloaded report. If a matching (EphID, timestamp) pair is found, the user has come in close contact with an infected patient. A likelihood of becoming infected can be computed based on the duration of contact with some infectious person. Contact logs are never transmitted to third parties, and the central reporting server cannot by itself ascertain the identity or contact log of any user in the software ecosystem.

Table 10. List of main **decentralized** or **federated** protocols in contact tracing, proximity detection, and user tracking (as of September 2020).

Protocol Name	Strengths	Challenges
DP-3T [103]	Ensures a sufficient level of user privacy; open source; the protocol has proved a good accuracy in several field tests; works with both Android and iOS devices.	Relies on voluntary actions from infected users (to upload own EphIDs to a cloud server) and on available long-range and short-range connectivity.
GAEN [104]	Already deployed in some countries; relies on existing infrastructure; no additional costs to the users with smart devices; suitable for both iOS and Android devices.	It has proprietary software; battery consumption may be an issue; privacy level highly relate to the Apple and Google technical platforms and their vulnerabilities.
ROBERT and DESIRE [148]	Open-source protocols; low-power and it relies on BLE widely spread infrastructure.	Advantages over GAEN and DP-3T (if any) are unclear; relies on setting new legal structures for inter-governemts collaboration.
SafePaths and PACT [91]	Open-source contact-tracing app and protocol with privacy by design; it relies on random user IDs, as GAEN and DP-3T; works on both iOS and Android.	Advantages over GAEN and DP-3T are unclear; authors say it is identical to Covid-Watch app and very close to DP-3T.
Covid-Watch [149]	It does not collect user location data; relies on low-power BLE technology available on most iOS and Android devices.	Same challenges as SafePaths/PACT.
TCN [150]	Open-source contact-tracing app working on iOS and Android; relies on BLE and temporary and random user IDs, as DP-3T.	Advantages over GAEN and DP-3T are unclear; the main difference is that the participation of a health authority in the protocol chain is optional; this opens the paths to possibly fake reports from users in the fully crowdsourced mode.
OpenCovidTrace [151]	Open source; aims at integrating several existing protocols such as GAEN, DP-3T, BlueTrace, among others.	Location of users is also stored in encrypted form, thus it is less private than other decentralized approaches which do not store the user location.
Whisper Tracing [152]	This protocol uses 'interaction IDs' based on secured/hash exchanges between users in proximity to each other; interaction IDs are seen as more private than temporary IDs used in DP-3T and GAEN; it can work both in centralized and decentralized modes; no health authority is needed in the protocol chain to certify the users.	Still in research phase; might introduce long delays due to a long hash security key needed by the protocol; fake reports possible as no certification stage exists.

Table 10 lists the main decentralized or federated protocols for digital solutions to cope with COVID-19, their main strengths, and their challenges towards mass adoption, in the authors' view.

One of the most popular decentralized protocols on social media nowadays is the open source DP-3T [103], the protocol also known to stay as the basis on GAEN protocol [104]. One of the main characteristics of DP-3T and GAEN protocols is the fact the true user identities are never disclosed in clear; instead, the EphIDs are broadcast, and the EphIDs are changing randomly after a pre-defined interval (e.g., 15 min). The EphIDs are created according to some hash keys known only by the user device who has that EphID; the hash keys are stored temporarily (e.g., for 14 days) on the mobile user device. Distances between any two users are estimated based on RSS measurements. If another user is detected at less than 2 m distance, the mobile app stores his/her EphIDs together with the timestamps. A cloud server is only needed to upload information about an infected user and to broadcast information about all infected users who voluntarily uploaded their sequences of EphIDs and timestamps during the infectiousness period (recall Figure 6). Another decentralized protocol is ROBERT [38], which relies on so-called federated architectures (another name for decentralized ones) and also uses temporary user identities. Yet other decentralized protocols have been proposed by an PACT team under the name of SafePaths or PACT protocol, or by an alliance of researchers under the bane COVID-watch [149]. Few more decentralized protocols and their advantages are challenges are given in Table 10, with the main note that multiple are conceptually close to DP-3T and GAEN protocols.

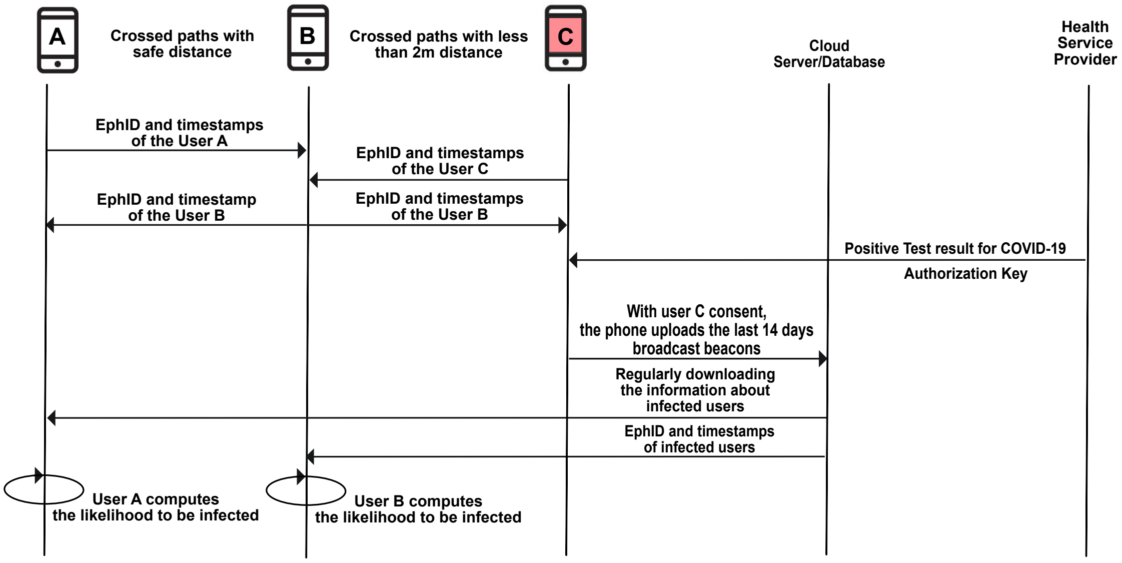
A
Crossed paths with safe distance
B
Crossed paths with less than 2m distance
C
Cloud Server/Database
Health Service Provider
EphID and timestamps of the User A
EphID and timestamps of the User C
EphID and timestamp of the User B
EphID and timestamps of the User B
Positive Test result for COVID-19
Authorization Key
With user C consent, the phone uploads the last 14 days broadcast beacons
Regularly downloading the information about infected users
EphID and timestamps of infected users
User A computes the likelihood to be infected
User B computes the likelihood to be infected

Figure 6. Decentralized Protocol Scheme.

5.3. Users' Perception of the Usefulness of Decentralized Architectures

According to the online study designed by the Authors[2], with 190 completed responses (a detailed demographic description of the survey is presented in Table 11): 37.4% female, 57.4% male, 0.5% other, and 4.7% of those preferred do not disclose their gender. There is a shred of evidence that a user's perception of centralized and decentralized architectures differs slightly. A part of our online survey's scope has been dedicated to highlight the perceived awareness among users about centralized and decentralized approaches and their relationship with data privacy. Our findings are shown in Figure 7. The question whose answers are summarized in Figure 7 aimed to understand the user's attitude to the contact-tracing apps using centralized and decentralized architecture and to summarize which one of the two approaches, from the respondent's point of view, preserves better the location information privacy. The responses are divided into five categories, where 1 stands for "not at all" and refers to privacy protection, and 5 stands for "very well". The numbers on the figure represent the number of total votes per category, where blue bars stand for centralized architecture, and the light blue color corresponds with a decentralized architecture. The dashed blue and orange curves correspond to the interpolated trends among the answers, for centralized and decentralized architectures, respectively. Respondents with various occupations provided their opinion on the subject, such as experts from the computer and electronics manufacturing, information technology, science, technology, engineering, and mathematics, and telecommunications domain.

[2] See "Location Privacy Survey", https://sites.tuni.fi/survey-of-digital-solutions/location-privacy-survey/.

Table 11. Demographic characteristics of the respondents of the survey.

Demographic Characteristics	Number	Percentage
Gender		
Male	109	57.4%
Female	71	37.4%
Other	1	0.5%
Prefer not to disclose	9	4.7%
Age		
18–20	2	1.1%
21–29	69	36.3%
30–39	49	25.8%
40–59	49	25.8%
60–69	7	3.7%
70 or more	7	3.7%
Prefer not to disclose	7	3.7%
The living area		
Village	10	5.3%
Town	40	21.1%
City	137	72.1%
Prefer not to disclose	3	1.6%

It is clear from Figure 7 that our findings go hand in hand with the accepted assumption that decentralized architectures are perceived as more private than the centralized architectures. Nevertheless, a non-negligible percentage of respondents, namely, 35%, also consider that decentralized architectures offer zero or very little privacy protection, as well as close to 16% of the respondents, consider that centralized solutions are also able to protect well or very well the user's location privacy.

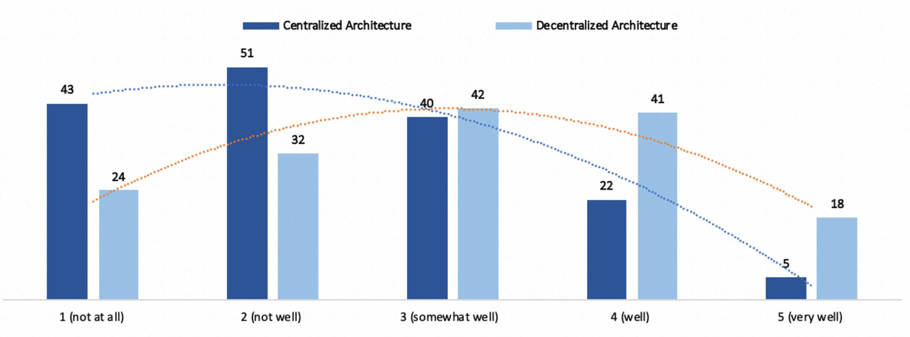

Figure 7. Question asked: "In your opinion, how well do centralized and decentralized location tracing approaches protect the privacy of your location data?" Answers summarized via bar plots above.

6. Privacy-Preservation Aspects in Contact Tracing and User Tracking

A comprehensive survey on location privacy in Wireless Sensor Networks (WSN) can be found in [153], where the focus was on centralized approaches, where the privacy of the so-called source nodes (i.e., moving nodes or users) must be protected. Most of the privacy-preserving solutions described in there rely on a trustable server's existence and therefore are not highly relevant in the context of decentralized architectures.

In [154], the authors introduced a private set of protocols for contact tracing, and they talked about security and possible ways of mitigation of the most common attacks, such as integrity threats, inferential attacks, replay and reliability attacks, and also physical attacks.

In some approaches, privacy is preserved by introducing extra measures, such as enhancing anonymity by mixing users' tokens [146].

Decentralization, however, does not fully solve the issue of user privacy preservation robustly. In addition to decentralization, improved user privacy can be typically implemented at the protocol layer in the wireless transmission chain; also, some physical-layer-based location privacy solutions can be found in the literature. The list below summarizes some of the main privacy-enhancing methods which can be used in decentralized architectures:

- *Physical layer approaches*: physical layer approaches for increased location privacy typically rely on some form of obfuscation, i.e., concealment, of user-based measurements, e.g., by increasing the estimation error in the RSS reported measurements [155]. Nevertheless, such approaches are also likely to decrease the accuracy in detecting whether two users are in close vicinity of each other and may generate many false alarms or misdetections;
- *Enhanced security keys* for the generation of the temporary of ephemeral IDs; for example, attribute-based encryption based on multi-authorities/decentralization was proposed in [156], and homomorphic Paillier encryption with selective aggregation was proposed in [157]; the typical downside of such approaches is the long delay introduced during the generation of the encryption keys;
- *Use of decentralized identifiers* [158] are among the modern approaches for authentication of digital data; such approaches have not yet been investigated in the context of proximity detection, user location, or contact tracing;
- *Blockchain* concept: Blockchain is a type of Distributed Ledger Technology (DLT) where all transactions are recorded with a changeless cryptographic signature called a hash. In this case, any changes in the block are becoming apparent to the participant. To "lie" within a blockchain system, every block in the chain across all of the chain's distributed versions should be altered. As a system, Blockchain works as a stable ledger that allows performing transactions in a decentralized mode, which is known to be a privacy-preserving solution. Blockchain-based applications spring up, covering various fields, including financial services, healthcare domain, and IoT, among others. Despite its popularity, there is still room for improvement in the blockchain technology, such security obstacles remaining to be overcome [159].
- *Differential Privacy* concept: Differential privacy [141] has been implemented in centralized Location-Based Service providers' databases by adjusting partition structures of the current dataset on the spatial structure of the previous moment and adding Laplace noise. It proved to be a privacy-enhancing solution compared to obfuscated locations exclusively submitted by the users. As with background knowledge of a user's obscured locations, and an attacker could still presume actual locations by carrying out long-term observation attacks. Moreover, as stated in [140], merging the differential privacy concept with other privacy-preserving solutions such as Blockchain proved to be a working scheme in the users' location domain.
- *Audits and aggregation of data*: Auditing who accesses and publishes the patient data is mentioned in [160]. In [161] one proposed method is using aggregate location data. However, knowing how many people are traveling from hotspots to nearby towns and villages would still reveal the virus's possible spreading without personal data.

In contract-tracing apps, additional measures could be implemented to safeguard future patients from privacy leaks. Auditing who accesses and publishes the patient data is mentioned in [160]. In [161] one proposed method is using aggregate location data. Knowing how many people are traveling from hotspots to nearby towns and villages would still reveal possible spreading of the virus without personal data. Differential privacy could allow a way to maintain a database of patients without revealing their identity. Local differential privacy for private indoor localization methods have been studied by [162], although it uses a central data aggregation server. Decentralized differential privacy has been studied for optimizing deep learning strategies in [163].

7. Energy-Efficiency Aspects

Energy consumption on a wireless device depends on several parameters such as protocol settings, number, frequency, and duration of packets exchanged with nearby devices, sleep mode duration and duty cycle, transmit powers, number of frequency channel in use, etc. Various models for energy consumption in Device-to-Device (D2D) communications can be found, for example, in [164,165].

The usefulness of a contact-tracing app is proportional to the likelihood that the mobile device or wearable running the app remains on for at least 12 successive hours, and preferably for days in a row, meaning that the application should consume very little power of the device battery. In other words energy efficiency of a COVID-19 contact-tracing mobile app is very important for an app to become useful.

Energy savings can be implemented at various stages in the wireless transmission chain:

- *Improved signal processing at the transmitter* side, for example, by the optimized power amplifier to obtain high efficiency at low transmit power levels [166];
- *Improved signal processing at the receiver side*—the authors of [31] used, for example, dynamic modeling via Markov chains for more efficient integration of sensors readings for positioning;
- *Improved communications and/or localization protocols* for example by optimized routing of the events or packets [167];
- *Ultra low-power communication technologies*: low-power technologies, such as BLE, ZigBee, LoRa, etc., are essential for a lasting battery life, but decreasing even more the power consumption is a topic of active research under the umbrella of "ultra low-power" technologies such as wireless-powered networks with back-scattered communications [168], tunable impulse radio UWB technologies [169], or wearable technologies relying on sensors which use the electrostatic induction current generated by human motion [170];
- *Data compression* methods for transmitting a lower amount of data by removing redundancies in data to be transmitted - while such methods have been vastly studied in the context of wireless communications, e.g., in [171] or via compressed sensing in [85], their applicability to user tracking and contact tracing is still to be determined;
- *Approximate computing* methods rely on trading accuracy for a lower power consumption [172], for example, by reducing the number of quantization bits of by approximating some tasks in the execution flow;
- *Task offloading* methods [173] rely on delegating/moving some of the more computationally demanding tasks to an edge or cloud server; such methods typically demand the presence of a centralized unit/server and therefore are not well suited to decentralized approaches. In addition, task offloading increases the wireless transmission delays and may hinder a real-time contact-tracing app's viability.
- *Energy harvesting* [174,175] from surroundings such as ambient back-scattering communications [176] rely on collecting additional energy from the surrounding environment, such as due to reflections, interferences, and body movements, and transforming it into useful energy for the desired purpose. These kinds of methods have not yet been studied in the context of contact tracing or user tracking to the best of the authors' knowledge.

8. Challenges to Overcome towards Mass Adoption of Contact-Tracing Applications

This section summarizes potential challenges and limitations towards the mass adoption of contact-tracing and/or user-tracking applications to fight infectious diseases. The following three domains and their associated challenges are discussed in details in the following three subsections.

- *Technical domain*—refers to challenges and errors caused by the wireless propagation of signals, as well as errors caused by the transmitter and/or receiver devices, such as device calibration errors or errors due to shadowing effects;

- *Medical domain*—refers to challenges and errors in evaluating the probability of getting infected due to variability of the human factor/immune system, the variability of the impact of the contact duration on the outcomes, as well as other medical factors related to human metabolism and genes.
- *Ethical domain*—refers to challenges in adopting or imposing a new mobile application due to ethical constraints such as the GDPR regulations in Europe. For example, as emphasized above, decentralized semi-automated applications cannot serve as a standalone solution to respond to virus exposure, as human actions are further needed (from governments, healthcare personnel, citizens, etc.) for efficient and robust solutions. However, a decentralized approach promises to benefit best in synchronization with preventive measures, a well developed public healthcare system, and thorough compliance with the government recommendations.

8.1. Technical Domain

As seen in previous sections, most contact-tracing applications rely on measuring the received signal strengths or received power on a user device. However, due to the heterogeneity of user devices, the reported RSS measurements vary according to the manufacturer and chipsets, as well as according to the body orientation and movements and number of surrounding people. This means that *calibration* step is a mandatory step towards achieving reliable results, and untreated calibration errors can trigger significant errors in the distance estimation process. Good examples of calibration methods can be found in [100,177]. Typically, calibration requires offline static measurements and some training databases created based on measurements from various devices in order to give the best results.

Another source of errors in RSS-based user tracking and contact tracing is the variability of the wireless channel, due to shadowing, multipath, and fading phenomena. Such variability translates into random fluctuations of the RSS, typically modeled in dB scale as a Gaussian random variable, as given previously in Equation (1).

8.2. Medical Domain

The impact of human immune system on COVID-19 severity has been widely studied so far, for example in [178–183], etc. Epidemiological models have been, for example, studied recently in [183]. They were grouped into two main categories: forecasting models, based on statistics and extrapolation models, and mechanistic models, trying to mimic how the COVID-19 spreads under various assumed parameters, such as population density, season and climate specifics, a number of current infections, etc.

In addition to the human immune system, the parameters of proximity to other devices and the contact duration depend on several environmental factors. The airflow dynamics are different in indoor and outdoor positions, as well as their temperature, humidity, and ozone levels [184]. These airflow dynamics will all affect how particles that contain the coronavirus and that are suspended in the air will spread to those in the vicinity. It may be the case that the airborne virus is blown away by the wind, away from other people close by, or in the opposite case, possible spread to everyone passing under a ventilation vent. In the case where a contact-tracing app has the ability to accurately detect all people that have been within, for example, 2 m of one virus carrier for any duration of time, it will cause many people to self-isolate for two weeks, while the number of actual transmissions would be much lower. Research is still being done on other important factors, such as the effectiveness of wearing a mask, the survival rate of the virus on different surface levels, and asymptotic carrier transmission [185].

8.3. Ethical Domain

There are multiple opinions on whether contact tracing is just an app or a solution to reopening the society and borders; however, most of the experts agree on the need for large efforts in the app adoption and on the benefits provided in particular circumstances [186]. In addition, there is a valid worry of risks related to long-term measures adoption not justified by enough evidence data [187], as well as the concern about temporal measures that might be unduly prolonged and invasive to users' privacy. Contact-tracing applications are typically useful in moderately close organizations with high adoption rates (e.g., universities, companies, and plants). For the public health purpose, the reasonable adoption rate is estimated as 60% [7]; however, this percentage must be taken with a grain of salt, as the success of an application also depends on many other factors, such as personal immunity to germs or spatial degree of pollution, and a high adoption rate alone cannot guarantee the success of an application in terms of disease prevention. The researchers in [8], highlighted the statement that all of the applications, as mentioned earlier, work only in conjunction with meticulous testing for COVID-19 and with following the strict order of a 14 days isolation.

In May 2020, WHO published an interim report with guidelines on the use of digital proximity-detection and user-tracking technologies for COVID-19 [92] in which they emphasized the need to protect the fundamental human rights and liberties and to create policies and mechanisms which place strict limits on the population surveillance. It has also been pointed out in [92] that the effectiveness of digital contact-tracing applications is still to be proved, and the recommendations were that all pertinent stakeholders, such as governments, healthcare institutions, non-state actors, and companies developing contact-tracing apps should collaborate and adhere to common ethical principles. Seventeen target principles were identified, with privacy preservation and security being among them. Decentralized approaches were mentioned as the ones more likely to ensure the privacy preservation of user data and allow users to exercise greater control over their data (such as the right of withdrawal and the exercise of the consent).

Ethical guidelines for COVID-19 contract-tracing apps have also been addressed in [188], with particular focus on privacy preservation, accessibility to all, effectiveness, and its time limitation (i.e., not using it beyond its primary purpose and having a predefined expiration date). Open source solutions were found to be more attractive from an ethical point of view than proprietary solutions. Decentralized approaches were also emphasized as ensuring better privacy protection than centralized approaches.

In [189], the authors also discussed the ethical implications of using COVID-19 digital contact-tracing apps. While no solution was provided, several questions were raised regarding the trade-offs between the possible benefits and harms of a digital contact-tracing application, and the paper concluded with the need of essential stakeholders to act wisely and consider all ethical implications before deploying a mass-market solution.

Moreover, in some countries, the ethical issue of free access to the applications installed on personal devices may occur, as high costs of the mobile devices supporting such an app may be prohibitive and may hinder the broad adoption of an app. The phones and wearable devices are suggested to be given to citizens for free to access digital solutions for everyone.

9. Conclusions and Way Ahead

This paper has provided a comprehensive overview of methods, solutions, and applications for user tracking, proximity detection, and contact tracing, with a particular focus on digital and wireless solutions, to assist in mitigation and prevention of the COVID-19 threat. The research on user tracking and proximity detection has been actively ongoing for more than one decade. Many automated or semi-automated digital contact-tracing solutions have been derived from classical approaches of distance estimation based on received signal strength, using, for example, BLE signals, as BLE chipsets are nowadays embedded in the majority of mobile devices. The challenges and possible impediments towards the mass adoption of digital contact-tracing solutions were also emphasized, with a particular focus on ethical and privacy constraints. Energy consumption issues were also briefly addressed. In addition, we also summarized existing protocols, architectures, and open access datasets related to digital contact-tracing apps. We concluded that applications involving centralized servers are more prone to privacy breaks than the fully decentralized applications. Still, the effectiveness of a fully decentralized app may be lower than in the case of a centralized app, as decentralized apps require more involvement from the users' side, such as active and timely reporting of a confirmed infection. The opinion regarding the increased privacy of decentralized apps compared to the centralized ones was also validated by the acquired insights of an online survey study conducted by the Authors.

Our paper also contains a discussion of the trade-offs and potential benefits of digital contact-tracing applications in preventing the spread of viruses and bacteria that carry infectious diseases. As an outcome, we highlight the fact that also the energy efficiency is more and more relevant in the context of digital solutions on wearables and other handheld devices. Our study has also shown that this is a research area of timely relevance and that technological solutions with mobile devices for user location tracking, proximity detection, and contact tracing continue to appear at a fast pace. As stated in [187], there are lessons learned, and comparisons of the COVID-19 pandemic with the 1918 influenza pandemic, but generalizations are also dangerous, and evidence-based data must be used as inputs for any decisions. As reminded by the authors in [190], the second wave of the pandemic, i.e., a sharp increase of incidence, rising again after reducing the virus's spread, appeared during the previous influenza pandemic of 1918, and preventive measures such as social distancing proved its effectiveness ans necessity. The history has a scenario where the authorities of multiple countries have reduced or prematurely suspended the social distancing measures after a significant decline in the number of new infections during the first wave. Moreover, the continuation of the survey in [190] provides a summary on the emerging technologies in assisting with a successful implementation of social distancing and highlights relevant challenges to be considered. As a supplement to the advanced wireless technologies with enabled high accuracy positioning, emerging solutions as AI, computer vision, ultrasound, VLC, and thermal imaging among others, have a promising augmentation to achieving and optimizing social distancing patterns.

In the near future, the estimated effect of digital contact-tracing apps could be calculated in the countries with the highest app adoption rate, which would allow the researchers to select the best approach for worldwide implementation. Additionally, with the advent of 5G- and beyond-5G-positioning research, more technologies in the field of wireless positioning are likely to be adopted for the purpose of contact tracing and appear on the market. Last but not least, the long-term implications of the wide-scale adoption of contact-tracing applications must also be considered, and ethical aspects must be carefully observed and addressed.

Author Contributions: Conceptualization, methodology, and software, V.S. and S.H.; writing—original draft preparation, V.S., S.H., and E.S.L.; writing—review and editing, supervision, and funding acquisition, E.S.L. and M.G. All authors have read and agreed to the published version of the manuscript.

Funding: The authors gratefully acknowledge funding from European Union's Horizon 2020 Research and Innovation programme under the Marie Skłodowska Curie grant agreement No. 813278 (A-WEAR: A network for dynamic wearable applications with privacy constraints, http://www.a-wear.eu/).

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

List of Acronyms

4G	Fourth-generation cellular systems
5G	Fifth-generation cellular systems
AI	Artificial Intelligence
AOA	Angle of Arrival
AOD	Angle of Departure
AR	Augmented Reality
BLE	Bluetooth Low Energy
COVID-19	Coronavirus infectious disease 2019
D2D	Device-to-Device
DOA	Direction of Arrival
DLT	Distributed Ledger Technology
DP-PPT	Decentralized Privacy-Preserving Proximity Tracing
DP-3T	Decentralized Privacy-Preserving Proximity Tracing (another abbreviation for DP-PPT)
EPIC	Efficient Privacy-Preserving Contact Tracing
EphID	Ephemeral ID
EU	European Union

FDOA	Frequency Difference of Arrival
FP	FingerPrinting
GAEN	Google/Apple Exposure Notification
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IMU	Inertial Measurement Unit
IR	Infrared
IoT	Internet of Things
kNN	k-Nearest Neighbours
LBSs	Location-Based Services
LoRa	Long Range Internet of Things technology
Li-Fi	Light Fidelity
LoRa	Long Range access
LOS	Line-of-Sight
LTE	Long-Term Evolution (of cellular systems)
MIT	Massachussets Institute of Technology
ML	Machine Learning
NB-IoT	NarrowBand Internet of Things
PACT	Private Automated Contact Tracing
PEPP-PT	Privacy-Preserving Proximity Tracing
POA	Phase of Arrival
QR code	Quick Response code
RFID	Radio Frequency Identification
ROBERT	ROBust and privacy-presERving proximity Tracing
RSS	Received Signal Strength
RTT	Round Trip Time
SARS-COV-2	Severe acute respiratory syndrome coronavirus 2
SVM	Support Vector Machines
TCN	Temporary Contact Numbers
TDOA	Time Difference of Arrival
THz	Terahertz
TOA	Time of Arrival
UWB	Ultra Wide Band
VLC	Visible Light Communications
VR	Virtual Reality
Wi-Fi	Wireless Fidelity
WHO	World Health Organization
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Networks
XR	Mixed Reality

References

1. Asaf, G.; Davis, H.; McCorkell, L.; Wei, H.; O'Neill, B.; Akrami, A. What Does COVID-19 Recovery Actually Look Like? An Analysis of the Prolonged COVID-19 Symptoms Survey by Patient-Led Research Team. 2020. Available online: https://patientresearchcovid19.com (accessed on 17 September 2020).
2. Liu, Q.; Liu, W.; Sha, D.; Kumar, S.; Chang, E.; Arora, V.; Lan, H.; Li, Y.; Wang, Z.; Zhang, Y.; et al. An Environmental Data Collection for COVID-19 Pandemic Research. *Data* **2020**, *5*, 68. [CrossRef]
3. Rogan, P.K. Geostatistical Analysis of SARS-CoV-2 Positive Cases in the United States. 2020. Available online: https://doi.org/10.5281/zenodo.3986171 (accessed on 13 September 2020).
4. Sixto-Costoya, A.; Aleixandre-Benavent, R.; Lucas-Domínguez, R.; Vidal-Infer, A. The Emergency Medicine Facing the Challenge of Open Science. *Data* **2020**, *5*, 28. [CrossRef]
5. He, X.; Lau, E.; Wu, P.; Deng, X.; Wang, J.; Hao, X.; Lau, Y.C.; Wong, J.Y.; Guan, Y.; Tan, X.; et al. Temporal dynamics in viral shedding and transmissibility of COVID-19. *Nat. Med.* **2020**, *26*, 672–675; preprinted in: **2020**, *26*, 1491–1493. [CrossRef] [PubMed]
6. Scudellari, M. COVID-19 Digital Contact Tracing: Apple and Google Work Together as MIT Tests Validity. 2020. Available online: https://spectrum.ieee.org/the-human-os/biomedical/devices/covid19-digital-contact-tracing-apple-google-mit-tests-validity (accessed on 13 September 2020).
7. Kreps, S.; Zhang, B.; McMurry, N. Contact-Tracing Apps Face Serious Adoption Obstacles. Available online: https://www.brookings.edu/techstream/contact-tracing-apps-face-serious-adoption-obstacles/ (accessed on 17 September 2020).
8. Salathe, M.; Althaus, C.L.; Neher, R.; Stringhini, S.; Hodcroft, E.; Fellay, J.; Zwahlen, M.; Senti, G.; Battegay, M.; Wilder-Smith, A.; et al. COVID-19 epidemic in Switzerland: On the importance of testing, contact tracing and isolation. *Swiss Med. Wkly.* **2020**, *150*, w20225. [PubMed]

9. Block, P.; Hoffman, M.; Raabe, I.; Dowd, J.B.; Rahal, C.; Kashyap, R.; Mills, M.C. Social network-based distancing strategies to flatten the COVID-19 curve in a post-lockdown world. *Nat. Hum. Behav.* **2020**, *4*, 588–596. [CrossRef] [PubMed]
10. Raskar, R.; Schunemann, I.; Barbar, R.; Vilcans, K.; Gray, J.; Vepakomma, P.; Kapa, S.; Nuzzo, A.; Gupta, R.; Berke, A.; et al. Apps gone rogue: Maintaining personal privacy in an epidemic. *arXiv* **2020**, arXiv:2003.08567.
11. Bansal, P.; Panchal, R.; Bassi, S.; Kumar, A. Blockchain for Cybersecurity: A Comprehensive Survey. In Proceedings of the 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), Gwalior, India, 10–12 April 2020; pp. 260–265.
12. Huang, C.; Lu, R.; Ni, J.; Shen, X. DAPA: A Decentralized, Accountable, and Privacy-Preserving Architecture for Car Sharing Services. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4869–4882.
13. Nanni, M.; Andrienko, G.; Boldrini, C.; Bonchi, F.; Cattuto, C.; Chiaromonte, F.; Comandé, G.; Conti, M.; Coté, M.; Dignum, F.; et al. Give more data, awareness and control to individual citizens, and they will help COVID-19 containment. *arXiv* **2020**, arXiv:2004.05222.
14. Valdivia, L.J.; Del-Valle-Soto, C.; Rodriguez, J.; Alcaraz, M. Decentralization: The Failed Promise of Cryptocurrencies. *IT Prof.* **2019**, *21*, 33–40.
15. Henry, R.; Herzberg, A.; Kate, A. Blockchain Access Privacy: Challenges and Directions. *IEEE Secur. Priv.* **2018**, *16*, 38–45.
16. Paillisse, J.; Manrique, J.; Bonet, G.; Rodriguez-Natal, A.; Maino, F.; Cabellos, A. Decentralized Trust in the Inter-Domain Routing Infrastructure. *IEEE Access* **2019**, *7*, 166896–166905. [CrossRef]
17. D'Souza, M.; Ananthanarayana, V.S. Decentralized registry based architecture for location-based services. In Proceedings of the 2011 6th International Conference on Industrial and Information Systems, Kandy, Sri Lanka, 16–19 August 2011; pp. 136–139.
18. Xiao, C.; Chen, Z.; Wang, X.; Zhao, J.; Chen, C. DeCache: A decentralized two-level cache for mobile location privacy protection. In Proceedings of the 2014 Sixth International Conference on Ubiquitous and Future Networks (ICUFN), Shanghai, China, 8–11 July 2014; pp. 81–86.
19. Gupta, R.; Rao, U.P. Achieving location privacy through CAST in location based services. *J. Commun. Netw.* **2017**, *19*, 239–249.
20. Nature. Coronavirus Contact-Tracing Apps: Can They Slow the Spread of COVID-19? 2020. Available online: https://www.nature.com/articles/d41586-020-01514-2 (accessed on 13 September 2020).
21. Amoretti, M.; Brambilla, G.; Medioli, F.; Zanichelli, F. Blockchain-Based Proof of Location. In Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 16–20 July 2018; pp. 146–153.
22. Li, M.; Zhu, L.; Lin, X. Efficient and Privacy-Preserving Carpooling Using Blockchain-Assisted Vehicular Fog Computing. *IEEE Internet Things J.* **2019**, *6*, 4573–4584. [CrossRef]
23. Martinez, M.; Hekmati, A.; Krishnamachari, B.; Yun, S. Mobile Encounter-based Social Sybil Control. In Proceedings of the 2020 Seventh International Conference on Software Defined Systems (SDS), Paris, France, 20–23 April 2020; pp. 190–195.
24. Raji, A.; Jeyasheeli, P.G.; Jenitha, T. IoT based classification of vital signs data for chronic disease monitoring. In Proceedings of the 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 7–8 January 2016; pp. 1–5.
25. Yuan, X.; Zhang, J.; Wang, Y. Probability Theory-Based SNP Association Study Method for Identifying Susceptibility Loci and Genetic Disease Models in Human Case-Control Data. *IEEE Trans. Nanobiosci.* **2010**, *9*, 232–241. [CrossRef]
26. Lee, M.; Kim, J.W.; Jang, B. DOVE: An Infectious Disease Outbreak Statistics Visualization System. *IEEE Access* **2018**, *6*, 47206–47216. [CrossRef]
27. Kim, J.; Chung, K. Multi-Modal Stacked Denoising Autoencoder for Handling Missing Data in Healthcare Big Data. *IEEE Access* **2020**, *8*, 104933–104943. [CrossRef]
28. Rustam, F.; Reshi, A.A.; Mehmood, A.; Ullah, S.; On, B.; Aslam, W.; Choi, G.S. COVID-19 Future Forecasting Using Supervised Machine Learning Models. *IEEE Access* **2020**, *8*, 101489–101499. [CrossRef]
29. Li, J.; Guo, X. COVID-19 Contact-tracing Apps: A Survey on the Global Deployment and Challenges. *arXiv* **2020**, arXiv:2005.03599.
30. Bolic, M.; Rostamian, M.; Djuric, P.M. Proximity Detection with RFID: A Step Toward the Internet of Things. *IEEE Pervasive Comput.* **2015**, *14*, 70–76. [CrossRef]

31. Ye, H.; Yang, W.; Yao, Y.; Gu, T.; Huang, Z. BTrack: Using Barometer for Energy Efficient Location Tracking on Mountain Roads. *IEEE Access* **2018**, *6*, 66998–67009. [CrossRef]
32. Chen, J.; Li, K.; Zhang, Z.; Li, K.; Yu, P.S. A Survey on Applications of Artificial Intelligence in Fighting Against COVID-19. *arXiv* **2020**, arXiv:2007.02202.
33. Kaptchuk, G.; Hargittai, E.; Redmiles, E.M. How good is good enough for COVID19 apps? The influence of benefits, accuracy, and privacy on willingness to adopt. *arXiv* **2020**, arXiv:2005.04343.
34. Li, T.; Yang, J.; Faklaris, C.; King, J.; Agarwal, Y.; Dabbish, L.; Hong, J.I. Decentralized is not risk-free: Understanding public perceptions of privacy-utility trade-offs in COVID-19 contact-tracing apps. *arXiv* **2020**, arXiv:2005.11957.
35. Ahmed, N.; Michelin, R.A.; Xue, W.; Ruj, S.; Malaney, R.; Kanhere, S.S.; Seneviratne, A.; Hu, W.; Janicke, H.; Jha, S. A Survey of COVID-19 Contact Tracing Apps. *arXiv* **2020**, arXiv:2006.10306.
36. Martin, T.; Karopoulos, G.; Hernández-Ramos, J.L.; Kambourakis, G.; Fovino, I.N. Demystifying COVID-19 digital contact tracing: A survey on frameworks and mobile apps. *arXiv* **2020**, arXiv:2007.11687.
37. Nasajpour, M.; Pouriyeh, S.; Parizi, R.M.; Dorodchi, M.; Valero, M.; Arabnia, H.R. Internet of Things for Current COVID-19 and Future Pandemics: An Exploratory Study. *arXiv* **2020**, arXiv:2007.11147.
38. Sun, R.; Wang, W.; Xue, M.; Tyson, G.; Camtepe, S.; Ranasinghe, D. Vetting Security and Privacy of Global COVID-19 Contact Tracing Applications. *arXiv* **2020**, arXiv:2006.10933.
39. Hernández-Orallo, E.; Manzoni, P.; Calafate, C.T.; Cano, J. Evaluating How Smartphone Contact Tracing Technology Can Reduce the Spread of Infectious Diseases: The Case of COVID-19. *IEEE Access* **2020**, *8*, 99083–99097. [CrossRef]
40. Reichert, L.; Brack, S.; Scheuermann, B. A Survey of Automatic Contact Tracing Approaches. 2020. Available online: https://eprint.iacr.org/2020/672.pdf (accessed on 13 September 2020).
41. Braithwaite, I.; Callender, T.; Bullock, M.; Aldridge, R.W. Automated and partly automated contact tracing: A systematic review to inform the control of COVID-19. *Lancet Glob. Health* **2020**. [CrossRef]
42. del Peral-Rosado, J.A.; Raulefs, R.; López-Salcedo, J.A.; Seco-Granados, G. Survey of Cellular Mobile Radio Localization Methods: From 1G to 5G. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 1124–1148. [CrossRef]
43. Tabassum, H.; Salehi, M.; Hossain, E. Fundamentals of Mobility-Aware Performance Characterization of Cellular Networks: A Tutorial. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2288–2308. [CrossRef]
44. Gandotra, P.; Jha, R.K.; Jain, S. Green communication in next generation cellular networks: A survey. *IEEE Access* **2017**, *5*, 11727–11758. [CrossRef]
45. Wen, F.; Wymeersch, H.; Peng, B.; Tay, W.P.; So, H.C.; Yang, D. A survey on 5G massive MIMO localization. *Digit. Signal Process.* **2019**, *94*, 21–28. [CrossRef]
46. Huang, J.; Liang, J.; Luo, S. Method and Analysis of TOA-Based Localization in 5G Ultra-Dense Networks with Randomly Distributed Nodes. *IEEE Access* **2019**, *7*, 174986–175002. [CrossRef]
47. Fascista, A.; Coluccia, A.; Wymeersch, H.; Seco-Granados, G. Millimeter-Wave Downlink Positioning with a Single-Antenna Receiver. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 4479–4490. [CrossRef]
48. Ding, J.; Nemati, M.; Ranaweera, C.; Choi, J. IoT Connectivity Technologies and Applications: A Survey. *IEEE Access* **2020**, *8*, 67646–67673. [CrossRef]
49. Shah, S.W.H.; Mian, A.N.; Crowcroft, J. Statistical Qos Guarantees for Licensed-Unlicensed Spectrum Interoperable D2D Communication. *IEEE Access* **2020**, *8*, 27277–27290. [CrossRef]
50. Ojo, M.O.; Giordano, S.; Procissi, G.; Seitanidis, I.N. A Review of Low-End, Middle-End, and High-End Iot Devices. *IEEE Access* **2018**, *6*, 70528–70554. [CrossRef]
51. Centenaro, M.; Vangelista, L.; Zanella, A.; Zorzi, M. Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios. *IEEE Wirel. Commun.* **2016**, *23*, 60–67. [CrossRef]
52. Pal, A.; Kant, K. NFMI: Connectivity for Short-Range IoT Applications. *Computer* **2019**, *52*, 63–67. [CrossRef]
53. Haartsen, J.C.; Mattisson, S. Bluetooth-a new low-power radio interface providing short-range connectivity. *Proc. IEEE* **2000**, *88*, 1651–1661.
54. Roy, S.; Foerster, J.R.; Somayazulu, V.S.; Leeper, D.G. Ultrawideband radio design: The promise of high-speed, short-range wireless connectivity. *Proc. IEEE* **2004**, *92*, 295–311.
55. Silva, P.; Kaseva, V.; Lohan, E. Wireless Positioning in IoT: A Look at Current and Future Trends. *Sensors* **2018**, *18*, 2470. [CrossRef]
56. Tomic, S.; Beko, M.; Dinis, R. RSS-based localization in wireless sensor networks using convex relaxation: Noncooperative and cooperative schemes. *IEEE Trans. Veh. Technol.* **2014**, *64*, 2037–2050.

57. Sadowski, S.; Spachos, P. Rssi-based indoor localization with the internet of things. *IEEE Access* **2018**, *6*, 30149–30161. [CrossRef]
58. Lohan, E.S.; Talvitie, J.; Figueiredo e Silva, P.; Nurminen, H.; Ali-Löytty, S.; Piché, R. Received signal strength models for WLAN and BLE-based indoor positioning in multi-floor buildings. In Proceedings of the 2015 International Conference on Localization and GNSS (ICL-GNSS), Gothenburg, Sweden, 22–24 June 2015; pp. 1–6.
59. Conesa, J.; Perez-Navarro, A.; Sospedra, J.T.; Montoliu, R. *Geographical and Fingerprinting Data to Create Systems for Indoor Positioning and Indoor/Outdoor Navigation*; Elsevier: Amsterdam, The Netherlands, 2018.
60. Torres-Sospedra, J.; Richter, P.; Moreira, A.; Mendoza-Silva, G.; Lohan, E.; Trilles, S.; Matey-Sanz, M.; Huerta, J. A Comprehensive and Reproducible Comparison of Clustering and Optimization Rules in Wi-Fi Fingerprinting. *IEEE Trans. Mob. Comput.* **2020**. [CrossRef]
61. Wolf, F. Multi-Channel Ranging System for the Localization of Wireless Connected Objects in Low Power Wide Area Networks: From Modeling to Field Trials. Ph.D. Thesis, University of Limoges, Limoges, France, 2020.
62. Zafari, F.; Gkelias, A.; Leung, K.K. A Survey of Indoor Localization Systems and Technologies. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2568–2599.
63. Torres-Sospedra, J.; Richter, P.; Mendoza-Silva, G.; Lohan, E.S.; Huerta, J. Characterising the Alteration in the AP Distribution with the RSS Distance and the Position Estimates. In Proceedings of the 2018 International Conference on Indoor Positioning and Indoor Navigation (IPIN), Nantes, France, 24–27 September 2018; pp. 1–8.
64. del Corte, A.; Gutierrez, O.; Gómez, J.M. Fingerprinting location estimation and tracking in critical wireless environments based on accuracy ray-tracing algorithms. In *Distributed Computing and Artificial Intelligence*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 251–258.
65. Torres-Sospedra, J.; Quezada-Gaibor, D.; Mendoza-Silva, G.M.; Nurmi, J.; Koucheryavy, Y.; Huerta, J. New Cluster Selection and Fine-grained Search for k-Means Clustering and Wi-Fi Fingerprinting. In Proceedings of the 2020 International Conference on Localization and GNSS (ICL-GNSS), Tampere, Finland, 2–4 June 2020; pp. 1–6.
66. Zhu, S.; Ding, Z. Joint synchronization and localization using TOAs: A linearization based WLS solution. *IEEE J. Sel. Areas Commun.* **2010**, *28*, 1017–1025.
67. Hashem, O.; Youssef, M.; Harras, K.A. WiNar: RTT-based Sub-meter Indoor Localization using Commercial Devices. In Proceedings of the 2020 IEEE International Conference on Pervasive Computing and Communications (PerCom), Austin, TX, USA, 23–27 March 2020; pp. 1–10.
68. Zou, Y.; Liu, H. TDOA Localization with Unknown Signal Propagation Speed and Sensor Position Errors. *IEEE Commun. Lett.* **2020**, *24*, 1024–1027. [CrossRef]
69. Cao, S.; Chen, X.; Zhang, X.; Chen, X. Combined Weighted Method for TDOA-Based Localization. *IEEE Trans. Instrum. Meas.* **2020**, *69*, 1962–1971.
70. Zhou, X.; Chen, L.; Yan, J.; Chen, R. Accurate DOA Estimation with Adjacent Angle Power Difference for Indoor Localization. *IEEE Access* **2020**, *8*, 44702–44713. [CrossRef]
71. Rodrigues, W.d.C.; Apolinário, J.A. An on-the-Fly FDOA-based Target Localization System. In Proceedings of the 2020 IEEE 11th Latin American Symposium on Circuits & Systems (LASCAS), San Jose, CA, USA, 25–28 February 2020; pp. 1–4.
72. Li, Y.; Qi, G.; Sheng, A. Performance Metric on the Best Achievable Accuracy for Hybrid TOA/AOA Target Localization. *IEEE Commun. Lett.* **2018**, *22*, 1474–1477. [CrossRef]
73. Guo, G.; Chen, R.; Ye, F.; Peng, X.; Liu, Z.; Pan, Y. Indoor Smartphone Localization: A Hybrid WiFi RTT-RSS Ranging Approach. *IEEE Access* **2019**, *7*, 176767–176781. [CrossRef]
74. Deng, B.; Sun, Z.B.; Peng, H.F.; Xiong, J.Y. Source localization using TDOA/FDOA/DFS measurements with erroneous sensor positions. In Proceedings of the 2016 CIE International Conference on Radar (RADAR), Guangzhou, China, 10–13 October 2016; pp. 1–4.
75. Chamola, V.; Hassija, V.; Gupta, V.; Guizani, M. A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact. *IEEE Access* **2020**, *8*, 90225–90265. [CrossRef]

76. Koivisto, M.; Costa, M.; Werner, J.; Heiska, K.; Talvitie, J.; Leppänen, K.; Koivunen, V.; Valkama, M. Joint Device Positioning and Clock Synchronization in 5G Ultra-Dense Networks. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 2866–2881. [CrossRef]
77. Lu, Y.; Koivisto, M.; Talvitie, J.; Valkama, M.; Lohan, E.S. Positioning-Aided 3D Beamforming for Enhanced Communications in mmWave Mobile Networks. *IEEE Access* **2020**, *8*, 55513–55525. [CrossRef]
78. Lin, Z.; Lv, T.; Zhang, J.A.; Liu, R.P. Tensor-based High-Accuracy Position Estimation for 5G mmWave Massive MIMO Systems. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6.
79. Zhang, S.; Wu, Q.; Xu, S.; Li, G.Y. Fundamental Green Tradeoffs: Progresses, Challenges, and Impacts on 5G Networks. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 33–56. [CrossRef]
80. Laoudias, C.; Moreira, A.; Kim, S.; Lee, S.; Wirola, L.; Fischione, C. A Survey of Enabling Technologies for Network Localization, Tracking, and Navigation. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3607–3644. [CrossRef]
81. Jin, F.; Liu, K.; Zhang, H.; Ng, J.K.; Guo, S.; Lee, V.C.S.; Son, S.H. Toward Scalable and Robust Indoor Tracking: Design, Implementation, and Evaluation. *IEEE Internet Things J.* **2020**, *7*, 1192–1204. [CrossRef]
82. Kim, H.; Granström, K.; Gao, L.; Battistelli, G.; Kim, S.; Wymeersch, H. 5G mmWave Cooperative Positioning and Mapping Using Multi-Model PHD Filter and Map Fusion. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 3782–3795. [CrossRef]
83. Shao, C.; Kim, Y.; Lee, W. Zero-Effort Proximity Detection with ZigBee. *IEEE Commun. Lett.* **2020**, 1. [CrossRef]
84. Jarvinen, K.; Kiss, A.; Schneider, T.; Tkachenko, O.; Yang, Z. Faster privacy-preserving location proximity schemes for circles and polygons. *IET Inf. Secur.* **2020**, *14*, 254–265. [CrossRef]
85. Ng, P.C.; She, J.; Ran, R. A Compressive Sensing Approach to Detect the Proximity Between Smartphones and BLE Beacons. *IEEE Internet Things J.* **2019**, *6*, 7162–7174. [CrossRef]
86. Ding, H.; Qian, C.; Han, J.; Xiao, J.; Zhang, X.; Wang, G.; Xi, W.; Zhao, J. Close-Proximity Detection for Hand Approaching Using Backscatter Communication. *IEEE Trans. Mob. Comput.* **2019**, *18*, 2285–2297. [CrossRef]
87. Carreras, I.; Matic, A.; Saar, P.; Osmani, V. Comm2Sense: Detecting proximity through smartphones. In Proceedings of the 2012 IEEE International Conference on Pervasive Computing and Communications Workshops, Lugano, Switzerland, 19–23 March 2012; pp. 253–258.
88. Tuesta, J.; Albornoz, D.; Kemper, G.; Almenara, C.A. A Sociometric Sensor Based on Proximity, Movement and Verbal Interaction Detection. In Proceedings of the 2019 International Conference on Information Systems and Computer Science (INCISCOS), Quito, Ecuador, 20–22 November 2019; pp. 216–221.
89. Li, J.; Jobes, C.C.; Carr, J.L. Comparison of Magnetic Field Distribution Models for a Magnetic Proximity Detection System. *IEEE Trans. Ind. Appl.* **2013**, *49*, 1171–1176. [CrossRef]
90. Tupper, A.; Green, R. Pedestrian Proximity Detection using RGB-D Data. In Proceedings of the 2019 International Conference on Image and Vision Computing New Zealand (IVCNZ), Dunedin, New Zealand, 2–4 December 2019; pp. 1–6.
91. Rivest, R.L.; Callas, J.; Canetti, R.; Esvelt, K.; Gillmor, D.K.; Kalai, Y.T.; Lysyanskaya, A.; Norige, A.; Raskar, R.; Shamir, A.; et al. The PACT Protocol Specification—Version 0.1. 2020. Available online: https://pact.mit.edu/technial-reports/ (accessed on 13 September 2020).
92. Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 Contact Tracing. Available online: https://www.who.int/publications/i/item/WHO-2019-nCoV-Contact_Tracing-Tools_Annex-2020.1 (accessed on 10 September 2020).
93. Liu, Y.; Peng, M.; Shou, G. Mobile Edge Computing-Enhanced Proximity Detection in Time-Aware Road Networks. *IEEE Access* **2019**, *7*, 167958–167972. [CrossRef]
94. Mackey, A.; Spachos, P.; Song, L.; Plataniotis, K.N. Improving ble beacon proximity estimation accuracy through bayesian filtering. *IEEE Internet Things J.* **2020**, *7*, 3160–3169. [CrossRef]
95. Ng, P.C.; She, J.; Park, S. High resolution beacon-based proximity detection for dense deployment. *IEEE Trans. Mob. Comput.* **2017**, *17*, 1369–1382. [CrossRef]
96. Ng, P.C.; Spachos, P.; Plataniotis, K. COVID-19 and Your Smartphone: BLE-based Smart Contact Tracing. *arXiv* **2020**, arXiv:2005.13754.
97. Ng, P.C.; Spachos, P.; Gregori, S.; Plataniotis, K. Epidemic Exposure Notification with Smartwatch: A Proximity-Based Privacy-Preserving Approach. *arXiv* **2020**, arXiv:2007.04399.

98. Clark, L.; Papalia, A.; Carvalho, J.T.; Mastrostefano, L.; Krishnamachari, B. Inter-Mobile-Device Distance Estimation using Network Localization Algorithms for Digital Contact Logging Applications. *arXiv* **2020**, arXiv:2007.10162.
99. Bianconi, G.; Sun, H.; Rapisardi, G.; Arenas, A. A message-passing approach to epidemic tracing and mitigation with apps. *arXiv* **2020**, arXiv:2007.05277.
100. Meckelburg, H.J. Contact Tracing Coronavirus COVID-19 -Calibration Method and Proximity Accuracy. 2020. Available online: https://doi.org/10.13140/RG.2.2.36337.22884 (accessed on 13 September 2020).
101. Jeong, S.; Kuk, S.; Kim, H. A Smartphone Magnetometer-Based Diagnostic Test for Automatic Contact Tracing in Infectious Disease Epidemics. *IEEE Access* **2019**, *7*, 20734–20747. [CrossRef]
102. Altuwaiyan, T.; Hadian, M.; Liang, X. EPIC: Efficient Privacy-Preserving Contact Tracing for Infection Detection. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6.
103. Troncoso, C.; Payer, M.; Hubaux, J.P.; Salathé, M.; Larus, J.; Bugnion, E.; Lueks, W.; Stadler, T.; Pyrgelis, A.; Antonioli, D.; et al. Decentralized Privacy-Preserving Proximity Tracing. *arXiv* **2020**, arXiv:2005.12273.
104. Google/Apple. Privacy-Preserving Contact Tracing. Available online: https://www.apple.com/covid19/contacttracing (accessed on 10 September 2020).
105. Tripathy, A.K.; Mohapatra, A.G.; Mohanty, S.P.; Kougianos, E.; Joshi, A.M.; Das, G. EasyBand: A Wearable for Safety-Aware Mobility during Pandemic Outbreak. *IEEE Consum. Electron. Mag.* **2020**, *9*, 57–61. [CrossRef]
106. Accent System Wristband for Contact Tracing. Available online: https://accent-systems.com/covid-19-contact-tracing-solution/ (accessed on 13 September 2020).
107. Salathe, M.; Kazandjieva, M.; Lee, J.W.; Levis, P.; Feldman, M.W.; Jones, J.H. A high-resolution human contact network for infectious disease transmission. *Proc. Natl. Acad. Sci. USA* **2010**, *107*, 22020–22025. [CrossRef]
108. Kotaru, M.; Katti, S. Position Tracking for Virtual Reality Using Commodity WiFi. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Honolulu, HI, USA, 21–26 July 2017; pp. 2671–2681.
109. TSINGOAL. Social Distancing and Contact Tracing. 2020. Available online: https://www.uwb-social-distancing.com/?gclid=EAIaIQobChMI-rjk77mf6gIViQ8YCh1dTgcmEAAYAiAAEgLk0PD_BwE (accessed on 13 September 2020).
110. Isella, L.; Romano, M.; Barrat, A.; Cattuto, C.; Colizza, V.; Van den Broeck, W.; Gesualdo, F.; Pandolfi, E.; Ravà, L.; Rizzo, C.; et al. Close Encounters in a Pediatric Ward: Measuring Face-to-Face Proximity and Mixing Patterns with Wearable Sensors. *PLoS ONE* **2011**, *6*, e17144. [CrossRef]
111. Chen, H.; Yang, B.; Pei, H.; Liu, J. Next Generation Technology for Epidemic Prevention and Control: Data-Driven Contact Tracking. *IEEE Access* **2019**, *7*, 2633–2642. [CrossRef]
112. Kim, H.; Lim, J.; Hong, W.; Park, J.; Kim, Y.; Kim, M.; Lee, Y. Design of a Low-Power BLE5-Based Wearable Device for Tracking Movements of Football Players. In Proceedings of the International SoC Design Conference (ISOCC), Jeju, Korea, 6–9 October 2019; pp. 11–12.
113. Comarch LifeWristband. Available online: https://www.comarch.com/healthcare/products/remote-medical-care/remote-care-services/e-careband/ (accessed on 13 September 2020).
114. Moko Smart LoraWan-Based Wearable for Contact Tracing. Available online: https://www.mokosmart.com/lorawan-ble-\wearable-wristband-beacon-covid-19-contact-tracing-solution/ (accessed on 5 June 2020).
115. Adiono, T.; Armansyah, R.F.; Nolika, S.S.; Ikram, F.D.; Putra, R.V.W.; Salman, A.H. Visible light communication system for wearable patient monitoring device. In Proceedings of the 2016 IEEE Region 10 Conference (TENCON), Singapore, 22–25 November 2016; pp. 1969–1972.
116. Liu, T.; Niu, X.; Kuang, J.; Cao, S.; Zhang, L.; Chen, X. Doppler shift mitigation in acoustic positioning based on pedestrian dead reckoning for smartphone. *IEEE Trans. Instrum. Meas.* **2020**, 1. [CrossRef]
117. Popoola, O.R.; Popoola, W.O.; Ramirez-Iniguez, R.; Sinanović, S. Design of improved IR protocol for LED indoor positioning system. In Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017; pp. 882–887.
118. Malmström, M.; Skog, I.; Razavi, S.M.; Zhao, Y.; Gunnarsson, F. 5G Positioning—A Machine Learning Approach. In Proceedings of the 2019 16th Workshop on Positioning, Navigation and Communications (WPNC), Bremen, Germany, 23–24 October 2019; pp. 1–6.

119. Aranda, F.J.; Parralejo, F.; Álvarez, F.J.; Torres-Sospedra, J. Multi-Slot BLE Raw Database for Accurate Positioning in Mixed Indoor/Outdoor Environments. *Data* **2020**, *5*, 67. [CrossRef]
120. Noremark, M.; Widgren, S. EpiContactTrace: An R-package for contact tracing during livestock disease outbreaks and for risk-based surveillance. *BMC Vet. Res.* **2014**, *10*, 71. [CrossRef] [PubMed]
121. Haus, M.; Ding, A.Y.; Ott, J. CRAWDAD Dataset Tum/Proximityness (v. 2020-02-18). 2020. Available online: https://crawdad.org/tum/proximityness/20200218 (accessed on 25 August 2020).
122. Haus, M.; Ding, A.Y.; Ott, J. Multimodal Co-Presence Detection with Varying Spatio-Temporal Granularity. In Proceedings of the 2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Austin, TX, USA, 23–27 March 2020; pp. 1–7.
123. Tan, H.Y.; Bay, J. OpenTrace Calibration. Device Calibration Data and Trial Methodologies for Testing Implementations of the BlueTrace Protocol. Available online: https://github.com/opentrace-community/opentrace-calibration (accessed on 24 August 2020).
124. Mendoza-Silva, G.; Matey-Sanz, M.; Torres-Sospedra, J.; Huerta, J. BLE RSS Measurements Dataset for Research on Accurate Indoor Positioning. *Data* **2019**, *4*, 12. [CrossRef]
125. Raza, U.; Khan, A.; Kou, R.; Farnham, T.; Premalal, T.; Stanoev, A.; Thompson, W. Dataset: Indoor Localization with Narrow-band, Ultra-Wideband, and Motion Capture Systems. In *DATA'19: Proceedings of the 2nd Workshop on Data Acquisition to Analysis, New York, NY, USA, 10 November 2019*; Association for Computing Machinery: New York, NY, USA, 2019. [CrossRef]
126. Ruiz, A.R.J.; Mendoza-Silva, G.M.; Seco, F.; Torres-Sospedra, J. Datasets and Supporting Materials for the IPIN 2017 Competition Track 3 (Smartphone-Based, Off-Site). 2017. Available online: https://doi.org/10.5281/zenodo.2823924 (accessed on 10 September 2020).
127. Barral, V.; Suarez-Casal, P.; Escudero, C.J.; García-Naya, J.A. Multi-Sensor Accurate Forklift Location and Tracking Simulation in Industrial Indoor Environments. *Electronics* **2020**, *8*, 1152. [CrossRef]
128. Biala, T.; Afolabi, Y.; Khaliq, A. How Efficient is Contact Tracing in Mitigating the Spread of Covid-19? A Mathematical Modeling Approach. *arXiv* **2020**, arXiv:2008.03859.
129. Grassly, N.C.; Pons-Salort, M.; Parker, E.P.; White, P.J.; Ferguson, N.M.; Ainslie, K.; Baguelin, M.; Bhatt, S.; Boonyasiri, A.; Brazeau, N.; et al. Comparison of molecular testing strategies for COVID-19 control: A mathematical modelling study. *Lancet Infect. Dis.* **2020**. [CrossRef]
130. Ashcroft, P.; Huisman, J.S.; Lehtinen, S.; Bouman, J.A.; Althaus, C.L.; Regoes, R.R.; Bonhoeffer, S. COVID-19 infectivity profile correction. *arXiv* **2020**, arXiv:2007.06602.
131. Hellewell, J.; Abbott, S.; Gimma, A.; Bosse, N.I.; Jarvis, C.I.; Russell, T.W.; Munday, J.D.; Kucharski, A.J.; Edmunds, W.J.; Sun, F.; et al. Feasibility of controlling COVID-19 outbreaks by isolation of cases and contacts. *Lancet Glob. Health* **2020**, *8*, e488–e496.
132. Talmoudi, K. Estimating Transmission Dynamics and Serial Interval of the First Wave of COVID-19 Infections under Different Control Measures: A Statistical Analysis in Tunisia from February 29 to May 5, 2020, Dryad, Dataset. 2020. Available online: https://doi.org/10.5061/dryad.b8gtht799 (accessed on 13 September 2020).
133. Champredon, D.; Dushoff, J. Data from: Intrinsic and Realized Generation Intervals in Infectious-Disease Transmission, Dryad, Dataset. 2015. Available online: https://doi.org/10.5061/dryad.4dd3s (accessed on 13 September 2020).
134. Irani, P.; Bharadwaj, P.; Ospina, J.; Chauhan, S.; Eutialia; Dylanzxc; Wang, J.; Gosain, M. A List of High Quality Open Datasets for COVID-19 Data Analysis. GitHub Repository. 2020. Available online: https://github.com/sfu-db/covid19-datasets (accessed on 10 September 2020).
135. Yalaman, A.; Basbug, G.; Elgin, C.; Galvani, A.P. Contact Tracing is Associated with Lower COVID-19 Case Fatality Rates: Evidence from 40 Countries. 2020. Available online: https://doi.org/10.5281/zenodo.3991877 (accessed on 10 September 2020).
136. Jenssen, H. COVID-19 CT Segmentation Dataset. 2020. Available online: http://medicalsegmentation.com/covid19/ (accessed on 10 September 2020).
137. Virufy. Cough-Based Datasets for COVID-19 Diagnosis. 2020. Available online: https://github.com/virufy/covid (accessed on 13 September 2020).
138. Bilello, E. Chest Imaging with Clinical and Genomic Correlates Representing a Rural COVID-19 Positive Population (COVID-19-AR). 2020. Available online: https://wiki.cancerimagingarchive.net/pages/viewpage.action?pageId=70226443 (accessed on 13 September 2020).

139. Qazi, U.; Imran, M.; Ofli, F. GEOCOV19: A Dataset of Hundreds of Millions of Multilingual COVID-19 Tweets with Location Information. *arXiv* **2020**, arXiv:2005.11177. [CrossRef]
140. Gai, K.; Wu, Y.; Zhu, L.; Zhang, Z.; Qiu, M. Differential Privacy-Based Blockchain for Industrial Internet-of-Things. *IEEE Trans. Ind. Informa.* **2019**, *16*, 4156–4165. [CrossRef]
141. Niu, B.; Chen, Y.; Wang, Z.; Wang, B.; Li, H. Eclipse: Preserving Differential Location Privacy Against Long-Term Observation Attacks. *IEEE Trans. Mob. Comput.* **2020**. [CrossRef] [PubMed]
142. Jung, G.; Lee, H.; Kim, A.; Lee, U. Too Much Information: Assessing Privacy Risks of Contact Trace Data Disclosure on People with COVID-19 in South Korea. *Front. Public Health* **2020**, *8*.
143. BBC. *Coronavirus Privacy: Are South Korea's Alerts Too Revealing*? BBC: London, UK, 2020.
144. Bay, J.; Kek, J.; Tan, A.; Hau, C.S.; Yongquan, L.; Tan, J.; Quy, T.A. BlueTrace: A pRivacy-Preserving Protocol for Community-Driven Contact Tracing Across Borders. 2020. Available online: https://bluetrace.io (accessed on 13 September 2020).
145. Bell, J.; Butler, D.; Hicks, C.; Crowcroft, J. TraceSecure: Towards Privacy Preserving Contact Tracing. *arXiv* **2020**, arXiv:2004.04059.
146. Cho, H.; Ippolito, D.; Yu, Y.W. Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs. *arXiv* **2020**, arXiv:2003.11511.
147. PEPPPTl. Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) Protocol- Documentation Files. 2020. Available online: https://github.com/pepp-pt/pepp-pt-documentation (accessed on 18 July 2020).
148. PRIVATICS. ROBERT: ROBust and Privacy-Preserving Proximity Tracing. Available online: https://github.com/ROBERT-proximity-tracing/documents/blob/master/ROBERT-specification-EN-v1_0.pdf (accessed on 10 September 2020).
149. CovidWatch. Covid-Watch: Our Privacy-Preserving Protocol. 2020. Available online: https://www.covid-watch.org/ (accessed on 13 September 2020).
150. TCN. TCN Coalition: TCN Source Code. 2020. Available online: https://github.com/TCNCoalition (accessed on 13 September 2020).
151. OpenCovidTrace. Open Covid Trace-Full Privacy Open Source Contact Tracing. 2020. Available online: https://github.com/OpenCovidTrace (accessed on 13 September 2020).
152. Loiseau, L.; Bellet, V.; Bento, T.; Teissonniere, E.; Benoliel, M.; Kinsman, G.; Milne, P. Whisper Tracing Version 3 an Open and Privacy First Protocol for Contact Tracing. 2020. Available online: https://docsend.com/view/nis3dac (accessed on 13 September 2020). [CrossRef]
153. Conti, M.; Willemsen, J.; Crispo, B. Providing Source Location Privacy in Wireless Sensor Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 1238–1280.
154. Chan, J.; Gollakota, S.; Horvitz, E.; Jaeger, J.; Kakade, S.; Kohno, T.; Langford, J.; Larson, J.; Singanamalla, S.; Sunshine, J.; et al. Pact: Privacy sensitive protocols and mechanisms for mobile contact tracing. *arXiv* **2020**, arXiv:2004.03544. [CrossRef]
155. Taha, S.; Shen, X. A Physical-Layer Location Privacy-Preserving Scheme for Mobile Public Hotspots in NEMO-Based VANETs. *IEEE Trans. Intell. Transp. Syst.* **2013**, *14*, 1665–1680. [CrossRef]
156. Han, J.; Susilo, W.; Mu, Y.; Yan, J. Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption. *IEEE Trans. Parallel Distrib. Syst.* **2012**, *23*, 2150–2162. [CrossRef]
157. Mustafa, M.A.; Zhang, N.; Kalogridis, G.; Fan, Z. DEP2SA: A Decentralized Efficient Privacy-Preserving and Selective Aggregation Scheme in Advanced Metering Infrastructure. *IEEE Access* **2015**, *3*, 2828–2846. [CrossRef]
158. Alzahrani, B.A. An Information-Centric Networking based Registry for Decentralized Identifiers and Verifiable Credentials. *IEEE Access* **2020**, *8*, 137198–137208.
159. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564. [CrossRef]
160. Sharon, T. Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers. *Ethics Inf. Technol.* **2020**.
161. Stanley, B.J.; Granick, J.S. *The Limits of Location Tracking in an Epidemic*; American Civil Liberties Union: New York, NY, USA, 2020; pp. 1–9. [CrossRef]
162. Kim, J.W.; Kim, D.H.; Jang, B. Application of Local Differential Privacy to Collection of Indoor Positioning Data. *IEEE Access* **2018**, *6*, 4276–4286.

163. Xiao, H.; Ye, Y.; Devadas, S. Local Differential Privacy in Decentralized Optimization. 2019. Available online: http://xxx.lanl.gov/abs/1902.06101 (accessed on 13 September 2020).
164. Vazifehdan, J.; Prasad, R.V.; Jacobsson, M.; Niemegeers, I. An Analytical Energy Consumption Model for Packet Transfer over Wireless Links. *IEEE Commun. Lett.* **2012**, *16*, 30–33.
165. Tharinda Nishantha Vidanagama, V.G.; Arai, D.; Ogishi, T. M2M gateway selection scheme for smart wireless devices: An energy consumption perspective. In Proceedings of the 2015 10th Asia-Pacific Symposium on Information and Telecommunication Technologies (APSITT), Colombo, Sri Lanka, 4–7 August 2015; pp. 1–3.
166. Chen, X.; Breiholz, J.; Yahya, F.B.; Lukas, C.J.; Kim, H.; Calhoun, B.H.; Wentzloff, D.D. Analysis and Design of an Ultra-Low-Power Bluetooth Low-Energy Transmitter with Ring Oscillator-Based ADPLL and 4 × Frequency Edge Combiner. *IEEE J. Solid-State Circuits* **2019**, *54*, 1339–1350.
167. Zhu, W.; Cao, J.; Raynal, M. Energy-Efficient Composite Event Detection in Wireless Sensor Networks. *IEEE Commun. Lett.* **2018**, *22*, 177–180.
168. Rezaei, F.; Tellambura, C.; Herath, S. Large-Scale Wireless-Powered Networks with Backscatter Communications—A Comprehensive Survey. *IEEE Open J. Commun. Soc.* **2020**, *1*, 1100–1130.
169. Radic, J.; Brkic, M.; Djugova, A.; Videnovic-Misic, M.; Goll, B.; Zimmermann, H. Ultra-low power low-complexity 3–7.5 GHz IR-UWB transmitter with spectrum tunability. *IET Circuits Devices Syst.* **2020**, *14*, 521–527.
170. Fuketa, H.; Morita, Y. Ultra-Low Power Human Proximity Sensor Using Electrostatic Induction. *IEEE Sens. J.* **2020**, *20*, 7819–7825.
171. Pushpalatha, S.; Shivaprakasha, K. Energy-Efficient Communication Using Data Aggregation and Data Compression Techniques in Wireless Sensor Networks: A Survey. In *Advances in Communication, Signal Processing, VLSI, and Embedded Systems*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 161–179.
172. Stanley-Marbell, P.; Alaghi, A.; Carbin, M.; Darulova, E.; Dolecek, L.; Gerstlauer, A.; Gillani, G.; Jevdjic, D.; Moreau, T.; Daglis, A.; et al. Exploiting Errors for Efficiency: A Survey from Circuits to Algorithms. *arXiv* **2020**, arXiv:1809.05859.
173. Yang, Y.; Geng, Y.; Qiu, L.; Hu, W.; Cao, G. Context-aware Task Offloading for Wearable Devices. In Proceedings of the 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, Canada, 31 July–3 August 2017; pp. 1–9.
174. Cheng, Q.; Peng, Z.; Lin, J.; Li, S.; Wang, F. Energy harvesting from human motion for wearable devices. In Proceedings of the 10th IEEE International Conference on Nano/Micro Engineered and Molecular Systems, Xi'an, China, 7–11 April 2015; pp. 409–412.
175. Ruan, T.; Chew, Z.J.; Zhu, M. Energy-Aware Approaches for Energy Harvesting Powered Wireless Sensor Nodes. *IEEE Sens. J.* **2017**, *17*, 2165–2173.
176. Guo, H.; Liang, Y.; Long, R.; Zhang, Q. Cooperative Ambient Backscatter System: A Symbiotic Radio Paradigm for Passive IoT. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 1191–1194.
177. Kuxdorf-Alkirata, N.; Maus, G.; Brückmann, D. Efficient calibration for robust indoor localization based on low-cost BLE sensors. In Proceedings of the 2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS), Dallas, TX, USA, 4–7 August 2019; pp. 702–705. [CrossRef] [PubMed]
178. Grifoni, A.; Weiskopf, D.; Ramirez, S.I.; Mateus, J.; Dan, J.M.; Moderbacher, C.R.; Rawlings, S.A.; Sutherland, A.; Premkumar, L.; Jadi, R.S.; et al. Targets of T Cell Responses to SARS-CoV-2 Coronavirus in Humans with COVID-19. *Cell* **2020**, *181*, 1489–1501.e15. [CrossRef] [PubMed]
179. Wang, F.; Nie, J.; Wang, H.; Zhao, Q.; Xiong, Y.; Deng, L.; Song, S.; Ma, Z.; Mo, P.; Zhang, Y. Characteristics of Peripheral Lymphocyte Subset Alteration in COVID-19 Pneumonia. *J. Infect. Dis.* **2020**, *221*, 1762–1769. [CrossRef] [PubMed]
180. Haberman, R.; Axelrad, J.; Chen, A.; Castillo, R.; Yan, D.; Izmirly, P.; Neimann, A.; Adhikari, S.; Hudesman, D.; Scher, J.U. Covid-19 in Immune-Mediated Inflammatory Diseases—Case Series from New York. *N. Engl. J. Med.* **2020**, *383*, 85–88. [CrossRef] [PubMed]
181. Koff, W.C.; Williams, M.A. Covid-19 and Immunity in Aging Populations—A New Research Agenda. *N. Engl. J. Med.* **2020**. [CrossRef]
182. Gandhi, R.T.; Lynch, J.B.; del Rio, C. Mild or Moderate Covid-19. *N. Engl. J. Med.* **2020**. [CrossRef] [PubMed]
183. Holmdahl, I.; Buckee, C. Wrong but Useful—What Covid-19 Epidemiologic Models Can and Cannot Tell Us. *N. Engl. J. Med.* **2020**. [CrossRef]

184. Yao, M.; Zhang, L.; Ma, J.; Zhou, L. On airborne transmission and control of SARS-Cov-2. *Sci. Total. Environ.* **2020**, *731*, 139178. [CrossRef]
185. Sunjaya, A.P. Implications of respiratory pathogen transmission dynamics on prevention and testing. *Int. J. Hyg. Environ. Health* **2020**, *228*, 113551.
186. Ungar, L. Everything You Have Read about Contact Tracing Apps Is Wrong. 2020. Available online: https://knowledge.wharton.upenn.edu/article/everything-read-contact-tracing-apps-wrong/ (accessed on 13 September 2020).
187. Ioannidis, J.P. Coronavirus disease 2019: The harms of exaggerated information and non-evidence-based measures. *Eur. J. Clin. Investig.* **2020**, *50*, e13222.
188. Morley, J.; Cowls, J.; Taddeo, M.; Floridi, L. Ethical Guidelines for COVID-19 Tracing Apps. Nature. 2020. Available online: https://www.nature.com/articles/d41586-020-01578-0 (accessed on 13 September 2020). [CrossRef]
189. Parker, M.J.; Fraser, C.; Abeler-Dörner, L.; Bonsall, D. Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic. *J. Med. Ethics* **2020**, *46*, 427–431. [CrossRef]
190. Nguyen, C.T.; Saputra, Y.M.; Van Huynh, N.; Nguyen, N.T.; Khoa, T.V.; Tuan, B.M.; Nguyen, D.N.; Hoang, D.T.; Vu, T.X.; Dutkiewicz, E.; et al. A comprehensive survey of enabling and emerging technologies for social distancing—Part I: Fundamentals and enabling technologies. *IEEE Access* **2020**, *8*, 153479–153507.