

Perspective

Towards Privacy Paradigm Shift Due to the Pandemic: A Brief Perspective

Abdul Majeed  and Sungchang Lee * 

School of Information and Electronics Engineering, Korea Aerospace University, Goyang 10540, Korea; abdulmajid09398@kau.kr or abdulmajid09398@gmail.com

* Correspondence: sclee@kau.ac.kr

Abstract: With the advent of the pandemic (e.g., novel corona virus disease 2019 (COVID-19)), a tremendous amount of data about individuals are collected by the health authorities on daily basis for curbing the disease's spread. The individuals' data collection/processing at a massive scale for community well-being with the help of digital solutions (e.g., mobile apps for mobility and proximity analysis, contact tracing through credit card usage history, facial recognition through cameras, and crowd analysis using cellular networks data etc.) raise several privacy concerns. Furthermore, the privacy concerns that are arising mainly due to the fine-grained data collection has hindered the response to tackle this pandemic in many countries. Hence, acquiring/handling individuals data with privacy protection has become a vibrant area of research in these pandemic times. This paper explains the shift in privacy paradigm due to the pandemic (e.g., COVID-19) which involves more and detailed data collection about individuals including locations and demographics. We explain technical factors due to which the people's privacy is at higher risk in the COVID-19 time. In addition, we discuss privacy concerns in different epidemic control measures (ECMs) (e.g., contact tracing, quarantine monitoring, and symptoms reporting etc.) employed by the health authorities to tackle this disease. Further, we provide an insight on the data management in the ECMs with privacy protection. Finally, the future prospects of the research in this area tacking into account the emerging technologies are discussed. Through this brief article, we aim to provide insights about the vulnerability to user's privacy in pandemic times, likely privacy issues in different ECMs adopted by most countries around the world, how to preserve user's privacy effectively in all phases of the ECMs considering relevant data in loop, and conceptual foundations of ECMs to fight with future pandemics in a privacy preserving manner.



Citation: Majeed, A.; Lee, S. Towards Privacy Paradigm Shift Due to the Pandemic: A Brief Perspective. *Inventions* **2021**, *6*, 24. <https://doi.org/10.3390/inventions6020024>

Academic Editor: Francisco Manzano Agugliaro

Received: 19 February 2021

Accepted: 24 March 2021

Published: 28 March 2021

Corrected: 25 February 2022

Keywords: privacy; COVID-19; pandemic; personal data; digital solutions; healthcare systems

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Privacy is one of the fundamental human rights, and it is needed for individualism, self respect, and autonomy [1]. Moreover, due to excessive digitization, the protection of individual's privacy has become a challenging task [2–4]. Privacy issues are advancing from unique identifications of individuals to the credit card theft, cyber stalking, sentiment manipulation, unsuspected people's profiling, movement tracking, flow modeling, and financial losses etc. Online/offline firms are deploying plenty of solutions such as encryption, anonymization, masking, watermarking, access controls, and randomization algorithms to safeguard the individual's privacy [5,6]. Moreover, the digital innovation including Internet of things (IoT), industrial Internet of things (IIoT), Internet of medical things (IoMT), Internet of everything (IoE), cloud computing (CC), cyber physical social systems (CPSSs), social networks (SNs), and location based systems (LBS), to name a few, have revolutionized they way of living life and increased people's reliance on the technology. On the one hand, these technologies have improved the people's quality of life. On the other hand, these technologies are facing adoption issues at a wider scale due to

the unexpected privacy problems reported by their users. Hence, privacy protection goes hand in hand with digital innovation as a proactive measure for sustaining people's trust in the digital era.

Owing to the unanticipated and on-going global challenge of a novel corona virus disease 2019 (COVID-19), all countries across the globe are continually exploring/implementing new digital solutions to cope with this disease in order to alleviate healthcare workers burden [7,8]. Although reliance on such system has helped in curbing the spread of this disease. Meanwhile, majority of people felt hesitation while using the digital systems due to privacy concerns. As these systems are designed to collect information like, where someone go, to whom someone meet, how often someone meet, at what time someone meet, what and from where someone buy daily usage things, what are someone plans regarding travel in near future, how often someone visit pharmacy or nearby clinic, what is the profession of someone, what are activities of someone in leisure time, in which infrastructure some data may go and for which purpose it will be used, and what is the religion of someone, to name a few are pertinent data collection items due to which people are concerned more about their privacy in the COVID-19 era [9,10]. Hence, the need for an in-depth understanding of what roles information systems and technology researchers can play in this global pandemic has become more emergent than ever [11,12]. The future systems should address the privacy challenges by collecting minimal data that is of paramount to deal with epidemic/pandemic, safe storage of personal data, secure processing, privacy preserving computing-based analytics, and distribution and use in a privacy preserving manner to augment people trust on such systems. Meanwhile, identification and implementation of the privacy requirements of users and their incorporation in the design of systems/software is very challenging. Hence, the privacy protection in epidemic control measures has become the conceptual foundations of futures research and digital healthcare solutions [13–15].

This work aims to present brief perspectives of the privacy paradigm shift in the context of COVID-19, and recent privacy implications arising from deploying digital solutions. Specifically, this work explains privacy items (e.g., demographics, location information, mobility data, stay points, health information, and social activities etc.) related to the information privacy protection that are frequently collected for keeping people away from the COVID-19 contaminated places. The main contributions of this brief perspective in the field of information privacy topic are summarized as follows:

- It explains the shift in privacy paradigm in the context of COVID-19 which includes, data privacy to location privacy, privacy in non-pharmaceutical epidemic control measures including social distancing enforcement and mobility/proximity detection, analytics to privacy preserving computing (e.g., confidential computing), manual epidemiological investigation for close contact finding to automated contact tracing, data sharing from domestic to international researchers for disease's propagation-modes understanding, and announcing the locations of the facilities to whom an infected persons have visited etc.
- It presents technical factors due to which privacy has become a major concerns in the epidemic times.
- it describes privacy issues in the epidemic control measures (ECMs) that are used by health authorities to slow down the progression of the disease utilizing the multitude of personal data.
- It provides an insight on the data management in the ECMs with privacy protection.
- it discusses the future prospects of the research in privacy area tacking into account the current emerging digital technologies.
- Through this brief overview, we hope to provide a solid baseline for future studies in the privacy area dealing with future epidemics.
- From the technical point of view, this study results can be utilized to develop more secure healthcare solutions/systems that can incorporate the privacy requirements in

all phases of data life-cycle (e.g., collection, storage, analytics, distribution, use, and archival) to alleviate people's hesitation while providing personal data.

The remainder of this paper is organized as follows. Section 2 explains the conceptual overview of the privacy paradigm shift in the context of COVID-19, and provides the technical features due to which privacy has become a vibrant area of research in the recent times. Section 3 presents the privacy issues in the epidemic control measures that are used by the health authorities to block the disease's propagation. Section 4 provides insights on data management in the epidemic control measures with privacy guarantee. Section 5 discusses the future prospects of the research in the privacy area tacking into account the current emerging technologies. Finally, Section 6 concludes the paper.

2. Conceptual Overview of the Privacy Paradigm Shift in the Context of COVID-19

This section describes the conceptual overview of the paradigm shift of the information privacy due to the prevalence of the COVID-19. The main driver of the privacy concerns in the context of COVID-19 is location information that is obtained by using geospatial technologies (e.g., GPS data, Bluetooth data, cellular signals, wifi-access points etc.). In addition, various mitigation methods employed to control COVID-19 that harness people's sensitive location information can significantly contribute in privacy breaches. In addition, the communication mechanisms assisted by GPS, Wi-Fi, and Bluetooth etc. augments contact tracing by identifying potentially unknown and susceptible contacts thereby proving their usefulness. The release of the patients routes along with the visited places and demographics information has a range of privacy concerns. In addition, due to hidden data reporting to health agencies without explicit users consent, majority of the digital solutions have lower adoption across the globe [16]. The conceptual overview of the privacy paradigm shift in the context of COVID-19, and digital solutions employed to curb the spread of COVID-19 are demonstrated in Figure 1. In Figure 1, we present the data resources, pertinent technologies and their utility, and privacy problems.

To emphasize the subject matter well, we categorize the privacy problems into two categories, common privacy problems (e.g., general privacy problems of pre-COVID era), and privacy problems in the COVID-19's era. Meanwhile, some of the privacy problems listed in the COVID-19's era are generic for healthcare and IoT device related. For example, the disease predictions and aggregation is possible in the healthcare settings even in the pre-COVID era. On the other hand, the usage of transport data disclosure can also occur through IoT device data accumulation in the pre-COVID era. Meanwhile, in COVID-19 era, these privacy problems can occur frequently due to the close monitoring of individuals using heterogeneous data sources. Therefore, we placed such active privacy problems in the COVID-19 era. Furthermore, we provide the more refine coverage of privacy problems that are unique in COVID-19's context while keeping data in loop in Section 3.

Common privacy problems have been studied well, and many methods have been proposed to tackle those problems. The privacy problems of COVID-19's era are recent, and many researchers are suggesting privacy mechanisms to resolve these problems. After detailed synthesis of the literature, we summarize specific technical features that have made the privacy a very attractive research area in recent times in Figure 2. Due to these technical features, majority of the people's privacy is at risk during pandemic times. Therefore, the policy maker, healthcare sector, and developer can adopt these technical factors to effectively preserve user's privacy to overcome people's worry while providing personal data. Consequently, the higher adoption of the digital solutions can be obtained that can assist in fighting with any kind of infectious diseases in future.

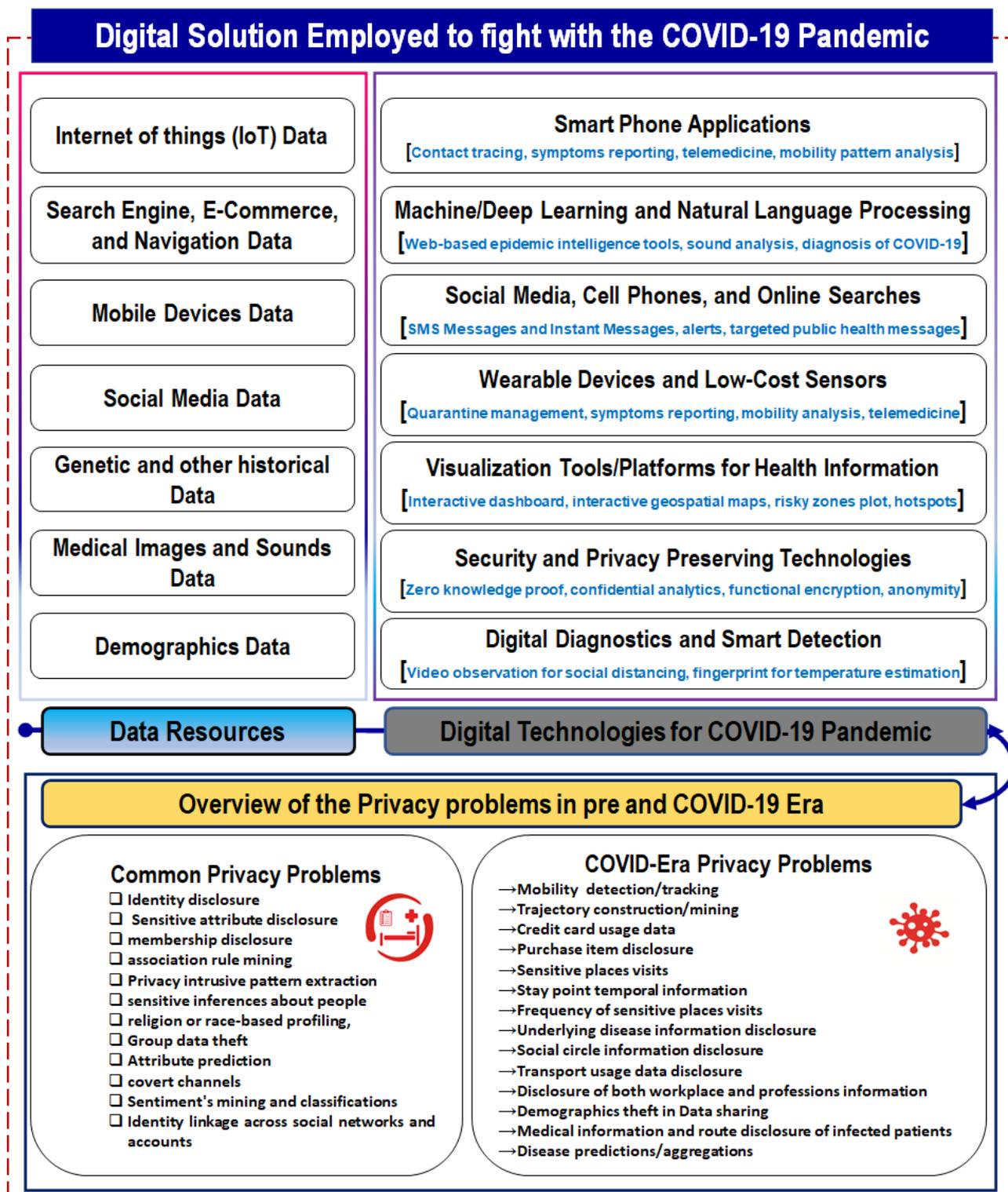


Figure 1. Conceptual overview of digital solutions and privacy issues in the COVID era.

Why privacy becomes a hot research topic in the COVID-19 Era?

List of technical factors due to which privacy has become a vibrant area of research in COVID-19 era
→ More data collection and processing in a centralized setting (e.g., servers).
→ Excessive utilization of the individual's precise location information.
→ Heavy reliance on the technology for most of the activities (e.g., reporting health status, SMS, alerts).
→ Excessive logging of the users visits of each facility and place.
→ The data sharing readily for the sake of health's safety and excessive reporting of symptoms.
→ Usage of the services that harness location information for most functions (e.g., POI and travel sites etc.)
→ Providing data to the service provides for acquiring diverse services (e.g., telemedicine, mobile health).
→ Data transition between different systems, infrastructure, and agencies for tracking the suspected patients.
→ Usage of third-party applications for analytics on the private data.
→ Data distribution across the border and with domestic researcher for dynamics understanding.
→ Posting more data about the disease outbreak on social network sites.
→ Fusion of heterogeneous data resources (CCTV, credit card, cellular network) for tracing the contacts of patients.
→ Installing multiple Apps without getting awareness about their working and servicing mechanism.
→ Providing precise information while installing each app and ignoring the installation of security patches.

Figure 2. Technical features that made privacy a dilemma of research in recent times.

3. Privacy Issues in the Epidemic Control Measures

From the beginning of the pandemic, plenty of solutions/mechanisms were adopted to control the spread of the COVID-19. The common measures that were adopted are, school closures, remote work, reduction in public transport, travel restrictions, cancellation of events and parties, workplace closures, lock downs, city closures, public information campaigns, cancellation of gathering and graduation ceremonies, social distancing, and excessive logs of the visits, to name a few. These control measures were generic, and were usually enforced at national/regional level. Meanwhile, the digital solutions were also used as a control measure during the epidemic times in the absence of potential vaccine. These control measures were distinct in each country and region level depending upon the severity of the disease, and other spatial factors such as population density and demographics etc. In this work, we classify the epidemic control measures into seven broad categories, and highlight their privacy issues taking into account the data utilized in each category. We present epidemic control measures in Figure 3. All these control measures listed in Figure 3 yield unique privacy concerns based on the data in loop. For example, the contact tracing measure can lead to identity disclosure of an individual if detailed information is published or credit card data is utilized for suspects finding. Similarly, quarantine monitoring with realtime data can expose the user's stay points or visits to the sensitive places (i.e., gays club, and tobacco shops). In following subsections, we discuss the privacy issues in each control measure depending upon the data collected/used, and latest technologies/solutions devised so far to alleviate those privacy concerns.

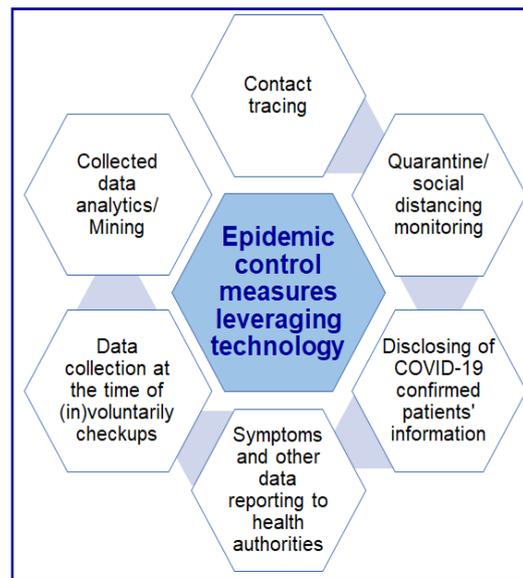


Figure 3. Overview of the pertinent epidemic control measures leveraging technology.

3.1. Contact Tracing

In this epidemic control measure, the health authorities usually trace back the activities/routes of confirmed patients to find people who might have been in close contact with the confirmed patients and might need to get tested or self-quarantine immediately [17]. In this method, both manual and automated solutions are utilized to find the suspects. However, the manual methods are time consuming, and rely on the memory of the individuals [18]. In contrast, the automated methods have demonstrated effectiveness to control the disease's spread [19,20]. In some countries, both these methods were jointly used to find the exposed people to lower the reproduction rate (R_0) in order to lower economic losses.

3.1.1. Data in Loop

The contact tracing is generally performed leveraging the mobility and proximity data. The mobility data is related to individuals moving patterns and the proximity data is about the closeness with other people while doing the daily routine works. The types of data processed and used for the contact tracing purposes is, (i) credit card usage history, (ii) mobile phone apps data/logs, (iii) cellular networks data, (iii) CCTV footage, (iv) cell phone location history, and (v) QR codes etc. Furthermore, social networks data can be used for the suspects finding leveraging the interactions and social circles data.

3.1.2. Likely Privacy Concerns/Issues in the Control Measure

The likely privacy problems in this control measure are, (i) identity disclosure, (ii) purchasing items disclosure, (iii) sensitive places visits disclosure (e.g., gay club visited by majority of adults in the South Korea), (iv) stay points disclosures, (v) trajectories disclosures, (vi) automated profiling, (vii) religions beliefs disclosure, and (viii) social relations disclosures. All these concerns can occur in the contact tracing measures when it is carried out with the help of technical solutions (e.g., apps, frameworks/prototypes).

3.1.3. Latest Technologies/Solutions Devised so far to Alleviate Privacy Concerns/Issues

There exist plenty of solutions that have been proposed to resolve the privacy problems of the latest technologies that are used for the containing the disease spread. The most famous and practical solutions is the contact tracing via decentralized manner [21]. In such applications, the majority of computation is carried out on user's own devices thereby privacy is preserved [22]. The other notable solutions that have demonstrated effectiveness in terms of privacy are, block chain technology based contact tracing [23,24], combining historical and centralized data [25], and group signature-based apps [26]. All these solu-

tions have demonstrated effectiveness to trace the contacts of COVID-19's suspects with privacy guarantees. Despite the success of such solutions, the user's willingness to utilize digital solutions for contact tracing remained low due to the privacy concerns during the pandemic times. Therefore, numerous efforts are underway to devise and implement privacy preserving contact tracing solutions across the globe.

3.2. Quarantine/Social-Distancing Monitoring

In this epidemic control measure, it is determined that whether people are properly practicing self-quarantine or not. The reason behind monitoring self-quarantine is to preserve violations or non-compliance, which may spread the virus to the community [27,28]. During this pandemic times, the quarantine/social-distancing monitoring remains the main focus of the health authorities. With the help of the quarantine/social-distancing monitoring, many countries effectively controlled this pandemic [29].

3.2.1. Data in Loop

There exist plenty of ways to monitor people's compliance with the quarantine/social-distancing measure. The types of data processed and used for the quarantine/social-distancing purposes is, (i) mobile phone signals data, (ii) real time location data by calling, (iii) cellular networks data, (iii) CCTV footage for wear/non-wearing masks analysis, and (iv) certificates for obtaining the facilities visited by a person etc. Furthermore, transport usage data and flow modeling is also used to analyze the people movements and compliance with the epidemic control measure.

3.2.2. Likely Privacy Concerns/Issues in the Control Measure

The likely privacy problems in this control measure are, (i) trajectory disclosure, (ii) sensitive places visits disclosure, (iii) stay points (e.g., tobacco shops or other controversial places etc.) disclosures, (iv) mobility disclosures, (v) identity disclosure, and (vi) travel data disclosure. All these concerns can occur in the quarantine/social-distancing monitoring measure when it is carried out with the help of technical solutions.

3.2.3. Latest Technologies/Solutions Devised so far to Alleviate Privacy Concerns/Issues

The most famous and practical solutions is the quarantine/social-distancing monitoring via home quarantine [30]. In such a way, the movement data are not collected/processed thereby result in privacy preservation of individuals. The other notable solutions that have demonstrated effectiveness in terms of privacy are, clustering events without proximity detection [31], voluntary reduction of social activities [32], and lowering the contact rate [33]. All these solutions have demonstrated effectiveness for preserving people's privacy. Despite the success of such solutions, the user's willingness to wear bands or use certificates for the location data provision remained low due to the privacy concerns. Therefore, numerous efforts are underway to devise and implement anonymized solutions across the globe for quarantine/social-distancing monitoring.

3.3. Disclosing Information of Confirmed Cases of COVID-19

In this epidemic control measure, the information of individuals who have tested +ve for the COVID-19 is shared with the public for immediate isolation/testing of the close contact [34]. In this measure, the degree of information varies across the countries. For instance, in South Korea, the complete location information and demographics information is also released. Furthermore, temporal information and mask status is also published for the people's awareness [35]. Many studies reported that people with individualistic orientation are less likely to consider the control measures acceptable because they have higher privacy concerns and lower perceptions of the social benefits.

3.3.1. Data in Loop

The types of data processed and used for the disclosing information of confirmed cases of COVID-19 is, (i) facilities he/she visits, (ii) temporal information of visits, (iii) activities data (meeting/food), (iii) demographics (mainly age and gender), and (iv) description about the transport (public/local) and mask wearing/not-wearing status etc. Furthermore, the close contacts information is also published sometime to find the suspects.

3.3.2. Likely Privacy Concerns/Issues in the Control Measure

The likely privacy problems in this control measure are, (i) identity disclosure, (ii) sensitive places visits disclosure, (iii) attribute disclosure, (iv) activities disclosure, and (v) temporal based activities disclosure. In some cases, the healthcare authorities publish the status of patient as a super spreader which results into defamation, hates, and discrimination etc. All these concerns can occur in while disclosing the information of patients for public's well being.

3.3.3. Latest Technologies/Solutions Devised so far to Alleviate Privacy Concerns/Issues

The most famous and practical solutions is the disclosing patients information via user-centered privacy controls [36]. By using this method, users have strong control over their personal information and effective transparency on how their data are handled. These systems provide protections of the civil liberties and are respectful of social norms. The other notable solutions that have demonstrated effectiveness in terms of privacy preservation are, information communication technologies [37], legal construction of the privacy [38], adoption of the latest technologies [39], and geospatial technologies [40]. All these solutions have demonstrated effectiveness for preserving people's privacy when data are distributed for analysis or determining the probability of exposure. Despite the success of such solutions, the user's privacy breaches can occur through data correlation and auxiliary information [41].

3.4. Symptoms and Other Data Reporting to Health Authorities

In some countries, symptoms (e.g., fever, muscle pain, and runny nose etc.) and other valuable data (e.g., travel visit in last 14 days, visit to an exposed facility, history of diagnosis with COVID-19, and contact with a confirmed patient etc.) is reported to health authorities on daily basis. This tremendous amount of data is usually stored in a centralized server consequently privacy issues can occur frequently. Hence, there are many developments underway to gather data about individuals for better handling of this pandemic [42]. Due to the industrial development, wearable sensor and related technologies are effectively contributing in symptoms reporting and managing the disease [43,44]. Furthermore, the latest technologies such as deep learning (DL) has also been effectively applied on the user's generated/reported data for the diagnosis of COVID-19 in recent times [45]. These technologies have assisted in detecting pre-symptomatic patients to reduce the healthcare workers burden significantly [46–48]. Due to effective utilizing these latest technologies, the disease's transmission can be reduced and healthcare workers' burden can be lowered in unprecedented times.

3.4.1. Data in Loop

The types of data processed and used for the symptoms and other data reporting purposes can be classified into two categories. The first category is about symptoms data collection/reporting which includes, (i) fever readings, (ii) breathing patterns (e.g., oxygen levels), (iii) heart beat, (iii) muscle pain, (iv) headache, and other useful data that can depict the buildup of the COVID-19. Furthermore, the location information can also be reported for curbing the disease spread or keeping people away from the hotspots. The second category is about other useful data collection/reporting which includes, (i) demographics (name, workplace, job type, and cell phone number etc), (ii) travel history of past 14 days, (iii) visit to some contaminated place/facility, (iv) contact with confirm/exposed person,

and (v) whether some is at stay at home order or not. These data are collected and processed for handling the epidemic. In addition, the physical activities data and nature of the work is also monitored continuously to effectively control the disease [49]. Recently, methods that can exploit the power of both wearable devices and mobile technology have become an effective solution to handle the epidemic [50].

3.4.2. Likely Privacy Concerns/Issues in the Control Measure

The likely privacy problems in this control measure are, (i) movement tracking, (ii) identity and attribute disclosure by correlating relationships between buying habits and health, (iii) location disclosure, (iv) physical activities disclosure, and (v) sensitive diseases disclosure (e.g., underlying conditions). In some cases, the healthcare authorities publish the location trail of carrier that in turn can expose the group privacy. All these concerns can occur collecting/reporting the information of patients for public's well being through forms or wearable devices. The disclosure of the people's privacy through body sensors data and other reporting services may cause the humiliation/embarrassment to the patient if a data manipulation occurs. Hence, the infrastructure/systems designer need to pay special attention to these privacy problems and embed the privacy enhancing technologies while designing the systems.

3.4.3. Latest Technologies/Solutions Devised so far to Alleviate Privacy Concerns/Issues

The most famous and practical solutions is the symptoms and other data reporting to health authorities via anonymised sensor data [51]. By using this method, many operations related to the public health emergency surveillance can be performed in a privacy preserving manner. This system provides nationwide surveillance of the infectious diseases. The other notable solutions that have demonstrated effectiveness in terms of privacy protection are, digitally controlled health management system [52], privacy-aware energy-efficient framework (P-AEEF) protocol [53], spatio-temporal trajectory approaches with privacy [54], encryption mechanisms [55], and surveillance system [56]. All these solutions have demonstrated effectiveness for preserving people's privacy when data are collected/reported by the users for analysis or determining the probability of exposure. Despite the success of such solutions, the user's hesitation regarding their privacy manipulations remains vigilant during recent times [57].

3.5. Basic Data (E.G, Demographics) Collection at the Time of Both Voluntarily and Involuntarily Checkups

In this epidemic control measure, basic data (e.g, demographics) about the individuals are collected at the time of both voluntarily and involuntarily checkups [58]. This data assist in analyzing the causes of the spread as well as the estimation of lethality of the virus for different age-groups [59]. The collected data can be used for diverse objectives including recommendation or guidelines for preventive steps. For instance, it can be used to find the contacts of confirmed patients or it can be used for measuring the infections' risk based on the age/gender. Anna et al. [60] highlighted the changes in health behaviors of the Canadian adults based on demographics during the pandemic times. Thomas et al. [61] analyzed the suicide trends during the COVID-19 times based on demographics.

3.5.1. Data in Loop

The types of data processed and collected at the time of the checkup is, (i) patient ID, (ii) gender, (iii) age, (iv) race, (v) visit date, (vi) symptoms that he/she is experiencing, (vii) other biomedical parameters, (viii) travel data, (ix) zipcode, (x) profession, (xi) job nature, and (xii) other disease information etc. Furthermore, in some cases, the data is collected via digital solution in multiple times for better diagnosis [62]. These data can be used for range of services/applications including clinical decision support, disease surveillance, analytics, health insurance, and population health management.

3.5.2. Likely Privacy Concerns/Issues in the Control Measure

The likely privacy problems in this control measure are, (i) identity disclosure, (ii) sensitive attribute disclosure, (iii) location disclosure, (iv) membership disclosure, and (v) trajectories disclosures. In some cases, the healthcare authorities publish the data that in turn can expose the group privacy. Furthermore, as majority of the data is stored in a centralized server thereby hacking/theft can likely occur that can result into range of negative consequences on people's life [63]. Hence, many efforts are underway to collect and process users data with privacy guarantees [64].

3.5.3. Latest Technologies/Solutions Devised so far to Alleviate Privacy Concerns/Issues

The most famous and practical solution is the Basic data (e.g., demographics) collection via privacy preserving healthcare informatics that uses state-of-the-art privacy-enhancing methods [65]. By using this method, privacy violations can be reduced in a fine grained manner. The other notable solutions that have demonstrated effectiveness in terms of privacy preservation are, adaptive differential privacy algorithm [66], differential privacy approach [67], HealthyBlock-based approach for privacy preservation [68], federated learning [69], and privacy-preserving (PP) distributed learning techniques [70]. All these solutions have demonstrated effectiveness for preserving people's privacy when data are collected at the time of diagnosis/treatment.

3.6. Collected Data Analytics/Mining for Insights Finding

In this epidemic control measure, the collected data are analyzed to effectively tackle the pandemic as a proactive measure. The analytics/mining on the collected data for insights finding can assist in response planning and accurate estimation of disease virulence. Many modern technologies such as AI, big data, deep learning, federated learning, block chain, and confidential computing have demonstrated effectiveness for mitigating COVID-19 pandemic [71]. These technologies have enormous potential for analyzing the situation of COVID-19 in future based on the analysis of collected data. For example, AI and Big Data can be employed to track the virus's spread in real time, and plan/lift public health interventions accordingly, analyze their effectiveness, drugs re-purposing, as well as determine likely vaccine candidates and enhance the response of territories and communities to the ongoing epidemic [72]. Furthermore, the machine learning methods have demonstrated effectiveness in COVID-19's diagnosis (e.g., dissemination patterns analysis, cases classifications, and predictions etc.) [73]. During the pandemic times, AI has proven a powerful tool for public health authorities to mitigate the disease spread and building resilience against it [74–77].

3.6.1. Data in Loop

The types of data processed and used at the time of analytics/mining are, (i) medical images [78], (ii) cases data, (iii) locations/trajectories data, (iii) temporal data, (iv) IoT devices data, (v) social network/media data, (vi) flow graphs, (vii) social relations/interactions data, (viii) demographics, (ix) diseases and drugs data, (x) mobile phones data including apps and signals, (xi) internet data, (xii) facilities data, (xiii) purchases history, (xiv) religious activities, (xv) spatio-temporal trajectories, and (xvi) e-commerce data, to name a few. Furthermore, data are fused from the heterogeneous sources for actionable insights and desirable computations [79–81].

3.6.2. Likely Privacy Concerns/Issues in the Control Measure

The likely privacy problems in this control measure are, (i) identity/attribute/ membership disclosures, (ii) sensitive pattern derivation, (iii) mobility disclosure, (iv) association rule mining, (v) profiling, (vi) community privacy disclosure, (vii) sensitive/controversial places visit disclosure, (viii) activities disclosure, (ix) buying pattern disclosures, (x) location tapping, (xi) browsing behavior disclosure, (xii) stay points disclosure, (xiii) residence disclosure, (xiv) workplace/profession disclosure, (xv) political/religious beliefs

disclosures, (xvi) travel details disclosures, (xvii) facial recognition and gender disclosure, (xviii) medical history disclosure, (xix) group identity theft, and (xx) disease predictions/aggregations, to name a few. Due to massive data processing, majority of the privacy problems listed in Figure 1 can occur during collected data analytics/mining. Due to multiple privacy issues in the COVID-19 related data analytics/mining, policy makers and developers are exploring many way to effectively safeguard user's privacy.

3.6.3. Latest Technologies/Solutions Devised so far to Alleviate Privacy Concerns/Issues

The most famous and practical solutions in the collected data analytics/mining for insights finding is multi-pronged approach [82]. By using this method, health-relevant data is protected from privacy violations and can only be used in a privacy preserving manner. The other notable solutions that have demonstrated effectiveness in terms of privacy are, general data protection regulation (GDPR)-based computation [83], privacy-aware personalized information retrieval (PAPIR) method [84], privacy preserving data visualizations (PPDV) method [85], spatial k -anonymity method [86], and privacy preserving location-based services (LBS) method [87]. All these solutions have demonstrated effectiveness for preserving people's privacy when analytics/mining is performed on the collected data. Despite the success of such solutions, advanced solutions with privacy guarantees are paramount [88].

3.7. *Diagnosis/Tests Data (E.G., Electronic Health Records (Ehr)) Sharing with the Researchers for Secondary Use*

In this control measure, the collected/stored data (e.g., electronic health records (EHR)) is shared with the researchers for better understanding of the disease variants, and possible treatments. The EHRs are highly valuable for understanding the characteristics of the disease, and possible mitigation measures [89]. For instance, in COVID-19's context, the data sharing can assist in ranking the diseases which when combine with COVID-19 disease increase the mortality rates or EHRs can be utilized to predict the mortality rates [90,91]. Furthermore, the EHRs assist in analyzing the dynamics of newly emerging infectious diseases. Apart from such a helpful benefits, the EHRs can assist in performing demographic-based studies and diseases correlations for better handling of the diseases. Data sharing is paramount for handling any disease effectively, and EHRs are mainly shared in an anonymized form to preserve individuals' privacy.

3.7.1. Data in Loop

The types of data processed and shared in handling of the epidemics in an effective manner are, (i) medical images, (ii) test data, (iii) demographics data, (iii) diseases data, (iv) clinical trials data, (v) multiple diseases data, (vi) symptoms data, (vii) clinical parameters' data, (viii) finances and workplaces data, (ix) drugs' effectiveness data, (x) medical history (e.g., hospital visit dates, discharge summaries, clinical notes, and bills etc.), and (xi) diseases' origin etc., to name a few. Furthermore, in some cases, heterogeneous data are collected and shared for modeling the causes of diseases or factor analysis.

3.7.2. Likely Privacy Concerns/Issues in the Control Measure

The likely privacy problems in this control measure are, (i) identity/attribute/ membership disclosures, (ii) sensitive business pattern extraction, (iii) group identity theft, (iv) association rule mining, (v) unsuspected people's profiling, (vi) workplace/profession disclosure, (vii) political/religious beliefs disclosures, (viii) medical history disclosure, (ix) disease predictions, and (x) disease predictions/aggregations, to name a few. Due to massive data processing, majority of the general privacy problems listed in Figure 1 can occur during published data analytics.

3.7.3. Latest Technologies/Solutions Devised so far to Alleviate Privacy Concerns/Issues

The most famous and widely used solutions in the privacy protection in data publishing is anonymization [92]. By using this method, data is shared with the data-miners without compromising individual's privacy while knowledge is preserved in the published data [93]. The other notable solutions that have demonstrated effectiveness in terms of privacy in data publishing are, pseudonymization [94], privacy preservation leveraging machine learning models [95], data driven anonymization system [96,97], cyber security mechanisms [98], and non-cryptographic anonymization techniques [99]. All these solutions have demonstrated effectiveness for preserving people's privacy when data is published for research/innovation purposes. Despite the success of such solutions, advanced solutions with privacy guarantees are paramount, and research is underway for innovation solutions [100,101].

4. Brief Insights on Data Management in the Epidemic Control Measures with Privacy Guarantee

In Section 3, we provided detailed insight on the privacy issues that arise in epidemic control measures adopted by many countries across the globe to curb the COVID-19's spread by processing sensitive data. We noticed that in most epidemic control measures, the locations data were mostly collected and processed for finding the suspected cases that was rarely collected/processed before COVID times. In addition, each country adopted unique solutions to curb the spread and lower the healthcare workers. For instance, South Korea adopted heterogeneous sources data (e.g., credit card data, CCTV footage, and mobile phones' signals data) to find the potential cases that spark the criticism from most citizens due to privacy violations. Apart from South Korea, the no. of privacy violations in the healthcare sector related to individuals and organizations were 2X in Italy in the first four months of 2020. These privacy violations need robust, scalable, and correct algorithms/methodologies to address privacy concerns [102]. Furthermore, utilization of the security and privacy (SP) patterns in all phases of the data handling is of paramount to alleviate privacy concerns [103].

In addition, the trajectory data utilization with privacy preservation has become an active area of research in recent years [104]. Considering the diverse sources of the data (e.g., location data, trajectories data, demographics data, and medical images etc.), specific algorithms are needed to effectively resolve the individual's privacy issues. We present the taxonomy of privacy preservation in epidemic control measures in Figure 4. In Figure 4, we mainly discuss the common five phases (e.g., collection, storage, analytics, use, and removal) of the each epidemic control measure (ECM), provide the privacy implications/requirements in each phases of the ECM, the current solution in place to protect people's privacy in ECMs, and way forward (e.g., future technologies needed to fight with infectious diseases). With this comprehensive overview of the ECMs, the research gaps/directions can be identified to secure future systems and privacy issues. Moreover, the mechanism for data destruction/removal are still in early stage which needs better exploration [105].

The future technologies should focus more on the geospatial data masking to effectively preserve people's privacy. The important research direction is to preserve people's privacy in heterogeneous sources data fusion [106]. Since, fusing multiple and heterogeneous sources data can assist in impacting group privacy along with an individual's privacy which has a range of negative consequences. with the proliferation of data acquisition sources and big data technologies, the privacy issues are emerging in unique ways, and are much larger scale compared to recent past. Therefore, plenty of solutions are being devised/proposed to effectively address the privacy challenge across the globe during these pandemic times. In future, to increase adoption of the digital solutions, privacy needs to be embedded in the design of each ECMs. This will augment people's trust to use digital solutions for long time thereby assist in controlling disease's spread.

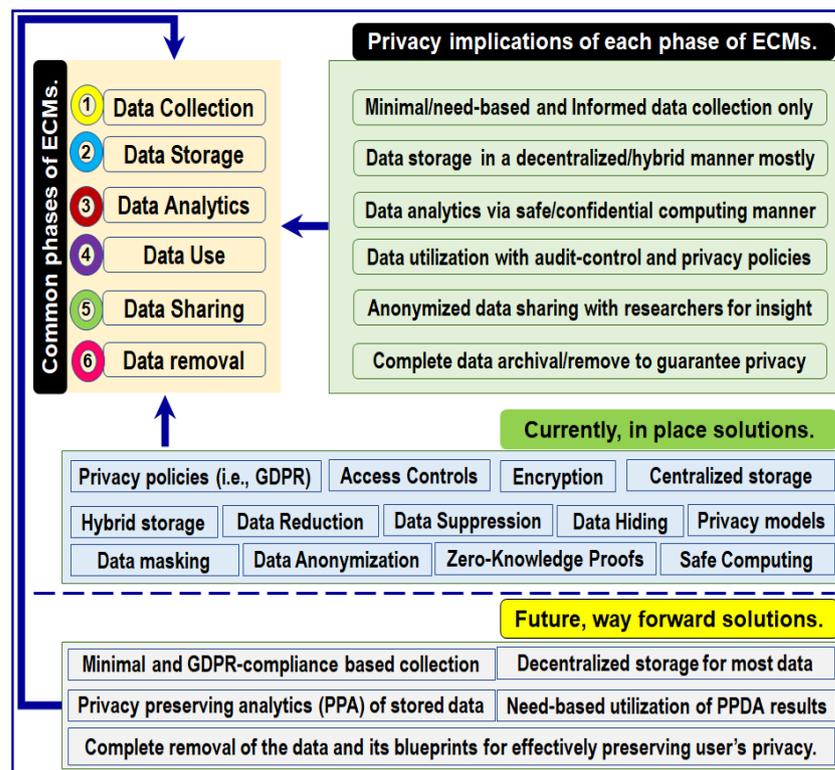


Figure 4. Overview of the taxonomy of privacy preservation in epidemic control measures, present solutions and way forward (future solutions).

5. Prospects of the Research in Privacy Area Tacking into Account the Current Emerging Technologies

The future of healthcare is likely to be more digital-oriented, and recognizing the essence of digitization in this field for the pandemic preparedness planning has become inevitable. There is a need of long-term partnership between technology companies and hospitals for handling future pandemics. Hence, the digital technologies need to strengthen pandemic management, response, resilience, mitigation, and future preparedness for COVID-19 and many other infectious diseases. The digital technologies have enormous potential to fight with the infectious diseases. However, the privacy issues hinder the adoption of such technologies thereby grave situations can occur. In addition, due to diverse formats of data and privacy implications, the reliance on one solution is inadequate. We describe, prospects of the research in privacy area tacking into account the current emerging technologies advantages in Figure 5. The challenges described in Figure 5 affect the utility of the digital solution and make them less effective due to privacy issues.

The emerging concept of mobile phone utilization to fight with the pandemic has gained popularity across the globe. This enabled the effective contact tracing, proximity analysis, and alerts for avoiding high risk zones. In addition, it has resolved the most of privacy problems that can emerge when data is stored at the centralized server. In future, it is expected that this trend of performing most of the computation at the client side will likely to grow. Therefore, the privacy analysis in this setting, and pertinent mechanism to keep most of the sensitive information on user own mobile devices will be an attractive area of research. The collection of the location information on the mobile phones can assist in protecting against the unsuspected surveillance and privacy issues. Despite, the success of such methods, the implementation and protection from the privacy issues will be longstanding challenge. Beside this digital innovation, the hardware challenges of cell-phone such as limited storage, communication costs, battery issues, and data theft/loss will significantly impact the utilization of this technology during pandemic times.

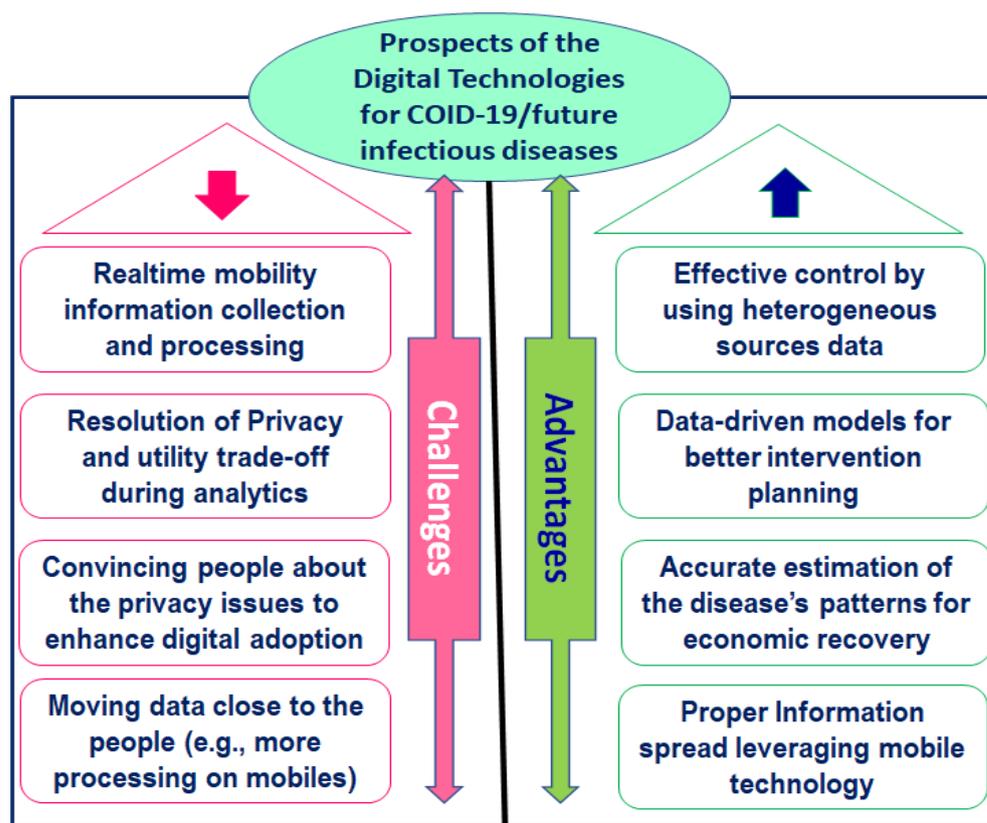


Figure 5. Prospects of the research in privacy area tacking into account the current emerging technologies advantages.

Apart from the success of current solutions, the future solutions should focus more on less and relevant data collection, differentiating between sensitive and non-sensitive data, storing most of the sensitive data on user’s own cell-phones, performing analytic on safe manner (mostly on user’s devices), and utilizing results with standards and privacy policies, and remove data after certain time-period. Apart from these things, analyzing and collecting data that can assist in lowering the spread rates, mortality rates, and ICU admittance etc. is of supreme importance. Apart from the unique characteristics of the future systems stated above, the processing of massive data including temporal activities of users and location data have raised technical challenges for the software developer. From the theoretical point of view, analyzing all situations for computing the exposure probability is non-trivial task. To address, these challenges, future systems should focus more on the multi varied types data processing and analytic. The individual’s Privacy need to be maintained in all phases from collection to archival phases to get higher adoption of the digital solution thereby effective pandemic’s control.

To highlight the significance of the presented concepts, we compared the proposed study results with five existing and closely related studies such as Sun et al. [13], Chan et al. [16], Kim et al. [18], Wang et al. [41], and Shin et al. [93]. All these studies have provided the privacy related issues and emerging solutions for the ongoing pandemic. Meanwhile, the proposed study provides more comprehensive coverage of the privacy topic considering main shift in privacy paradigm that collect/process location data, persona data items (e.g., demographics, credit card usage data, and logs etc.), emerging digital solutions, and technical factors that add vulnerability to user’s privacy. We compared the effectiveness of the proposed study with the existing studies in terms of the coverage of the epidemic control measures, privacy implications, items of the personal data discussed, emerging privacy solutions in the context of COVID-19, and general comparisons including privacy protection rules discussion, technical factors related discussion, and privacy description in five phases of data life cycle. The results of comprehensive comparisons with existing studies are shown in Table 1.

Table 1. Comprehensive comparisons with the existing and related studies.

Category	Description of the Category Category Items	Comparisons with Existing Studies					Proposed Study
		Sun et al. [13]	Chan et al. [16]	Kim et al. [18]	Wang et al. [41]	Shin et al. [93]	
Epidemic control measures	Contact tracing	x	✓	✓	✓	x	✓
	Quarantine monitoring	✓	x	✓	x	x	✓
	Disclosing COVID+ Information	x	x	✓	x	x	✓
	Symptoms/data reporting	✓	x	x	x	x	✓
	Checkup data collection	✓	x	x	x	x	✓
	Collected data analytics	x	✓	x	✓	✓	✓
	Data distribution with analysts	✓	x	x	✓	✓	✓
Privacy implications	General implications (IoT + healthcare)	x	x	x	x	x	✓
	COVID-19 specific implications	✓ (brief)	✓ (brief)	✓ (detailed)	✓ (brief)	✓ (brief)	✓ (comprehensive)
Personal data's item discussed	Demographics	✓	✓	✓	✓	✓	✓
	Mobility/trajectory data	✓	✓	✓	✓	x	✓
	cellular network data	x	x	✓	x	x	✓
	mobile apps data	x	x	✓	x	x	✓
	symptoms data	✓	x	✓	✓	x	✓
	COVID-19 cases data	✓	x	✓	✓	x	✓
	comorbidity data	✓	x	x	✓	✓	✓
	buying patterns data	x	x	✓	✓	x	✓
	CCTV data	x	x	x	x	x	✓
	Credit card usage data	x	x	x	x	x	✓
	IoT devices data	✓	x	✓	✓	x	✓
Stay points data	x	x	x	✓	✓	✓	
Emerging privacy solutions' discussion	Blockchain Technology	x	x	x	x	x	✓
	Encryption	x	✓	x	x	✓	✓
	Anonymization	x	x	✓	✓	✓	✓
	Deep/Machine Learning	✓	✓	x	x	x	✓
General comparisons	Technical factors discussion	✓	✓	✓	x	x	✓
	GDPR/PIPA discussion	x	x	x	x	✓ (PIPA)	✓ (GDPR)
	privacy analysis in phases of data life cycle	✓ (3 only)	✓ (3 only)	✓ (4 only)	✓ (3 only)	✓ (2 only)	✓ (all Six)

Through comprehensive comparison with related studies as given in Table 1, it can be observed that proposed study covers many aspects of the privacy in COVID-19's context. Furthermore, the proposed study discusses the privacy issues in all phases of data life cycle and all ECMs that are not comprehensively covered by the existing studies. These results verify the essence of proposed study. In order to highlight the significance of this article to readers or for applications, we identify 10 actors and provide this article's significance to them in Table 2. Through this brief description, we aim to highlight helpful knowledge/significance of subject matter presented in this study for different actors.

Table 2. Significance of the proposed study for different actors.

Sr. No.	Actors	Proposed Study's Significance for Each Actor
1.	Users (record owners)	Provide understanding about what constitute in his/her privacy and how to protect it effectively.
2.	Data owners/holders	Provide the comprehensive overview of privacy concerns and enables them to plan/develop more secure methods.
3.	Researchers/data analyst	To get the knowledge of current modalities used in this pandemic and research gaps for proposing better methods.
4.	Data publisher	To plan about the data sharing at a larger scale for data mining and research purposes without privacy issues.
5.	Policy makers	To plan/suggest better pandemic information/handling systems to alleviate people's anxiety while providing data.
6.	Developers	To develop systems/software in which privacy is used as a proactive measure not reactive to gain people's trust.
7.	Health authorities	To devise methods for collecting data for which people has less privacy concerns, and controlling data manipulations.
8.	Governments	To use people data for the intended purpose and plan the interventions for which people willingness is high regarding data provision.
9.	Applications	From applications point of view the apps that are currently working for the tracing/monitoring can be made more privacy preserving.
10.	Third-party apps	The privacy and corresponding data items that jeopardize someone privacy must be identified and protected in data exchange/use.

6. Conclusions and Future Work

This paper explains the shift in privacy paradigm due to the pandemic (e.g., COVID-19) which involves more and detailed data collection about individuals' activities, locations, buying patterns, and mobility/trajectories etc. The main goals of the proposed research are to provide a compact review of the digital solutions employed by the health authorities to tackle the challenge of the COVID-19 and their privacy implications. Furthermore, we explain technical factors due to which the people's privacy is at higher risk in the COVID-19 time. We explained the privacy concerns in different epidemic control measures employed by the health authorities to tackle this disease taking relevant data types in loop. Further, we provide a brief insight on the data management in the epidemic control measure with privacy protection. We explained the technical challenges and implications that are arising in COVID-19 times due to heterogeneous data collection and processing. Finally, the future prospects of the research in this area tacking into account the emerging technologies are discussed. To the best of our knowledge, this is the first work that provides a brief and concise perspective on the privacy topic in COVID-19 context. In future, we planned to explore the privacy issues of the systems that harness locations data and wearable devices data. We intend to study the people's orientation and privacy concerns of different nations to better understand the privacy area. Finally, analyzing the social networks data as a supportive tool to fight with infectious diseases and highlighting privacy issues in it is another important extension of the presented work. In recent years, there's an increasing focus on the rapid development of more practical privacy preserving solutions leveraging industry 4.0 technologies (e.g., block chain, smart contracts, federated learning, and few short learning etc.). Hence, describing all these technologies essence in the pandemic situations is a promising avenue for future research.

Author Contributions: Conceptualization: A.M. and S.L.; writing, data curation, methodology: A.M.; resources, supervision, project administration, funding acquisition: S.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by National Research Foundation of Korea (NRF) Grant funded by the Korean Government (Ministry of Science and ICT) NRF-2020K1A3A1A47110830.

Acknowledgments: The authors would like to thank the editor and reviewers for their insightful comments and valuable suggestions, which helped improve the paper significantly.

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

References

1. Xu, L.; Jiang, C.; Wang, J.; Yuan, J.; Ren, Y. Information Security in Big Data: Privacy and Data Mining. *IEEE Access* **2014**, *2*, 1149–1176. [[CrossRef](#)]
2. Landau, O.; Cohen, A.; Gordon, S.; Nissim, N. Mind your privacy: Privacy leakage through BCI applications using machine learning methods. *Knowl. Based Syst.* **2020**, *198*, 105932. [[CrossRef](#)]
3. Bleier, A.; Goldfarb, A.; Tucker, C. Consumer privacy and the future of data-based innovation and marketing. *Int. J. Res. Mark.* **2020**, *37*, 466–480. [[CrossRef](#)]
4. Kannan, P. Introduction to the Special Section: Research for the New Normal. *Int. J. Res. Mark.* **2020**, *37*, 441–442. [[CrossRef](#)]
5. Aloui, A.; Okba, K. A Survey on Privacy Preservation in Location-Based Mobile Business: Research Directions. *Int. J. Web Portals (IJWP)* **2021**, *13*, 20–39. [[CrossRef](#)]
6. Yin, C.; Shi, L.; Sun, R.; Wang, J. Improved collaborative filtering recommendation algorithm based on differential privacy protection. *J. Supercomput.* **2019**, *76*, 5161–5174. [[CrossRef](#)]
7. Rob, K. Using digital technologies to tackle the spread of the coronavirus: Panacea or folly. *Program. City Work. Pap.* **2020**, *44*, 1–24.
8. He, W.; Zhang, Z.; Li, W. Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic. *Int. J. Inf. Manag.* **2021**, *57*, 102287. [[CrossRef](#)]
9. Maytin, L.; Maytin, J.; Agarwal, P.; Krenitsky, A.; Krenitsky, J.; Epstein, R.S. Attitudes and Perceptions Toward COVID-19 Digital Surveillance: Survey of Young Adults in the United States. *JMIR Form. Res.* **2021**, *5*, e23000. [[CrossRef](#)]
10. Kim, J.; Ohbyung, K. A Model for Rapid Selection and COVID-19 Prediction with Dynamic and Imbalanced Data. *Sustainability* **2021**, *13*, 3099. [[CrossRef](#)]
11. Subbian, V.; Solomonides, A.; Clarkson, M.; Rahimzadeh, V.N.; Petersen, C.; Schreiber, R.; DeMuro, P.R.; Dua, P.; Goodman, K.W.; Kaplan, B.; et al. Ethics and informatics in the age of COVID-19: Challenges and recommendations for public health organization and public policy. *J. Am. Med. Inform. Assoc.* **2021**, *28*, 184–189. [[CrossRef](#)]
12. Pee, L.; Pan, S.L.; Wang, J.; Wu, J. Designing for the future in the age of pandemics: A future-ready design research (FRDR) process. *Eur. J. Inf. Syst.* **2021**, 1–19. [[CrossRef](#)]
13. Sun, S.; Xie, Z.; Yu, K.; Jiang, B.; Zheng, S.; Pan, X. COVID-19 and healthcare system in China: Challenges and progression for a sustainable future. *Glob. Health* **2021**, *17*, 1–8. [[CrossRef](#)]
14. Wu, T. The socioeconomic and environmental drivers of the COVID-19 pandemic: A review. *Ambio* **2021**, *50*, 822–833. [[CrossRef](#)]
15. Marabelli, M.; Vaast, E.; Li, J.L. Preventing the digital scars of COVID-19. *Eur. J. Inf. Syst.* **2021**, 1–17. [[CrossRef](#)]
16. Chan, E.Y.; Saqib, N.U. Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. *Comput. Hum. Behav.* **2021**, *119*, 106718. [[CrossRef](#)]
17. Eames, K.T.D.; Keeling, M.J. Contact tracing and disease control. *Proc. R. Soc. London. Ser. B Biol. Sci.* **2003**, *270*, 2565–2571. [[CrossRef](#)] [[PubMed](#)]
18. Kim, J.; Kwan, M.-P. An Examination of People’s Privacy Concerns, Perceptions of Social Benefits, and Acceptance of COVID-19 Mitigation Measures That Harness Location Information: A Comparative Study of the U.S. and South Korea. *ISPRS Int. J. Geo-Inf.* **2021**, *10*, 25. [[CrossRef](#)]
19. Lunz, D.; Batt, G.; Ruess, J. To quarantine, or not to quarantine: A theoretical framework for disease control via contact tracing. *Epidemics* **2021**, *34*, 100428. [[CrossRef](#)] [[PubMed](#)]
20. Johannes, M.; Kretschmar, M. Contact tracing—Old models and new challenges. *Infect. Dis. Model.* **2021**, *6*, 222–231.
21. Wen, H.; Zhao, Q.; Lin, Z.; Xuan, D.; Shroff, N. A Study of the Privacy of COVID-19 Contact Tracing Apps. In *International Conference on Security and Privacy in Communication Systems*; Springer: Cham, Switzerland, 2020; pp. 297–317.
22. Michael, V. Privacy Is Not the Problem with the Apple-Google Contact-Tracing Toolkit. *The Guardian*, 1 July 2020.
23. Klaine, P.V.; Zhang, L.; Zhou, B.; Sun, Y.; Xu, H.; Imran, M. Privacy-Preserving Contact Tracing and Public Risk Assessment Using Blockchain for COVID-19 Pandemic. *IEEE Internet Things Mag.* **2020**, *3*, 58–63. [[CrossRef](#)]
24. Xu, H.; Zhang, L.; Onireti, O.; Fang, Y.; Buchanan, W.J.; Imran, M.A. BeepTrace: Blockchain-Enabled Privacy-Preserving Contact Tracing for COVID-19 Pandemic and Beyond. *IEEE Internet Things J.* **2021**, *8*, 3915–3929. [[CrossRef](#)]
25. Demirag, D.; Ayday, E. Tracking the Invisible: Privacy-Preserving Contact Tracing to Control the Spread of a Virus. In *Lecture Notes in Computer Science*; Springer: Cham, Switzerland, 2020; pp. 240–249.
26. Wan, Z.; Liu, X. *ContactChaser: A Simple Yet Effective Contact Tracing Scheme with Strong Privacy*; Report 2020/630; Cryptology ePrint Archive: Washington, DC, USA, 2020.
27. Suppawattaya, P.; Yiemphat, P.; Yasri, P. Effects of social distancing, self-quarantine and self-isolation during the COVID-19 pandemic on people’s well-being, and how to cope with it. *Int. J. Sci. Healthc. Res.* **2020**, *5*, 12–20.
28. Taiwo, O.; Ezugwu, A.E. Smart healthcare support for remote patient monitoring during covid-19 quarantine. *Inform. Med. Unlocked* **2020**, *20*, 100428. [[CrossRef](#)]
29. Kaur, A.; Mittal, N.; Khosla, P.K.; Mittal, M. Machine Learning Tools to Predict the Impact of Quarantine. In *Predictive and Preventive Measures for Covid-19 Pandemic*; Springer: Singapore, 2021; pp. 307–323.
30. Gietl, S.; Schönegger, C.M.; Falk, M.; Weiler, S.; Obererlacher, S.; Jansen, B.; Sonnleitner, S.-T.; Walder, G. Home quarantine in COVID-19: A study on 50 consecutive patients in Austria. *Clin. Med.* **2021**, *21*, e9–e13. [[CrossRef](#)]

31. Syverson, P. *Privacy-Protecting COVID-19 Exposure Notification Via Cluster Events Without Proximity Detection*; NIST Workshop: Challenges for Digital Proximity Detection in Pandemics: Privacy, Accuracy, and Impact; NIST: Boulder, CO, USA, 2021.
32. Aum, S.; Lee, S.Y.; Shin, Y. Inequality of fear and self-quarantine: Is there a trade-off between GDP and public health? *J. Public Econ.* **2021**, *194*, 104354. [[CrossRef](#)]
33. Milenkovic, A.; Dragan, J.; Petar, R. Extensions and adaptations of existing medical information system in order to reduce social contacts during COVID-19 pandemic. *Int. J. Med. Inform.* **2020**, *141*, 104224. [[CrossRef](#)] [[PubMed](#)]
34. Her, M. How Is COVID-19 Affecting South Korea? What Is Our Current Strategy? *Disaster Med. Public Health Prep.* **2020**, *14*, 684–686. [[CrossRef](#)]
35. Weinstein, B.; Da Silva, A.R.; Kouzoukas, D.E.; Bose, T.; Kim, G.-J.; Correa, P.A.; Pondugula, S.; Lee, Y.; Kim, J.; Carpenter, D.O. Precision Mapping of COVID-19 Vulnerable Locales by Epidemiological and Socioeconomic Risk Factors, Developed Using South Korean Data. *Int. J. Environ. Res. Public Health* **2021**, *18*, 604. [[CrossRef](#)]
36. Sharma, T.; Hunter, A.D.; Masooda, B. Enabling User-centered Privacy Controls for Mobile Applications: COVID-19 Perspective. *ACM Trans. Internet Technol. (TOIT)* **2021**, *21*, 1–24. [[CrossRef](#)]
37. Paek, H.-J.; Hove, T. Information Communication Technologies (ICTs), Crisis Communication Principles and the COVID-19 Response in South Korea. *J. Creative Commun.* **2021**. [[CrossRef](#)]
38. Kui, S. The Stumbling Balance between Public Health and Privacy amid the Pandemic in China. *Chin. J. Comp. Law* **2021**. [[CrossRef](#)]
39. Abir, S.M.; Islam, S.N.; Anwar, A.; Mahmood, A.N.; Oo, A.M.T. Building Resilience against COVID-19 Pandemic using Artificial Intelligence, Machine Learning, and IoT: A Survey of Recent Progress. *IoT* **2020**, *1*, 506–528. [[CrossRef](#)]
40. Iyer, R.; Regina, R.; Kevin, P.M.; Darshan, G.; Aryan, M.; Abhishek, S.; Ramesh, R. Spatial K-anonymity: A Privacy-preserving Method for COVID-19 Related Geospatial Technologies. *arXiv* **2021**, arXiv:2101.02556.
41. Wang, J. An In-depth Review of Privacy Concerns Raised by the COVID-19 Pandemic. *arXiv* **2021**, arXiv:2101.10868.
42. Drew, D.A.; Nguyen, L.H.; Steves, C.J.; Menni, C.; Freydin, M.; Varsavsky, T.; Sudre, C.H.; Cardoso, M.J.; Ourselin, S.; Wolf, J.; et al. Rapid implementation of mobile technology for real-time epidemiology of COVID-19. *Science* **2020**, *368*, 1362–1367. [[CrossRef](#)]
43. Quer, G.; Radin, J.M.; Gadaleta, M.; Baca-Motes, K.; Ariniello, L.; Ramos, E.; Kheterpal, V.; Topol, E.J.; Steinhubl, S.R. Wearable sensor data and self-reported symptoms for COVID-19 detection. *Nat. Med.* **2021**, *27*, 73–77. [[CrossRef](#)] [[PubMed](#)]
44. Oyewole, A.; Barrass, L.; Robertson, E.; Woltmann, J.; O’Keefe, H.; Sarpal, H.; Dangova, K.; Richmond, C.; Craig, D. COVID-19 Impact on Diagnostic Innovations: Emerging Trends and Implications. *Diagnostics* **2021**, *11*, 182. [[CrossRef](#)]
45. Bogu, G.K.; Snyder, M.P. Deep learning-based detection of COVID-19 using wearables data. *medRxiv* **2021**. [[CrossRef](#)]
46. Mishra, T.; Wang, M.; Metwally, A.A.; Bogu, G.K.; Brooks, A.W.; Bahmani, A.; Alavi, A.; Celli, A.; Higgs, E.; Dagan-Rosenfeld, O.; et al. Pre-symptomatic detection of COVID-19 from smartwatch data. *Nat. Biomed. Eng.* **2020**, *4*, 1208–1220. [[CrossRef](#)]
47. Lukas, H.; Xu, C.; Yu, Y.; Gao, W. Emerging Telemedicine Tools for Remote COVID-19 Diagnosis, Monitoring, and Management. *ACS Nano* **2020**, *14*, 16180–16193. [[CrossRef](#)]
48. Goodday, S.M.; Geddes, J.R.; Friend, S.H. Disrupting the power balance between doctors and patients in the digital era. *Lancet Digit. Health* **2021**, *3*, e142–e143. [[CrossRef](#)]
49. Mair, J.; Campbell, A.; Hayes, L.; Sculthorpe, N. The Power of Wearables: Is it Time to Use Commercially Available Activity Tracker Data Retrospectively to Understand Population Physical Activity Patterns? *SSRN Electron. J.* **2021**, 3773475. [[CrossRef](#)]
50. Manekiya, M.; Donelli, M. Monitoring the covid-19 diffusion by combining wearable biosensors and smartphones. *Prog. Electromagn. Res. M* **2021**, *100*, 13–21. [[CrossRef](#)]
51. Zhu, G.; Li, J.; Meng, Z.; Yu, Y.; Li, Y.; Tang, X.; Dong, Y.; Sun, G.; Zhou, R.; Wang, H.; et al. Learning from Large-Scale Wearable Device Data for Predicting the Epidemic Trend of COVID-19. *Discret. Dyn. Nat. Soc.* **2020**, *2020*, 1–8. [[CrossRef](#)]
52. Javaid, M.; Khan, I.H. Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic. *J. Oral Biol. Craniofacial Res.* **2021**, *11*, 209–214. [[CrossRef](#)] [[PubMed](#)]
53. Al-Turjman, F.; Deebak, B. Privacy-Aware Energy-Efficient Framework Using the Internet of Medical Things for COVID-19. *IEEE Internet Things Mag.* **2020**, *3*, 64–68. [[CrossRef](#)]
54. Su, J.; He, X.; Qing, L.; Niu, T.; Cheng, Y.; Peng, Y. A novel social distancing analysis in urban public space: A new online spatio-temporal trajectory approach. *Sustain. Cities Soc.* **2021**, *68*, 102765. [[CrossRef](#)]
55. Pahlevanzadeh, B.; Koleini, S.; Fadilah, S.I. Security in IoT: Threats and Vulnerabilities, Layered Architecture, Encryption Mechanisms, Challenges and Solutions. In Proceedings of the International Conference on Advances in Cyber Security, Penang, Malaysia, 8–9 December 2020; Springer: Singapore; pp. 267–283.
56. Jethani, S.; Jain, E.; Thomas, I.S.; Pechetti, H.; Pareek, B.; Gupta, P.; Veeramsetty, V.; Singal, G. Surveillance System for Monitoring Social Distance. In *Advanced Computing, IACC 2020. Communications in Computer and Information Science*; Garg D., Wong K., Sarangapani J., Gupta S.K., Eds.; Springer: Singapore, 2021; Volume 1367.
57. Aman, A.H.M.; Hassan, W.H.; Sameen, S.; Attarbashi, Z.S.; Alizadeh, M.; Latiff, L.A. IoMT amid COVID-19 pandemic: Application, architecture, technology, and security. *J. Netw. Comput. Appl.* **2021**, *174*, 102886. [[CrossRef](#)]
58. Udgata, S.K.; Suryadevara, N.K. COVID-19: Challenges and Advisory. In *Tunable Low-Power Low-Noise Amplifier for Healthcare Applications*; Springer: Singapore, 2020; pp. 1–17.

59. St-Denis, X. Sociodemographic Determinants of Occupational Risks of Exposure to COVID-19 in Canada. *Can. Rev. Sociol. Can. Sociol.* **2020**, *57*, 399–452. [CrossRef]
60. Zajacova, A.; Jehn, A.; Stackhouse, M.; Denice, P.; Ramos, H. Changes in health behaviours during early COVID-19 and socio-demographic disparities: A cross-sectional analysis. *Can. J. Public Health* **2020**, *111*, 953–962. [CrossRef]
61. Mitchell, T.O.; Li, L. State-Level Data on Suicide Mortality During COVID-19 Quarantine: Early Evidence of a Disproportionate Impact on Racial Minorities. *Psychiatry Res.* **2021**, *295*, 113629. [CrossRef] [PubMed]
62. Shah, R.U.; Curtis, L.H. Data Quarantine in the Time of the COVID-19 Pandemic. *Circ. Cardiovasc. Qual. Outcomes* **2020**, *13*, 006908. [CrossRef] [PubMed]
63. Natu, P.; Shachi, N.; Upasana, A. 4 Privacy Issues in Medical. In *Data Protection and Privacy in Healthcare: Research and Innovations*; CRC Press: Boca Raton, FC, USA, 2021; Volume 51.
64. Terry, N.; Christine, N.C. A Virtuous Circle: How Health Solidarity Could Prompt Recalibration of Privacy and Improve Data and Research. *Okla. Law Rev.* **2021**, Forthcoming. Available online: <https://ssrn.com/abstract=3774366> (accessed on 14 February 2021).
65. Chong, K.M. Privacy-preserving healthcare informatics: A review. In *ITMWeb of Conferences*; EDP Sciences: Penang, Malaysia, 2021; Volume 36, p. 04005.
66. Alnemari, A.; Romanowski, C.J.; Raj, R.K. An Adaptive Differential Privacy Algorithm for Range Queries over Healthcare Data. In Proceedings of the 2017 IEEE International Conference on Healthcare Informatics (ICHI), Park City, UT, USA, 23–26 August 2017; pp. 397–402.
67. Zia, M.T.; Khan, M.A.; El-Sayed, H. Application of Differential Privacy Approach in Healthcare Data—A Case Study. In Proceedings of the 2020 14th International Conference on Innovations in Information Technology (IIT), Al Ain, United Arab Emirates, 17–18 November 2020; pp. 35–39.
68. Gutiérrez, O.; Romero, G.; Pérez, L.; Salazar, A.; Charris, M.; Wightman, P. HealthyBlock: Blockchain-Based IT Architecture for Electronic Medical Records Resilient to Connectivity Failures. *Int. J. Environ. Res. Public Health* **2020**, *17*, 7132. [CrossRef] [PubMed]
69. Mothukuri, V.; Parizi, R.M.; Pouriyeh, S.; Huang, Y.; Dehghantanha, A.; Srivastava, G. A survey on security and privacy of federated learning. *Futur. Gener. Comput. Syst.* **2021**, *115*, 619–640. [CrossRef]
70. Gawali, M.; Shriya, S.; Harshit, M.; Ashrika, G.; Bhanu, P.K.N.; Viraj, K.; Aniruddha, P. Comparison of Privacy-Preserving Distributed Deep Learning Methods in Healthcare. *arXiv* **2020**, arXiv:2012.12591.
71. Vaishya, R.; Javaid, M.; Khan, I.H.; Vaish, A.; Iyengar, K.P. Significant Role of Modern Technologies for COVID-19 Pandemic. *J. Ind. Integr. Manag.* **2021**, 1–13. [CrossRef]
72. Bragazzi, N.L.; Dai, H.; Damiani, G.; Behzadifar, M.; Martini, M.; Wu, J. How Big Data and Artificial Intelligence Can Help Better Manage the COVID-19 Pandemic. *Int. J. Environ. Res. Public Health* **2020**, *17*, 3176. [CrossRef]
73. Mottaqi, M.S.; Fatemeh, M.; Hedieh, S. Contribution of Machine Learning Approaches in Response to SARS-CoV-2 Infection. *Inform. Med. Unlocked* **2021**, *23*, 100526. [CrossRef]
74. Iqbal, S.; Shahzad, A.; Bushra, B.; Khalid, A.; Manal, A.A.A.; Alreuof, M.A. A Systematic Review: Role of Artificial Intelligence During the COVID-19 Pandemic in the Healthcare System. *Int. J. Intell. Inf. Technol. (IJIT)* **2021**, *17*, 1–18. [CrossRef]
75. Vaishya, R.; Mohd, J.; Ibrahim, H.K.; Abid, H. Artificial Intelligence (AI) applications for COVID-19 pandemic. *Diabetes Metab. Syndr. Clin. Res. Rev.* **2020**, *14*, 337–339. [CrossRef] [PubMed]
76. Bullock, J.; Luccioni, A.; Pham, K.H.; Lam, C.S.N.; Luengo-Oroz, M. Mapping the landscape of Artificial Intelligence applications against COVID-19. *J. Artif. Intell. Res.* **2020**, *69*, 807–845. [CrossRef]
77. Agbehadji, I.E.; Awuzie, B.O.; Ngowi, A.B.; Millham, R.C. Review of Big Data Analytics, Artificial Intelligence and Nature-Inspired Computing Models towards Accurate Detection of COVID-19 Pandemic Cases and Contact Tracing. *Int. J. Environ. Res. Public Health* **2020**, *17*, 5330. [CrossRef]
78. Bhattacharya, S.; Maddikunta, P.K.R.; Pham, Q.-V.; Gadekallu, T.R.; Chowdhary, C.L.; Alazab, M.; Piran, J. Deep learning and medical image processing for coronavirus (COVID-19) pandemic: A survey. *Sustain. Cities Soc.* **2021**, *65*, 102589. [CrossRef]
79. Group, The UPMC REMAP-COVID, and REMAP-CAP Investigators. Implementation of the Randomized Embedded Multifactorial Adaptive Platform for COVID-19 (REMAP-COVID) trial in a US health system—lessons learned and recommendations. *Trials* **2021**, *22*, 1–11.
80. Fong, S.J.; Dey, N.; Chaki, J. AI-Empowered Data Analytics for Coronavirus Epidemic Monitoring and Control. In *Therapeutic and Diagnostic Nanomaterials*; Springer: Singapore, 2021; pp. 47–71.
81. Singh, Y.S.; Kirani, Y. Local Analytical System for Early Epidemic Detection. In *Recent Trends in Information and Communication Technology*; Springer: Singapore, 2021; pp. 29–37.
82. McGraw, D.; Mandl, K.D. Privacy protections to encourage use of health-relevant digital data in a learning health system. *NPJ Digit. Med.* **2021**, *4*, 1–11. [CrossRef]
83. Voigt, P.; Bussche, A.V.D. The eu general data protection regulation (gdpr). In *A Practical Guide*, 1st ed.; Springer Science and Business Media LLC.: Cham, Switzerland, 2017; Volume 10, p. 3152676.
84. El-Ansari, A.; Beni-Hssane, A.; Saadi, M.; El Fissauoui, M. PAPIR: Privacy-aware personalized information retrieval. *J. Ambient. Intell. Humaniz. Comput.* **2021**, 1–17. [CrossRef]

85. Avraam, D.; Wilson, R.; Butters, O.; Burton, T.; Nicolaides, C.; Jones, E.; Boyd, A.; Burton, P. Privacy preserving data visualizations. *EPJ Data Sci.* **2021**, *10*, 1–34. [[CrossRef](#)] [[PubMed](#)]
86. Zhang, S.; Li, X.; Tan, Z.; Peng, T.; Wang, G. A caching and spatial K -anonymity driven privacy enhancement scheme in continuous location-based services. *Future Gener. Comput. Syst.* **2019**, *94*, 40–50. [[CrossRef](#)]
87. Barsocchi, P.; Calabrò, A.; Crivello, A.; Daoudagh, S.; Furfari, F.; Girolami, M.; Marchetti, E. COVID-19 & privacy: Enhancing of indoor localization architectures towards effective social distancing. *Array* **2021**, *9*, 100051. [[CrossRef](#)]
88. Uwaoma, C.; Clement, C.A. Mobile Technology Support for the Assessment and Management of COVID-19 Outbreak: Benefits and Challenges. In *Optimizing Health Monitoring Systems With Wireless Technology*; IGI Global: Hershey, PA, USA, 2021; pp. 13–24.
89. Benefits of EHRs. Available online: <https://www.healthit.gov/topic/health-it-basics/benefits-ehrs> (accessed on 14 February 2021).
90. Bramante, C.T.; E Ingraham, N.; A Murray, T.; Marmor, S.; Hovertsen, S.; Gronski, J.; McNeil, C.; Feng, R.; Guzman, G.; Abdelwahab, N.; et al. Metformin and risk of mortality in patients hospitalised with COVID-19: A retrospective cohort analysis. *Lancet Health Longev.* **2021**, *2*, e34–e41. [[CrossRef](#)]
91. Estiri, H.; Strasser, Z.H.; Klann, J.G.; Naseri, P.; Waghlikar, K.B.; Murphy, S.N. Predicting COVID-19 mortality with electronic medical records. *NPJ Digit. Med.* **2021**, *4*, 1–10. [[CrossRef](#)]
92. Yang, W.; Qiao, S. A novel anonymization algorithm: Privacy protection and knowledge preservation. *Expert Syst. Appl.* **2010**, *37*, 756–766. [[CrossRef](#)]
93. Shin, S.-Y. Privacy Protection and Data Utilization. *Health Inform. Res.* **2021**, *27*, 1–2. [[CrossRef](#)] [[PubMed](#)]
94. Menges, F.; Latzo, T.; Vielberth, M.; Sobola, S.; Pöhls, H.C.; Taubmann, B.; Köstler, J.; Puchta, A.; Freiling, F.; Reiser, H.P.; et al. Towards GDPR-compliant data processing in modern SIEM systems. *Comput. Secur.* **2021**, *103*, 102165. [[CrossRef](#)]
95. Vilorio, A.; Alberto, N.; Turriago, J.R. Machine Learning Techniques as Mechanisms for Data Protection and Privacy. In *Proceedings of the Advances in Human Factors, Business Management, Training and Education*; Springer: Singapore, 2021; pp. 367–374.
96. Nettleton, D.F.; Salas, J. A data driven anonymization system for information rich online social network graphs. *Expert Syst. Appl.* **2016**, *55*, 87–105. [[CrossRef](#)]
97. Majeed, A. Attribute-centric anonymization scheme for improving user privacy and utility of publishing e-health data. *J. King Saud Univ. Comput. Inf. Sci.* **2019**, *31*, 426–435. [[CrossRef](#)]
98. Zhu, S.; Saravanan, V.; Muthu, B. Achieving data security and privacy across healthcare applications using cyber security mechanisms. *Electron. Libr.* **2020**, *38*, 979–995. [[CrossRef](#)]
99. El Ouazzani, Z.; El Bakkali, H. A Classification of non-Cryptographic Anonymization Techniques ensuring Privacy in Big Data. *Int. J. Commun. Netw. Inf. Secur.* **2020**, *12*, 142–152.
100. El Ouazzani, Z.; El Bakkali, H.; Sadki, S. Privacy Preserving in Digital Health: Main Issues, Technologies, and Solutions. In *Social, Legal, and Ethical Implications of IoT, Cloud, and Edge Computing Technologies*; IGI Global: Hershey, PA, USA, 2020; pp. 253–276.
101. Ezhilarasan, E.; Dinakaran, M. Privacy preserving and data transpiration in multiple cloud using secure and robust data access management algorithm. *Microprocess. Microsyst.* **2021**, *82*, 103956. [[CrossRef](#)]
102. Clark, L.; Woll, A.; Owens, T.L.; Shropshire, D.; Kiser, B.; Gephardt, G.; Park, C.S. SP safety, autonomy and healthcare simulation practice in the COVID-19 era. *BMJ Simul. Technol. Enhanc. Learn.* **2021**, *2020*. [[CrossRef](#)]
103. Papoutsakis, M.; Fysarakis, K.; Spanoudakis, G.; Ioannidis, S.; Koloutsou, K. Towards a Collection of Security and Privacy Patterns. *Appl. Sci.* **2021**, *11*, 1396. [[CrossRef](#)]
104. Li, S.; Tian, H.; Shen, H.; Sang, Y. Privacy-Preserving Trajectory Data Publishing by Dynamic Anonymization with Bounded Distortion. *ISPRS Int. J. Geo-Inf.* **2021**, *10*, 78. [[CrossRef](#)]
105. Koo, J.; Kang, G.; Kim, Y.-G. Security and Privacy in Big Data Life Cycle: A Survey and Open Challenges. *Sustainability* **2020**, *12*, 10571. [[CrossRef](#)]
106. Li, B.; Zhu, H.; Xie, M. Quantifying Location Privacy Risks Under Heterogeneous Correlations. *IEEE Access* **2021**, *9*, 23876–23893. [[CrossRef](#)]