IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 15, 2021, accepted November 12, 2021, date of publication November 25, 2021,
date of current version December 20, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3130610

A Comprehensive Analysis of Privacy Protection Techniques Developed for COVID-19 Pandemic

ABDUL MAJEED AND SEONG OUN HWANG, (Senior Member, IEEE)
Department of Computer Engineering, Gachon University, Seongnam 13120, South Korea

Corresponding authors: Seong Oun Hwang (sohwang@gachon.ac.kr) and Abdul Majeed (ab09@gachon.ac.kr)

This work was supported by the National Research Foundation of Korea (NRF) Grant by the Korean Government through Ministry of Science and ICT (MSIT) under Grant 2020R1A2B5B01002145.

ABSTRACT Since the emergence of coronavirus disease–2019 (COVID-19) outbreak, every country has implemented digital solutions in the form of mobile applications, web-based frameworks, and/or integrated platforms in which huge amounts of personal data are collected for various purposes (e.g., contact tracing, suspect search, and quarantine monitoring). These systems not only collect basic data about individuals but, in most cases, very sensitive data like their movements, spatio-temporal activities, travel history, visits to churches/clubs, purchases, and social interactions. While collection and utilization of person-specific data in different contexts is essential to limiting the spread of COVID-19, it increases the chances of privacy breaches and personal data misuse. Recently, many privacy protection techniques (PPTs) have been proposed based on the person-specific data included in different data types (e.g., tables, graphs, matrixes, barcodes, and geospatial data), and epidemic containment strategies (ECSs) (contact tracing, quarantine monitoring, symptom reports, etc.) in order to minimize privacy breaches and to permit only the intended uses of such personal data. In this paper, we present an extensive review of the PPTs that have been recently proposed to address the diverse privacy requirements/concerns stemming from the COVID-19 pandemic. We describe the heterogeneous types of data collected to control this pandemic, and the corresponding PPTs, as well as the paradigm shifts in personal data handling brought on by this pandemic. We systemically map the recently proposed PPTs into various ECSs and data lifecycle phases, and present an in-depth review of existing PPTs and evaluation metrics employed for analysis of their suitability. We describe various PPTs developed during the COVID-19 period that leverage emerging technologies, such as federated learning, blockchain, privacy by design, and swarm learning, to name a few. Furthermore, we discuss the challenges of preserving individual privacy during a pandemic, the role of privacy regulations/laws, and promising future research directions. With this article, our aim is to highlight the recent PPTs that have been specifically proposed for the COVID-19 arena, and point out research gaps for future developments in this regard.

INDEX TERMS COVID-19, privacy, contact tracing, sensitive data, privacy protection techniques, epidemic containment strategies, data lifecycle, personal data, emerging technologies, geo-spatial data.

I. INTRODUCTION

The ongoing coronavirus disease–2019 (COVID-19) pandemic caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) is one of the most extraordinary challenges humanity has ever faced in terms of infectious diseases. During this pandemic, an enormous number of people got infected, and millions lost their lives. Despite vaccinations on a large scale, there is only a slim chance of containing the disease in the near future. This pandemic has severely affected the job market; many have lost their jobs amid the lingering pandemic. COVID-19 has forced the closure of many entertainment facilities, educational institutes, sports avenues, religious places, tourist spots, and public facilities in most parts of the world. Researchers are working towards minimizing the economic effects of COVID-19 by proposing unique research methods. The number of paper on COVID-19 are twenty-times higher than previous infectious diseases [1]. In Figure 1, we present an increase in the number of articles concerned with the COVID-19[1] and their effect on the economics[2] of the world in the last three years.

The associate editor coordinating the review of this manuscript and approving it for publication was Yu-Chi Chen.

[1]https://www.ncbi.nlm.nih.gov/research/coronavirus/
[2]https://sgp.fas.org/crs/row/R46270.pdf

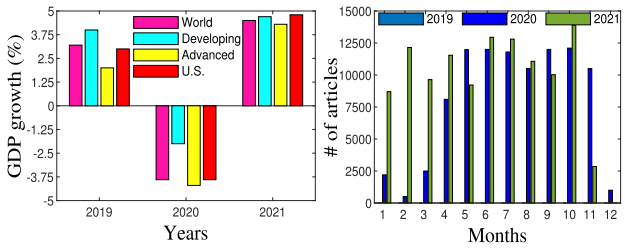

FIGURE 1. (Left) Economics status of the world, and (Right) number of research papers concerned with the COVID-19 pandemic in the last 3 years.

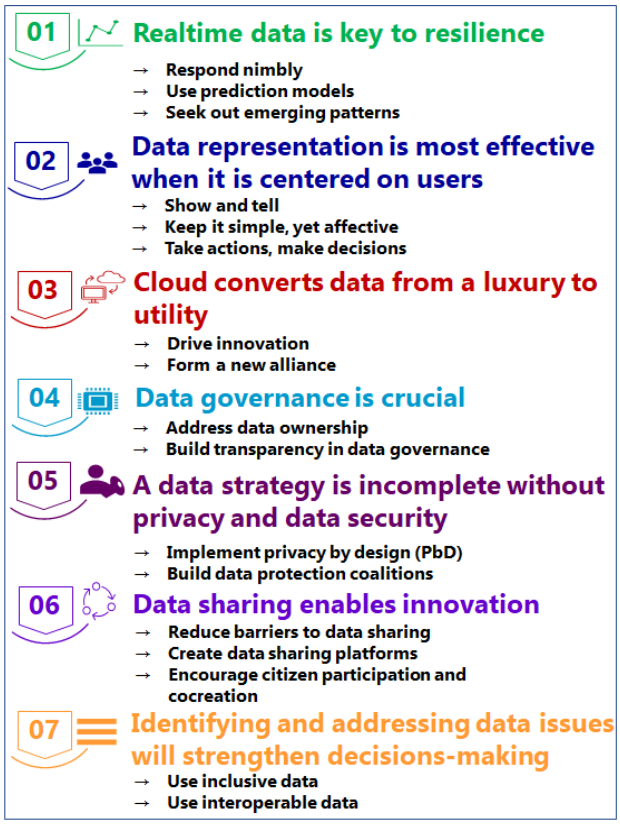

FIGURE 2. Overview of seven important lessons from COVID-19 regarding data strategies (adapted from Deloitte's website).

In these unanticipated times, the only solution available to people to keep them socially active or to continue their businesses is technology (a.k.a. digital solutions). For instance, people can communicate with their friends using a variety of social networks (SNs), share activities/events over SNs via images or videos, identify and make new friends on SNs, and go online to buy product/services, take classes, attend religious events, and work from home. Governments in each country have implemented a variety of digital solutions (e.g., epidemic handling systems) such as mobile apps, web-based frameworks, and integrated platforms in order to reduce the effects of this pandemic, and to constrain the disease's spread as quickly as possible. In these digital solutions, huge amounts and a wide variety of personal data are collected to accomplish multiple objectives (e.g., identify the disease's hidden routes of transmission, control its spread, and forecast trends). Additionally, governments have used digital solutions to prevent burnout in healthcare workers and for appropriate resource planning, taking into account the prevalence of COVID-19 [2]. We present in Figure 2 seven key lessons about data strategies in COVID-19's context.

As shown in Figure 2, data are essential for fighting the pandemic, but collecting them can be subject to manipulation/misuse if ample attention is not paid to individual privacy amid this digital surge in recent times. In some sense, privacy issues have put digital innovations under immense pressure [3]. Due to the extensive use of digital solutions as a mechanism to fight COVID-19, privacy violations have significantly increased, and the need for divergence from *data-first* to *privacy-first* becomes inevitable [4]. Interestingly, convincing people to use pandemic-related apps for their own well-being has also become challenging for many governments across the globe due to privacy concerns [5].

In this pandemic, the chances of group privacy breaches are relatively higher, rather than individual privacy breaches, because most countries are using the latest technologies like big data and artificial intelligence. One incident happened in South Korea when COVID-19's spread was linked to a minor religious sect (the Shincheonji church) [6]. Consequently, the government accessed a huge variety of fine-grained data, including the credit card usage, telephone and social security numbers, transactions, and pharmacy visits of all Shincheonji church members. As a result, some members committed suicide due to these privacy violations and the interference in their personal lives due to the aggressive measures adopted by the South Korean government against them. In countries such as Singapore, the balance between public safety and individual privacy is largely maintained through legal mechanisms (i.e., for the collective benefit), but it may lead to a range of negative consequences in the post–COVID-19 era due to the huge data transition into digital space [7]. Importantly, in the absence of legal mechanisms for COVID-19–like disaster scenarios, the preservation of privacy against corporate and government misuse is challenging [8]. Furthermore, the amount and variety of personal data collected have significantly increased, and that might help corporate/political players take advantage of the current situation to advocate even more intrusive use of data for political campaigns in the near future. In the post–COVID-19 era, besides the surge in digitization, privacy and cybersecurity issues are likely to emerge in large numbers [9].

Thus far, a considerable effort has been made to address privacy concerns stemming from COVID-19–related digital solutions and the data collection/processing to curtail the pandemic. Noticeable and remarkable development/research efforts include the decentralized and privacy-ensured contact tracing systems of Apple and Google [10], privacy-assured contact tracing based on call data record

analysis (CDRA) [11], privacy-preserved tracking of suspected COVID-19 infections [12], personal data–protection laws [13], informed processing of personal data [14], consent-based data utilization [15], statistical disclosure control (SDC) techniques [16], data sharing based on the recommendations of the RDA [17], responsible data governance [18], blockchain-based privacy preserving systems [19], anonymized data based cluster identification [20], artificial intelligence–driven software for privacy protection [21], and differential privacy-based privacy protection methods [22], to name a few. Although these methods have contributed firmly to addressing different privacy requirements, cohesive and substantial efforts are still needed from the research and development community to curtail privacy breaches and personal-data abuses in the ongoing/post–COVID-era.

Prior surveys related to privacy in the context of COVID-19 covered various important aspects, such as privacy issues in digital solutions, anonymization operations and techniques for healthcare data, privacy requirements amid the digital surge, personal data–anonymity frameworks, ethical issues with the information technology used to fight the pandemic, balancing privacy versus public safety during the pandemic, and privacy problems in contact-tracing applications. A survey by Sowmiya *et al.* [23] highlighted privacy and security issues in contact-tracing apps that have been developed to curtail the spread of COVID-19. In addition, the authors suggested valuable guidelines to protect personal data in the cloud setting. A study by Vadrevu *et al.* [24] discussed many state-of-the-art methods for privacy preservation in video surveillance and healthcare data. Zeinalipour and Claramunt [25] discussed the main privacy implications of contact-tracing apps in the post–COVID-19 era through a set of eight questions with multidisciplinary panelists. This study provides a solid understanding of the benefits from contact-tracing apps and the privacy risks. Schmidtke [26] discussed the privacy issues and challenges in implementing digital solutions that harness location data for containing COVID-19 infections. The author stressed the need for situation-adapted models when addressing privacy issues while fighting COVID-19–like pandemics. Shuja *et al.* [27] discussed the privacy problems of open source data related to COVID-19. These authors highlighted the need for a data federation to fight the pandemic, and for user privacy preservation through anonymity. Sihombing *et al.* [28] discussed the privacy protection methods adopted by nine different countries. In addition, other researchers have presented reviews about the country-specific privacy-protection methods used in the COVID-19 era [29]–[31]. Furthermore, some surveys have been published on the quantification of privacy risks [32], as to the nature of digital solutions (e.g., centralized or decentralized) [33], on the (non)acceptability of digital apps [34], on emerging technologies' privacy issues in COVID-19 context [35], about privacy controversies towards aggressive use of information technology amid the pandemic [36], and on healthcare privacy challenges in COVID-19 period [37].

Although we fully agree with the contributions of previous surveys, the concepts/techniques covered in those surveys were limited, and privacy protection techniques (PPTs) were not covered from broader perspectives. To the best of our knowledge, none of the existing surveys covered PPTs that have been proposed for most epidemic containment strategies (ECSs) and the data lifecycle. To cover this gap, we present an insightful review of PPTs that were recently proposed (i.e., 2020 and beyond) in the era of COVID-19. The main contributions of this review paper are summarized as follows. (i) It presents various state-of-the-art PPTs that have been proposed to address the diverse privacy requirements arising from the ongoing pandemic, and the fundamental concepts and ideas related to PPTs. (ii) It provides an overview of personal data enclosed in heterogeneous types, and the corresponding PPTs used for alleviating privacy concerns in the context of COVID-19. (iii) It describes various PPTs that have been suggested to solve privacy issues in epidemic containment strategies (e.g., contact tracing, quarantine monitoring, route disclosure of infected people). (iv) It systematically categorizes different PPTs in relation to the phases (e.g., collection, storage, processing, and use) of the data lifecycle adopted by most countries to fight the pandemic by leveraging digital solutions. (v) It highlights the latest developments leveraging emerging technologies (e.g., federated learning, blockchain, swarm learning, searchable encryption) to address the privacy concerns during the pandemic. (vi) It describes various PPTs that have been proposed, considering privacy regulations and laws, in order to curtail privacy violations in recent times. (vii) It presents the challenges in preserving user privacy amid the pandemic, and lists promising avenues for research that need further development. With this review, we aim to provide broader coverage of the privacy concept in the COVID-19 context that will lay a solid foundation for future research.

The rest of this paper is organized as follows. Section II provides background about the privacy definition and scope, the information embedded in different types of data, the privacy threats, the PPT types, and the notable operations of each PPT. Section III presents a conceptual overview of this paper and the paradigm shifts brought about by the pandemic in personal data handling. Section IV describes PPTs that have been proposed for heterogeneous data types. Section V presents PPTs that have been proposed to protect privacy in multiple epidemic containment strategies. Section VI presents PPTs that have been proposed to protect privacy in the eight different phases of the data lifecycle. Section VII presents various proposed PPTs that leverage emerging technologies. Section VIII discusses PPTs that adhere to privacy regulations and laws. Section IX discusses the challenges in protecting user privacy during a pandemic, and suggests promising future directions for research. Finally, this paper concludes in Section X.

II. BACKGROUND

Privacy is highly subjective, meaning its perception/definition varies from person to person [38]. Generally, privacy is mainly concerned about keeping private information away from public access. Privacy is paramount for individualism, autonomy, and self-respect. The scope of privacy is mainly classified into four categories, as shown in Figure 3.

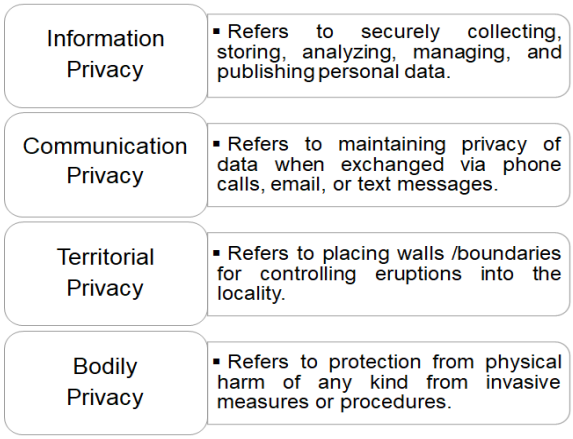

FIGURE 3. Classifications in the scope of privacy (adapted from Mendes and Vilela [39]).

Most researchers have primarily focused on privacy preservation in the first two categories (information and communication privacy). In this work, we mainly cover concepts and techniques related to information privacy that encompasses personal data. Personal data can be collected, stored, processed, and distributed in different ways. For example, SN data are mainly represented/modeled with the help of graphs. In contrast, the hospital/healthcare sector manages personal data in tabular form. We present a generic overview in Figure 4 of the different types/styles in which personal data are enclosed. In some cases, the same personal information can consistently be represented in multiple styles. For example, user data can be interchangeably represented in both tables and graphs.

The different types of data shown in Figure 4 can also be classified as unstructured, semi-structured, and structured data. Cunha *et al.* [40] recently presented a detailed taxonomy of data considering the structure. The authors also presented various privacy-preserving mechanisms for each data type. However, they primarily focused on the data and corresponding privacy preserving mechanisms in pre–COVID-19. In contrast, we consider different data types and corresponding PPTs specifically in the era of COVID-19. Due to the proliferation of the digital solutions in most sectors, the amount and nature of privacy threats are also increasing drastically with the passage of time. Figure 5 presents an overview of the different well-known/traditional and emerging privacy threats.

In Figure 5, we classify privacy threats into two categories: traditional and emerging. The privacy threats listed in the first category are well-known to the research community;

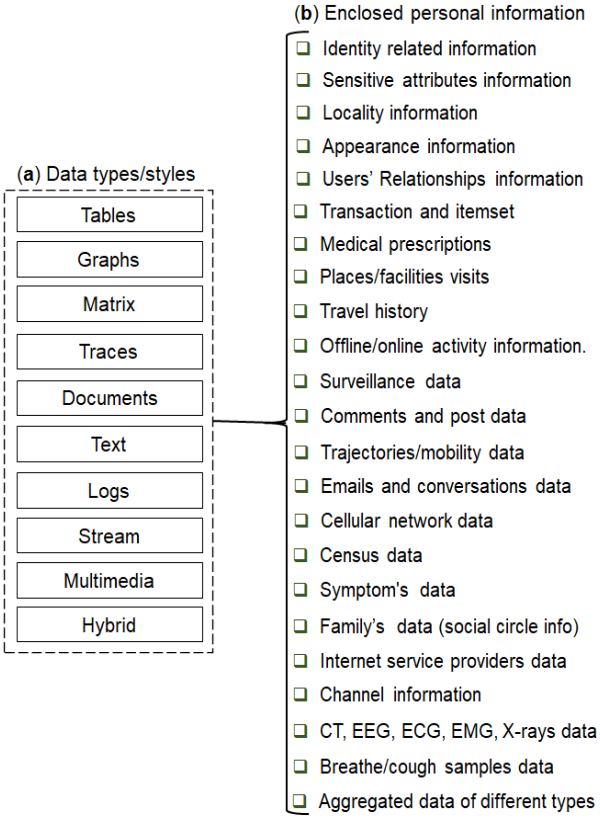

FIGURE 4. Generic overview of different data types, and the personal information included.

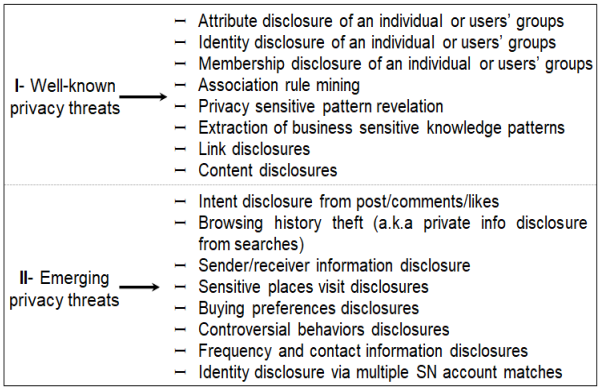

FIGURE 5. Overview of different information privacy-related threats.

however, the second category is relatively new, and has not been explored much. To that end, substantial and cohesive efforts are needed to cope with privacy threats that are emerging from heavy reliance on digital technologies during the pandemic. We invite readers to learn more about these privacy threats and the corresponding countermeasures from previous studies [41]–[46]. To preserve individual privacy from malevolent adversaries, many PPTs modify private values or break the associations between values. In some cases, noise is added to sensitive-attribute values to preserve privacy. PPTs can be categorized based on privacy threats, data types,

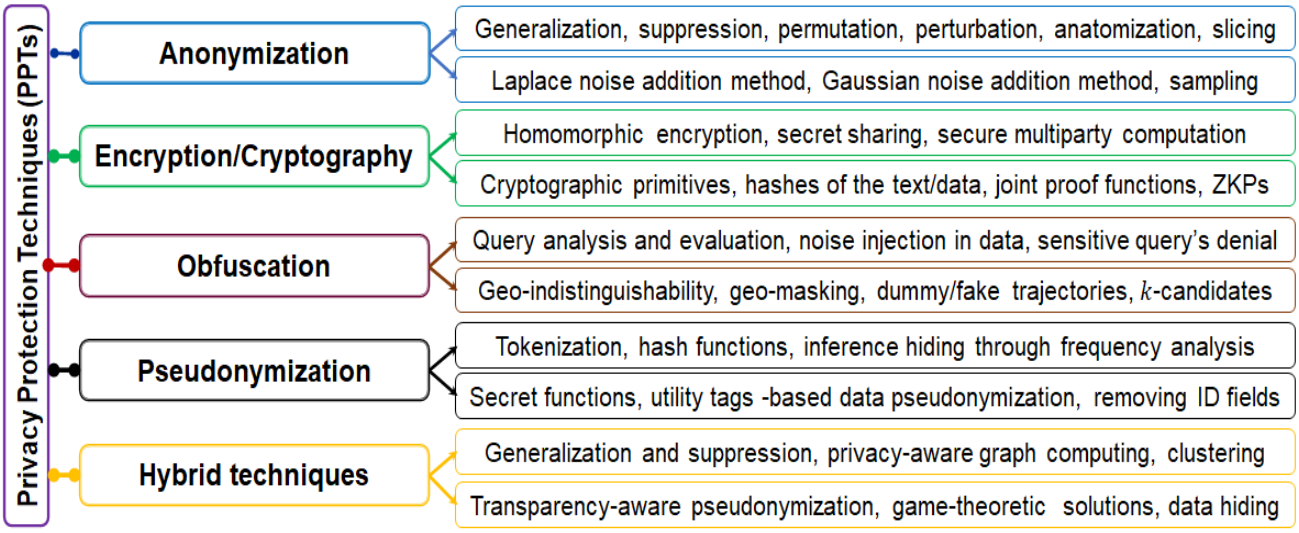

FIGURE 6. Brief overview of different operations performed by each privacy protection technique (PPT).

applications, and whether they are provable/non-provable and/or online/offline. In Table 1, we classify the existing PPTs based on such uses.

TABLE 1. Classification of privacy protection techniques.

Sr. no.	PPT	Working mechanism of the PPT
1.	Anonymization	Privacy protection by modifying or removing attributes' values.
2.	Encryption	Privacy protection by converting sensitive data items into an encrypted form.
3.	Obfuscation	Privacy protection by embedding noise in the sensitive data items' values.
4.	Pseudonymization	Privacy protection by replacing sensitive data items' values with pseudonyms (e.g., artificial identifier).
5.	Hybrid	Privacy protection by employing more than one PPT jointly (i.e., encryption and anonymization).

The PPTs listed in Table 1 perform a variety of operations with personal data in order to preserve individual privacy. We briefly summarize the taxonomy of operations performed by each PPT in Figure 6. Each operation has some advantages/drawbacks in terms of conceptual simplicity, superiority in utility/privacy results, robustness, number of intermediate sub-operations, and computing complexity. For example, generalization and suppression operations performed in anonymization techniques have a distinct impact on individual privacy and anonymous data utility, respectively. Generalization retains more utility for information seekers; however, suppression ensures better privacy preservation. Cryptography-based operations can be slow in practice, but they enable trans-border data flow with privacy guarantees. Obfuscation-based operations are extremely useful in privacy protection of geo-spatial data (i.e., location-based systems/services) by injecting an appropriate amount of noise. The operations performed by pseudonymization techniques assist in preserving privacy of sensitive items in data. Moreover, the hybrid PPTs employ multiple operations based on data type, the nature of the attributes, and privacy/utility objectives to effectively preserve privacy.

The main PPTs presented in Table 1 can be further classified into subcategories based on the operations in each category. For example, anonymization methods can be classified into syntactic (a.k.a. non-perturbative) and semantic (perturbative) methods. The famous and state-of-the-art anonymity methods in the former subcategory are the k-anonymity model [47], the ℓ-diversity model [48], and the t-closeness model [49]. These models are recognized as pioneers in privacy, and many ramifications of these models have been proposed for privacy preservation in different contexts [50]–[52]. Similarly, differential privacy (DP) is one of the state-of-the-art perturbative methods for privacy preservation while answering statistical queries [53]. Recently, many researchers have extended the DP concept for privacy protection from different perspectives [54]–[60]. Similarly, cryptography/encryption-based PPTs can be further classified into cryptographic protocols and cryptography-based mechanisms for heterogeneous data types (images, time series, genomics, streaming data, etc.). For example, the garbled circuit is a well-known cryptographic protocol that enables two parties to perform computing on sensitive data in a privacy-preserved way [61]. We invite readers to gain insights from previous studies into the detailed classification of PPTs based on data types [40], [62], [63].

Recently, in contrast to the conventional PPTs cited above, machine learning (ML) techniques open new opportunities and challenges in the privacy preservation domain [64]. Therefore, the relationship between ML techniques and PPTs is likely to increase in the near future. The existing work in this regard can be categorized from three aspects (as shown in Table 2). Some ML techniques can belong to more than one

TABLE 2. Role of ML in the privacy preservation domain (adapted from [64]).

Sr. no.	Aspect (i.e., category)	ML role in privacy preservation
1.	Making ML system (model, parameters, and data) private	Protection of target.
2.	ML enhanced privacy preservation	Protection tool.
3.	ML-powered privacy attacks	Attack tool.

category (e.g., privacy preservation and launching attacks, simultaneously) based on their generality and adoption in diverse fields.

Although many data-type–specific, domain-specific, attack-specific, application-specific, sector-specific, and ML-powered PPTs have been proposed, the current pandemic has spotlighted the privacy issues in different contexts. Therefore, the rest of this paper solely explores privacy issues/developments in the context of COVID-19.

III. PRIVACY PARADIGM SHIFT DURING THE COVID-19 PANDEMIC

The COVID-19 pandemic has swiftly increased personal data generation, collection, utilization, analysis, storage, distribution, mining, aggregation, and transmission/transfer to cloud/third-party infrastructures. As a result, people's concerns regarding privacy have significantly increased, and privacy has become one of the most discussed topics in the current literature. Recent examples, such as a lack of digital solution uptake by 45% of people in most countries [65], exposure of people's identifiable information by digital contact–tracing mobile apps [66], mass data collection and online tracking of people [67], 48.7% disclosure of social relationships via contact-tracing data [32], movement and contact tracking of individuals by governments [68], predicting the behavior and hobbies of a person by using location data [69], and data manipulations by algorithms [70] have highlighted the need for aggressive privacy protection solutions. In Figure 7, we present an overview of the paradigm shifts in the data privacy domain amid the COVID-19 pandemic. As shown in Figure 7, the pandemic brought a drastic change to the domain of personal data handling. Consequently, the possibility of privacy threats has also increased. Aside from the analysis presented in Figure 7, to fight the pandemic in some countries, more data-intensive digital solutions are in place that can precisely predict sensitive data about individuals [71], [72]. We next summarize a few paradigm shifts related to recent experiences from South Korea (i.e., from January 2020 on) that can contribute to privacy breaches.

- Before the pandemic, there was no obstacle to entering any facility (e.g., universities, cafes, public offices, and institutes), but during the pandemic, entry logs (i.e., data donations) are maintained digitally that can contribute to data misuse in the absence of laws/regulations for COVID-19–like pandemics.
- Many external institutions, such as police forces, mobile carriers, credit card companies, and insurance providers, have been closely working with healthcare workers since the COVID-19 outbreak. Although this close co-operation can help find infected individuals and any close contacts, it can jeopardize an individual's privacy due to fine-grained data transfer between the different stakeholders.
- Hospitals and related institutes were publishing personal data once or twice a year before the pandemic, but the frequency has increased significantly with COVID-19. Health authorities are continuously publishing the routes, facilities visited, mask-wearing status, and demographics of infected individuals, which can lead to a range of privacy breaches (i.e., identity/attribute disclosures of infected people). Furthermore, infected individuals can face discrimination and/or social stigma from the community.
- The extensive and rigorous use of multiple mobile apps for handling the pandemic in South Korea increases the chances of privacy violations via data aggregation. These apps enable continuous and detailed data collection about individuals, and they are utilized in different contexts. As mentioned in Section I, detailed inspection of infected/suspected individuals via such apps has led to many social problems (stigma, depression, suicide ideation, etc.).
- The tendency towards, and sources of, data collection as a proactive measure to fight the pandemic are relatively higher in South Korea. For example, while entering any facility, contact information is collected on paper, via QR codes, and with cameras, etc. Although collection of contact data with the help of different media is handy, secure disposal of data from all sources is challenging, and can lead to privacy breaches of various kinds.
- Due to extensive usage of heterogeneous sources of data, such as CCTV, mobile phone signals, and credit cards, to find who infected individuals had contact with, disclosure of activities based on spatial/temporal information can occur. Furthermore, the chances of family and community privacy disclosures is likely to increase.
- To curb the spread of COVID-19, the South Korean government is keeping an eye on purchasing histories in pharmacies and convenience stores to enable immediate testing of suspected individuals if they purchase body temperature measuring instruments and/or COVID-19–related medicine. Although it is essential to curtail the spread of COVID-19, such monitoring can lead to sensitive item–set disclosures. Furthermore, there is a relatively higher probability that sensitive data can be manipulated for business objectives.
- The use of government-designated mobile apps for most tasks (e.g., symptom reporting, test reservations, dissemination of relief funds, getting vaccinations) means personal data transfer to government-owned, centralized servers has increased significantly. Since the data are

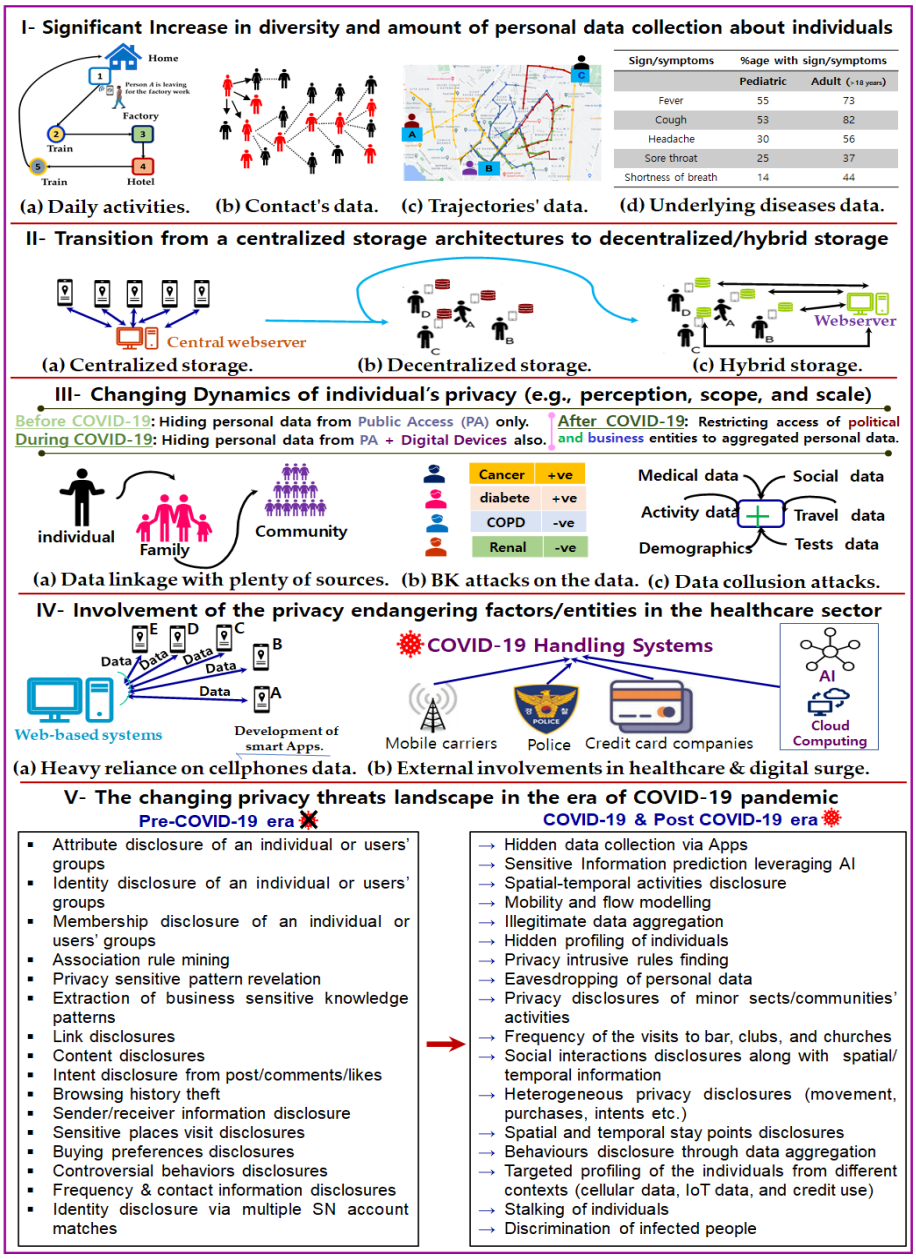

FIGURE 7. Generic overview of the privacy paradigm shifts amid the COVID-19 pandemic across the globe.

stored in centralized servers, they are subject to manipulation/disclosures to third parties without explicit consent, and thereby, privacy risks/leakage can be higher.

- One of the potential solutions adopted by the South Korean government in order to contain the spread of COVID-19 is by collecting location information in real time by calling people at random times of the day. Although this procedure was proven effective to prevent quarantine violations, it can disclose the spatial and temporal activities of those people. Furthermore, it can lead to the disclosure of social relationships if many people are located in close proximity to each other.
- The majority of the young people in South Korea use mobile phones extensively for a variety of purposes (e.g., gaming, information sharing/seeking, social interactions, hotel/room reservations, and online shopping). Each phone number is one of the most commonly used, and explicit identifiers because the majority of service subscriptions (e.g., health insurance, taxation, driving license, and underlying disease information) are linked to a person's phone number. Thus, privacy issues of various kinds (e.g., subscribing/terminating, mobility tracking) can occur based on phone numbers [73].

Besides the experiences/measures cited above, the government of South Korea has a partnership with many tech giants who apply analytics to aggregated personal data in order to analyze the dynamics of COVID-19 spread. Although it is handy to get insights about the pandemic via multi-party

computations, this can raise many privacy concerns pertaining to the personal data in question.

IV. PRIVACY PROTECTION TECHNIQUES FOR DIFFERENT DATA REPRESENTATIONS/TYPES

Generally, an individual's data can be enclosed/represented in multiple formats (e.g., tables, graphs, matrix, text, documents, and multimedia) as shown in Figure 4. Similarly, data owners (hospitals, healthcare units, policy makers, agencies, etc.) are maintaining personal data in different formats in the COVID-19 era to use it effectively. For example, underlying-disease data can be managed via tables [74], and the relationships between different COVID-19 entities can be modeled with the help of graphs [75]. The choice of data representation type is generally made based on the nature of the data. In Table 3, we classify different PPTs based on the data representation types in the context of COVID-19, and we briefly summarize the details. In some approaches listed in Table 3, more than one PPT/data-type was reported, which we classified as hybrid. Moreover, in some studies, only privacy problems were highlighted, and we therefore placed a hyphen in the cells for the PPTs employed. The PPT approaches named in the fifth column (Encryption, Obfuscation, Anonymization, etc.) relate to the data types (Table, Graph, Multimedia, etc.) named in the third column. The detailed analysis presented in Table 3 lays a solid foundation for future studies in this regard.

V. PRIVACY PROTECTION TECHNIQUES FOR DIFFERENT EPIDEMIC CONTAINMENT STRATEGIES

In this section, we summarize the contributions of previous studies regarding privacy protection in different epidemic containment strategies (contact tracing, quarantine monitoring, etc.). The utilization of ECSs varies from country to country. In some countries, only contact tracing is used to find who infected individuals had contact with in order to contain the spread of COVID-19. On the other hand, some countries rely solely on quarantine/social-distance monitoring to fight the pandemic. In some countries, multiple ECSs were employed to curtail the spread of the virus as quickly as possible. In this work, we select and discuss six of the most widely used ECSs that have played a vital role in COVID-19 containment. A generic overview of the selected ECSs is shown in Figure 8. Each ECS has a unique role in handling the pandemic. For example, contact tracing can help find the people an infected individual came into contact with, and reporting symptoms can help contain the disease proactively. We briefly summarize the overview of each ECS before presenting PPTs for them.

A. DIGITAL CONTACT TRACING

In this ECS, the close contacts of an infected individual are determined in order to test them or have them self-isolate. With the help of this ECS, not only is the spread contained but the potential carrier can also be treated immediately [124]. Meanwhile, digital contact tracing has raised several privacy concerns in developed countries [125]. Apple and Google are working on development of privacy-preserved contact-tracing apps [11].

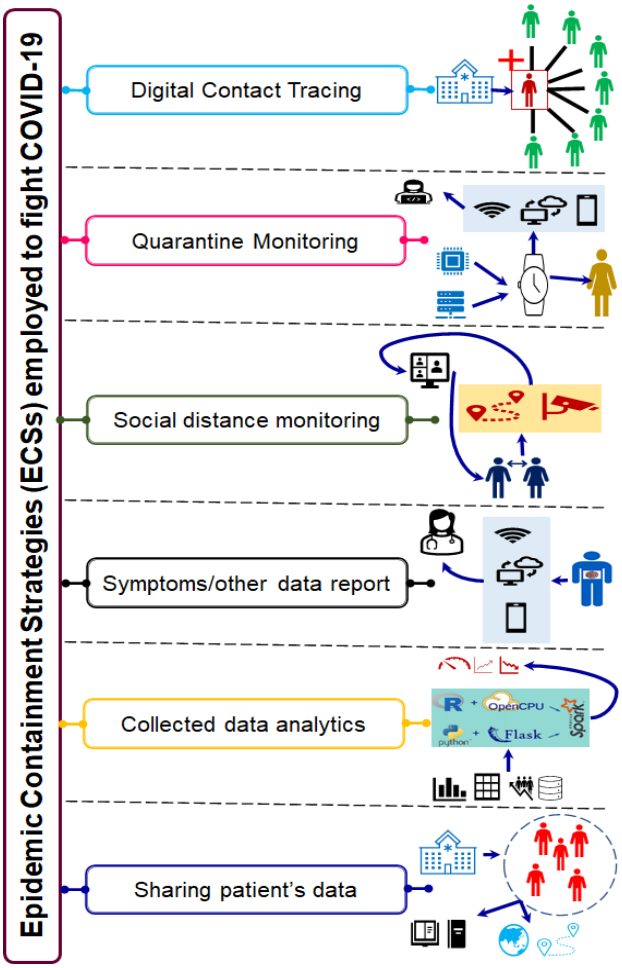

FIGURE 8. Overview for six of the main ECSs employed to fight COVID-19.

B. QUARANTINE MONITORING

In this ECS, individuals believed to be exposed/infected with COVID-19, but who do not show any symptoms, are separated from other people. This ECS requires provision of essentials (i.e., food and medicine), a private space, and an investment in enforcement [126]. Many digital apps have been developed to monitor and enforce quarantines.

C. SOCIAL DISTANCE MONITORING

In this ECS, close contact with other people is avoided in both indoor and outdoor environments. It is one of the main solutions recommended by health authorities to lower the spread of COVID-19 [127].

D. SYMPTOMS/OTHER DATA REPORTING

In this ECS, the disease's symptoms, risk factors, and other related data are collected via smartphones or surveys to

TABLE 3. Summary and classification of recently proposed PPTs for the COVID-19 pandemic based on the different data representation types.

Ref.	Year	Data type	Assertion (e.g., problem solved) in COVID-19-pandemic situations regarding individual privacy	PPTs employed to accomplish the task
Lyons et al. [76]	2020	Table	Analyzed different risk factors such as clinical, demographic, and socioeconomic jointly for possibility of COVID-19 infection, morbidity, and mortality in a privacy preserved way.	Anonymization and encryption
Linschoten et al. [77]	2021	Table	Described and compared the disease course as well as outcomes in hospitalized COVID-19 patients with & without pre-existing cardiac disease.	Anonymization
Jakob et al. [78]	2020	Table	Designed and evaluated data anonymization pipeline in order to promote open science on COVID-19 pandemic.	Anonymization
Brat et al. [79]	2020	Table	Focused on consolidation, sharing, and interpreting data about the clinical trajectories of the COVID-19 patients keeping laboratory values and comorbidities in loop.	Anonymization
Kuppa et al. [80]	2021	Table	Generated synthetic dataset by projecting original dataset by using instance level privacy score (PS) approach. The significant drop in membership inference attacks was observed empirically.	Anonymization
Walia et al. [81]	2020	Table	Produced categorical and continuous data as the synthetic data in a tabular form that showed preservation of patterns, relationships and distributions of the original dataset.	Anonymization
Moraes et al. [82]	2021	Table	Discussed privacy and transparency issues about COVID-19 public data, and stressed the need of privacy by design in COVID-19 era.	Anonymization
Guo et al. [83]	2021	Table	Proposed a practical privacy-preserving mechanism for ensuring data security and privacy in different phases of a wearable IoT-based framework.	Anonymization and encryption
Lee et al. [84]	2021	Table	Proposed a valuable solutions for automated data-generation without compromising individual privacy. The suggested concepts can enhanced the volume and timeliness of sharing data with researchers.	Anonymization
Cao et al. [85]	2020	Graph	Suggested a sanitization mechanism for location privacy preservation leveraging graph data for epidemic surveillance. It assists in epidemic analysis, contact tracing, and location monitoring.	Obfuscation
Vepakomma et al. [86]	2021	Graph	Suggested a privacy preserving contact tracing system that collects sketches of location visit of infected people, and computes histograms on server that can be downloaded by the querier clients.	Obfuscation
Mao et al. [87]	2021	Graph	Proposed a graph database algorithm in order to trace contacts of an infected individual in a centralized model. The suggested concepts can be employed in different regions and countries to respond to the ongoing epidemic.	Anonymization
Gaeta et al. [88]	2021	Graph	Suggested a method for modelling the spread of COVID-19 in different regions and analyzing the dynamics within each region. The proposed method is applicable for spread modeling in different regions/countries with privacy.	-
Hamed et al. [89]	2021	Graph	Suggested a design of a low-cost mobile app that can assist in finding the COVID-19 suspects in a privacy-preserved way. The proposed design adheres to the user trust, government policies, and existing apps.	Anonymization
Meirom et al. [90]	2021	Graph	Proposed a novel framework for correctly identifying the nodes that required COVID-19 tests, and suggested a method to control a diffusive process using temporally evolving graph.	Anonymization
Baker et al. [91]	2021	Graph	Proposed a framework for privately information sharing between infected and non-infected individuals to slow the progression of COVID-19.	Encryption and anonymization
Lachner et al. [92]	2021	Videos	Proposed a privacy preserving system for performing analytics on the video data. It only extracts relevant information from video data to support surveillance in a privacy-preserved way.	Encryption
Sugianto et al. [93]	2021	Videos	Proposed an AI-powered social distancing monitoring system for public spaces while safeguarding users' privacy.	Hybrid
Yang et al. [94]	2021	Videos	Proposed a mechanism for monitoring compliance with social distancing leveraging video data. The system preserves privacy by not storing any personally identifiable information.	Hybrid
Reyad et al. [95]	2021	Text	Secured text data from the disclosures leveraging key-based enhancement of the DES (KE-DES) is proposed. The suggested method secures text data.	Encryption
Catelli et al. [96]	2021	Text	Proposed a framework for privacy-sensitive information hiding within electronic health records leveraging deep learning and natural language processing concepts.	Anonymization
Libbi et al. [97]	2021	Text	Suggested a useful method for synthetic data generation in COVID-19-like pandemics when access to the real data is hard due to privacy concerns/issues.	Anonymization
Syed et al. [98]	2021	(non)Images	Developed an on-demand pseudonymization process that will assist researchers in getting a comprehensive and detailed view of personal data without compromising patients' privacy.	Pseudonymization
Reyad et al. [99]	2021	Images	Encrypted and secure transmission of real-world data (Computed Tomography (CT) chest scan) of COVID-19 infected patients in order to preserve privacy of patient data.	Encryption
Packh et al. [100]	2021	Images	Discussed the possibilities of privacy issues in publically available chest X-ray data leveraging deep learning-based re-identification algorithms.	-
Kaissis et al. [101]	2021	Images	Effective privacy preservation while sharing images data among different institutes. Furthermore, disclosure of both model and data are controlled in multi-party computation settings.	Encryption
Ziller et al. [102]	2021	Images	Developed a Gaussian Differential Privacy (GDP) based framework which provides a strict privacy guarantees, and ensure privacy preservation in most cases in images' data.	Anonymization
Ulhaq et al. [103]	2020	Images	Suggested a differential privacy by design (dPbD) framework for COVID-19 imaging data privacy preservation.	Anonymization
Nabil et al. [104]	2021	Images	Proposed a privacy-preserving surveillance system in which people's participation in not mandatory for COVID-19-like pandemics.	Encryption
Guo et al. [105]	2020	Images	Proposed a method based on the principles of artificial intelligence for securing medical images from adversaries.	Encryption
Liu et al. [106]	2021	Traces	Accurately predicted the travel time with privacy-preserving using the geo-indistinguishably sensitization and traces data.	Obfuscation
Farzanehfar et al. [107]	2021	Traces	Identified the relationship between people's re-identification in relation with the datasize.	Anonymization
Reichert et al. [108]	2021	Traces	Proposed a framework that alerts the attendees of a potential super-spreader event in a privacy-preserved way privacy.	Pseudonymization
Bozdemir et al. [109]	2021	Matrix	Implemented a low-cost privacy preservation method based on density-based clustering concept for privacy-preservation in trajectories data.	Obfuscation
Lesty et al. [110]	2020	Matrix	Developed a method for sharing mobility data with strong privacy guarantees with related information consumers.	Obfuscation
Lin et al. [111]	2020	streams	Proposed a novel privacy-enhanced data fusion strategy (PDFS) for COVID-19 applications. The proposed strategy performed analytics on data considering the sensitivity of data.	Encryption
Burkhalter etal. [112]	2021	streams	Developed a prototype based on the Zeph and Apache Kafka in order to ensure end-to-end privacy of users.	Encryption
Iyer et al. [113]	2021	Heat Map	Suggested a potential solution for addressing privacy and utility trade-off in data publishing and managing of COVID-19 affects using travel histories.	Anonymization
Iwendi et al. [114]	2021	Documents	Proposed a framework for privacy-preservation and utility-enhancements in documents in medical sector. The proposed framework has many applications in the COVID-19 context.	Anonymization
Lohr et al. [115]	2021	Documents	Proposed a method for privacy preservation in a health related data using semantic type-conformant. The proposed concept yields less errors in the transformed data.	Pseudonymization
Geller et al. [116]	2020	Genomics	Discussed several issues related to genomics data processing amid COVID-19 pandemic. Authors stressed the need of using genomics data ethically.	Hybrid
Abinaya et al. [117]	2021	Genomics	Discussed various privacy concerns in accessing, querying, and, computation, and storage of the genomics data.	Encryption
Scheibner et al. [118]	2021	Hybrid	Suggested approaches for accelerating the medical research pace by leveraging various privacy enhancing techniques and unified interoperability standards.	Hybrid
Barker et al. [119]	2020	Hybrid	Analyzed the dynamics of privacy of people amid the COVID-19 pandemic in different territories, and recommended valuable suggestion to control privacy violations.	Hybrid
Deb et al. [120]	2021	Hybrid	Thoroughly discussed the changing landscape of privacy amid COVID-19 pandemic. Furthermore, important regulations and trends have also been explored.	Hybrid
Becher et al. [121]	2020	Hybrid	Comprehensively discussed the workflow of personal privacy, privacy-aware processing of personal data, and discussed various privacy enhancing technologies (PETs) in the context of healthcare.	Hybrid
Masiero Silvia [122]	2020	Hybrid	Discussed various implications of COVID-19 in digital social protection systems keeping personal data in loop.	Hybrid
Pool et al. [123]	2021	Hybrid	Employed the social media data in order to assess the HIPAA policies in the context of COVID-19. Valuable guidelines regarding the digital solutions implementation, transformation, and use have been suggested.	Hybrid

proactively contain disease spread. It can assist in fighting an ongoing pandemic with the help of digital solutions [128].

E. COLLECTED DATA ANALYTICS

In this ECS, analytics performed on COVID-19-related data helps to understand the spatial–temporal dynamics of this deadly disease. Analysis of epidemiological data with the latest big data technologies helps to find insights into the COVID-19 pandemic [129].

F. SHARING COVID-19 PATIENT DATA

In this ECS, clinical/general data about COVID-19 patients is shared with domestic/international researchers to understand the progression of the disease. Although data sharing brings

TABLE 4. A detailed comparison of the recent privacy protection techniques proposed for different epidemic containment strategies.

Method [Ref.]	Privacy problem solved	Evaluation metrics used	Merits	Demerits	ECS
REACT framework [131]	Location privacy preservation	Precision & recall	Privacy-ensured contact tracing and risk monitoring	Less adoption due to realtime data collection	A
HealthDist system [132]	Mobility privacy preservation	Accuracy	Preference-based privacy protection in mobility data	Only offline datasets were used in evaluation	A
DIMY protocol [133]	Privacy protection in full-lifecycle data	Queries-based analysis	Better privacy by integrating multiple PPTs	Overall computing complexity is very high	A
PTBM scheme [134]	Privacy-preserved patients' tracing	Queries-based analysis	Effective tracing of patients and their close contacts	Latency can increase rapidly with patients' count	A
Khopesh systen [135]	Hides contact and locations info	Accuracy	Provides higher anonymity and better privacy protection	Privacy disclosure can occur based on linking	A
PPCT approach [136]	Hides location and identity data	Probabilistic anonymity	Identity & mobility privacy preservation	Can be slow due to cryptographic operations	A
CT model [137]	Resolves multiple privacy issues	Privacy-preserved contacts	Effective tracing of people with cellular data	Vulnerability in terms of data security is high	A
PIM module [138]	Privacy and security of carrier	Accuracy	Privacy-aware host identification in crowded areas	Need constant internet connectivity for working	A
CT solution [139]	Protects identity of infected user	Accuracy	First solution based on location data	Lack robustness in terms of latency	A
PIS approach [140]	Privacy protection of healthy & diagnosed user	Efficiency and scalability	Effective preservation of location privacy	Lack practical development and use	A
PPMF framework [141]	Privacy in tracing nationwide	Disclosure control	Effective privacy in different contexts	Fails to detect the sporadic spread/clusters	A
Proximity-based CT [142]	Device based contacts analysis	Accuracy	Effective privacy preservation by storing data locally	Slow due to manual list management and local data process	A
Caudht System [143]	Highly private CT system	Privacy risk minimization	Effective privacy preservation due to decentralization	Subject to data manipulation	A
PCT technique [144]	Protects privacy in trajectories	Queries privacy	Effectively preserve privacy	Employed offline datasets only	A
TraceAll Technique [145]	Better privacy in answering CT queries	Queries' accuracy	Effective tracing of infected patient's contacts	Sensitive information disclosure is possible via aggregation	A
P^2B-Trace system [146]	Effective privacy of user's contact records	Integrity verification	Decentralized architecture-based privacy preservation	Prone to latency issues due to cryptography	A
CT system [147]	Contacts and relations privacy	Probabilistic anonymity	Strong prevention of identity disclosure	Subject to false reports & membership disclosure	A
IoTrace System [148]	Location privacy protection	Scalablility and flexibility	Effective privacy protection in crowded areas	Adoption can be low due to centrality	A
CTA solution [149]	Mobility and identity privacy	Histogram	Less infringement of individual's privacy	Personal data can be manipulated at server side	A
SSI proofs based CT [150]	Identity and activity trace privacy	Privacy levels	Higher privacy via mobile wallet	Data loss and manipulations	A
PROTECT System [151]	Limit location privacy issues	Probabilistic anonymity	Do not expose the location information	Can be subject to data revelation hiddenly	A
BU-Trace system [152]	Locations and contacts privacy	Masked anonymity	Effective privacy control via App	Privacy issues due to data aggregation	A
SCT system [153]	Identity and location privacy	Accuracy	Better privacy by storing data on phones	Data manipulations and less effective for CT	A
LCGCT System [154]	Protection of private data	Privacy in queries answer	Ensure secure data transfer	Rely on hard proof that augment complexity	A
LTESafe system [155]	Mobility privacy preservation	Accuracy	Effective privacy preservation in location data	Difficulty in identifying close contacts quickly	A
Bidirectional CT system [156]	Contacts privacy	Accuracy	Effective privacy control over personal data	Exposure notification can be manipulated	A
CONTAIN framework [157]	Protects trace's data	Probabilistic anonymity	Privacy-friendly CT for disease control	Prone to silent data collection	A
vContact system [158]	Stronger confidentiality of location info	User anonymity	First complete decentralized system for CT	Disclosure of data to adversaries	A
PvCT algorithm [159]	Protects diagnosed people's privacy	Security proof	CT leveraging cloud services	Hidden data transfer to the clouds	A
CSI CT system [160]	Spatio-temporal information privacy	Trajectory info hiding	Privacy protection in different context	Privacy disclosures can occur due to linking/EI	A
LTPPCP protocol [161]	Protects infected user's privacy	Multi-party disclosure control	CT by computing contacts on local devices	Token can be stolen to breach privacy	A
Intelligent system for QM [162]	Control of epidemic situation	Effective isolation	Ensures privacy of isolated people	Privacy issues can occur due to multiple entities	B
Monitoring platform [163]	Privacy-aware QM	Prototype	Effective solution of privacy needs	Data leakage due to central setting	B
IoT-enabled QM [164]	Location privacy control	Obfuscation	Strong privacy gurnatees within fence	Tracking of users is possible in some cases	B
QM framework [165]	Privacy-ensured QM	Survey-based analysis	Effective privacy preservation during the QM	Lack of legal methods to preserve privacy	B
General study [166]	Emphasize on the privacy protection	Surveys	Some apps are only privacy preserved	Disclosure of personal data can occur hiddenly	B
SQ QM system [167]	Safeguards identity/location privacy	Accuracy	Strong privacy by not sending data to cloud	Individual tracking is possible via estimates	B
Privacy-aware QM [168]	Privacy and security of QM apps	PbD followed or not	Analysis of privacy requirements	Data leakage due to centralized setting	B
P-AEEF protocol [169]	Secure medical information	Link breaches	Maintains privacy of sensitive data	Susceptible to patients' movement tracking	B
GF for QM [170]	Location privacy protection	Prototype	Robust security against tracking	Prone to sensitive information disclosure	B
EWS framework [171]	Ensures privacy in RM	Consent-based evaluation	Effective privacy protection by secure channel	privacy disclosures due to third-party apps use	B
SDM framework [93]	Privacy-aware monitoring	Case study	Maintain privacy of people at public places	Can lead to privacy beaches via constant monitoring	C
TSA framework [172]	Privacy-aware analysis of humans	Privacy & distance estimation	Effective privacy preservation in sensors data	Can lead to privacy beaches via data fusion	C
RSSI-based SDM system [173]	Privacy-aware SDM	Prototype	Effective privacy preservation of location and contacts	Subject to data disclosure by AI and other data	C
CV-based SDM system [174]	Privacy guarantee in images	Probabilistic anonymity	Privacy preservation via blurring	Susceptible to private activities disclosure	C
CN-based SDM [175]	Mobility privacy protection	Case study	Privacy protection in cellular network data	Can lead to disclosure via aggregation	C
CVaR SDM scheme [176]	Ensure trajectories privacy	Privacy-risk	Effective privacy preservation in mobility data	Subject to profiling of individuals	C
CATS system [177]	Community privacy protection	Data hiding	Effective privacy protection of diverse people	Can lead to privacy disclosure of known communities	C
Wearable-based SDM [178]	Maintain privacy of user data	Design analysis	Effective privacy of location/contacts data	Can lead to privacy due to identity data	A, C
COVTrac App [179]	Better privacy control	Prototype	Effective protection of mobility data	Prone to constant tracking via aggregation	C
ILS system [180]	Privacy and trust exploration	Architecture	Access control based better privacy	Ignores PbD/FL concepts and disclose PI	C
IoT Framework for DR [181]	Private data hiding	Prototype	Effective privacy of personal data	Privacy violations can occur over cloud	D
CoronaSurveys System [182]	Privacy-aware DC	Prototype	Effectively address privacy concerns	Tracking of users due to fine-grained data	D
CovChain system [183]	privacy of patients data	architecture	privacy from multiple views	high complexity and slow	D
IoT platform [184]	Maintain location & other data privacy	Suggestions	Effective privacy of sensitive data	Collusion attack due to multiple participants	D, A, B, C
IoT-based DR system [185]	Privacy of diverse data	Design	strong privacy of data in transit	Manipulation at server side	D
CC-based DR [186]	Resolves diverse privacy issues	Design	Privacy-aware analytics on personal data	Data abuse at the centralized server	D
Secure analytics [187]–[189]	Address diverse privacy needs	Simulations	Privacy protection by using non-personal data	Data and structure disclosure	E
Data publishing [190]	Privacy in CT and RS	Case study	Privacy protection of personal data	Route disclosure is not privacy-ensured	F, A

TABLE 5. Summaries of previous surveys, perspectives, or country-specific experiences regarding privacy in digital solutions.

ECS	Study's objectives/discussion-focus	References
A	Survey on CT apps in different settings, suggestions for privacy protection in CT apps, analysis of many apps that are in use and their privacy concerns, privacy issues in decentralized CT apps, privacy concerns of COVIDSafe app.	Ahmad et al. [191], Kolasa et al. [192], Elkhodr et al. [193], Li et al. [194], Lin et al. [195]
B	Analysis of privacy concerns in different QM apps, analyzed people attitude toward different apps in UK, design-to-deliver-based approaches for ehealth and their privacy issues, discussed IoT role in ongoing pandemic.	Park et al. [196], Lewandowsky et al. [197], Gios et al. [198], Chandrayan et al. [199]
C	Analyzed different cultural/ sociopolitical differences regarding privacy, discussed different mobile apps for pandemic monitoring, provide ethical consideration in digital tools' usage, analysis of early deployed mobile apps.	Huang et al. [200], Alves et al. [201], Mbunge et al. [202], Hatamian et al. [203]
D	Analyzed public attitudes towards privacy in pandemic times, discussed various privacy, security, and ethical concerns in apps, discussed privacy issues in CC and other technologies, reviewed different emerging technologies, suggestions for privacy-aware systems.	Bendechache et al. [204], Karale [205], Alashhab et al. [206], Mbunge et al. [207], Distler et al. [208]
E	Discussed the dynamics of privacy in COVID-19 era, analytics on patients EHR, privacy-aware data analytics.	Ahmad et al. [209], Kim et al. [210], Dwork et al. [211]
F	Role of mobility data in pandemic, ethical use of data, stressed the need of unified framework for data exchange	Buckee et al. [212], Dubov et al. [213], Lenert et al. [214]

Abbreviations: CT= contact tracing, QM= quarantine monitoring, UK= United Kingdom, CC= cloud computing, EHR= electronic health records.

innovation, it can lead to privacy issues. For example, in South Korea, upon positive test results, the places an infected individual went is shared with other people. Although it sparked criticism from the general public, it helped curb the spread of COVID-19 [130].

Apart from the ECSs cited above, alerting people to keep them away from hot spots and contaminated places, and implementing other preventive measures, played a vital role. Table 9 categorizes and summarizes recently proposed and/or developed PPTs for each ECS.

The abbreviations used in Table 9 are, CT = contact tracing, RM = remote monitoring, CC = cloud computing, QM = quarantine monitoring, CN = cellular network, DR = data reporting, RS = route sharing, SDM = social distance monitoring, DC = data collection, EI = external-info., PI = personal information, and AI = artificial intelligence. Moreover, the abbreviations used in methods' cell are described in respective studies. The letters A, B, C, D, E, and F correspond to each ECS in the subsections above. In some studies, the proposed approaches are applicable to more than one ECS, and therefore, we mention all of them in the ECS column. In the evaluation metrics column, we provide an evaluation of the approach based on extensive reviews. However, some approaches were only evaluated based on non-functional requirements (trust, safety, computing power, availability, ease of use, data collection, etc.) or they are just an architecture/design/prototype app. Therefore, we provide exact descriptions of the evaluation metrics along with the core privacy problem solved. Although we describe relatively fewer approaches for the last two ECSs, most of them are already described in Table 3. Besides the detailed coverage of various representative PPTs discussed in this survey, detailed knowledge regarding the generic overview of privacy protection or ECS-specific PPTs can be gathered from previous studies. To that end, we summarize such representative studies in Table 5.

VI. PRIVACY PROTECTION TECHNIQUES FOR DIFFERENT PHASES OF DATA LIFECYCLE

Generally speaking, in most epidemic handling systems (contact-tracing apps, alert systems, risk estimation, etc.), data undergo different phases (e.g., collection, pre-processing, analytics, and use) before finally leaving the system. Thence, data have a complete lifecycle that mostly starts with collection and ends at secure disposal. Most

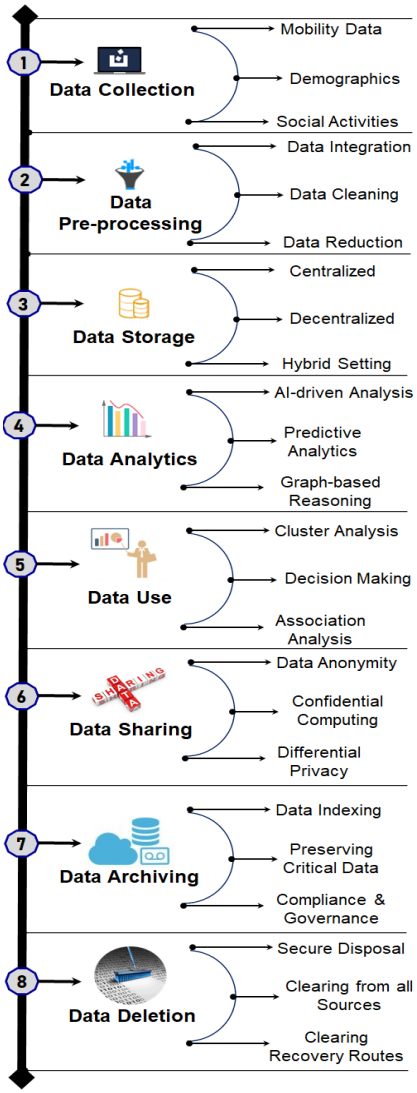

FIGURE 9. Overview of the eight main phases of the data lifecycle.

TABLE 6. Summary and classification of recently proposed state-of-the-art PPTs for each phase of the data lifecycle.

Phase	Solution type	Objectives of the proposed approach and methodology used to protect privacy in a respective phase	Ref.
Collection	Practical	Individual's privacy preservation at the time of data collection using clustering approaches	Onesimu et al. [217]
	Practical	Effective privacy preservation while collecting timestamped GPS data using cryptographic approaches	Berke et al. [218]
	Conceptual	Emphasized the need of data protection literacy and transparency in data collection that are vital to address privacy concerns	Trestian et al. [219]
	Theoretical	Described the need of amending consent form for data collection to protect privacy in an effective way	Garg et al. [220]
	Theoretical	Effective privacy guarantees against multiple attacks by limited data collection and decentralized storage	Canetti et al. [221]
	Conceptual	Significantly preserve user's privacy by collecting anonymized and GDPR-compliance location data from people	Pepe et al. [222]
	Practical	Individuals privacy preservation by solely collecting anonymized and aggregated mobility data	Lu et al. [223]
	Practical	Privacy-preserved correlated high dimensional data collection for practical settings without manipulations	Du et al. [224]
	Practical	Strong privacy protection while collecting $< key, value >$ pairs-based personal data items	Gu et al. [225]
	Practical	Ensuring individual's privacy at the time of data collection by giving discriminative protection based on data types	Gu et al. [226]
	Theoretical	Stressed the need of critically evaluating data acquisition and surveillance systems regarding privacy implications	Butler et al. [227]
	Practical	Two-way privacy protection of the sensitive data during collection and sharing with information consumers	Sun et al. [228]
	Practical	Privacy protection while collecting mobile GPS, card payment, and self report data with functional encryption	Kim et al. [229]
	Practical	Effective solution for mobility privacy preservation of individuals who provide their GPS data	Liu et al. [106]
	Practical	Incentive-aware data collection where users can choose their response strategies based on personal privacy requirements	Wang et al. [230]
Pre-processing	Conceptual	Effective preservation of individual's privacy in data pre-processing by using federated learning approach	Fourati et al. [231]
	Practical	Effective preservation of individual's privacy by filtering the sensitive data before sending to cloud environments	Li et al. [232]
	Practical	Strong privacy protection against paralinguistic-based privacy breaches using representation learning framework	Aloufi et al. [233]
	Practical	Effective privacy preservation by keeping majority of the sensitive data at the edge	Aazam et al. [234]
	Protocol	Privacy preserving information pre-processing to eliminate the risk of privacy breaches	Amano et al. [235]
	Practical	Effective privacy preservation via anonymization module to protect user privacy, and hiding identity information via pseudo-random identification number	Hu et al. [236]
	Practical	Privacy preservation in data acquisition/pre-processing via re-encryption methodologies	Rivadeneira et al. [237]
	Practical	Effective privacy preservation in pr-processing leveraging data integration techniques	Bellandi et al. [238]
	Practical	Effective privacy preservation and violations control on personal data via federated learning approach	Zhang et al. [239]
	Practical	Strong resilience against privacy breaches by encrypted database processing in cloud environments	Krishnan et al. [240]
	Practical	Strong privacy against sensitive information inference using Paillier homomorphic encryption approach	Yang et al. [241]
Storage	Practical	General trustworthy DB system for ensuring end-to-end privacy and security guarantees	He et al. [242]
	Theoretical	Privacy protection in querying the databases with strong privacy in multiple aspects	Prasanna et al. [243]
	Practical	Strong privacy protection by storing most data in a decentralized setting, and preventing adversary to get a complete picture of data	Anjum et al. [244]
	Practical	Sufficient privacy preservation in remotely collecting and storing data using encryption mechanisms and back-checking	Li et al. [245]
	Conceptual	Strong privacy protection by enabling users to set privacy based on preferences and make privacy-aware decisions	Psychoula et al. [246]
	Theoretical	Strong privacy protection in different environments taking into account users' concerns	Hopfgartner et al. [247]
	Theoretical	Effective privacy preservation while storing locations data with quantization-based obfuscation encoding	Biswas et al. [248]
	Practical	Effective privacy preservation of users by using cryptographic approach (e.g., Shamir Secret sharing algorithm)	Ali et al. [249]
	Practical	Users privacy protection leveraging emerging technology (i.e., blockchain technology) in data storing in cloud environments	Shaikh et al. [250]
	Practical	Strong privacy preservation system to support queries on an encrypted data	Moghadam et al. [251]
	Practical	Privacy protection of the sensitive data using smart contract and privacy-preserved ledgers	Kim et al. [252]
	Practical	Strong safeguarding against various privacy threats on individuals data without degrading utility leveraging blockchain	Miyachi et al. [253]
	Practical	Effective privacy protection by replacing centralized architectures with the uniqueness of blockchain (data provenance, enhancing transparency, and immutability)	Platt et al. [254]
	Theoretical	Discussed and analyzed the privacy issues of centralized and decentralized data storage. Results reveal that decentralized apps are more acceptable by the general public since they have less privacy concerns	Zhang et al. [255]
Analytics	Practical	Privacy-preserved analytics of the diagnosed/confirmed patients leveraging cell-phones data and tokens stored at the server with the help of PSI-CA algorithm	Trieu et al. [256]
	Theoretical	Privacy protection while performing analytics on the trajectory data using feature vectors based approaches	Rintoul et al. [257]
	Theoretical	Strong privacy preservation while performing analytics on the users data in a server-less architecture using machine learning	Golec et al. [258]
	Practical	Supporting analytics on a large scale data enclosed in a graph form using spectral clustering approach for COVID-19 tracking	El et al. [259]
	Theoretical	Suggested valuable guidelines to protect the users privacy in different settings and potential for lowering data breaches	Yu et al. [260]
	Theoretical	Discussed the possibilities of data disclosure and effective ways to protect individual's privacy	Dolgin Elie [261]
	Practical	Strong privacy guarantees during epidemiological modeling using real contact graphs by not disclosing private data to the system administrator or other participants	Daniel et al. [262]
	Practical	Effective privacy preservation in the videos data using tracking mechanisms and face recognition for surveillance purposes (i.e., people identification, face recognition, and activity recognition)	Tu et al. [263]
	Practical	Effective privacy preservation in mining and performing analytics on the location data obtained from cell-phones	Yin et al. [264]
	Practical	Effective privacy preservation by processing an encrypted information in the spatiotemporal-based analytics framework	Zhang et al. [265]
	Practical	Effective privacy preservation in mobility modeling by collecting the location data in anonymized form and using fuzzy theory	Rahimipour et al. [266]
	Practical	Effective privacy preservation in mining trajectories data using data augmentation approaches and identities are usually encrypted to preserve privacy	Zhou et al. [267]
	Practical	Effective privacy preservation in vertical data mining using variety of algorithms (dEclat, Eclat, and VIPER)	Gupta et al. [268]
Use	Practical	Privacy preserved contact tracing without revealing the locations of infected people and system user's information using MPC	Reichert et al. [269]
	Practical	Individual's privacy preservation and data governance for intended use leveraging ontologies and permissioned blockchain	Alves et al. [270]
	Practical	Ensures privacy of sensitive data in exposure notifications by processing data in a decentralized manner and using two privacy enhancing techniques	Canetti et al. [271]
	Practical	Alleviation of user's privacy concerns leveraging network structure in motioning and control of disease progression	Srinivasavaradhan et al. [272]
	Practical	Strongly protects users' privacy information in vulnerability map generation using federated learning approach	Chen et al. [273]
	Practical	Effective privacy preservation of individual's vaccine details using authentication mechanism and distributed ledger technologies	Chaudhari et al. [274]
	Practical	Privacy preservation of users data in a multi-agent learning environment leveraging differential privacy	Nagar et al. [275]
	Practical	Effective privacy preservation of medical data during examination leveraging federated learning framework	Kulkarni et al. [276]
	Practical	Effectively preserves medical data privacy using distributed learning mechanism and machine learning approaches	Zerka et al. [277]
	Practical	Preserving privacy of individual's sensitive information in predictions using differential private ANN	Prakash et al. [278]
	Practical	Effective protection of patient privacy in medical settings using federated learning-based approach	Abdul et al. [279]
Distribution	Practical	Strong protection of patients' medical and identity-related data during transmission using LiFi and meta-material antenna node	Garhwal et al. [280]
	Practical	Effective privacy preserving by prioritizing the sensitive data before sending to cloud system using differential privacy	Vadrevu et al. [281]
	Conceptual	Effective privacy preservation in time-series data using local differential privacy in temporal setting approach	Ye et al. [282]
	Practical	Effective privacy preservation in data sharing by using cryptographic approaches and smart-contract	Christodoulou et al. [283]
	Practical	Effective privacy preservation in data sharing leveraging emerging technologies (block chain & federated learning)	Zhang et al. [284]
	Theoretical	Effective privacy preservation of mobility data by employing anonymized and aggregated data (e.g., required data usage)	Kristofer et al. [285]
	Conceptual	Effective privacy preservation in data sharing using encryption techniques in integrated care systems	Kouroubali et al. [286]
	Theoretical	Emphasized the need of privacy preservation by amending the available regulations considering the information dynamics	Vlahou et al. [287]
	Practical	Strong privacy guarantees against location disclosure risk by processing mobile-phone users' mobility data anonymously	Silva et al. [288]
	Practical	Effective privacy preservation of demographics and location data leveraging disparate coverage approach	Coston et al. [289]
	Theoretical	Safeguarding individual's privacy in data sharing with third parties (e.g., researchers, data miners, etc.) using anonymization	Biancotti et al. [290]
	Practical	Strong privacy protection against the identity exposure by using the contact duration minimally and encoded data sharing	Dyo et al. [291]
	Conceptual	Stressed the need of effective privacy protection in unprecedented times via multitude of technical and legal approaches	Chauhan et al. [292]
Archiving	Conceptual	Emphasized the need of COVID-19 data archiving with privacy for the community well-being in the future	Jones et al. [293]
	Theoretical	Safeguarding individual's privacy by leveraging archived data of the medical staff using sample study approach	Feng et al. [294]
	Conceptual	Stressed the need of maintaining balance between data protection without lowering the potential use amid innovative technologies development	Cortez et al. [295]
Deletion	Practical	Safeguarding individual's privacy by deleting personal mobility data periodically and retention of limited data with anonymity	Ponce Aida [296]
	Conceptual	Effective privacy protection by removing unneeded data and not collecting any data that can violate privacy via periodical audit	Wacksman et al. [297]
	Conceptual	Highlighted the need of privacy preservation via legal measures, and stressed the need of multi-party collaboration to protect privacy effectively in post pandemic arena	Correia et al. [298]
	Practical	Safeguard against identity disclosure of individual/groups of people or communities in location by deleting sensitive data	Iacus et al. [299]

epidemic handling systems that are currently used to fight a pandemic also employ a similar data lifecycle, either fully or partially [215], [216]. During this lifecycle, data are collected from the relevant individuals, are processed and used for the intended purposes, and are then removed from the system based on defined policies. In Figure 9, we present an overview of the phases of data lifecycles along with recent PPTs for each phase. Table 6 summarizes and compares state-of-the-art and recently proposed/developed PPTs for each phase of the data lifecycle.

The abbreviations used in Table 6 are GPS = global positioning system, GDPR = general data protection regulation, DB = database, MPC = multi-party computation, ANN = artificial neural network, and PSI-CA = private set intersection cardinality. In Table 6, we classified the existing approaches into three categories: practical, theoretical, and conceptual. Practical approaches have been completely developed and deployed to some extent for the intended purposes, whereas theoretical approaches have been tested in limited scenarios or via simulation only. In contrast, the conceptual approaches highlight the privacy-enhancing technologies that will be paramount in the near future in order to preserve individual privacy, or they critically analyzed the recently developed PPTs. The evaluation metrics used to determine the feasibility of these PPTs cover computing time, accuracy, privacy protection level, resilience against various potential privacy threats, safeguards from various active privacy attacks, query result accuracy, probabilistic anonymity, association-rule hiding, data linkage prevention, sensitive data division into secret shares, and the whole process of data lifecycle/flow privacy preservation.

VII. PRIVACY PROTECTION TECHNIQUES THAT LEVERAGE EMERGING TECHNOLOGIES

During the ongoing pandemic, emerging technologies such as blockchain (BC), federated learning (FL), privacy by design (PbD), and artificial intelligence (AI), to name a few, have played a vital role in addressing privacy implications of various kinds [300]–[302]. These technologies have addressed the emerging privacy concerns and requirements that have arisen from digital solutions used to bring the pandemic under control. These technologies remain an integral part of many digital solutions developed to fight the pandemic in a privacy-preserving way. Additionally, these technologies have assisted in alleviating people's worries regarding personal data manipulation. We refer to these technologies as emerging technologies because they are relatively new, and their potential has not been fully investigated in different contexts. Nevertheless, many studies have reported their unique advantages in alleviating privacy concerns from the COVID-19 pandemic due to their proliferation in digital solutions.

These emerging technologies have helped to significantly restrict privacy breaches from digital solutions developed for different epidemic containment strategies, in the data lifecycle phases, and for general e-health services. For example, BC can be used for multiple services in the healthcare industry (e.g., contact tracing, EHR privacy, and collaboration between different entities in a privacy-preserving manner) [303]. FL has reshaped the whole healthcare industry (e.g., in transitions from hospital-centered procedures to patient-centered or device-centered procedures) by performing analytics federally without revealing actual data to centralized servers [304]. AI has played a vital role in developing privacy-aware approaches [305], and the PbD concept plays a dominant role in developing digital solutions by keeping privacy in focus from the early development stages [306]. In Figure 10, we present an overview of five emerging technologies that have helped reduce privacy breaches of various types. Later, we describe various PPTs that have adopted some unique features of these emerging technologies in order to protect an individual's privacy.

Key characteristics in BC technology, such as decentralization, distributed ledgers, immutability, and transparency, make it suitable for private data sharing, collaboration between different entities in a confidential manner, data leakage prevention, and smart-contract–based agreement execution among different parties [307]. This is one of the most widely used technologies for data protection, and its use in the healthcare industry is increasing day by day. PbD is an emerging concept for privacy protection in digital solutions [308]. Its seven key principles (listed in Figure 10) lay a solid foundation for software development that keeps privacy in mind, addressing many privacy concerns that can arise due to digital solution use. Furthermore, PbD principles are highly flexible, meaning they can be modified to fulfill the diverse privacy needs of different sectors. FL has revolutionized the data privacy domain by keeping data in local devices instead, with only model parameters/weights shared centrally [309]. By keeping data at the edge or within devices, privacy can be effectively guaranteed in most cases. Swarm learning (SL) is one of the recent technologies for data protection, and is an enhancement of the FL concept [310]. In this model, not only the data but the model parameters are kept at the edge or in the devices. By not sharing the model's parameters and the underlying data, privacy can be preserved significantly. SL has the potential to become a real game changer for privacy-preserved data sharing in the near future. Finally, searchable encryption (SE) can assist in privacy protection by enabling analytics to be applied to encrypted data. By performing analytics on encrypted data, a user's privacy can be maintained consistently, and privacy violations can be restricted to the extent possible [311], [312]. All these emerging technologies have contributed significantly to addressing the diverse privacy requirements arising at the present time. Furthermore, adoption of these technologies is likely to grow in the near future, because personal data circulation in cyberspace has increased significantly.

In Table 7, we present an overview of PPTs that employ emerging technologies in order to preserve a user's privacy. Apart from the state-of-the-art studies listed in Table 7,

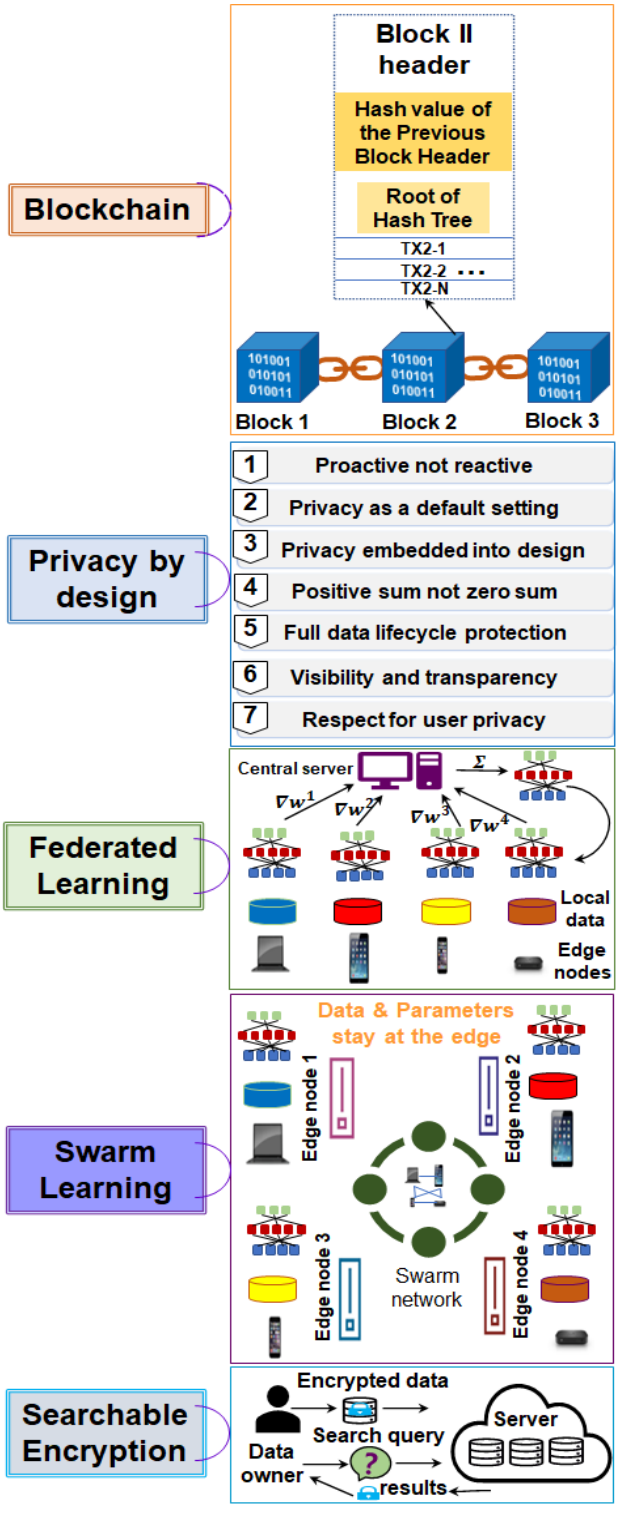

FIGURE 10. Conceptual overview of emerging technologies in the context of COVID-19.

other studies have reviewed the potential application of these emerging technologies to privacy protection in the healthcare industry. Shah *et al.* [313] discussed the potential application of BC to protecting an individual's privacy from the authorities, snoopers, and mutual contacts. Wei *et al.* [314] discussed the uses and designs of various FL algorithms to protect the privacy of patient data. Gerunov [315] discussed the potential uses of the PbD concept to address privacy concerns of individuals. Bahmani *et al.* [316] discussed SL use in protecting an individual's privacy from malevolent attackers. Wang and Papadopoulos [317] discussed three SE approaches to effectively preserve privacy while outsourcing data to cloud settings. Zerka *et al.* [318] discussed the privacy implications of adopting AI-based techniques in the healthcare sector. Zapechnikov *et al.* [319] discussed privacy protection in ML algorithms and suggested FL architectures for effective privacy preservation. All these authors emphasized the need for algorithmic solutions in effectively preserving individual privacy.

TABLE 7. Summary of PPTs that employ emerging technologies to protect user privacy.

Technology	Objectives achieved regarding user's privacy	References
BC	-Privacy protection in medical record sharing -Resolves multiple privacy concerns of EHR -Maintain privacy of personal data -Privacy preservation in mobility data -Privacy protection of personal and tests data	Tan et al. [320] Reegu et al. [321] Tsoi et al. [322] Hiten et al. [323] Abid et al. [324]
PbD	-Privacy guarantee as per user's preferences -Data subject's rights protection via patterns -Privacy preservation in digital systems -Ensures privacy in multiple real-world sectors -Personal data leakage control in algorithms	Ayalon et al. [325] Coelho et al. [326] Emilia et al. [327] Qu et al. [328] Himani et al. [329]
FL	-Restricts privacy issues by sharing model partially -Strong privacy control in care delivery apps -Strong privacy protection in data aggregation -Significant reduction in privacy leakage risk -Effective solution of PUT for researchers	Yang et al. [330] Brooke et al. [331] Yang et al. [332] Sittijuk et al. [333] Eder et al. [334]
SL	-Privacy protection of different data formats in sharing -Personal data privacy protection among peers -Privacy protection of genomics data sharing -Privacy protection in sharing data world-wide -Prevents sensitive information leakage via sanitization	Warnat et al. [335] Yuan et al. [336] Marie et al. [337] Warnat et al. [338] Ahmed et al. [339]
SE	-Privacy control in network logs sharing -Privacy protection in location-based services -Privacy protection in personal data handling -Privacy protection of private data in queries -Privacy protection in data lifecycle -Protection of personal data in query search	Florea et al. [340] Shaham et al. [341] Akremi et al. [342] Li et al. [343] Satish et al. [344] Ibrahim et al. [345]
Hybrid	-PHR protection using BC and FL -Maintain participant's privacy in data -Privacy control in queries via hybrid methods -Personal data privacy protection using CI -Strong control on inference using PPC	Aich et al. [346] Kasyap et al. [347] Zhang et al. [348] Khadam et al. [349] Xue et al. [350]

Abbreviations: EHR= electronic health records, PUT= privacy utility trade-off, PHR= personal health record, CI= computational intelligence, PPC= privacy preserving computing, BC= blockchain, PbD= privacy by design, FL=federated learning, SL= swarm learning, SE= searchable encryption.

VIII. PRIVACY PROTECTION TECHNIQUES THAT ADOPT PRIVACY REGULATIONS/LAWS

Privacy laws and regulations have enormous benefits for the people of any country. They are essential to preserving an individual's rights against powerful authorities, including governments, corporate/political players, service providers and other stakeholders. They enable accountability for privacy violations and personal data abuses. Amid the COVID-19 pandemic, the necessity for legal measures to

TABLE 8. Summary of privacy laws/regulations and their respective studies.

Laws/regulations	Brief description	Corresponding studies
GDPR	-Ensures privacy based on the 'data protection by design' and 'data protection by default' principles. It has suggested plenty of guidelines for protecting personal data. It is one of the most famous laws in the world.	Malina et al. [352], Haque et al. [353], Carvalho et al. [354], Meszaros et al. [355], Gambino et al. [356], Broen et al. [357]
HIPAA	-Ensures privacy of the people by sharing data anonymously, notifying relevant people incase of their privacy breaches, extensive auditing of accesses to personal data, and limiting unauthorized data access.	Pool et al. [123], Harris et al. [358], Ganeshan et al. [359], Sanderson et al. [360], Yoo et al. [361], Choi et al. [362], Khan et al. [363]
PIPA	-Ensures privacy of personal information via data classification (sensitive and non-sensitive), and pseudonymization guideline. This law is solely used in South Korea.	Shin et al. [364], Min et al. [365], Lee et al. [366], Lim et al. [367], Silva et al. [368], Kim et al. [369]
CCPA	-Emphasized the need of personal data collection and processing transparently by respecting individual's privacy.	Rix Ashley [370], Oliva et al. [371], Terry et al. [372], Amankwah et al. [373]
GPL	-Ensures people's privacy in data collection, use, and sharing etc. via technical and organizational privacy measures.	Ramos et al. [374], Pape et al. [375], Kudo et al. [376]

Abbreviations: GDPR= general data protection regulations, HIPAA= health insurance potability and accountability act, PIPA= personal information protection act, CCPA= California consumer privacy act, GPL= German privacy laws.

protect the privacy of minor sects/tribes has been greatly felt under many circumstances around the globe [351]. Furthermore, privacy laws and regulations are paramount for the greater good. Despite World Health Organization (WHO) recommendations regarding discrimination prevention against infected/exposed people, some communities have felt insecure or stigmatized when a virus connection was linked to them. Furthermore, due to non-availability of laws and regulations governing COVID-19–like pandemics, many communities were discriminated against with regard to mobile app use and data collection. Considering the need for laws and regulations, cohesive and substantial efforts are needed to devise rational legal measures. In this work, we present in Table 8 five relevant privacy laws and regulations and recent corresponding studies. Although these laws were proposed before the pandemic, their need has been greatly felt amid the ongoing pandemic. Therefore, some parts and/or chapters have been adopted to address emerging privacy concerns/requirements in recent times.

Although legal measures have tangible benefits for people in general and for service providers, some studies have recently regarded these legal measures (i.e., privacy laws and regulations) as a barrier to system development [377], [378]. Nevertheless, substantial efforts are underway in each country to amend or propose new privacy laws to ensure people's autonomy and self-respect. For example, a new law named the Personal Data Protection Bill (PDP Bill) was recently proposed to preserve people's privacy in India [379]. The seven points of the PDP Bill adhere to changing technologies, and can ensure people's privacy to a great extent. To preserve people's privacy in unanticipated situations like COVID-19, significant amendments are needed in existing laws to better cope with the emerging privacy requirements. Furthermore, new laws that can take into account the unique characteristics of the ongoing pandemic are needed in the near future [380]. In addition, incorporating the role of emerging technologies like BC, FL, SL, and PbD in legal measures in order to address privacy concerns has become more emergent than ever. Additionally, creating awareness among people as to what constitutes privacy, and communicating the risks of privacy disclosures via legal measures, is of paramount importance.

Finally, we demonstrate the quantitative analysis such as the percentage of successful privacy protection rates of PPTs described in the previous five sections in Figure 11. These results are average results obtained from the studies who have reported the privacy-protection-related statistics. This analysis shows the success of PPTs in preserving privacy from different perspectives in the context of COVID-19 pandemic.

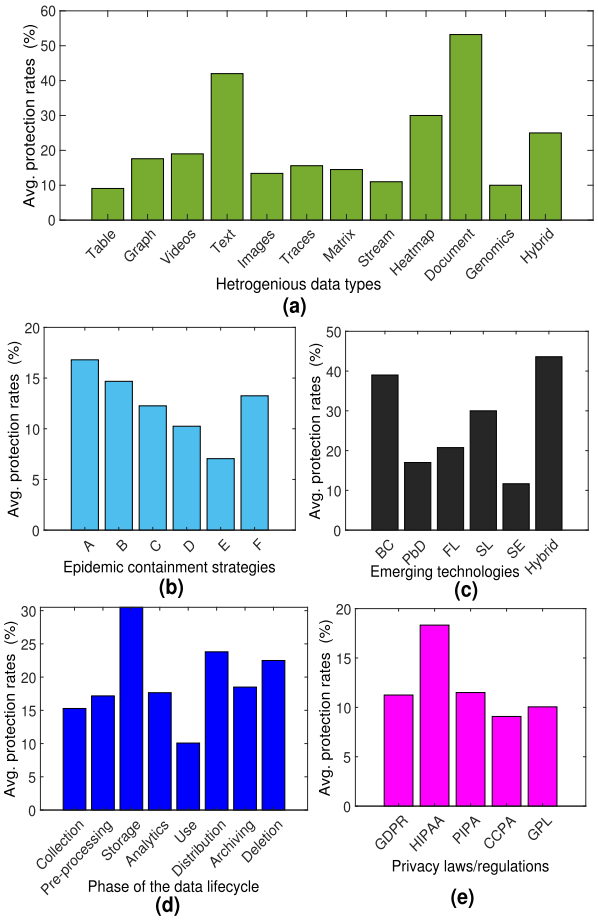

FIGURE 11. Quantitative analysis of recently proposed PPTs in terms of percentage of successful privacy protection rates in the context of COVID-19.

IX. CHALLENGES IN PRESERVING INDIVIDUAL PRIVACY AND PROMISING RESEARCH DIRECTIONS

In this section, we discuss the challenges of preserving individual privacy in recent times, and we suggest promising

research directions regarding privacy preservation for the future.

A. CHALLENGES IN PRESERVING INDIVIDUAL PRIVACY

Due to the significant rise in digital-solution adoption and use, privacy preservation has become more challenging in recent times. Owing to drastic technological developments, many people are concerned about the privacy of their personal information because sensitive data about their daily activities and routines can easily be gathered now. In addition, a 34% increase in digital tracking tools amid the pandemic has spotlighted privacy as an essential requirement for future software development. The collection of personal data is increasing at a rapid pace, and the tendency and scale of the privacy issues is likely to grow in the near future. We summarize 13 unique challenges in preserving individual privacy in recent times.

- *Hidden data collection:* In many digital solutions, personal data are often collected without the user's knowledge and are transferred to corporate/political players. These data can be subject to manipulation for individual tracking and spatial–temporal activity disclosure. Hence, to protect against hidden data collection and the corresponding privacy issues is very challenging.
- *Sensitive information derivation and prediction:* Due to the significant increase in AI use and data availability, sensitive data about a targeted person can now be easily predicted/derived. For example, by correlating demographics and publicly available information, disease/salary information can easily be predicted using AI. To this end, safeguarding sensitive information against AI-based prediction/derivation attacks is very challenging.
- *Illegitimate data aggregation:* Recently, many companies have been collecting massive amounts of personal data for various purposes, including job creation, making recommendations, marketing products, etc. On one hand, the data are handy for data-driven analytics. On the other hand, the practice increases the risk of hidden profiling and misusing aggregate information (e.g., average-age people vs. their interests), because people are mostly unaware of such data processing and handling. To control data aggregation amid this digital surge is challenging.
- *Contextual information disclosure via heterogeneous sources data fusion:* Many individuals use multiple digital solutions (mobile devices, laptops, and online portals) simultaneously. To this end, collection of different information, such as spatial–temporal activities, residential information, social interactions and their frequency, workplaces, etc., can easily be obtained. This information can be fused with other data collection sources (e.g., cellular network data and credit card data) to infer sensitive information about individuals derived via analytics [381]. Hence, providing sufficient resilience against privacy threats that can occur due to heterogeneous source data fusion is challenging.
- *Implementation of strict privacy-enhancing technologies (PETs):* To preserve an individual's privacy from malevolent adversaries, some strict PETs (e.g., PbD, zero-knowledge proofs, and confidential computing) have recently been suggested. However, the true realization of these PETs in order to restrict privacy breaches is very challenging from all perspectives.
- *Shifting most computations from centralized to decentralized/hybrid settings:* Thus far, personal data are mainly collected from relevant individuals, and are processed in centralized settings (e.g., servers). By removing the data from the users, processing at a central server can be subject to manipulation and/or abuse. In some cases, personal data can be stolen from the server or sold to third parties to accomplish scientific/business goals. Hence, transitioning from centralized settings to hybrid/decentralized settings has become imperative, but it is not straightforward, because processing personal data in a decentralized/hybrid manner can still be subject to manipulation, and can result in less utility. Thence, devising methods in order to move computation from central to local/hybrid settings is a challenging task.
- *Inadequate mechanisms for appropriate data collection:* Generally, personal data are collected from individuals without communicating the risks from doing it. In some cases, unneeded (but private) data are collected as a pro-active measure. For example, in South Korea at the beginning of the pandemic, everyone was supposed to report medical information every morning before going to work. On one hand, that can assist in understanding the problem from multiple perspectives, or can help lower disease propagation. On the other hand, it can increase the chances of privacy violations and personal data misuse. Hence, devising mechanisms to collect fewer—but relevant—data is very challenging.
- *Chain of custody of personal information:* Generally, after collecting personal data, the use of those personal data no longer remains visible to the data providers. Thus, personal information can be subject to hidden manipulations and cross-system transfers. On top of that, complete trails of personal information (where it goes, who processed it, where it is now), and whether it has been removed completely from the system or not, remain questionable. Therefore, addressing all these concerns by making personal information processing transparent, and ensuring chain of custody of personal information, is very challenging.
- *Creating personalized privacy protection and user-centric tools:* As mentioned earlier, privacy is highly subjective, and its perception varies from person to person. Recently, in order to address the varying privacy requirements of a subset of people, personalized PPTs have been developed [382]–[384]. Despite the success of these approaches, incorporating each user's privacy requirements is challenging. Furthermore, developing highly user-centric tools can increase the variability in

data, which in turn can impact the quality of analysis. Thence, addressing personalized privacy problems and developing systems based on user's expectations/preferences has become challenging in recent times.

- *Developing generic solutions that can work with diverse data styles:* Generally, person-specific data can exist in multiple styles (graphs, matrix, traces, tables, etc.), and existing privacy protection tools can find it hard to process more than one or two data styles. For instance, PPTs proposed for tabular data yield infeasible results from graph data, and vice versa. Hence, developing PPTs that can function with different styles of data enclosing sensitive and non-sensitive information is challenging. In addition, evaluation metrics that quantify the privacy-preservation and utility-enhancement level across diverse data styles is also challenging.
- *Development of low-cost privacy preserving solutions that can work on client devices:* A lot of effort is now underway to move computations from centralized architectures to decentralized architectures (a.k.a. cellphones/edge devices) [385]–[387]. Moreover, due to the resource-constrained nature of these devices, making lightweight, privacy-preserving solutions is very challenging. Additionally, formal analysis and experimental evaluation of such PPTs regarding performance is guaranteed to impose significant challenges for developers/researchers.
- *Safeguarding personal information from AI-powered attacks:* Recently, AI techniques have shown great promise against knowledge extraction from large-scale and high-dimensional person-specific datasets [388]. These techniques have also been used to secure personal data from a variety of practical attacks that occur during data collection, transfer, publishing, and/or storage, etc. [389]–[391]. On one hand, AI techniques are used to address privacy issues. On the other hand, these techniques assist malevolent adversaries to compromise individual as well as group privacy [392]–[394]. Hence, safeguarding personal information from AI-powered attacks, and preventing large-scale privacy attacks, is very challenging.
- *Addressing the privacy-versus-utility trade-off:* Privacy and utility are two conflicting goals—optimizing privacy can downgrade utility [395], [396]. To this end, devising low-cost solutions that can effectively address this long-standing problem is very challenging. On top of that, quantifying the exact amount of privacy and utility while handling personal data is also very difficult.

B. PROMISING FUTURE RESEARCH DIRECTIONS

Due to the significant rise in digitization, privacy protection is gaining more and more attention, and it has become an active area of research in recent times [397]–[399]. Based on extensive analysis of the published literature, the challenges/threats to individual privacy, and the recently developed countermeasures, we suggest in Figure 12 various promising open problems that need further development and research from both industry and academia in the near future.

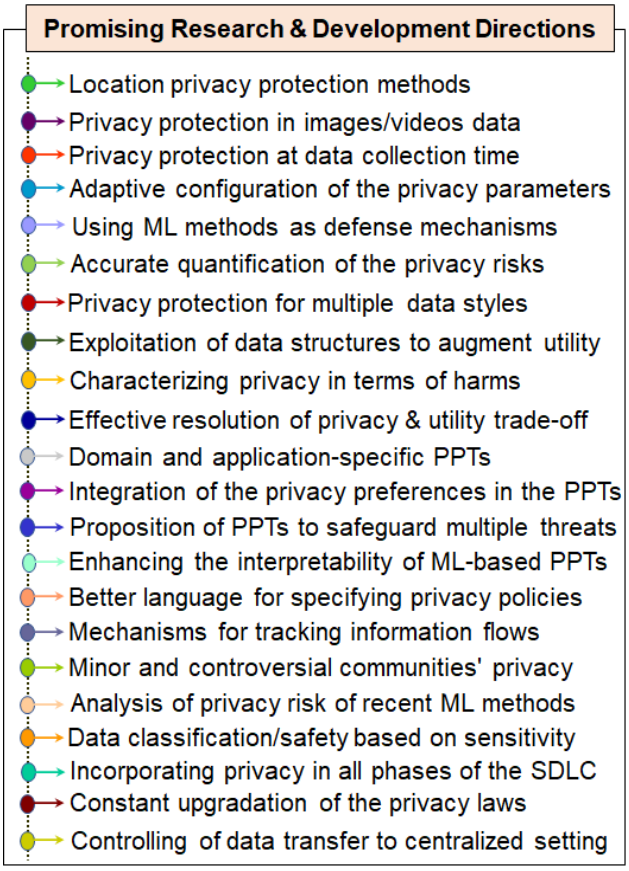

FIGURE 12. Promising research and development directions for the future.

Since the COVID-19 outbreak, location data have been extensively used for multiple purposes (e.g., flow modeling, mobility analysis, contact tracing, and compliance monitoring within government guidelines), and many digital services are harnessing location data constantly. Accordingly, various PPTs have been proposed to address the emerging privacy issues in handling location data [400]. Despite the success of these approaches, devising more practical solutions for privacy protection in trajectory/location data is an important avenue for future research. Recently, due to significant advancements in AI and computer vision techniques, multimedia data (i.e., images and videos) are being processed in multiple applications. However, there is a lack of practical PPTs to address privacy issues in multimedia. Hence, devising low-cost and practical solutions to address privacy issues in multimedia is a vibrant area of research. As stated in a previous study [40], there is a significant lack of PPTs that can be applied at data collection time. Therefore, devising robust PPTs that can address privacy issues at data collection time is still an open research direction. Many PPTs require parameter configuration (k, ℓ, t, ϵ, etc.), and their values can significantly impact the level of both privacy and utility [401].

Therefore, devising PPTs with fewer parameters for configuration, or possibly self-learning parameter values based on data, is still an open issue in the privacy domain. In recent years, ML has been extensively used to address various privacy concerns emerging from digitization [402]–[405]. Therefore, employing different ML concepts and techniques to secure personal data is an interesting area of research.

Generally, privacy risks are highly associated with the nature of the data, the data owners, the settings for data processing (centralized, decentralized, hybrid), adversaries' skills, etc. Quantifying privacy risks accurately needs domain expertise and underlying data knowledge in a fine-grained manner [406]. Thus, devising accurate privacy-risk quantification methods for different data styles/sectors is an important avenue for future research. Most of the existing PPTs are data type–dependent, meaning one PPT that has been proposed for tabular data yields infeasible results when processing, for example, graphs. To increase privacy protection for different data styles, development of unified frameworks that can process and ensure privacy in different data styles is needed in the near future. In some scenarios, utility is preferred over privacy for the national interest or to understand an underlying problem. To this end, proposing and evaluating PPTs that can exploit data structures in order to yield superior utility with considerable privacy is an open research area. Harms due to a privacy breach varies in nature (for example, loss of service/benefits due to a privacy breach, psychological damage due to unconventional sex practices or cosmetics surgery information disclosures, and/or loss of an employment opportunity due to personal information disclosure) [407]. Hence, there is an emerging need for methods that can accurately characterize harm in different privacy contexts. Another long-standing challenge in PPT development is effective resolution of the privacy-versus-utility trade-off. Despite many developments, this dilemma is still unsolved [408]. To this end, devising new data-driven and adaptive PPTs, or improving the performance of existing PPTs in this regard, is a promising research area.

Due to the change in features and data types of each domain and application, there is a significant lack of reusability in existing PPTs. The PPT proposed for one domain yields inconsistent performance in another, slightly different, domain. To address this issue, developing flexible PPTs that can be used in multiple domains/applications with slight modification/tuning is a vibrant research area. Recently, there has been increasing focus on developing privacy preferences–aware PPTs [409]–[411]. Meanwhile, due to huge diversities in privacy preferences, devising unified frameworks is very challenging. Thus, in order to preserve individual privacy, preferences-aware PPTs are needed in the near future. Apart from the promising directions cited above, developing PPTs that can ensure resilience against multiple privacy threats is an emerging area of research. Recently, many AI-powered methods are using tremendous amounts of personal data enclosed in tables, images, videos, and sequences, etc., for training [412], [413]. However, due to the complex nature of these methods, hidden data leakages are possible. Thence, augmenting the interpretability and explainability of the PPTs that employ AI-based methods is one of the promising avenues for future research. The last eight directions listed in Figure 12 are mainly related to development. In this regard, choosing reasonable language when writing privacy policies, ensuring end-to-end security of data, protecting against cluster/sparsity effects, data classification (based on sensitivity) in software, analyzing the risk of ML techniques, upgrading and following privacy laws, and controlling data transfer to central servers, need significant development from industry.

Besides the promising research and development directions cited above, a promising avenue for future research is preserving individual privacy in synthetic data. On one hand, synthetic data can aid in conducting research on personal data with relatively fewer privacy concerns, and synthetic data can be extensively used in training ML methods [414], [415]. On the other hand, it can be subject to manipulation and privacy issues if it is closely tailored by the original data [80]. Therefore, analyzing the privacy and utility levels offered by synthetic data is a promising avenue to help the community when access to the original data is restricted due to privacy issues [416]. In addition, devising feasible synthetic data–generation tools for the greater good is an interesting research direction. Recently, due to the advancements in FL techniques, record-level disclosures can occur while processing personal data [417]. Therefore, practical countermeasures to avoid such attacks are needed in the emerging technologies context. Furthermore, applying a weightage concept to attribute values in order to safeguard individual privacy is a relatively new research area [418]–[420]. Therefore, devising PPTs that can extract attribute information to the greatest extent possible in order to enable secure personal data sharing is a vibrant area of research. Last but not least, there is a lack of unified privacy and utility evaluation metrics. The existing metrics are highly domain- and data style–dependent. Therefore, feasibility analysis of the existing metrics based on the emerging types of data (e.g., sensors, SNs, and wearables), and proposing new evaluation metrics that can have wider applicability, are emerging avenues for future research.

X. CONCLUSION

In this paper, we reviewed and described the findings of most of the recent studies that have proposed ways to combat emerging privacy threats in the context of the ongoing COVID-19 pandemic. Recently, there has been an increasing focus on developing practical PPTs as quickly as possible due to the significant rise in personal data transitions into cyberspace via digital solutions, and the corresponding rise in privacy issues. Owing to the drastic software development in the ''new normal,'' a huge amount of personal data can now be easily collected about individual activities, daily routines, stay points, hobbies, social interactions, and work schedules, to name a few. Although such data are invaluable for managing and containing the pandemic, collecting

them can increase the chances of privacy breaches. Thus, privacy protection will likely remain in the spotlight in the near future amid continuous technical developments. In this work, we provided detailed background about information privacy before discussing the paradigm shifts triggered by the ongoing pandemic in personal data handling and the corresponding privacy issues. We categorized the existing PPTs based on the different types of data and anonymity operations employed to protect privacy in the respective data types. We provided a systemic mapping of PPTs to different epidemic containment strategies (contact tracing, quarantine monitoring, symptom reporting, etc.) that are used to fight the pandemic. We mapped the existing PPTs to eight phases of the data lifecycle adopted by most epidemic handling systems across the globe. In addition, we discussed PPTs that employ the concepts of five emerging technologies in order to preserve individual privacy effectively. We summarized the recent PPTs that have followed the guidelines of famous privacy laws and regulations in order to preserve individual and minority sects/communities' privacy. Finally, promising avenues for future research in the privacy area, and challenges involved in protecting privacy amid continuous technical developments, were discussed. The detailed analysis presented in this article provides deeper insights into recently developed PPTs and future research dynamics. Based on extensive analysis, we found that no single PPT can mitigate all kinds of privacy threats stemming from the ongoing pandemic. However, PPTs that employ emerging technologies concepts are believed to be the most efficient solution for safeguarding individuals' privacy from contemporary privacy threats such as tracking, profiling, and daily activities disclosures. Recently, federated analytics has emerged as a new paradigm that effectively solves the tasks related to data analytics without centralizing personal data from devices [421], [422]. In future work, we plan to analyze the efficacy of federated analytics regarding individual privacy protection, and examine the recent developments in this regard.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

REFERENCES

[1] C. S. Wagner, X. Cai, Y. Zhang, and C. V. Fry, "One-year in: COVID-19 research at the international level in CORD-19 data," *SSRN Electron. J.*, pp. 1–43, Sep. 2021, doi: 10.2139/ssrn.3874974.

[2] Y. Nishimura, T. Miyoshi, H. Hagiya, Y. Kosaki, and F. Otsuka, "Burnout of healthcare workers amid the COVID-19 pandemic: A Japanese cross-sectional survey," *Int. J. Environ. Res. Public Health*, vol. 18, no. 5, p. 2434, Mar. 2021.

[3] G. Newlands, C. Lutz, A. Tamò-Larrieux, E. F. Villaronga, R. Harasgama, and G. Scheitlin, "Innovation under pressure: Implications for data privacy during the COVID-19 pandemic," *Big Data Soc.*, vol. 7, no. 2, 2020, Art. no. 2053951720976680.

[4] R. A. Fahey and A. Hino, "COVID-19, digital privacy, and the social limits on data-focused public health responses," *Int. J. Inf. Manage.*, vol. 55, Dec. 2020, Art. no. 102181.

[5] F. Hassandoust, S. Akhlaghpour, and A. C. Johnston, "Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective," *J. Amer. Med. Inform. Assoc.*, vol. 28, no. 3, pp. 463–471, Mar. 2021.

[6] N. Y. Ahn, J. E. Park, D. H. Lee, and P. C. Hong, "Balancing personal privacy and public safety during COVID-19: The case of South Korea," *IEEE Access*, vol. 8, pp. 171325–171333, 2020.

[7] H. O'Connor, W. J. Hopkins, and D. Johnston, "For the greater good? Data and disasters in a post-COVID world," *J. Roy. Soc. New Zealand*, vol. 51, no. 1, pp. S214–S231, May 2021.

[8] A. Zwitter and O. J. Gstrein, "Big data, privacy and COVID-19–learning from humanitarian expertise in data protection," Wellcome Trust, London, U.K., Tech. Rep. PMC7808050, 2020.

[9] F. Almeida, J. D. Santos, and J. A. Monteiro, "The challenges and opportunities in the digitalization of companies in a post-COVID-19 world," *IEEE Eng. Manag. Rev.*, vol. 48, no. 3, pp. 97–103, Sep. 2020.

[10] K. Michael and R. Abbas, "Behind COVID-19 contact trace apps: The Google—Apple partnership," *IEEE Consum. Electron. Mag.*, vol. 9, no. 5, pp. 71–76, Sep. 2020.

[11] S. Nisar, M. A. Zuhaib, A. Ulasyar, and M. Tariq, "A privacy-preserved and cost-efficient control scheme for coronavirus outbreak using call data record and contact tracing," *IEEE Consum. Electron. Mag.*, vol. 10, no. 2, pp. 104–110, Mar. 2021.

[12] S. Nisar, M. A. Zuhaib, A. Ulasyar, and M. Tariq, "A robust tracking system for COVID-19 like pandemic using advanced hybrid technologies," *Computing*, pp. 1–15, May 2021, doi: 10.1007/s00607-021-00946-6.

[13] S. McLennan, L. A. Celi, and A. Buyx, "COVID-19: Putting the general data protection regulation to the test," *JMIR Public Health Surveill.*, vol. 6, no. 2, May 2020, Art. no. e19279.

[14] M. Ienca and E. Vayena, "On the responsible use of digital data to tackle the COVID-19 pandemic," *Nature Med.*, vol. 26, no. 4, pp. 463–464, Apr. 2020.

[15] B. M. Knoppers, M. J. S. Beauvais, Y. Joly, M. H. Zawati, S. Rousseau, M. Chassé, and V. Mooser, "Modeling consent in the time of COVID-19," *J. Law Biosci.*, vol. 7, no. 1, Jul. 2020, Art. no. lsaa020.

[16] S. Sauermann, C. Kanjala, M. Templ, and C. C. Austin, "Preservation of individuals' privacy in shared COVID-19 related data," *SSRN Electron. J.*, pp. 1–13, Jul. 2020, doi: 10.2139/ssrn.3648430.

[17] C. C. Austin, A. Bernier, L. Bezuidenhout, J. Bicarregui, T. Biro, A. Cambon-Thomsen, S. R. Carroll, Z. Cournia, P. W. Dabrowski, G. Diallo, and T. Duflot, "Fostering global data sharing: Highlighting the recommendations of the research data alliance COVID-19 working group," *Wellcome Open Res.*, vol. 5, p. 267, May 2021.

[18] B. D. A. Almeida, D. Doneda, M. Y. Ichihara, M. Barral-Netto, G. C. Matta, E. T. Rabello, F. C. Gouveia, and M. Barreto, "Personal data usage and privacy considerations in the COVID-19 global pandemic," *Ciência Saúde Coletiva*, vol. 25, pp. 2487–2492, Jun. 2020.

[19] K. Yu, L. Tan, X. Shang, J. Huang, G. Srivastava, and P. Chatterjee, "Efficient and privacy-preserving medical research support platform against COVID-19: A blockchain-based approach," *IEEE Consum. Electron. Mag.*, vol. 10, no. 2, pp. 111–120, Mar. 2021.

[20] W. Houfaf-Khoufaf and G. Touya, "Geographically masking addresses to study COVID-19 clusters," *Cartography Geographic Inf. Sci.*, 2020, doi: 10.1080/15230406.2021.1977709.

[21] H. Diddee and B. Kansra, "CrossPriv: User privacy preservation model for cross-silo federated software," in *Proc. 35th IEEE/ACM Int. Conf. Automated Softw. Eng.*, Dec. 2020, pp. 1370–1372.

[22] P. K. Vadrevu, S. K. Adusumalli, and V. K. Mangalapalli, "A hybrid approach for personal differential privacy preservation in homogeneous and heterogeneous health data sharing," *High Technol. Lett.*, vol. 26, no. 9, pp. 1–17, 2020.

[23] B. Sowmiya, V. S. Abhijith, S. Sudersan, R. S. J. Sundar, M. Thangavel, and P. Varalakshmi, "A survey on security and privacy issues in contact tracing application of COVID-19," *Social Netw. Comput. Sci.*, vol. 2, no. 3, pp. 1–11, May 2021.

[24] P. K. Vadrevu, S. K. Adusumalli, V. K. Mangalapalli, and S. K. Swain, "A review on privacy preservation techniques in surveillance and health care data publication," *Int. J. Eng. Res. Technol.*, vol. 9, no. 5, 2021.

[25] D. Zeinalipour-Yazti and C. Claramunt, "COVID-19 mobile contact tracing apps (MCTA): A digital vaccine or a privacy demolition?" in *Proc. 21st IEEE Int. Conf. Mobile Data Manage. (MDM)*, Jun. 2020, pp. 1–4.

[26] H. R. Schmidtke, "Location-aware systems or location-based services: A survey with applications to CoViD-19 contact tracking," *J. Reliable Intell. Environ.*, vol. 6, no. 4, pp. 191–214, Dec. 2020.

[27] J. Shuja, E. Alanazi, W. Alasmary, and A. Alashaikh, "COVID-19 open source data sets: A comprehensive survey," *Appl. Intell.*, vol. 51, no. 3, pp. 1296–1325, 2020.

[28] E. N. Sihombing, C. Hadita, and M. Y. A. Syaputra, "Legal securities against privacy data for Covid-19 patients in Indonesia," *Veteran Law Rev.*, vol. 4, no. 1, pp. 35–52, 2021.

[29] V. von Wyl, M. Höglinger, C. Sieber, M. Kaufmann, A. Moser, M. Serra-Burriel, T. Ballouz, D. Menges, A. Frei, and M. A. Puhan, "Drivers of acceptance of COVID-19 proximity tracing apps in Switzerland: Panel survey analysis," *JMIR Public Health Surveill.*, vol. 7, no. 1, Jan. 2021, Art. no. e25701.
[30] B. M. Zimmermann, A. Fiske, S. McLennan, A. Sierawska, N. Hangel, and A. Buyx, "Motivations and limits for COVID-19 policy compliance in Germany and Switzerland," *Int. J. Health Policy Manage.*, pp. 1–12, Apr. 2021, doi: 10.34172/ijhpm.2021.30.
[31] J. Kim and M.-P. Kwan, "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.*, vol. 10, no. 1, p. 25, Jan. 2021.
[32] G. Jung, H. Lee, A. Kim, and U. Lee, "Too much information: Assessing privacy risks of contact trace data disclosure on people with COVID-19 in South Korea," *Frontiers Public Health*, vol. 8, p. 305, Jun. 2020.
[33] V. Shubina, S. Holcer, M. Gould, and E. S. Lohan, "Survey of decentralized solutions with mobile devices for user location tracking, proximity detection, and contact tracing in the COVID-19 era," *Data*, vol. 5, no. 4, p. 87, Sep. 2020.
[34] S. Altmann, L. Milsom, H. Zillessen, R. Blasone, F. Gerdon, R. Bach, F. Kreuter, D. Nosenzo, S. Toussaert, and J. Abeler, "Acceptability of app-based contact tracing for COVID-19: Cross-country survey study," *JMIR mHealth uHealth*, vol. 8, no. 8, Aug. 2020, Art. no. e19857.
[35] M. A. Ferrag, L. Shu, and K.-K.-R. Choo, "Fighting COVID-19 and future pandemics with the Internet of Things: Security and privacy perspectives," *IEEE/CAA J. Automatica Sinica*, vol. 8, no. 9, pp. 1477–1499, Sep. 2021.
[36] S. Park, G. J. Choi, and H. Ko, "Information technology–based tracing strategy in response to COVID-19 in South Korea-privacy controversies," *Jama*, vol. 323, no. 21, pp. 2129–2130, 2020.
[37] Y. He, A. Aliyu, M. Evans, and C. Luo, "Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review," *J. Med. Internet Res.*, vol. 23, no. 4, Apr. 2021, Art. no. e21747.
[38] M. Becker, "Privacy in the digital age: Comparing and contrasting individual versus social approaches towards privacy," *Ethics Inf. Technol.*, vol. 21, no. 4, pp. 307–317, Dec. 2019.
[39] R. Mendes and J. P. Vilela, "Privacy-preserving data mining: Methods, metrics, and applications," *IEEE Access*, vol. 5, pp. 10562–10582, 2016.
[40] M. Cunha, R. Mendes, and J. P. Vilela, "A survey of privacy-preserving mechanisms for heterogeneous data types," *Comput. Sci. Rev.*, vol. 41, Aug. 2021, Art. no. 100403.
[41] A. Majeed and S. Lee, "Anonymization techniques for privacy preserving data publishing: A comprehensive survey," *IEEE Access*, vol. 9, pp. 8512–8545, 2021.
[42] A. Majeed, "Towards privacy paradigm shift due to the pandemic: A brief perspective," *Inventions*, vol. 6, no. 2, p. 24, Mar. 2021.
[43] R. E. Foraker, A. M. Lai, T. G. Kannampallil, K. F. Woeltje, A. M. Trolard, and P. R. O. Payne, "Transmission dynamics: Data sharing in the COVID-19 era," *Learn. Health Syst.*, vol. 5, no. 1, Jan. 2021, Art. no. e10235.
[44] J. Ahmed and Q. Tushar, "COVID-19 pandemic: A new era of cyber security threat and holistic approach to overcome," in *Proc. IEEE Asia–Pacific Conf. Comput. Sci. Data Eng. (CSDE)*, Dec. 2020, pp. 1–5.
[45] F. Almeida, J. D. Santos, and J. A. Monteiro, "The challenges and opportunities in the digitalization of companies in a Post-COVID-19 world," *IEEE Eng. Manag. Rev.*, vol. 48, no. 3, pp. 97–103, Sep. 2020.
[46] A. Zigomitros, F. Casino, A. Solanas, and C. Patsakis, "A survey on privacy properties for data publishing of relational data," *IEEE Access*, vol. 8, pp. 51071–51099, 2020.
[47] L. Sweeney, "K-anonymity: A model for protecting privacy," *Int. J. Uncertainty, Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, 2002.
[48] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "L-diversity: Privacy beyond k-anonymity," *ACM Trans. Knowl. Discovery From Data*, vol. 1, no. 1, p. 3, 2007.
[49] N. Li, T. Li, and S. Venkatasubramanian, "T-closeness: Privacy beyond k-anonymity and l-diversity," in *Proc. IEEE 23rd Int. Conf. Data Eng.*, Apr. 2007, pp. 106–115.
[50] H. Xu and N. Zhang, "Implications of data anonymization on the statistical evidence of disparity," *Manage. Sci.*, Jun. 2021, doi: 10.1287/mnsc.2021.4028.
[51] K. Nissim, "Privacy: From database reconstruction to legal theorems," in *Proc. 40th ACM SIGMOD-SIGACT-SIGAI Symp. Princ. Database Syst.*, Jun. 2021, pp. 33–41.
[52] J. Wieringa, P. K. Kannan, X. Ma, T. Reutterer, H. Risselada, and B. Skiera, "Data analytics in a privacy-concerned world," *J. Bus. Res.*, vol. 122, pp. 915–925, Jan. 2021.
[53] C. Dwork, "Differential privacy: A survey of results," in *Proc. Int. Conf. Theory Appl. Models Comput.* Berlin, Germany: Springer, 2008, pp. 1–19.
[54] Z. Luo, D. J. Wu, E. Adeli, and L. Fei-Fei, "Scalable differential privacy with sparse network finetuning," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2021, pp. 5059–5068.
[55] Y. Tian, B. Song, T. Ma, A. Al-Dhelaan, and M. Al-Dhelaan, "Bi-tier differential privacy for precise auction-based people-centric IoT service," *IEEE Access*, vol. 9, pp. 55036–55044, 2021.
[56] M. Ye, G. Hu, L. Xie, and S. Xu, "Differentially private distributed Nash equilibrium seeking for aggregative games," *IEEE Trans. Autom. Control*, early access, Apr. 27, 2021, doi: 10.1109/TAC.2021.3075183.
[57] C. Liu, J. Yang, W. Zhao, Y. Zhang, J. Li, and C. Mu, "Face image publication based on differential privacy," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–20, Jan. 2021.
[58] X. Li, J. Liu, S. Liu, and J. Wang, "Differentially private ensemble learning for classification," *Neurocomputing*, vol. 430, pp. 34–46, Mar. 2021.
[59] H. Yan, X. Li, H. Li, J. Li, W. Sun, and F. Li, "Monitoring-based differential privacy mechanism against query flooding-based model extraction attack," *IEEE Trans. Depend. Sec. Comput.*, early access, Mar. 29, 2021, doi: 10.1109/TDSC.2021.3069258.
[60] J. Zhao, S. Liu, X. Xiong, and Z. Cai, "Differentially private autocorrelation time-series data publishing based on sliding window," *Secur. Commun. Netw.*, vol. 2021, pp. 1–10, Apr. 2021.
[61] M. Bellare, V. T. Hoang, and P. Rogaway, "Foundations of garbled circuits," in *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*, 2012, pp. 784–796.
[62] M. Binjubeir, A. A. Ahmed, M. A. B. Ismail, A. S. Sadiq, and M. K. Khan, "Comprehensive survey on big data privacy protection," *IEEE Access*, vol. 8, pp. 20067–20079, 2020.
[63] Y. Qu, M. R. Nosouhi, L. Cui, and S. Yu, "Existing privacy protection solutions," in *Personalized Privacy Protection Big Data*. Singapore: Springer, 2021, pp. 5–13.
[64] B. Liu, M. Ding, S. Shaham, W. Rahayu, F. Farokhi, and Z. Lin, "When machine learning meets privacy: A survey and outlook," *ACM Comput. Surv.*, vol. 54, no. 2, pp. 1–36, Apr. 2021.
[65] V. Wylde and E. Prakash, "COVID-19 crisis: Is our personal data likely to be breached," Cardiff Metrop. Univ., Cardiff, U.K., Tech. Rep. 28067658, 2021.
[66] H. Wen, Q. Zhao, Z. Lin, D. Xuan, and N. Shroff, "A study of the privacy of COVID-19 contact tracing apps," in *Proc. Int. Conf. Secur. Privacy Commun. Syst.* New York, NY, USA: Springer, 2020, pp. 297–317.
[67] S. Ribeiro-Navarrete, J. R. Saura, and D. Palacios-Marqués, "Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy," *Technol. Forecasting Social Change*, vol. 167, Jun. 2021, Art. no. 120681.
[68] Y. K. Dwivedi, D. L. Hughes, C. Coombs, I. Constantiou, Y. Duan, J. S. Edwards, B. Gupta, B. Lal, S. Misra, P. Prashant, R. Raman, N. P. Rana, S. K. Sharma, and N. Upadhyay, "Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life," *Int. J. Inf. Manage.*, vol. 55, Dec. 2020, Art. no. 102211.
[69] J. Wu, J. Wang, S. Nicholas, E. Maitland, and Q. Fan, "Application of big data technology for COVID-19 prevention and control in China: Lessons and recommendations," *J. Med. Internet Res.*, vol. 22, no. 10, Oct. 2020, Art. no. e21980.
[70] P. Hacker, "Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law," *Eur. Law J. (Forthcoming)*, May 2021. [Online]. Available: https://ssrn.com/abstract=3835259
[71] C. Menni, A. M. Valdes, M. B. Freidin, C. H. Sudre, L. H. Nguyen, D. A. Drew, S. Ganesh, T. Varsavsky, M. J. Cardoso, J. S. E.-S. Moustafa, A. Visconti, P. Hysi, R. C. E. Bowyer, M. Mangino, M. Falchi, J. Wolf, S. Ourselin, A. T. Chan, C. J. Steves, and T. D. Spector, "Real-time tracking of self-reported symptoms to predict potential COVID-19," *Nature Med.*, vol. 26, no. 7, pp. 1037–1040, Jul. 2020.
[72] A. R. Shree, P. Kiran, N. Mohith, and M. Kavya, "Sensitivity context aware privacy preserving disease prediction," in *Expert Clouds and Applications*. Singapore: Springer, 2022, pp. 11–20.
[73] H. Kim, "COVID-19 apps as a digital intervention policy: A longitudinal panel data analysis in South Korea," *Health Policy*, vol. 125, no. 11, pp. 1430–1440, Nov. 2021.

[74] T. Timmers, L. Janssen, J. Stohr, J. L. Murk, and M. A. H. Berrevoets, "Using eHealth to support COVID-19 education, self-assessment, and symptom monitoring in The Netherlands: Observational study," *JMIR mHealth uHealth*, vol. 8, no. 6, Jun. 2020, Art. no. e19822.

[75] T. Kim, Y. Yun, and N. Kim, "Deep learning-based knowledge graph generation for COVID-19," *Sustainability*, vol. 13, no. 4, p. 2276, Feb. 2021.

[76] J. Lyons, A. Akbari, F. Torabi, G. I. Davies, L. North, R. Griffiths, R. Bailey, J. Hollinghurst, R. Fry, S. L. Turner, and D. Thompson, "Understanding and responding to COVID-19 in wales: Protocol for a privacy-protecting data platform for enhanced epidemiology and evaluation of interventions," *BMJ Open*, vol. 10, no. 10, Oct. 2020, Art. no. e043010.

[77] M. Linschoten, "Clinical presentation, disease course and outcome of COVID-19 in hospitalized patients with and without pre-existing cardiac disease: A cohort study across sixteen countries," *MedRxiv*, Mar. 2021, doi: 10.1101/2021.03.11.21253106.

[78] C. E. M. Jakob, F. Kohlmayer, T. Meurers, J. J. Vehreschild, and F. Prasser, "Design and evaluation of a data anonymization pipeline to promote open science on COVID-19," *Sci. Data*, vol. 7, no. 1, pp. 1–10, Dec. 2020.

[79] G. A. Brat, G. M. Weber, N. Gehlenborg, P. Avillach, N. P. Palmer, L. Chiovato, J. Cimino, L. R. Waitman, G. S. Omenn, A. Malovini, and J. H. Moore, "International electronic health record-derived COVID-19 clinical course profiles: The 4ce consortium," *NPJ Digit. Med.*, vol. 3, no. 1, pp. 1–9, 2020.

[80] A. Kuppa, L. Aouad, and N.-A. Le-Khac, "Towards improving privacy of synthetic datasets," in *Annual Privacy Forum*. New York, NY, USA: Springer, May 2021, pp. 106–119, doi: 10.1007/978-3-030-76663-4_6.

[81] M. S. Walia, B. Tierney, and S. McKeever, "Synthesising tabular datasets using wasserstein conditional GANs with gradient penalty (WCGAN-GP)," Technol. Univ. Dublin, Dublin, Ireland, Tech. Rep. 289, 2020.

[82] T. G. Moraes, A. N. L. E. Lemos, A. K. Lopes, C. Moura, and J. R. L. de Pereira, "Open data on the COVID-19 pandemic: Anonymisation as a technical solution for transparency, privacy, and data protection," *Int. Data Privacy Law*, vol. 11, no. 1, pp. 32–47, May 2021.

[83] J. Guo, M. Yang, and B. Wan, "A practical privacy-preserving publishing mechanism based on personalized k-anonymity and temporal differential privacy for wearable IoT applications," *Symmetry*, vol. 13, no. 6, p. 1043, Jun. 2021.

[84] B. Lee, B. Dupervil, N. P. Deputy, W. Duck, S. Soroka, L. Bottichio, B. Silk, J. Price, P. Sweeney, J. Fuld, J. T. Weber, and D. Pollock, "Protecting privacy and transforming COVID-19 case surveillance datasets for public use," *Public Health Rep.*, vol. 136, no. 5, pp. 554–561, Sep. 2021.

[85] Y. Cao, S. Takagi, Y. Xiao, L. Xiong, and M. Yoshikawa, "PANDA: Policy-aware location privacy for epidemic surveillance," 2020, *arXiv:2005.00186*.

[86] P. Vepakomma, S. N. Pushpita, and R. Raskar, "Dams: Meta-estimation of private sketch data structures for differentially private COVID-19 contact tracing," Tech. Rep., 2021. Accessed: Aug. 25, 2021. [Online]. Available: https://www.media.mit.edu/publications/dams-meta-estimation-of-private-sketch-data-structures-for-differentially-private-covid-19-contact-tracing/

[87] Z. Mao, H. Yao, Q. Zou, W. Zhang, and Y. Dong, "Digital contact tracing based on a graph database algorithm for emergency management during the COVID-19 epidemic: Case study," *JMIR mHealth uHealth*, vol. 9, no. 1, Jan. 2021, Art. no. e26836.

[88] A. Gaeta, V. Loia, and F. Orciuoli, "A method based on graph theory and three way decisions to evaluate critical regions in epidemic diffusion: An analysis of COVID-19 in Italy," *Int. J. Speech Technol.*, vol. 51, no. 5, pp. 2939–2955, May 2021.

[89] K. M. Ben Hamed and A. Baryun, "Designing a mobile app to trace covid-19 using social networks," in *Proc. IEEE 1st Int. Maghreb Meeting Conf. Sci. Techn. Autom. Control Comput. Eng. (MI-STA)*, May 2021, pp. 276–281.

[90] E. Meirom, H. Maron, S. Mannor, and G. Chechik, "Controlling graph dynamics with reinforcement learning and graph neural networks," in *Proc. Int. Conf. Mach. Learn.*, 2021, pp. 7565–7577.

[91] A. Baker, I. Biazzo, A. Braunstein, G. Catania, L. Dall'Asta, A. Ingrosso, F. Krzakala, F. Mazza, M. Mézard, A. P. Muntoni, M. Refinetti, S. S. Mannelli, and L. Zdeborová, "Epidemic mitigation by statistical inference from contact tracing data," *Proc. Nat. Acad. Sci. USA*, vol. 118, no. 32, Aug. 2021, Art. no. e2106548118.

[92] C. Lachner, T. Rausch, and S. Dustdar, "A privacy preserving system for AI-assisted video analytics," in *Proc. IEEE 5th Int. Conf. Fog Edge Comput. (ICFEC)*, May 2021, pp. 74–78.

[93] N. Sugianto, D. Tjondronegoro, R. Stockdale, and E. I. Yuwono, "Privacy-preserving AI-enabled video surveillance for social distancing: Responsible design and deployment for public spaces," *Inf. Technol. People*, Jul. 2021, doi: 10.1108/ITP-07-2020-0534.

[94] D. Yang, E. Yurtsever, V. Renganathan, K. A. Redmill, and Ü. Özgüner, "A vision-based social distancing and critical density detection system for COVID-19," *Sensors*, vol. 21, no. 13, p. 4608, Jul. 2021.

[95] O. Reyad, H. M. Mansour, M. Heshmat, and E. A. Zanaty, "Key-based enhancement of data encryption standard for text security," in *Proc. Nat. Comput. Colleges Conf. (NCCC)*, Mar. 2021, pp. 1–6.

[96] R. Catelli, F. Gargiulo, V. Casola, G. De Pietro, H. Fujita, and M. Esposito, "A novel COVID-19 data set and an effective deep learning approach for the de-identification of Italian medical records," *IEEE Access*, vol. 9, pp. 19097–19110, 2021.

[97] C. A. Libbi, J. Trienes, D. Trieschnigg, and C. Seifert, "Generating synthetic training data for supervised de-identification of electronic health records," *Future Internet*, vol. 13, no. 5, p. 136, 2021.

[98] S. Syed, M. Syed, H. B. Syeda, M. Garza, W. Bennett, J. Bona, S. Begum, A. Baghal, M. Zozus, and F. Prior, "API driven on-demand participant ID pseudonymization in heterogeneous multi-study research," *Healthcare Informat. Res.*, vol. 27, no. 1, pp. 39–47, Jan. 2021.

[99] O. Reyad and M. E. Karar, "Secure CT-image encryption for COVID-19 infections using HBBS-based multiple key-streams," *Arabian J. Sci. Eng.*, vol. 46, no. 4, pp. 3581–3593, Apr. 2021.

[100] K. Packhäuser, S. Gündel, N. Münster, C. Syben, V. Christlein, and A. Maier, "Is medical chest X-ray data anonymous?" 2021, *arXiv:2103.08562*.

[101] G. Kaissis, A. Ziller, J. Passerat-Palmbach, T. Ryffel, D. Usynin, A. Trask, I. Lima, J. Mancuso, F. Jungmann, M.-M. Steinborn, A. Saleh, M. Makowski, D. Rueckert, and R. Braren, "End-to-end privacy preserving deep learning on multi-institutional medical imaging," *Nature Mach. Intell.*, vol. 3, no. 6, pp. 473–484, Jun. 2021.

[102] A. Ziller, D. Usynin, R. Braren, M. Makowski, D. Rueckert, and G. Kaissis, "Medical imaging deep learning with differential privacy," *Sci. Rep.*, vol. 11, no. 1, pp. 1–8, Dec. 2021.

[103] A. Ulhaq and O. Burmeister, "COVID-19 imaging data privacy by federated learning design: A theoretical framework," 2020, *arXiv:2010.06177*.

[104] M. Nabil, A. Sherif, M. Mahmoud, W. Alsmary, and M. Alsabaan, "Privacy-preserving non-participatory surveillance system for COVID-19-like pandemics," *IEEE Access*, vol. 9, pp. 79911–79926, 2021.

[105] C. Guo, J. Jia, K.-K.-R. Choo, and Y. Jie, "Privacy-preserving image search (PPIS): Secure classification and searching using convolutional neural network over large-scale encrypted medical images," *Comput. Secur.*, vol. 99, Dec. 2020, Art. no. 102021.

[106] F. Liu, D. Wang, and Z.-Q. Xu, "Privacy-preserving travel time prediction with uncertainty using GPS trace data," *IEEE Trans. Mobile Comput.*, early access, Apr. 21, 2021, doi: 10.1109/TMC.2021.3074865.

[107] A. Farzanehfar, F. Houssiau, and Y.-A. de Montjoye, "The risk of re-identification remains high even in country-scale location datasets," *Patterns*, vol. 2, no. 3, Mar. 2021, Art. no. 100204.

[108] L. Reichert, S. Brack, and B. Scheuermann, "Lighthouses: A warning system for super-spreader events," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2021, pp. 1–6.

[109] B. Bozdemir, S. Canard, O. Ermis, H. Möllering, M. Önen, and T. Schneider, "Privacy-preserving density-based clustering," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, May 2021, pp. 658–671.

[110] S. Lestyán, G. Ács, and G. Biczók, "Privacy-preserving release of mobility data: A clean-slate approach," 2020, *arXiv:2008.01665*.

[111] H. Lin, S. Garg, J. Hu, X. Wang, M. Jalil Piran, and M. S. Hossain, "Privacy-enhanced data fusion for COVID-19 applications in intelligent Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15683–15693, Nov. 2021.

[112] L. Burkhalter, N. Küchler, A. Viand, H. Shafagh, and A. Hithnawi, "Zeph: Cryptographic enforcement of end-to-end data privacy," in *Proc. 15th USENIX Symp. Operating Syst. Design Implement. (OSDI)*, 2021, pp. 387–404.

[113] R. Iyer, R. Rex, K. P. McPherson, D. Gandhi, A. Mahindra, A. Singh, and R. Raskar, "Spatial K-anonymity: A privacy-preserving method for COVID-19 related geospatial technologies," 2021, *arXiv:2101.02556*.

[114] C. Iwendi, S. A. Moqurrab, A. Anjum, S. Khan, S. Mohan, and G. Srivastava, "N-sanitization: A semantic privacy-preserving framework for unstructured medical datasets," *Comput. Commun.*, vol. 161, pp. 160–171, Sep. 2020.

[115] C. Lohr, E. Eder, and U. Hahn, "Pseudonymization of PHI items in German clinical reports," in *Public Health and Informatics*. Amsterdam, The Netherlands IOS Press, 2021, pp. 273–277.
[116] G. Geller, P. Duggal, C. L. Thio, D. Mathews, J. P. Kahn, L. L. Maragakis, and B. T. Garibaldi, "Genomics in the era of COVID-19: Ethical implications for clinical practice and public health," *Genome Med.*, vol. 12, no. 1, pp. 1–4, Dec. 2020.
[117] B. Abinaya and S. Santhi, "A survey on genomic data by privacy-preserving techniques perspective," *Comput. Biol. Chem.*, vol. 93, Aug. 2021, Art. no. 107538.
[118] J. Scheibner, J. L. Raisaro, J. R. Troncoso-Pastoriza, M. Ienca, J. Fellay, E. Vayena, and J.-P. Hubaux, "Revolutionizing medical data sharing using advanced privacy-enhancing technologies: Technical, legal, and ethical synthesis," *J. Med. Internet Res.*, vol. 23, no. 2, Feb. 2021, Art. no. e25120.
[119] K. Barker, E. Uribe-Jongbloed, and T. Scholz, "Privacy as public good—A comparative assessment of the challenge for CoronApps in Latin America," *J. Law, Technol. Trust*, vol. 1, no. 1, pp. 1–24, Dec. 2020.
[120] G. Deb, "The data privacy landscape during COVID-19: An exploration of some of the major data privacy regulations and trends," *DePaul J. Art, Technol. Intellectual Property Law*, vol. 31, no. 1, p. 1, 2021.
[121] S. Becher, A. Gerl, B. Meier, and F. Bölz, "Big picture on privacy enhancing technologies in e-health: A holistic personal privacy workflow," *Information*, vol. 11, no. 7, p. 356, Jul. 2020.
[122] S. Masiero, "COVID-19: What does it mean for digital social protection?" *Big Data Soc.*, vol. 7, no. 2, Jul. 2020, Art. no. 205395172097899.
[123] J. Pool, S. Akhlaghpour, and F. Fatehi, "Health data privacy in the COVID-19 pandemic context: Discourses on HIPAA," in *Navigating Healthcare Through Challenging Times*. Amsterdam, The Netherlands: IOS Press, 2021, pp. 70–77.
[124] V. Shubina, A. Ometov, A. Basiri, and E. S. Lohan, "Effectiveness modelling of digital contact-tracing solutions for tackling the COVID-19 pandemic," *J. Navigat.*, vol. 74, pp. 1–34, Apr. 2021.
[125] T. Carter, J. A. Kroll, and J. Bret Michael, "Lessons learned from applying the NIST privacy framework," *IT Prof.*, vol. 23, no. 4, pp. 9–13, Jul. 2021.
[126] C. M. Peak, R. Kahn, Y. H. Grad, L. M. Childs, R. Li, M. Lipsitch, and C. O. Buckee, "Individual quarantine versus active monitoring of contacts for the mitigation of COVID-19: A modelling study," *Lancet Infectious Diseases*, vol. 20, no. 9, pp. 1025–1033, Sep. 2020.
[127] M. Rezaei and M. Azarmi, "DeepSOCIAL: Social distancing monitoring and infection risk assessment in COVID-19 pandemic," *Appl. Sci.*, vol. 10, no. 21, p. 7514, Oct. 2020.
[128] A. T. Chan and J. S. Brownstein, "Putting the public back in public health—Surveying symptoms of COVID-19," *New England J. Med.*, vol. 383, no. 7, p. e45, Aug. 2020.
[129] Y. Chen, C. K. Leung, S. Shang, and Q. Wen, "Temporal data analytics on COVID-19 data with ubiquitous computing," in *Proc. IEEE Int. Conf Parallel Distrib. Process. With Appl., Big Data Cloud Comput., Sustain. Comput. Commun., Social Comput. Netw. (ISPA/BDCloud/SocialCom/SustainCom)*, Dec. 2020, pp. 958–965.
[130] A. S. Arora, H. Rajput, and R. Changotra, "Current perspective of COVID-19 spread across South Korea: Exploratory data analysis and containment of the pandemic," *Environ., Develop. Sustainability*, vol. 23, no. 5, pp. 6553–6563, May 2021.
[131] L. Xiong, C. Shahabi, Y. Da, R. Ahuja, V. Hertzberg, L. Waller, X. Jiang, and A. Franklin, "React: Real-time contact tracing and risk monitoring using privacy-enhanced mobile tracking," *SIGSPATIAL Special*, vol. 12, no. 2, pp. 3–14, 2020.
[132] C. Costa, B. T. Nixon, S. Bhattacharjee, B. Graybill, D. Zeinalipour-Yazti, W. Schneider, and P. K. Chrysanthis, "A context, location and preference-aware system for safe pedestrian mobility," in *Proc. 22nd IEEE Int. Conf. Mobile Data Manage. (MDM)*, Jun. 2021, pp. 217–224.
[133] N. Ahmed, R. A. Michelin, W. Xue, G. D. Putra, W. Song, S. Ruj, S. S. Kanhere, and S. Jha, "Towards privacy-preserving digital contact tracing," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2021, pp. 1–3.
[134] C. Zhang, C. Xu, K. Sharif, and L. Zhu, "Privacy-preserving contact tracing in 5G-integrated and blockchain-based medical applications," *Comput. Standards Interface*, vol. 77, Aug. 2021, Art. no. 103520.
[135] F. Doku and E. Doku, "Khopesh-contact tracing without sacrificing privacy," in *Proc. Int. Conf. Secur. Privacy Commun. Syst.* New York, NY, USA: Springer, 2020, pp. 475–486.
[136] J. K. Liu, M. H. Au, T. H. Yuen, C. Zuo, J. Wang, A. Sakzad, X. Luo, and L. Li, "Privacy-preserving COVID-19 contact tracing app: A zero-knowledge proof approach," *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 528, Jan. 2020.
[137] M. T. Rahman, R. T. Khan, M. R. A. Khandaker, M. Sellathurai, and M. S. A. Salan, "An automated contact tracing approach for controlling COVID-19 spread based on geolocation data from mobile cellular networks," *IEEE Access*, vol. 8, pp. 213554–213565, 2020.
[138] V. P. Yanambaka, A. Abdelgawad, and K. Yelamarthi, "PIM: A PUF-based host tracking protocol for privacy aware contact tracing in crowded areas," *IEEE Consum. Electron. Mag.*, vol. 10, no. 4, pp. 90–98, Jul. 2021.
[139] J. González-Cabañas, Á. Cuevas, R. Cuevas, and M. Maier, "Digital contact tracing: Large-scale geolocation data as an alternative to Bluetooth-based apps failure," *Electronics*, vol. 10, no. 9, p. 1093, May 2021.
[140] D. Demirag and E. Ayday, "Tracking the invisible: Privacy-preserving contact tracing to control the spread of a virus," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. New York, NY, USA: Springer, 2020, pp. 240–249.
[141] M. Whaiduzzaman, M. R. Hossain, A. R. Shovon, S. Roy, A. Laszka, R. Buyya, and A. Barros, "A privacy-preserving mobile and fog computing framework to trace and prevent COVID-19 community transmission," *IEEE J. Biomed. Health Informat.*, vol. 24, no. 12, pp. 3564–3575, Dec. 2020.
[142] A. F. Lubis, "Proximity-based COVID-19 contact tracing system devices for locally problems solution," in *Proc. 3rd Int. Seminar Res. Inf. Technol. Intell. Syst. (ISRITI)*, Dec. 2020, pp. 365–370.
[143] S. Brack, L. Reichert, and B. Scheuermann, "CAUDHT: Decentralized contact tracing using a DHT and blind signatures," in *Proc. IEEE 45th Conf. Local Comput. Netw. (LCN)*, Nov. 2020, pp. 337–340.
[144] F. Kato, Y. Cao, and M. Yoshikawa, "Secure and efficient trajectory-based contact tracing using trusted hardware," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2020, pp. 4016–4025.
[145] L. Alarabi, S. Basalamah, A. Hendawi, and M. Abdalla, "TraceAll: A real-time processing for contact tracing using indoor trajectories," *Information*, vol. 12, no. 5, p. 202, May 2021.
[146] Z. Peng, C. Xu, H. Wang, J. Huang, J. Xu, and X. Chu, "P 2 B-trace: Privacy-preserving blockchain-based contact tracing to combat pandemics," in *Proc. Int. Conf. Manage. Data*, Jun. 2021, pp. 2389–2393.
[147] S. A. Alansari, M. M. Badr, M. Mahmoud, and W. Alasmary, "Efficient and privacy-preserving contact tracing system for COVID-19 using blockchain," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2021, pp. 1–6.
[148] P. Tedeschi, S. Bakiras, and R. Di Pietro, "IoTrace: A flexible, efficient, and privacy-preserving IoT-enabled architecture for contact tracing," *IEEE Commun. Mag.*, vol. 59, no. 6, pp. 82–88, Jun. 2021.
[149] N. Fenton, S. McLachlan, P. Lucas, K. Dube, G. Hitman, M. Osman, E. Kyrimi, and M. Neil, "A privacy-preserving Bayesian network model for personalised COVID-19 risk assessment and contact tracing," *MedRxiv*, pp. 1–21, Jan. 2021, doi: 10.1101/2020.07.15.20154286.
[150] E. Bandara, X. Liang, P. Foytik, S. Shetty, C. Hall, D. Bowden, N. Ranasinghe, and K. D. Zoysa, "A blockchain empowered and privacy preserving digital contact tracing platform," *Inf. Process. Manage.*, vol. 58, no. 4, Jul. 2021, Art. no. 102572.
[151] Y. An, S. Lee, S. Jung, H. Park, Y. Song, and T. Ko, "Protect: Privacy-preserving contact tracing for COVID-19 with homomorphic encryption," *J. Med. Internet Res.*, vol. 23, no. 7, Apr. 2021, Art. no. e26371, doi: 10.2196/26371.
[152] Z. Peng, J. Huang, H. Wang, S. Wang, X. Chu, X. Zhang, L. Chen, X. Huang, X. Fu, Y. Guo, and J. Xu, "BU-trace: A permissionless mobile system for privacy-preserving intelligent contact tracing," in *Proc. Int. Conf. Database Syst. Adv. Appl.*, Taipei, Taiwan: Springer, Apr. 2021, pp. 381–397.
[153] P. C. Ng, P. Spachos, and K. N. Plataniotis, "COVID-19 and your smartphone: BLE-based smart contact tracing," *IEEE Syst. J.*, early access, Mar. 9, 2021, doi: 10.1109/JSYST.2021.3055675.
[154] M. Dhiman, N. Gupta, U. Gupta, and Y. Kumar, "Lattice cryptography based Geo-encrypted contact tracing for infection detection," TechRxiv, USA, Tech. Rep. 14572059, 2021.
[155] F. Yi, Y. Xie, and K. Jamieson, "Cellular-assisted COVID-19 contact tracing," in *Proc. 2nd Workshop Deep Learn. Wellbeing Appl. Leveraging Mobile Devices Edge Comput.*, Jun. 2021, pp. 1–6.

[156] W. J. Bradshaw, E. C. Alley, J. H. Huggins, A. L. Lloyd, and K. M. Esvelt, "Bidirectional contact tracing could dramatically improve COVID-19 control," *Nature Commun.*, vol. 12, no. 1, pp. 1–9, Dec. 2021.

[157] A. Hekmati, G. Ramachandran, and B. Krishnamachari, "CONTAIN: Privacy-oriented contact tracing protocols for epidemics," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM)* May 2021, pp. 872–877.

[158] G. Li, S. Hu, S. Zhong, W. L. Tsui, and S.-H.-G. Chan, "VContact: Private WiFi-based IoT contact tracing with virus lifespan," *IEEE Internet Things J.*, early access, Jul. 26, 2021, doi: 10.1109/JIOT.2021.3100276.

[159] Y. Zhu, W. Ma, J. Cui, X. Xia, Y. Peng, and J. Ning, "PvCT: A publicly verifiable contact tracing algorithm in cloud computing," *Secur. Commun. Netw.*, vol. 2021, pp. 1–18, May 2021.

[160] Z. Wen, K. Yu, X. Qi, T. Sato, Y. Katsuyama, T. Sato, W. Kameyama, F. Kato, Y. Cao, M. Yoshikawa, and M. Luo, "Blockchain-empowered contact tracing for COVID-19 using crypto-spatiotemporal information," in *Proc. IEEE Int. Conf. E-health Netw., Appl. Services (HEALTHCOM)*, Mar. 2021, pp. 1–6.

[161] E. Lee, K. Park, D. J. Park, J. Kim, and C. Jo, "Locally testable privacy-preserving contact tracing protocol without exposing secret seed," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2021, pp. 1–5.

[162] D. Chumachenko and S. Yakovlev, "Intelligent system of epidemic situation monitoring and control," in *Proc. 5th Int. Conf. Comput. Linguistics Intell. Syst.*, vol. 1, 2021, pp. 46–55.

[163] D. G. Katehakis, G. Kavlentakis, S. Kostomanolakis, F. Logothetidis, Y. Petrakis, N. Stathiakis, V. Tzikoulis, H. Kondylakis, and A. Kouroubali, "Safe in COVID-19: A platform to support effective monitoring of incidents during a pandemic," *EAI Endorsed Trans. Bioeng. Bioinf.*, vol. 1, no. 2, Mar. 2021, Art. no. 169027.

[164] M. F. Monir, A. H. Chowdhury, R. Anzum, and M. A. Amin, "IoT enabled geofencing for COVID-19 home quarantine," in *Proc. 8th Int. Conf. Comput. Commun. Eng. (ICCCE)*, Jun. 2021, pp. 373–378.

[165] P. Sopory, J. M. Novak, and J. P. Noyes, "Quarantine acceptance and adherence: Qualitative evidence synthesis and conceptual framework," *J. Public Health*, pp. 1–11, Apr. 2021, doi: 10.1007/s10389-021-01544-8.

[166] A. Calderon, S. Gonzales, and A. Ruiz, "Privacy, personal data protection, and freedom of expression under quarantine? The Peruvian experience," *Int. Data Privacy Law*, vol. 11, no. 1, pp. 48–62, May 2021.

[167] M. Pezzutto, N. B. Rosselló, L. Schenato, and E. Garone, "Smart testing and selective quarantine for the control of epidemics," *Annu. Rev. Control*, vol. 51, pp. 540–550, Mar. 2021.

[168] T. Sharma, H. A. Dyer, and M. Bashir, "Enabling user-centered privacy controls for mobile applications: COVID-19 perspective," *ACM Trans. Internet Technol.*, vol. 21, no. 1, pp. 1–24, Feb. 2021.

[169] F. Al-Turjman and B. Deebak, "Privacy-aware energy-efficient framework using the Internet of Medical Things for COVID-19," *IEEE Internet Things Mag.*, vol. 3, no. 3, pp. 64–68, Sep. 2020.

[170] R. Lalitha, G. Hariharan, and N. Lokesh, "Tracking the COVID zones through Geo-fencing technique," *Int. J. Pervas. Comput. Commun.*, vol. 16, no. 5, pp. 409–417, Jul. 2020.

[171] A. I. Paganelli, P. E. Velmovitsky, P. Miranda, A. Branco, P. Alencar, D. Cowan, M. Endler, and P. P. Morita, "A conceptual IoT-based early-warning architecture for remote monitoring of COVID-19 patients in wards and at home," *Internet Things*, Apr. 2021, Art. no. 100399, doi: 10.1016/j.iot.2021.100399.

[172] A. Naser, A. Lotfi, and J. Zhong, "A novel privacy-preserving approach for physical distancing measurement using thermal sensor array," in *Proc. 14th Pervasive Technol. Rel. Assistive Environ. Conf.*, Jun. 2021, pp. 81–85.

[173] A. A. Narvaez and J. G. Guerra, "Received signal strength indication-based COVID-19 mobile application to comply with social distancing using Bluetooth signals from smartphones," in *Data Science for COVID-19*. Amsterdam, The Netherlands: Elsevier, 2021, pp. 483–501.

[174] S. Das, A. Nag, D. Adhikary, R. J. Ram, A. Br, S. K. Ojha, and G. M Hegde, "Computer vision-based social distancing surveillance solution with optional automated camera calibration for large scale deployment," 2021, *arXiv:2104.10891*.

[175] E. J. Khatib, M. J. P. Roselló, J. Miranda-Páez, V. Giralt, and R. Barco, "Mass tracking in cellular networks for the COVID-19 pandemic monitoring," *Sensors*, vol. 21, no. 10, p. 3424, May 2021.

[176] M. S. Munir, D. H. Kim, A. K. Bairagi, and C. S. Hong, "When CVaR meets with Bluetooth PAN: A physical distancing system for COVID-19 proactive safety," *IEEE Sensors J.*, vol. 21, no. 12, pp. 13858–13869, Jun. 2021.

[177] K. J. Almalki, S. Song, M. Mohzary, and B.-Y. Choi, "CATS: Crowd-based alert and tracing services for building a safe community cluster against COVID-19," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM)*, May 2021, pp. 697–701.

[178] Y. Verbelen, S. Kaluvan, U. Haller, M. Boardman, and T. B. Scott, "Design and implementation of a social distancing and contact tracing wearable," in *Proc. 6th IEEE Congr. Inf. Sci. Technol. (CiSt)*, Jun. 2020, pp. 466–471.

[179] S. D. Mohapatra, S. C. Nayak, S. Parida, C. R. Panigrahi, and B. Pati, "COVTrac: COVID-19 tracker and social distancing app," in *Progress in Advanced Computing and Intelligent Engineering*. Singapore: Springer, 2021, pp. 607–619.

[180] P. Barsocchi, A. Calabrò, A. Crivello, S. Daoudagh, F. Furfari, M. Girolami, and E. Marchetti, "COVID-19 & privacy: Enhancing of indoor localization architectures towards effective social distancing," *Array*, vol. 9, Mar. 2021, Art. no. 100051.

[181] H. Mukhtar, S. Rubaiee, M. Krichen, and R. Alroobaea, "An IoT framework for screening of COVID-19 using real-time data from wearable sensors," *Int. J. Environ. Res. Public Health*, vol. 18, no. 8, p. 4022, Apr. 2021.

[182] C. Baquero, P. Casari, A. F. Anta, A. García-García, D. Frey, A. Garcia-Agundez, C. Georgiou, B. Girault, A. Ortega, M. Goessens, H. A. Hernández-Roig, N. Nicolaou, E. Stavrakis, O. Ojo, J. C. Roberts, and I. Sanchez, "The CoronaSurveys system for COVID-19 incidence data collection and processing," *Frontiers Comput. Sci.*, vol. 3, p. 52, Jun. 2021.

[183] P. K. Deb, A. Mukherjee, and S. Misra, "CovChain: Blockchain-enabled identity preservation and anti-infodemics for COVID-19," *IEEE Netw.*, vol. 35, no. 3, pp. 42–47, May 2021.

[184] Y. Dong and Y.-D. Yao, "IoT platform for COVID-19 prevention and control: A survey," *IEEE Access*, vol. 9, pp. 49929–49941, 2021.

[185] I. D. Sabukunze, D. B. Setyohadi, and M. Sulistyoningsih, "Designing an IoT based smart monitoring and emergency alert system for COVID19 patients," in *Proc. 6th Int. Conf. Converg. Technol. (I2CT)*, Apr. 2021, pp. 1–5.

[186] R. Singh, "Cloud computing and COVID-19," in *Proc. 3rd Int. Conf. Signal Process. Commun. (ICPSC)*, May 2021, pp. 552–557.

[187] E. Elbasi, A. E. Topcu, and S. Mathew, "Prediction of COVID-19 risk in public areas using IoT and machine learning," *Electronics*, vol. 10, no. 14, p. 1677, Jul. 2021.

[188] K. Koch, S. Krenn, D. Pellegrino, and S. Ramacher, "Privacy-preserving analytics for data markets using MPC," 2021, *arXiv:2103.03739*.

[189] A. Bampoulidis, A. Bruni, L. Helminger, D. Kales, C. Rechberger, and R. Walch, "Privately connecting mobility to infectious diseases via applied cryptography," 2020, *arXiv:2005.02061*.

[190] S. Park, G. J. Choi, and H. Ko, "Privacy in the time of COVID-19: Divergent paths for contact tracing and route-disclosure mechanisms in South Korea," *IEEE Secur. Privacy*, vol. 19, no. 3, pp. 51–56, May 2021.

[191] N. Ahmed, R. A. Michelin, W. Xue, S. Ruj, R. Malaney, S. S. Kanhere, A. Seneviratne, W. Hu, H. Janicke, and S. K. Jha, "A survey of COVID-19 contact tracing apps," *IEEE Access*, vol. 8, pp. 134577–134601, 2020.

[192] K. Kolasa, F. Mazzi, E. Leszczuk-Czubkowska, Z. Zrubka, and M. Péntek, "State of the art in adoption of contact tracing apps and recommendations regarding privacy protection and public health: Systematic review," *JMIR mHealth uHealth*, vol. 9, no. 6, Jun. 2021, Art. no. e23250.

[193] M. Elkhodr, O. Mubin, Z. Iftikhar, M. Masood, B. Alsinglawi, S. Shahid, and F. Alnajjar, "Technology, privacy, and user opinions of COVID-19 mobile apps for contact tracing: Systematic search and content analysis," *J. Med. Internet Res.*, vol. 23, no. 2, Feb. 2021, Art. no. e23467.

[194] T. Li, Y. Jackie, C. Faklaris, J. King, Y. Agarwal, L. Dabbish, and J. I. Hong, "Decentralized is not risk-free: Understanding public perceptions of privacy-utility trade-offs in COVID-19 contact-tracing apps," 2020, *arXiv:2005.11957*.

[195] J. Lin, L. Carter, and D. Liu, "Privacy concerns and digital government: Exploring citizen willingness to adopt the COVIDSafe app," *Eur. J. Inf. Syst.*, pp. 1–14, May 2021, doi: 10.1080/0960085X.2021.1920857.

[196] J. Park, J. Han, Y. Kim, and M. J. Rho, "Development, acceptance, and concerns surrounding app-based services to overcome the COVID-19 outbreak in South Korea: Web-based survey study," *JMIR Med. Informat.*, vol. 9, no. 7, Jul. 2021, Art. no. e29315.

[197] S. Lewandowsky, S. Dennis, A. Perfors, Y. Kashima, J. P. White, P. Garrett, D. R. Little, and M. Yesilada, "Public acceptance of privacy-encroaching policies to address the COVID-19 pandemic in the United Kingdom," *PLoS ONE*, vol. 16, no. 1, Jan. 2021, Art. no. e0245740.

[198] L. Gios, G. C. Falceri, S. Micocci, L. Patil, S. Testa, S. Sforzin, E Turra, D. Conforti, G. Malfatti, M. Moz, and A. Nicolini, "Use of eHealth platforms and apps to support monitoring and management of home-quarantined patients with COVID-19 in the province of Trento, Italy: App development and implementation," *JMIR Formative Res.*, vol. 5, no. 5, May 2021, Art. no. e25713.

[199] S. S. Chandrayan, S. Suman, and T. Mazumder, "IoT for COVID-19: A descriptive viewpoint," in *Impact AI Data Science Response to Coronavirus Pandemic*. Singapore: Springer, 2021, pp. 193–208.

[200] J. Huang, M.-P. Kwan, and J. Kim, "How culture and sociopolitical tensions might influence People's acceptance of COVID-19 control measures that use individual-level georeferenced data," *ISPRS Int. J. Geo-Inf.*, vol. 10, no. 7, p. 490, Jul. 2021.

[201] B. Alves, V. Afonso, A. P. Silva, F. R. Ribeiro, and A. Silva, "Mobile applications for pandemic monitoring : Approaches, challenges and opportunities," in *Proc. 16th Iberian Conf. Inf. Syst. Technol. (CISTI)*, Jun. 2021, pp. 1–6.

[202] E. Mbunge, R. C. Millham, M. N. Sibiya, S. G. Fashoto, B. Akinnuwesi, S. Simelane, and N. Ndumiso, "Framework for ethical and acceptable use of social distancing tools and smart devices during COVID-19 pandemic in Zimbabwe," *Sustain. Oper. Comput.*, vol. 2, pp. 190–199, Jan. 2021.

[203] M. Hatamian, S. Wairimu, N. Momen, and L. Fritsch, "A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps," *Empirical Softw. Eng.*, vol. 26, no. 3, pp. 1–51, May 2021.

[204] M. Bendechache, P. Lohar, G. Xie, R. Brennan, R. Trestian, E. Celeste, K. Kapanova, E. Jayasekera, and I. Tal, "Public attitudes towards privacy in COVID-19 times in the republic of ireland: A pilot study," *Inf. Secur. J., Global Perspective*, vol. 30, no. 5, pp. 281–293, Sep. 2021.

[205] A. Karale, "The challenges of IoT addressing security, ethics, privacy, and laws," *Internet Things*, vol. 15, Sep. 2021, Art. no. 100420.

[206] Z. R. Alashhab, M. Anbar, M. M. Singh, Y.-B. Leau, Z. A. Al-Sai, and S. A. Alhayja'a, "Impact of coronavirus pandemic crisis on technologies and cloud computing applications," *J. Electron. Sci. Technol.*, vol. 19, no. 1, Mar. 2021, Art. no. 100059.

[207] E. Mbunge, B. Akinnuwesi, S. G. Fashoto, A. S. Metfula, and P. Mashwama, "A critical review of emerging technologies for tackling COVID-19 pandemic," *Hum. Behav. Emerg. Technol.*, vol. 3, no. 1, pp. 25–39, 2021.

[208] V. Distler, C. Lallemand, and V. Koenig, "How acceptable is this? How user experience factors can broaden our understanding of the acceptance of privacy trade-offs," *Comput. Hum. Behav.*, vol. 106, May 2020, Art. no. 106227.

[209] N. Ahmad and P. Chauhan, "State of data privacy during COVID-19," *IEEE Ann. Hist. Comput.*, vol. 53, no. 10, pp. 119–122, Oct. 2020.

[210] J. Kim, L. Neumann, P. Paul, M. E. Day, M. Aratow, D. S. Bell, J. N. Doctor, L. C. Hinske, X. Jiang, K. K. Kim, M. E. Matheny, D. Meeker, M. J. Pletcher, L. M. Schilling, S. SooHoo, H. Xu, K. Zheng, and L. Ohno-Machado, "Privacy-protecting, reliable response data discovery using COVID-19 patient observations," *J. Amer. Med. Inform. Assoc.*, vol. 28, no. 8, pp. 1765–1776, Jul. 2021.

[211] C. Dwork, A. Karr, K. Nissim, and L. Vilhuber, "On privacy in the age of COVID-19," *J. Privacy Confidentiality*, vol. 10, no. 2, pp. 1–6, Jun. 2020.

[212] C. O. Buckee, S. Balsari, J. Chan, M. Crosas, F. Dominici, U. Gasser, Y. H. Grad, B. Grenfell, M. E. Halloran, M. U. G. Kraemer, M. Lipsitch, C. J. E. Metcalf, L. A. Meyers, T. A. Perkins, M. Santillana, S. V. Scarpino, C. Viboud, A. Wesolowski, and A. Schroeder, "Aggregated mobility data could help fight COVID-19," *Science*, vol. 368, no. 6487, pp. 145–146, Apr. 2020.

[213] A. Dubov and S. Shoptawb, "The value and ethics of using technology to contain the COVID-19 epidemic," *Amer. J. Bioethics*, vol. 20, no. 7, pp. W7–W11, Jul. 2020.

[214] L. Lenert and B. Y. McSwain, "Balancing health privacy, health information exchange, and research in the context of the COVID-19 pandemic," *J. Amer. Med. Inform. Assoc.*, vol. 27, no. 6, pp. 963–966, Jun. 2020.

[215] B. Ferrari, D. P. D. S. Junior, and R. Pereira, "Systemic view of human-data interaction: Analyzing a COVID-19 data visualization platform," in *Proc. 19th Brazilian Symp. Hum. Factors Comput. Syst.*, Oct. 2020, pp. 1–6.

[216] U. Gasser, M. Ienca, J. Scheibner, J. Sleigh, and E. Vayena, "Digital tools against COVID-19: Taxonomy, ethical challenges, and navigation aid," *Lancet Digit. Health*, vol. 2, no. 8, pp. e425–e434, Aug. 2020.

[217] J. A. Onesimu, J. Karthikeyan, and Y. Sei, "An efficient clustering-based anonymization scheme for privacy-preserving data collection in IoT based healthcare services," *Peer Peer Netw. Appl.*, vol. 14, no. 3, pp. 1629–1649, May 2021.

[218] A. Berke, M. Bakker, P. Vepakomma, K. Larson, and A. S. Pentland, "Assessing disease exposure risk with location data: A proposal for cryptographic preservation of privacy," 2020, *arXiv:2003.14412*.

[219] R. Trestian, G. Xie, P. Lohar, E. Celeste, M. Bendechache, R. Brennan, E. Jayasekera, R. Connolly, and I. Tal, "Data privacy in a time of COVID-19: How concerned are you," *IEEE Security Privacy*, vol. 19, no. 5, pp. 26–35, Sep./Oct. 2021.

[220] H. Garg and P. Khanna, "Consent in COVID: A researcher's dilemma," *Trends Anaesthesia Crit. Care*, vol. 38, pp. 10–12, Apr. 2021, doi: 10.1016/j.tacc.2021.03.010.

[221] R. Canetti, A. Trachtenberg, and M. Varia, "Anonymous collocation discovery: Harnessing privacy to tame the coronavirus," 2020, *arXiv:2003.13670*.

[222] E. Pepe, P. Bajardi, L. Gauvin, F. Privitera, B. Lake, C. Cattuto, and M. Tizzoni, "COVID-19 outbreak response, a dataset to assess mobility changes in Italy following national lockdown," *Sci. Data*, vol. 7, no. 1, pp. 1–7, Dec. 2020.

[223] X. Lu, J. Tan, Z. Cao, Y. Xiong, S. Qin, T. Wang, C. Liu, S. Huang, W. Zhang, L. B. Marczak, S. I. Hay, L. Thabane, G. H. Guyatt, and X. Sun, "Mobile phone-based population flow data for the COVID-19 outbreak in mainland China," *Health Data Sci.*, vol. 2021, pp. 1–9, Jun. 2021.

[224] R. Du, Q. Ye, Y. Fu, and H. Hu, "Collecting high-dimensional and correlation-constrained data with local differential privacy," in *Proc. 18th Annu. IEEE Int. Conf. Sens., Commun., Netw. (SECON)*, Jul. 2021, pp. 1–9.

[225] X. Gu, M. Li, Y. Cheng, L. Xiong, and Y. Cao, "PCKV: Locally differentially private correlated key-value data collection with optimized utility," in *Proc. 29th USENIX Secur. Symp. (USENIX Secur.)*, 2020, pp. 967–984.

[226] X. Gu, M. Li, L. Xiong, and Y. Cao, "Providing input-discriminative protection for local differential privacy," in *Proc. IEEE 36th Int. Conf. Data Eng. (ICDE)*, Apr. 2020, pp. 505–516.

[227] A. Butler and E. Zhou, "Disease and data in society: How the pandemic expanded data collection and surveillance systems," *Amer. Univ. Law Rev.*, vol. 70, p. 1577, 2020.

[228] Y. Sun, J. Liu, K. Yu, M. Alazab, and K. Lin, "PMRSS: Privacy-preserving medical record searching scheme for intelligent diagnosis in IoT healthcare," *IEEE Trans. Ind. Informat.*, early access, Apr. 2, 2021, doi: 10.1109/TII.2021.3070544.

[229] W. Kim, H. Lee, and Y. D. Chung, "Safe contact tracing for COVID-19: A method without privacy breach using functional encryption techniques based-on spatio-temporal trajectory data," *PLoS ONE*, vol. 15, no. 12, Dec. 2020, Art. no. e0242758.

[230] P. Wang, C. Lin, M. S. Obaidat, Z. Yu, Z. Wei, and Q. Zhang, "Contact tracing incentive for COVID-19 and other pandemic diseases from a crowdsourcing perspective," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15863–15874, Nov. 2021.

[231] L. C. Fourati and S. Ayed, "Federated learning toward data preprocessing: COVID-19 context," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2021, pp. 1–6.

[232] X. Li, R. Dowsley, and M. De Cock, "Privacy-preserving feature selection with secure multiparty computation," 2021, *arXiv:2102.03517*.

[233] R. Aloufi, H. Haddadi, and D. Boyle, "Paralinguistic privacy protection at the edge," 2020, *arXiv:2011.02930*.

[234] M. Aazam, S. Zeadally, and E. F. Flushing, "Task offloading in edge computing for machine learning-based smart healthcare," *Comput. Netw.*, vol. 191, May 2021, Art. no. 108019.

[235] T. Amano, H. Yamaguchi, and T. Higashino, "Connected AR for combating COVID-19," *IEEE Internet Things Mag.*, vol. 3, no. 3, pp. 46–51, Sep. 2020.

[236] R. Hu, B. Michel, D. Russo, N. Mora, G. Matrella, P. Ciampolini, F. Cocchi, E. Montanari, S. Nunziata, and T. Brunschwiler, "An unsupervised behavioral modeling and alerting system based on passive sensing for elderly care," *Future Internet*, vol. 13, no. 1, p. 6, Dec. 2020.

[237] J. E. Rivadeneira, J. Sa Silva, R. Colomo-Palacios, A. Rodrigues, J. M. Fernandes, and F. Boavida, "A privacy-aware framework integration into a human-in-the-loop IoT system," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, May 2021, pp. 1–6.

[238] V. Bellandi, P. Ceravolo, and M. Ehsanpour, "A case study in smart healthcare platform design," in *Proc. IEEE World Congr. Services (SERVICES)*, Oct. 2020, pp. 7–12.

[239] D. Y. Zhang, Z. Kou, and D. Wang, "FairFL: A fair federated learning approach to reducing demographic bias in privacy-sensitive classification models," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2020, pp. 1051–1060.

[240] C. Krishnan and T. Lalitha, "Attribute-based encryption for securing healthcare data in cloud environment," *PalArch's J. Archaeol. Egypt/Egyptol.*, vol. 17, no. 9, pp. 10134–10143, 2020.

[241] E. Yang, Y. Huang, F. Liang, W. Pan, and Z. Ming, "FCMF: Federated collective matrix factorization for heterogeneous collaborative filtering," *Knowl.-Based Syst.*, vol. 220, May 2021, Art. no. 106946.

[242] X. He, J. Rogers, J. Bater, A. Machanavajjhala, C. Wang, and X. Wang, "Practical security and privacy for database systems," in *Proc. Int. Conf. Manage. Data*, Jun. 2021, pp. 2839–2845.

[243] S. Prasanna and P. Rao, "A data science perspective of real-world COVID-19 databases," in *Leveraging Artificial Intelligence in Global Epidemics*. Amsterdam, The Netherlands: Elsevier, 2021, pp. 133–163.

[244] M. M. Anjum and N. Mohammed, "PAARS: Privacy aware access regulation system," in *Proc. 11th IEEE Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Oct. 2020, pp. 0155–0161.

[245] H. Li, H. Lu, S. Huang, W. Ma, M. Zhang, Y. Liu, and S. Ma, "Privacy-aware remote information retrieval user experiments logging tool," in *Proc. 44th Int. ACM SIGIR Conf. Res. Develop. Inf. Retr.*, Jul. 2021.

[246] I. Psychoula, L. Chen, and O. Amft, "Privacy risk awareness in wearables and the Internet of Things," *IEEE Pervas. Comput.*, vol. 19, no. 3, pp. 60–66, Jul. 2020.

[247] F. Hopfgartner, C. Gurrin, and H. Joho, "Guest editorial: Special issue on lifelogging behaviour and practice," *Online Inf. Rev.*, vol. 44, no. 2, pp. 477–481, 2020.

[248] C. Biswas, D. Ganguly, and U. Bhattacharya, "Approximate nearest neighbour search on privacy-aware encoding of user locations to identify susceptible infections in simulated epidemics," 2020, *arXiv:2004.08851*.

[249] J. Ali and V. Dyo, "Cross hashing: Anonymizing encounters in decentralised contact tracing protocols," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2021, pp. 181–185.

[250] M. Shaikh, C. Shibu, E. Angeles, and D. Pavithran, "Data storage in blockchain based architectures for Internet of Things (IoT)," in *Proc. IEEE Int. IoT, Electron. Mechatronics Conf. (IEMTRONICS)*, Apr. 2021, pp. 1–5.

[251] S. S. Moghadam, A. Fayoumi, and P. Vafadoost, "Pavan: A privacy-preserving system for DB-as-a-service," *ICT Exp.*, vol. 7, no. 2, pp. 259–264, Jun. 2021.

[252] J. Kim and M. Kim, "Intelligent mediator-based enhanced smart contract for privacy protection," *ACM Trans. Internet Technol.*, vol. 21, no. 1, pp. 1–16, Feb. 2021.

[253] K. Miyachi and T. K. Mackey, "HOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design," *Inf. Process. Manage.*, vol. 58, no. 3, May 2021, Art. no. 102535.

[254] M. Platt, A. Hasselgren, J. M. Román-Belmonte, M. Tuler de Oliveira, H. D. L. Corte-Rodríguez, S. Delgado Olabarriaga, E. C. Rodríguez-Merchán, and T. K. Mackey, "Test, trace, and put on the blockchain?: A viewpoint evaluating the use of decentralized systems for algorithmic contact tracing to combat a global pandemic," *JMIR Public Health Surveill.*, vol. 7, no. 4, Apr. 2021, Art. no. e26460.

[255] B. Zhang, S. Kreps, N. McMurry, and R. M. McCain, "Americans' perceptions of privacy and surveillance in the COVID-19 pandemic," *PLoS ONE*, vol. 15, no. 12, 2020, Art. no. e0242652.

[256] N. Trieu, K. Shehata, P. Saxena, R. Shokri, and D. Song, "Epione: Lightweight contact tracing with strong privacy," 2020, *arXiv:2004.13293*.

[257] M. D. Rintoul, J. L. Jones, B. D. Newton, K. L. Wisniewski, A. T. Wilson, M. J. Ginaldi, C. A. Waddell, K. Goss, and K. J. Ward, "Large-scale trajectory analysis via feature vectors," Sandia Nat. Lab. (SNL-NM), Albuquerque, NM, USA, Tech. Rep. SAND2021-2703R, 2021.

[258] M. Golec, R. Ozturac, Z. Pooranian, S. S. Gill, and R. Buyya, "iFaaS-Bus: A security and privacy based lightweight framework for serverless computing using IoT and machine learning," *IEEE Trans. Ind. Informat.*, early access, Jul. 7, 2021, doi: 10.1109/TII.2021.3095466.

[259] Z. A. El Mouden, R. M. Taj, A. Jakimi, and M. Hajar, "Towards using graph analytics for tracking COVID-19," *Proc. Comput. Sci.*, vol. 177, pp. 204–211, Jan. 2020.

[260] S. Yu, Q. Qing, C. Zhang, A. Shehzad, G. Oatley, and F. Xia, "Data-driven decision-making in COVID-19 response: A survey," *IEEE Trans. Comput. Social Syst.*, vol. 8, no. 4, pp. 1016–1029, Aug. 2021.

[261] E. Dolgin, "Core concept: The pandemic is prompting widespread use—And misuse—Of real-world data," *Proc. Nat. Acad. Sci. USA*, vol. 117, no. 45, pp. 27754–27758, Nov. 2020.

[262] D. Günther, M. Holz, B. Judkewitz, H. Möllering, B. Pinkas, and T. Schneider, "PEM: Privacy-preserving epidemiological modeling," Cryptol. ePrint Arch., USA, Tech. Rep. 1546, 2020.

[263] N. A. Tu, K. S. Wong, M. F. Demirci, and Y. K. Lee, "Toward efficient and intelligent video analytics with visual privacy protection for large-scale surveillance," *J. Supercomput.*, vol. 77, pp. 1–31, May 2021.

[264] L. Yin, N. Lin, and Z. Zhao, "Mining daily activity chains from large-scale mobile phone location data," *Cities*, vol. 109, Feb. 2021, Art. no. 103013.

[265] X. Zhang, F. Gao, S. Liao, F. Zhou, G. Cai, and S. Li, "Portraying citizens' occupations and assessing urban occupation mixture with mobile phone data: A novel spatiotemporal analytical framework," *ISPRS Int. J. Geo-Inf.*, vol. 10, no. 6, p. 392, Jun. 2021.

[266] S. Rahimipour, M. Ghatee, S. M. Hashemi, and A. Nickabadi, "A hybrid of neuro-fuzzy inference system and hidden Markov model for activity-based mobility modeling of cellphone users," *Comput. Commun.*, vol. 173, pp. 79–94, May 2021.

[267] F. Zhou, R. Yin, G. Trajcevski, K. Zhang, J. Wu, and A. Khokhar, "Improving human mobility identification with trajectory augmentation," *GeoInformatica*, vol. 25, no. 3, pp. 453–483, Jul. 2021.

[268] P. Gupta, C. S. Hoi, C. K. Leung, Y. Yuan, X. Zhang, and Z. Zhang, "Vertical data mining from relational data and its application to COVID-19 data," in *Proc. Int. Conf. Big Data Appl. Services*. Singapore: Springer, 2018, pp. 106–116.

[269] L. Reichert, S. Brack, and B. Scheuermann, "Privacy-preserving contact tracing of COVID-19 patients," *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 375, Jan. 2020.

[270] P. Alves, I. Frajhof, F. Correia, C. de Souza, and H. Lopes, "Controlling personal data flow: An ontology in the COVID-19 outbreak using a permissioned blockchain," in *Proc. 23rd Int. Conf. Enterprise Inf. Syst.*, 2021, pp. 1–8.

[271] R. Canetti, Y. T. Kalai, A. Lysyanskaya, R. L. Rivest, A. Shamir, E. Shen, A. Trachtenberg, M. Varia, and D. J. Weitzner, "Privacy-preserving automated exposure notification," IACR Cryptol. ePrint Arch., USA, Tech. Rep. 863, 2020.

[272] S. R. Srinivasavaradhan, P. Nikolopoulos, C. Fragouli, and S. Diggavi, "Dynamic group testing to control and monitor disease progression in a population," 2021, *arXiv:2106.10765*.

[273] J. J. Chen, R. Chen, X. Zhang, and M. Pan, "A privacy preserving federated learning framework for COVID-19 vulnerability map construction," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2021, pp. 1–6.

[274] S. Chaudhari, M. Clear, P. Bradish, and H. Tewari, "Framework for a DLT based COVID-19 passport," in *Intelligent Computing*. New York, NY, USA: Springer, 2021, pp. 108–123.

[275] A. Nagar, C. Tran, and F. Fioretto, "Privacy-preserving and accountable multi-agent learning," in *Proc. 20th Int. Conf. Auto. Agents MultiAgent Syst.*, 2021, pp. 1605–1606.

[276] P. P. Kulkarni, H. Kasyap, and S. Tripathy, "DNet: An efficient privacy-preserving distributed learning framework for healthcare systems," in *Proc. Int. Conf. Distrib. Comput. Internet Technol.* New York, NY, USA: Springer, 2021, pp. 145–159.

[277] F. Zerka, V. Urovi, F. Bottari, R. T. H. Leijenaar, S. Walsh, H. Gabrani-Juma, M. Gueuning, A. Vaidyanathan, W. Vos, M. Occhipinti, H. C. Woodruff, M. Dumontier, and P. Lambin, "Privacy preserving distributed learning classifiers—Sequential learning with small sets of data," *Comput. Biol. Med.*, vol. 136, Sep. 2021, Art. no. 104716.

[278] A. Prakash, P. Sharma, I. K. Sinha, and U. P. Singh, "Spread & peak prediction of COVID-19 using ANN and regression (workshop paper)," in *Proc. IEEE 6th Int. Conf. Multimedia Big Data (BigMM)*, Sep. 2020, pp. 356–365.

[279] M. A. Salam, S. Taha, and M. Ramadan, "COVID-19 detection using federated machine learning," *PLoS ONE*, vol. 16, no. 6, Jun. 2021, Art. no. e0252573.

[280] A. Garhwal, M. Bunruangses, A. E. Arumona, P. Youplao, K. Ray, S. Suwandee, and P. Yupapin, "Integrating metamaterial antenna node and LiFi for privacy preserving intelligent COVID-19 hospital patient management," *Cognit. Comput.*, pp. 1–14, Jan. 2021, doi: 10.1007/s12559-020-09778-6.

[281] P. K. Vadrevu, S. K. Adusumalli, and V. K. Mangalapalli, "Personal privacy preserving data publication of COVID-19 pandemic data using edge computing," *J. Crit. Rev.*, vol. 7, no. 1, pp. 8103–8111, 2020.

[282] Q. Ye, H. Hu, N. Li, X. Meng, H. Zheng, and H. Yan, "Beyond value perturbation: Local differential privacy in the temporal setting," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, May 2021, pp. 1–10.
[283] K. Christodoulou, P. Christodoulou, Z. Zinonos, E. G. Carayannis, and S. A. Chatzichristofis, "Health information exchange with blockchain amid COVID-19-like pandemics," in *Proc. 16th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, May 2020, pp. 412–417.
[284] H. Zhang, G. Li, Y. Zhang, K. Gai, and M. Qiu, "Blockchain-based privacy-preserving medical data sharing scheme using federated learning," in *Proc. Int. Conf. Knowl. Sci., Eng. Manage.* New York, NY, USA: Springer, 2021, pp. 634–646.
[285] K. Ågren, P. Bjelkmar, and E. Allison, "The use of anonymized and aggregated telecom mobility data by a public health agency during the COVID-19 pandemic: Learnings from both the operator and agency perspective," *Data Policy*, vol. 3, p. e17, Aug. 2021, doi: 10.1017/dap.2021.11.
[286] A. Kouroubali, H. Kondylakis, and D. G. Katehakis, "Integrated care in the era of COVID-19: Turning vision into reality with digital health," *Frontiers Digit. Health*, vol. 3, p. 83, Aug. 2021.
[287] A. Vlahou, D. Hallinan, R. Apweiler, A. Argiles, J. Beige, A. Benigni, R. Bischoff, P. C. Black, F. Boehm, J. Céraline, and G. P. Chrousos, "Data sharing under the general data protection regulation: Time to harmonize law and research ethics," *Hypertension*, vol. 77, no. 4, pp. 1029–1035, 2021.
[288] J. C. S. Silva, D. F. de Lima Silva, A. D. S. D. Neto, A. Ferraz, J. L. Melo, N. R. F. Júnior, and A. T. de Almeida Filho, "A city cluster risk-based approach for Sars-CoV-2 and isolation barriers based on anonymized mobile phone users' location data," *Sustain. Cities Soc.*, vol. 65, Feb. 2021, Art. no. 102574.
[289] A. Coston, N. Guha, D. Ouyang, L. Lu, A. Chouldechova, and D. E. Ho, "Leveraging administrative data for bias audits: Assessing disparate coverage with mobility data for COVID-19 policy," in *Proc. ACM Conf. Fairness, Accountability, Transparency*, Mar. 2021, pp. 173–184.
[290] C. Biancotti, O. Borgogno, and G. F. Veronese, "Principled data access: Building public-private data partnerships for better official statistics," *SSRN Electron. J.*, no. 629, pp. 1–19, Jul. 2021, doi: 10.2139/ssrn.3896309.
[291] V. Dyo and J. Ali, "Privacy-preserving identity broadcast for contact tracing applications," in *Proc. Wireless Days (WD)*, Jun. 2021, pp. 1–6.
[292] P. S. Chauhan and N. Kshetri, "2021 state of the practice in data privacy and security," *Computer*, vol. 54, no. 8, pp. 125–132, Aug. 2021.
[293] E. W. Jones, S. Sweeney, I. Milligan, G. Bak, and J.-A. McCutcheon, "Remembering is a form of honouring: Preserving the COVID-19 archival record," Can. Sci. Publishing, Ottawa, ON, Canada, Tech. Rep. facets-2020-0115, 2021.
[294] N. Yi-Feng Chen, J. M. Crant, N. Wang, Y. Kou, Y. Qin, J. Yu, and R. Sun, "When there is a will there is a way: The role of proactive personality in combating COVID-19," *J. Appl. Psychol.*, vol. 106, no. 2, pp. 199–213, Feb. 2021.
[295] E. K. Cortez, "Data protection around the world: Future challenges," in *Data Protection Around World*. The Hague, The Netherlands: Springer, 2021, pp. 269–279.
[296] A. Ponce, "COVID-19 contact-tracing apps: How to prevent privacy from becoming the next victim," *ETUI Res. Paper-Policy Brief*, vol. 5, no. 5, pp. 1–5, May 2020, doi: 10.2139/ssrn.3593405.
[297] J. Wacksman, "Digitalization of contact tracing: Balancing data privacy with public health benefit," *Ethics Inf. Technol.*, pp. 1–7, Jun. 2021, doi: 10.1007/s10676-021-09601-2.
[298] M. Correia, G. Rego, and R. Nunes, "The right to be forgotten and COVID-19: Privacy versus public interest," *Acta bioethica*, vol. 27, no. 1, pp. 59–67, Jun. 2021.
[299] S. M. Iacus, F. Sermi, S. Spyratos, D. Tarchi, and M. Vespe, "Anomaly detection of mobile positioning data with applications to covid-19 situational awareness," *Jpn. J. Statist. Data Sci.*, vol. 4, pp. 1–19, Mar. 2021.
[300] M. M. Khubrani and S. Alam, "A detailed review of blockchain-based applications for protection against pandemic like covid-19," *Telkomnika*, vol. 19, no. 4, pp. 1185–1196, 2021.
[301] F. Qian and A. Zhang, "The value of federated learning during and post-COVID-19," *Int. J. Qual. Health Care*, vol. 33, no. 1, Mar. 2021, Art. no. mzab010.
[302] R. Sun, W. Wang, M. Xue, G. Tyson, and D. C. Ranasinghe, "VenueTrace: A privacy-by-design COVID-19 digital contact tracing solution," in *Proc. 18th Conf. Embedded Netw. Sensor Syst.*, Nov. 2020, pp. 790–791.
[303] P. Gupta, "Blockchain-based solutions for COVID-19: Challenges, advantages, and applications," in *Blockchain for Healthcare Systems*. Boca Raton, FL, USA: CRC Press, pp. 133–147.
[304] V. Dhillon, D. Metcalf, and M. Hooper, "The art of the newly possible: Transforming health with emerging technology and federated learning," in *Blockchain Enabled Applications*. Berkeley, CA, USA: Springer, 2021, pp. 345–356.
[305] D. Khemasuwan and H. G. Colt, "Applications and challenges of AI-based algorithms in the COVID-19 pandemic," *BMJ Innov.*, vol. 7, no. 2, pp. 387–398, Apr. 2021.
[306] X. Larrucea and I. Santamaria, "Dealing with privacy for protecting information," in *Proc. Eur. Conf. Softw. Process Improvement*. Springer, 2021, pp. 518–530.
[307] M. E. Ghamry, I. T. A. Halim, and A. M. Bahaa-Eldin, "Secular: A decentralized blockchain-based data privacy-preserving model training platform," in *Proc. Int. Mobile, Intell., Ubiquitous Comput. Conf. (MIUCC)*, May 2021, pp. 357–363.
[308] A. Cavoukian, "Understanding how to implement privacy by design, one step at a time," *IEEE Consum. Electron. Mag.*, vol. 9, no. 2, pp. 78–82, Mar. 2020.
[309] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Process. Mag.*, vol. 37, no. 3, pp. 50–60, May 2020.
[310] P. S. Kumar, P. Dixit, and N. Gayathri, "Healthcare data analytics using swarm intelligence," *Swarm Intell. Optim., Algorithms Appl.*, pp. 101–121, Dec. 2020, doi: 10.1002/9781119778868.ch7.
[311] F. Song, Z. Qin, L. Xue, J. Zhang, X. Lin, and X. Shen, "Privacy-preserving keyword similarity search over encrypted spatial data in cloud computing," *IEEE Internet Things J.*, early access, Sep. 6, 2021, doi: 10.1109/JIOT.2021.3110300.
[312] X. Wang, J. Ma, X. Liu, R. H. Deng, Y. Miao, D. Zhu, and Z. Ma, "Search me in the dark: Privacy-preserving Boolean range query over encrypted spatial data," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, Jul. 2020, pp. 2253–2262.
[313] H. Shah, M. Shah, S. Tanwar, and N. Kumar, "Blockchain for COVID-19: A comprehensive review," *Pers. Ubiquitous Comput.*, pp. 1–28, Aug. 2021, doi: 10.1007/s00779-021-01610-8.
[314] K. Wei, J. Li, M. Ding, C. Ma, H. H. Yang, F. Farokhi, S. Jin, Q. S. T. Quek, and H. V. Poor, "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3454–3469, 2020.
[315] A. A. Gerunov, "Attitudes towards privacy by design in e-government: Views from the trenches," *J. Social Administ. Sci.*, vol. 7, no. 1, pp. 1–17, 2020.
[316] A. Bahmani, K. Ferriter, V. Krishnan, A. Alavi, A. Alavi, P. S. Tsao, M. P. Snyder, and C. Pan, "Swarm: A federated cloud framework for large-scale variant analysis," *PLOS Comput. Biol.*, vol. 17, no. 5, May 2021, Art. no. e1008977.
[317] Y. Wang and D. Papadopoulos, "Multi-user collusion-resistant searchable encryption with optimal search time," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, May 2021, pp. 252–264.
[318] F. Zerka, S. Barakat, S. Walsh, M. Bogowicz, R. T. H. Leijenaar, A. Jochems, B. Miraglio, D. Townend, and P. Lambin, "Systematic review of privacy-preserving distributed machine learning from federated databases in health care," *JCO Clin. Cancer Informat.*, no. 4, pp. 184–200, Sep. 2020.
[319] S. Zapechnikov, "Contemporary trends in privacy-preserving data pattern recognition," *Proc. Comput. Sci.*, vol. 190, pp. 838–844, Jan. 2021.
[320] L. Tan, K. Yu, N. Shi, C. Yang, W. Wei, and H. Lu, "Towards secure and privacy-preserving data sharing for COVID-19 medical records: A blockchain-empowered approach," *IEEE Trans. Netw. Sci. Eng.*, early access, Aug. 4, 2021, doi: 10.1109/TNSE.2021.3101842.
[321] F. A. Reegu, S. Mohd, Z. Hakami, K. K. Reegu, and S. Alam, "Towards trustworthiness of electronic health record system using blockchain," *Ann. Romanian Soc. Cell Biol.*, vol. 25, no. 6, pp. 2425–2434, 2021.
[322] K. K. F. Tsoi, J. J. Y. Sung, H. W. Y. Lee, K. K. L. Yiu, H. Fung, and S. Y. S. Wong, "The way forward after COVID-19 vaccination: Vaccine passports with blockchain to protect personal privacy," *BMJ Innov.*, vol. 7, no. 2, pp. 337–341, Apr. 2021.
[323] H. Choudhury, B. Goswami, and S. K. Gurung, "CovidChain: An anonymity preserving blockchain based framework for protection against COVID-19," *Inf. Secur. J., Global Perspective*, vol. 30, pp. 1–24, May 2021.
[324] A. Abid, S. Cheikhrouhou, S. Kallel, and M. Jmaiel, "NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates," *Softw., Pract. Exper.*, pp. 1–27, May 2021, doi: 10.1002/spe.2983.
[325] O. Ayalon and E. Toch, "User-centered privacy-by-design: Evaluating the appropriateness of design prototypes," *Int. J. Hum.-Comput. Stud.*, vol. 154, Oct. 2021, Art. no. 102641.

[326] M. Coelho, A. Vasconcelos, and P. Sousa, "Privacy by design enterprise architecture patterns," in *Proc. 23rd Int. Conf. Enterprise Inf. Syst.*, 2021, pp. 1–8.
[327] E. Stefanova and A. Dimov, "Privacy enabled software architecture," in *Proc. Int. Symp. Bus. Model. Softw. Design*. New York, NY, USA: Springer, 2021, pp. 190–206.
[328] Y. Qu, M. R. Nosouhi, L. Cui, and S. Yu, "Personalized privacy protection solutions," in *Personalized Privacy Protection Big Data*. Singapore: Springer, 2021, pp. 23–130.
[329] H. Sivaraman, "A prodigal paradigm for the solution of issues and challenges which leads in big data security," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 12, pp. 2818–2823, 2021.
[330] Q. Yang, J. Zhang, W. Hao, G. Spell, and L. Carin, "FLOP: Federated learning on medical datasets using partial networks," 2021, *arXiv:2102.05218*.
[331] B. Rockwern, D. Johnson, and L. S. Sulmasy, "Health information privacy, protection, and use in the expanding digital health ecosystem: A position paper of the American college of physicians," *Ann. Internal Med.*, vol. 174, no. 7, pp. 994–998, Jul. 2021.
[332] G. Yang, S. Wang, and H. Wang, "Federated learning with personalized local differential privacy," in *Proc. IEEE 6th Int. Conf. Comput. Commun. Syst. (ICCCS)*, Apr. 2021, pp. 484–489.
[333] P. Sittijuk and K. Tamee, "Performance measurement of federated learning on imbalanced data," in *Proc. 18th Int. Joint Conf. Comput. Sci. Softw. Eng. (JCSSE)*, Jun. 2021, pp. 1–6.
[334] J. Eder and V. A. Shekhovtsov, "Data quality for federated medical data lakes," *Int. J. Web Inf. Syst.*, vol. 17, no. 5, pp. 407–426, Sep. 2021.
[335] S. Warnat-Herresthal, H. Schultze, K. L. Shastry, S. Manamohan, S. Mukherjee, V. Garg, R. Sarveswara, K. Händler, P. Pickkers, N. A. Aziz, and S. Ktena, "Swarm learning for decentralized and confidential clinical machine learning," *Nature*, vol. 594, no. 7862, pp. 265–270, 2021.
[336] Y. Yuan, J. Liu, D. Jin, Z. Yue, R. Chen, M. Wang, C. Sun, L. Xu, F. Hua, X. He, X. Yi, T. Yang, H.-T. Zhang, S. Sui, and H. Ding, "DeceFL: A principled decentralized federated learning framework," 2021, *arXiv:2107.07171*.
[337] M. Oestreich, D. Chen, J. L. Schultze, M. Fritz, and M. Becker, "Privacy considerations for sharing genomics data," *EXCLI J.*, vol. 20, p. 1243, Jul. 2021.
[338] S. Warnat-Herresthal, H. Schultze, K. L. Shastry, S. Manamohan, S. Mukherjee, V. Garg, R. Sarveswara, K. Händler, P. Pickkers, N. A. Aziz, and S. Ktena, "Swarm learning as a privacy-preserving machine learning approach for disease classification," *BioRxiv*, pp. 1–65, Jun. 2020, doi: 10.1101/2020.06.25.171009.
[339] U. Ahmed, G. Srivastava, and J. C.-W. Lin, "A machine learning model for data sanitization," *Comput. Netw.*, vol. 189, Apr. 2021, Art. no. 107914.
[340] I. M. Florea, G. Ghinita, and R. Rughinis, "Sharing of network flow data across organizations using searchable encryption," in *Proc. 23rd Int. Conf. Control Syst. Comput. Sci. (CSCS)*, May 2021, pp. 189–196.
[341] S. Shaham, G. Ghinita, and C. Shahabi, "An efficient and secure location-based alert protocol using searchable encryption and Huffman codes," 2021, *arXiv:2105.00618*.
[342] A. Akremi and M. Rouached, "A comprehensive and holistic knowledge model for cloud privacy protection," *J. Supercomput.*, vol. 77, pp. 1–33, Jan. 2021.
[343] X. Li, G. Long, and S. Li, "Encrypted medical records search with supporting of fuzzy multi-keyword and relevance ranking," in *Proc. Int. Conf. Artif. Intell. Secur.* New York, NY, USA: Springer, 2021, pp. 85–101.
[344] S. T. Pokharkar and L. K. Vishwamitra, "Securing data in decentralized cloud storage for authorized encrypted search with privacy-preserving on healthcare databases," in *Proc. 10th IEEE Int. Conf. Commun. Syst. Netw. Technol. (CSNT)*, Jun. 2021, pp. 755–760.
[345] I. Elhenawy, S. H. Mahmoud, and A. Moustafa, "A lightweight privacy preserving keyword search over encrypted data in cloud computing," *J. Cybersecurity Inf. Manage.*, vol. 3, no. 2, pp. 9–29, 2021.
[346] S. Aich, N. K. Sinai, S. Kumar, M. Ali, Y. R. Choi, M.-I. Joo, and H.-C. Kim, "Protecting personal healthcare record using blockchain & federated learning technologies," in *Proc. 23rd Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2021, pp. 109–112.
[347] H. Kasyap and S. Tripathy, "Privacy-preserving decentralized learning framework for healthcare system," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 17, no. 2s, pp. 1–24, Jun. 2021.
[348] L. Zhang, D. Liu, M. Chen, H. Li, C. Wang, Y. Zhang, and Y. Du, "A user collaboration privacy protection scheme with threshold scheme and smart contract," *Inf. Sci.*, vol. 560, pp. 183–201, Jun. 2021.
[349] U. Khadam, M. M. Iqbal, S. Jabbar, and S. A. Shah, "Data aggregation and privacy preserving using computational intelligence," *IEEE Internet Things Mag.*, vol. 4, no. 2, pp. 60–64, Jun. 2021.
[350] K. Xue, Z. Liu, H. Zhu, M. Pan, and D. S. Wei, "Advances in privacy-preserving computing," *Peer Peer Netw. Appl.*, vol. 14, no. 3, pp. 1348–1352, 2021.
[351] J. Labs and S. Terry, "Privacy in the coronavirus era," *Genetic Test. Mol. Biomarkers*, vol. 24, no. 9, pp. 535–536, Sep. 2020.
[352] L. Malina, P. Dzurenda, S. Ricci, J. Hajny, G. Srivastava, R. Matulevicius, A.-A.-O. Affia, M. Laurent, N. H. Sultan, and Q. Tang, "Post-quantum era privacy protection for intelligent infrastructures," *IEEE Access*, vol. 9, pp. 36038–36077, 2021.
[353] A. B. Haque, B. Naqvi, A. K. M. N. Islam, and S. Hyrynsalmi, "Towards a GDPR-compliant blockchain-based COVID vaccination passport," *Appl. Sci.*, vol. 11, no. 13, p. 6132, Jul. 2021.
[354] T. Carvalho, P. Faria, L. Antunes, and N. Moniz, "Fundamental privacy rights in a pandemic state," *PLoS ONE*, vol. 16, no. 6, Jun. 2021, Art. no. e0252169.
[355] J. Meszaros and C.-H. Ho, "AI research and data protection: Can the same rules apply for commercial and academic research under the GDPR?" *Comput. Law Secur. Rev.*, vol. 41, Jul. 2021, Art. no. 105532.
[356] A. M. Gambino and D. Tuzzolino, "Location data and privacy," in *Privacy and Data Protection in Software Services*. Singapore: Springer, 2022, pp. 141–152.
[357] K. Broen, R. Trangucci, and J. Zelner, "Measuring the impact of spatial perturbations on the relationship between data privacy and validity of descriptive statistics," *Int. J. Health Geographics*, vol. 20, no. 1, pp. 1–16, Dec. 2021.
[358] D. M. Harris, "The law of medical privacy in the USA: Not good enough for COVID-19," *Medicne Pravo*, vol. 27, no. 1, pp. 28–40, Feb. 2021.
[359] S. Ganeshan, E. Hsiang, T. Peng, N. Thomas, I. Garcia-Grossman, K. Javaherian, Z. Lyon, and A. Vidyarthi, "Enabling patient communication for hospitalised patients during and beyond the COVID-19 pandemic," *BMJ Innov.*, vol. 7, no. 2, pp. 316–320, Apr. 2021.
[360] P. Sanderson, "Balancing public health and civil liberties: Privacy aspects of contact-tracing technologies," *IEEE Secur. Privacy*, vol. 19, no. 4, pp. 65–69, Jul. 2021.
[361] C. S. Yoo and A. Vidyarthi, "Privacy in the age of contact tracing: An analysis of contact tracing apps in different statutory and disease frameworks," *Univ. Pennsylvania J. Law Innov.*, vol. 5, pp. 1–40, Jun. 2021. [Online]. Available: https://ssrn.com/abstract=3861268
[362] Y. B. Choi and C. E. Williams, "A HIPAA security and privacy compliance audit and risk assessment mitigation approach," *Int. J. Cyber Res. Educ.*, vol. 3, no. 2, pp. 28–45, Jul. 2021.
[363] M. S. Khan, A. Anjum, T. Saba, A. Rehman, and U. Tariq, "Improved generalization for secure personal data publishing using deviation," *IT Prof.*, vol. 23, no. 2, pp. 75–80, Mar. 2021.
[364] S.-Y. Shin, "Privacy protection and data utilization," *Healthcare Informat. Res.*, vol. 27, no. 1, pp. 1–2, Jan. 2021.
[365] Y.-A. Min, "Zero-knowledge proof algorithm for data privacy," *Int. J. Internet, Broadcast. Commun.*, vol. 13, no. 2, pp. 67–75, 2021.
[366] J.-S. Lee and S.-P. Jun, "Privacy-preserving data mining for open government data from heterogeneous sources," *Government Inf. Quart.*, vol. 38, no. 1, Jan. 2021, Art. no. 101544.
[367] S. Lim, "Tackling privacy paradox: Protecting right to self-determination of personal information by estimating the economic value of personal information and visualizing the price," *Int. J. Internet, Broadcast. Commun.*, vol. 13, no. 2, pp. 244–259, 2021.
[368] W. Silva and A. C. B. Garcia, "Where is our data? A blockchain-based information chain of custody model for privacy improvement," in *Proc. IEEE 24th Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, May 2021, pp. 329–334.
[369] K.-H. Kim, S. Lim, D.-Y. Hwang, and K.-H. Kim, "Analysis on the privacy of DID service properties in the DID document," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2021, pp. 745–748.
[370] A. Rix, "How data privacy regulations affect public corporations that profit from Consumers' data during an ongoing pandemic," *SSRN Electron. J.*, vol. 74, no. 1, pp. 1–28, Feb. 2021. [Online]. Available: https://ssrn.com/abstract=3774366
[371] J. Oliva, "Public health surveillance in the context of COVID-19," *Ind. Health L. Rev.*, vol. 18, no. 1, p. 107, 2021.

[372] N. Terry and C. N. Coughlin, "A virtuous circle: How health solidarity could prompt recalibration of privacy and improve data and research," *Oklahoma Law Rev., Forthcoming*, vol. 74, no. 1, pp. 1–28, Feb. 2021. [Online]. Available: https://ssrn.com/abstract=3774366
[373] J. Amankwah-Amoah, Z. Khan, G. Wood, and G. Knight, "COVID-19 and digitalization: The great acceleration," *J. Bus. Res.*, vol. 136, pp. 602–611, Nov. 2021.
[374] D. Bhattacharya and L. Ramos, "COVID-19: Privacy and confidentiality issues with contact tracing apps," in *Proc. 54th Hawaii Int. Conf. Syst. Sci.*, 2021, p. 2009.
[375] S. Pape, D. Harborth, and J. L. Kröger, "Privacy concerns go hand in hand with lack of knowledge: The case of the German corona-warn-app," in *Proc. IFIP Int. Conf. ICT Syst. Secur. Privacy Protection*. New York, NY, USA: Springer, 2021, pp. 256–269.
[376] H. Kudo, "COVID-19 digital contact tracing between privacy issues and co-production–why some have worked and some haven't," in *Proc. Central Eastern Eur. eDem eGov Days*, 2021, pp. 337–349.
[377] M. Smolenskiy and N. Levshin, "Gdpr implementation as the main reason for the regional fragmentation in the online mediasphere," in *Proc. E3S Web Conf.*, vol. 273. Les Ulis, France: EDP Sciences, 2021, Art. no. 08099.
[378] C. Bettini, S. Kanhere, M. Langheinrich, A. Misra, and D. Reinhardt, "Is privacy regulation slowing down research on pervasive computing?" *Computer*, vol. 53, no. 6, pp. 44–52, Jun. 2020.
[379] P. Churi, A. Pawar, and A.-J. Moreno-Guerrero, "A comprehensive survey on data utility and privacy: Taking Indian healthcare system as a potential case study," *Inventions*, vol. 6, no. 3, p. 45, Jun. 2021.
[380] T. Darbyshire, "Do we need a coronavirus (Safeguards) act 2020? Proposed legal safeguards for digital contact tracing and other apps in the COVID-19 crisis," *Patterns*, vol. 1, no. 4, Jul. 2020, Art. no. 100072.
[381] N. Vasupula, V. Munnangi, and S. Daggubati, "Modern privacy risks and protection strategies in data analytics," in *Soft Computing and Signal Processing*. Singapore: Springer, 2022, pp. 81–89.
[382] A. K M. N. Mehdy and H. Mehrpouyan, "Modeling of personalized privacy disclosure behavior: A formal method approach," 2021, *arXiv:2106.11762*.
[383] B. Niu, Y. Chen, B. Wang, Z. Wang, F. Li, and J. Cao, "AdaPDP: Adaptive personalized differential privacy," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, May 2021, pp. 1–10.
[384] H. Deng, Z. Wang, and Y. Zhang, "Overview of privacy protection data release anonymity technology," in *Proc. IEEE 7th IEEE Int. Conf. Big Data Secur. Cloud (BigDataSecurity) Int. Conf. High Perform. Smart Comput., (HPSC) IEEE Int. Conf. Intell. Data Secur. (IDS)*, May 2021, pp. 151–156.
[385] E. Antwi-Boasiako, S. Zhou, Y. Liao, Q. Liu, Y. Wang, and K. Owusu-Agyemang, "Privacy preservation in distributed deep learning: A survey on distributed deep learning, privacy preservation techniques used and interesting research directions," *J. Inf. Secur. Appl.*, vol. 61, Sep. 2021, Art. no. 102949.
[386] S. Zou, J. Xi, G. Xu, M. Zhang, and Y. Lu, "CrowdHB: A decentralized location privacy-preserving crowdsensing system based on a hybrid blockchain network," *IEEE Internet Things J.*, early access, May 31, 2021, doi: 10.1109/JIOT.2021.3084937.
[387] M. Hojati, C. Farmer, R. Feick, and C. Robertson, "Decentralized geoprivacy: Leveraging social trust on the distributed web," *Int. J. Geographical Inf. Sci.*, vol. 35, pp. 1–27, Jun. 2021.
[388] P. Davies, G. Parry, and J. Oh, "Introduction to the minitrack on personal data: Analytics and management," in *Proc. 54th Hawaii Int. Conf. Syst. Sci.*, 2021, p. 1685.
[389] M. S. Rahman, I. Khalil, M. Atiquzzaman, and X. Yi, "Towards privacy preserving AI based composition framework in edge networks using fully homomorphic encryption," *Eng. Appl. Artif. Intell.*, vol. 94, Sep. 2020, Art. no. 103737.
[390] G. Liu, C. Wang, X. Ma, and Y. Yang, "Keep your data locally: Federated-learning-based data privacy preservation in edge computing," *IEEE Netw.*, vol. 35, no. 2, pp. 60–66, Mar. 2021.
[391] X. Pan, S. Tang, and Z. Zhu, "Privacy-preserving multilayer in-band network telemetry and data analytics," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Aug. 2020, pp. 142–147.
[392] H. Yuliansyah, Z. A. Othman, and A. A. Bakar, "Taxonomy of link prediction for social network analysis: A review," *IEEE Access*, vol. 8, pp. 183470–183487, 2020.
[393] R. S. Hirschprung and O. Leshman, "Privacy disclosure by de-anonymization using music preferences and selections," *Telematics Inform.*, vol. 59, Jun. 2021, Art. no. 101564.
[394] N. Bouacida and P. Mohapatra, "Vulnerabilities in federated learning," *IEEE Access*, vol. 9, pp. 63229–63249, 2021.
[395] D. Deutch, A. Frankenthal, A. Gilad, and Y. Moskovitch, "On optimizing the trade-off between privacy and utility in data provenance," in *Proc. Int. Conf. Manage. Data*, Jun. 2021, pp. 379–391.
[396] X. Qian, X. Li, and Z. Zhou, "An efficient privacy-preserving approach for data publishing," *J. Ambient Intell. Humanized Comput.*, pp. 1–17, Aug. 2021, doi: 10.1007/s12652-021-03417-0.
[397] S. Furnell, P. Haskell-Dowland, M. Agrawal, R. Baskerville, A. Basu, M. Bishop, J. Cuellar, S. Foresti, L. Futcher, and N. Gal-Oz, "Information security and privacy–challenges and outlook," in *Advancing Research in Information and Communication Technology*. New York, NY, USA: Springer, 2021, pp. 383–401.
[398] E. De Cristofaro, "A critical overview of privacy in machine learning," *IEEE Secur. Privacy*, vol. 19, no. 4, pp. 19–27, Jul. 2021.
[399] N. Hajli, F. Shirazi, M. Tajvidi, and N. Huda, "Towards an understanding of privacy management architecture in big data: An experimental research," *Brit. J. Manage.*, vol. 32, no. 2, pp. 548–565, Apr. 2021.
[400] Y. Shui-lian, P. De-chang, and X. Meng, "Trajectory privacy protection method based on differential privacy," *Acta Electonica Sinica*, vol. 49, no. 7, p. 1266, 2021.
[401] D. Yu, H. Zhang, W. Chen, and T.-Y. Liu, "Do not let privacy overbill utility: Gradient embedding perturbation for private learning," 2021, *arXiv:2102.12677*.
[402] J. Chen, W. H. Wang, and X. Shi, "Differential privacy protection against membership inference attack on machine learning for genomic data," in *Proc. Biocomputing*, Nov. 2020, pp. 26–37.
[403] H. Xie, L. Wei, and F. Fang, "Research on privacy protection based on machine learning," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2021, pp. 1003–1006.
[404] W. Cheng, W. Ou, X. Yin, W. Yan, D. Liu, and C. Liu, "A privacy-protection model for patients," *Secur. Commun. Netw.*, vol. 2020, Dec. 2020, Art. no. 6647562.
[405] R. Xu, N. Baracaldo, and J. Joshi, "Privacy-preserving machine learning: Methods, challenges and directions," 2021, *arXiv:2108.04417*.
[406] B. Li, H. Zhu, and M. Xie, "Quantifying location privacy risks under heterogeneous correlations," *IEEE Access*, vol. 9, pp. 23876–23893, 2021.
[407] C. Landwehr, "Privacy research directions," *Commun. ACM*, vol. 59, no. 2, pp. 29–31, Jan. 2016.
[408] S. K. Kroes, M. P. Janssen, R. H. Groenwold, and M. van Leeuwen, "Evaluating privacy of individuals in medical data," *Health Informat. J.*, vol. 27, no. 2, Apr. 2021, Art. no. 146045822098339.
[409] J. Xiong, H. Liu, B. Jin, Q. Li, and Z. Yao, "A lightweight privacy protection scheme based on user preference in mobile crowdsensing," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 5, May 2021, Art. no. e4000.
[410] C. Dhasarathan, M. Kumar, A. K. Srivastava, F. Al-Turjman, A. Shankar, and M. Kumar, "A bio-inspired privacy-preserving framework for healthcare systems," *J. Supercomput.*, vol. 77, pp. 11099–11134, Mar. 2021.
[411] T. B. Ogunseyi, T. Bo, and C. Yang, "A privacy-preserving framework for cross-domain recommender systems," *Comput. Electr. Eng.*, vol. 93, Jul. 2021, Art. no. 107213.
[412] R. Naidu, A. Priyanshu, A. Kumar, S. Kotti, H. Wang, and F. Mireshghallah, "When differential privacy meets interpretability: A case study," 2021, *arXiv:2106.13203*.
[413] S. Lobner, W. B. Tesfay, T. Nakamura, and S. Pape, "Explainable machine learning for default privacy setting prediction," *IEEE Access*, vol. 9, pp. 63700–63717, 2021.
[414] H. Sun, J. Plawinski, S. Subramaniam, A. Jamaludin, T. Kadir, A. Readie, G. Ligozio, D. Ohlssen, M. Baillie, and T. Coroller, "A deep learning approach to private data sharing of medical images using conditional GANs," 2021, *arXiv:2106.13199*.
[415] R. J. Chen, M. Y. Lu, T. Y. Chen, D. F. Williamson, and F. Mahmood, "Synthetic data in machine learning for medicine and healthcare," *Nature Biomed. Eng.*, vol. 5, pp. 493–497, Jun. 2021.
[416] K. El Emam, L. Mosquera, E. Jonker, and H. Sood, "Evaluating the utility of synthetic COVID-19 case data," *JAMIA Open*, vol. 4, no. 1, Mar. 2021, Art. no. ooab012.
[417] X. Yuan, X. Ma, L. Zhang, Y. Fang, and D. Wu, "Beyond class-level privacy leakage: Breaking record-level privacy in federated learning," *IEEE Internet Things J.*, early access, Jun. 16, 2021, doi: 10.1109/JIOT.2021.3089713.

[418] A. Majeed and S. Lee, "Attribute susceptibility and entropy based data anonymization to improve users community privacy and utility in publishing data," *Int. J. Speech Technol.*, vol. 50, no. 8, pp. 2555–2574, Aug. 2020.
[419] Y. Yan, E. A. Herman, A. Mahmood, T. Feng, and P. Xie, "A weighted k-member clustering algorithm for k-anonymization," *Computing*, vol. 103, pp. 2251–2273, Feb. 2021.
[420] H. O. Mansour, M. M. Siraj, F. A. Ghaleb, F. Saeed, E. H. Alkhammash, and M. A. Maarof, "Quasi-identifier recognition algorithm for privacy preservation of cloud data based on risk reidentification," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–13, Aug. 2021.
[421] S. R. Pandey, M. N. H. Nguyen, T. N. Dang, N. H. Tran, K. Thar, Z. Han, and C. S. Hong, "Edge-assisted democratized learning towards federated analytics," *IEEE Internet Things J.*, early access, Jun. 2, 2021, doi: 10.1109/JIOT.2021.3085429.
[422] D. Chen, D. Wang, Y. Zhu, and Z. Han, "Digital twin for federated analytics using a Bayesian approach," *IEEE Internet Things J.*, vol. 8, no. 22, pp. 16301–16312, Nov. 2021.

ABDUL MAJEED received the B.S. degree in information technology from UIIT, PMAS-UAAR, Rawalpindi, Pakistan, in 2013, the M.S. degree in information security from COMSATS University, Islamabad, Pakistan, in 2016, and the Ph.D. degree in computer information systems and networks from Korea Aerospace University, South Korea, in 2021. He worked as a Security Analyst with Trillium Information Security Systems (TISS), Rawalpindi, from 2015 to 2016. He is currently working as an Assistant Professor with the Department of Computer Engineering, Gachon University, South Korea. His research interests include privacy preserving data publishing, statistical disclosure control, privacy-aware analytics, and machine learning.

SEONG OUN HWANG (Senior Member, IEEE) received the B.S. degree in mathematics from Seoul National University, in 1993, the M.S. degree in information and communications engineering from the Pohang University of Science and Technology, in 1998, and the Ph.D. degree in computer science from the Korea Advanced Institute of Science and Technology, South Korea, in 2004. He worked as a Software Engineer with LG-CNS Systems, Inc., from 1994 to 1996. He also worked as a Senior Researcher with the Electronics and Telecommunications Research Institute (ETRI), from 1998 to 2007. He worked as a Professor with the Department of Software and Communications Engineering, Hongik University, from 2008 to 2019. He is currently working as a Full Professor with the Department of Computer Engineering, Gachon University, South Korea. His research interests include cryptography, cybersecurity, and artificial intelligence.