IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 5 December 2022, accepted 14 December 2022, date of publication 21 December 2022,
date of current version 30 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3231446

SURVEY

The Next Generation of eHealth: A Multidisciplinary Survey

CHIARA SURACI[1], VINCENZO DE ANGELIS[1], GIUSEPPINA LOFARO[1], MICHELE LO GIUDICE[1,2], GIUSEPPE MARRARA[1], FEDERICA RINALDI[1], ANTONIA RUSSO[1], MARTINA TERESA BEVACQUA[1], GIANLUCA LAX[1], (Member, IEEE), NADIA MAMMONE[3], ANTONINO MAZZA LABOCCETTA[4], FRANCESCO CARLO MORABITO[3], (Senior Member, IEEE), AND GIUSEPPE ARANITI[1], (Senior Member, IEEE)

[1]Department of Information, Infrastructure and Sustainable Energy (DIIES), University Mediterranea of Reggio Calabria, 89100 Reggio Calabria, Italy
[2]Department of Medical and Surgery Sciences, University of Catanzaro, 88100 Catanzaro, Italy
[3]Department of Civil Engineering, Energy, Environment and Materials (DICEAM), University Mediterranea of Reggio Calabria, 89100 Reggio Calabria, Italy
[4]DIGIES Department, University Mediterranea of Reggio Calabria, 89100 Reggio Calabria, Italy

Corresponding author: Giuseppe Araniti (araniti@unirc.it)

This work was supported by the iCARE Project-action 10.5.12 funded within Programmi Operativi Regionali finanziati con Fondo Europeo di Sviluppo Regionale e Fondo Sociale Europeo (POR FESR FSE) 2014/2020 of Calabria Region with the participation of European Community Resources of FESR and FSE, Italy and Calabria, under Grant CUP J39J14001400007.

ABSTRACT Over the past two years, the spread of COVID-19 has spurred the use of information and communication technologies (ICT) in aid of healthcare. The need to guarantee continuity to care has promoted research and industry activities aimed at developing solutions for the digitalization of the procedures to be performed to provide health services, even in emergency scenarios. Digital collection, transmission, and processing of health data represent the starting point for fulfilling this innovation process but also bring heterogeneous challenges. These motivations led to the elaboration of this work, which analyzes innovative and technological tools for the development of digital health (eHealth) through the collection of multisectoral literature, produced thanks to the cooperation of varied research groups, thus providing a multidisciplinary survey. Since digital health is expected to be one of the leading applications of the sixth-generation (6G) wireless cellular networks, this paper covers the related telecommunications aspects. Furthermore, the exploitation of artificial intelligence paradigms to elaborate massive amounts of biological data is examined. Given the extreme sensitivity of health data, this paper also investigates security and privacy issues. In particular, the main techniques and approaches to guarantee security properties (i.e., anonymity, responsibility, authentication, confidentiality, integrity, non-repudiation, and revocability) are studied. Applications involving innovative electromagnetic systems for healthcare and assisted living services are described to provide an example of an eHealth scenario leveraging ICT. Finally, the telemedicine-related regulations of the European Commission are analyzed, with particular reference to the General Data Protection Regulation (GDPR).

INDEX TERMS eHealth, telemedicine, 6G, data, security, artificial intelligence, neural network, electromagnetism, GDPR.

I. INTRODUCTION

The worldwide and uncontrolled spread of COVID-19 infection has changed, for some years now, both the impact of technological progress on the quality of life of the worldwide population and the vision that the latter has of the digitalization of several activities affecting everyday life. In particular, the healthcare sector has been hit by a wave of change fostered by the need to guarantee continuity of care and health assistance during the lockdowns imposed in the different countries of the world, which have made in-person meetings between the doctor and the patient impracticable. Currently,

The associate editor coordinating the review of this manuscript and approving it for publication was Qingli Li.

the digitalization process of the healthcare sector is not at the same point in different parts of the world. However, it has undergone an acceleration everywhere. Data play a significant role in the provision of health services, and their effective digital treatment must be the basis of the innovation process. When digital health (eHealth) services are provisioned, technologies and paradigms from different fields can play critical functions in health data processing, including telecommunications for the collection and transmission of data, artificial intelligence for data elaboration, and security for the protection of data and people.

With regards to *telecommunications*, existing network infrastructures are insufficient to support the full achievement of a radically digitalized healthcare sector. This is confirmed by the authors of [1] and [2], who describe the trends that will lead to the development of the sixth generation (6G) of wireless mobile networks, placing healthcare among the driving applications of the next decade. The continuous growth in the percentage of the world's elderly population is among the factors that will spur the digitalization process of the medical field, leading to an increasingly pervasive presence of the eHealth paradigm among cellular network applications. The need to monitor chronic and old-age diseases will thrive over the years, thus fostering the tendency to resort to information and communication technologies (ICT) to support the remote execution of services, such as monitoring and medical assistance. The Internet of Things (IoT) technology has contributed to the digitalization process that has changed our current world and is considered disruptive and essential to provide connectivity to heterogeneous objects deployed for collecting data [3]. In particular, although the use of the Internet of Medical Things (IoMT) is already underway for the collection and transmission of data in healthcare scenarios, only the deployment of the Internet of Everything (IoE) paradigm (expected concurrently with the evolution of networks towards 6G) will enable the execution of many cutting-edge services. The discussion of how IoE and other 6G paradigms will empower eHealth will be addressed throughout the paper.

Advanced *artificial intelligence (AI)* algorithms for biological data elaboration are increasingly needed to aid the evolution of the eHealth sector. Biological data, by their nature, are very complex and originate from different application fields (e.g., neurophysiological signals, magnetic resonance imaging, blood oxygenation values) and sources (e.g., hospitals, telemedicine platforms), which determine their wide variety in terms of structure and availability. Therefore, properly elaborating these data implies a preliminary analysis of intrinsic characteristics, such as structure and amount. At an engineering design level, three macro-groups can be identified for the structure of the data: time series, images, and sequences [4]. The origin of data determines the type and, thus, a possible optimal elaboration pipeline, which could involve many algorithms of diverse complexity. Defining a tight cluster of sources is not trivial since they are very wide and related to the target application [5]. The amount of biological data determines the approach to use for their proper management. Biological data collected sporadically and in limited quantities can be processed by the physician or analyzed using standard signal elaboration methods. When quantity and frequency of acquisition far exceed the available elaboration capacity and time, it is essential to entrust autonomous systems equipped with AI to process or label them automatically. A considerable amount of data is also advantageous and necessary for training AI systems, but always considering that data must be adequately structured to be well-processed without human support.

The diverse stages of the data lifecycle present privacy and *security* concerns, especially if data contain highly sensitive information on users and come from heterogeneous sources. The benefits introduced by innovative paradigms and technologies have the side effect of increasing the attack surface for malicious adversaries. As a consequence, a dramatic number of cybersecurity attacks [6] have been conducted, also recently [7], [8], [9]. Applying security patches to existing solutions is not enough from this perspective, but it is very important to follow security-by-design methodologies.

When dealing with the digital treatment of health data, another aspect that should not be overlooked is that understanding the regulations of *health law* that govern the various processes is crucial. Without uniform legislation, eHealth services are governed by sectoral regulations, including best practices and guidelines, which should be approached with prudential criteria in light of the principle of self-determination and patient empowerment. Consequently, standards for the efficiency of the digital public health system should be adopted [10]. The security of personal and sensitive data used in the provision of services is a tool to realize the right to health, both in its individual and collective dimensions. There is a functional link, in the health sector, between the issue of security in the training, conservation, use, and circulation of clinical data and the one of privacy. According to the General Data Protection Regulation (GDPR), the strategy for the security of personal data is focused on the ''general principle of processing''. Therefore, a personal data protection approach emerges based on overall risk management and on the proactive accountability of the Data Controller, in charge of concretely modulating the implementation of the principles enshrined in the Regulation. With a view to accountability, the security of personal data, involving the application of different measures, requires an integrated vision of multiple competencies (including legal, IT, and organizational ones) in a balanced integration dimension between human and technological advancement in healthcare [11].

A. MOTIVATIONS AND TARGET AUDIENCE

The primary motivation that led to the elaboration of this work is to contribute with a multidisciplinary survey to the process of analyzing the role of data and their treatment in the context of eHealth.

To the best of our knowledge, there are no investigations of this type in the literature, but only works that individually face some of the aspects we examine. An in-depth review of security and privacy challenges can be found in [12], where no data transmission or elaboration aspects are treated. Another interesting discussion about security in eHealth is provided in [13], where we can find the same security properties presented in our paper in a slightly different meaning; the authors of [13] also mention biometric cryptography as a means of authentication, but there is no reference to blockchain technology. On the contrary, we have devoted much effort to discussing blockchain-based approaches, as it is a mature technology already implemented in several real-life eHealth applications. Likewise, a state-of-the-art review of the fifth-generation (5G) cellular networks and Internet of Things (IoT) enabled smart healthcare is in [14], which is very focused on 5G and communication technologies, neglecting the topics of artificial intelligence and regulations and lightly treating the security, trust, and privacy challenges. The work in [15] deals with themes similar to our paper despite the point of view of the proposed analysis and the insight provided for the various topics being different, and it does not mention the regulatory aspect that is fundamental for the success of the digitalization of health services. Our work provides an original approach as it introduces a classification of technologies linked to the use that they have in the processing of health data and proposes innovative electromagnetic systems for eHealth as an application example of the collection/elaboration/security paradigm described. Even the authors of [16] discuss the role of 6G in healthcare systems but, unlike our work, their study focuses on communication technologies suitable to emergency scenarios and disaster management. The authors of [4] thoroughly investigate different deep learning (DL) architectures and applications for processing biological data, but they do not address the complementary processes of data transmission and protection. The work in [17] provides an overview of the current and future potential of AI in medicine applications, including a historical outline of AI in medicine, deep neural network components, and different AI approaches; however, it does not address the benefits of integrating AI with efficient and secure transmissions for better accessibility and legal protection of biological data in medical workflows, which are necessary for decentralized eHealth services.

Table 1 highlights the differences between our paper and others similar in the recent literature, reporting which topics are covered in each work and to what extent; the ''partial'' value is to be understood with respect to how much the topic is deepened in our work.

We opine that in the future new professional profiles will arise in the eHealth sector, and they will require transversal competencies in different fields. Therefore, unlike other reviews that offer predominantly single-viewpoint analysis, we propose a cross-sectoral overview that could be very useful for the physician/scientist of the future, who, beyond traditional medical skills, should be characterized by highly technological and multidisciplinary knowledge. This paper is intended both for expert readers (interested in investigating a particular approach or technology) and non-expert readers (interested in a high-level vision of eHealth) who might benefit from this paper to acquire a multidisciplinary view of eHealth.

The multidisciplinarity in our work is achieved thanks to the collaboration of different research groups gathered within the *iCare* project (it is a University project funded within POR FESR FSE 2014/2020 of Calabria Region with the participation of European Community Resources of FESR and FSE, of Italy and of Calabria), which has the dual purpose of strengthening research infrastructures and enriching the healthcare sector. In detail, this project will contribute to the realization of a state-of-the-art telemedicine research laboratory within the university, which will foster the cooperation of worldwide researchers to conduct activities targeted at studying innovative solutions for the management of health services. The latter aspect is directly addressed by the project, since, also thanks to the collaboration with external consultants from the industrial and business sectors, it aims to create a telemedicine system that integrates the procedures that are currently implemented by some local health facilities with others that leverage ICT for remote management of services. Therefore, the synergy between University, Industry, and Hospital represents the backbone of the iCare project, promoter of research and development activities supporting the healthcare sector. Almost at the end of the first year of the project, this work has been produced to reap the benefits of the research activities on the topics of telecommunications, artificial intelligence, information technology, electromagnetism, and health law, which can contribute to providing different viewpoints on the analysis of the digital processing of health data.

A taxonomy of the topics subject of the multidisciplinary survey on eHealth we provide is illustrated in Figure 1.

B. CONTRIBUTIONS

Based on these considerations, the main contribution of this work is to address the matter of data processing in the provision of eHealth services by offering a multidisciplinary survey, which provides insight into the fields of artificial intelligence, electromagnetism, health law, security, and telecommunications, for the first time in literature to the best of our knowledge. This is articulated in the delivery of the following micro-contributions:

1) The central role that data play in eHealth services is emphasized by dealing with a thorough technical analysis of the different steps necessary for their processing. In particular, the three steps of *(i)* collection and transmission, *(ii)* elaboration, and *(iii)* security are identified and individually addressed through the gathering and analysis of the related literature. A Readiness to Adopt (RTA) value is indicated to provide a qualitative estimate of the readiness to be adopted in eHealth applications for each technology or technique mentioned for

TABLE 1. Comparison between our paper and others similar in the recent literature.

Reference	Artificial Intelligence	Electromagnetic systems	Health law	Security	Telecommunications
[4]	YES	NO	NO	NO	NO
[12]	NO	NO	NO	YES	NO
[13]	NO	NO	NO	YES	NO
[14]	NO	NO	NO	PARTIAL	YES
[15]	YES	NO	NO	PARTIAL	YES
[16]	PARTIAL	NO	NO	PARTIAL	YES
[17]	YES	NO	PARTIAL	NO	NO
Our paper	**YES**	**YES**	**YES**	**YES**	**YES**

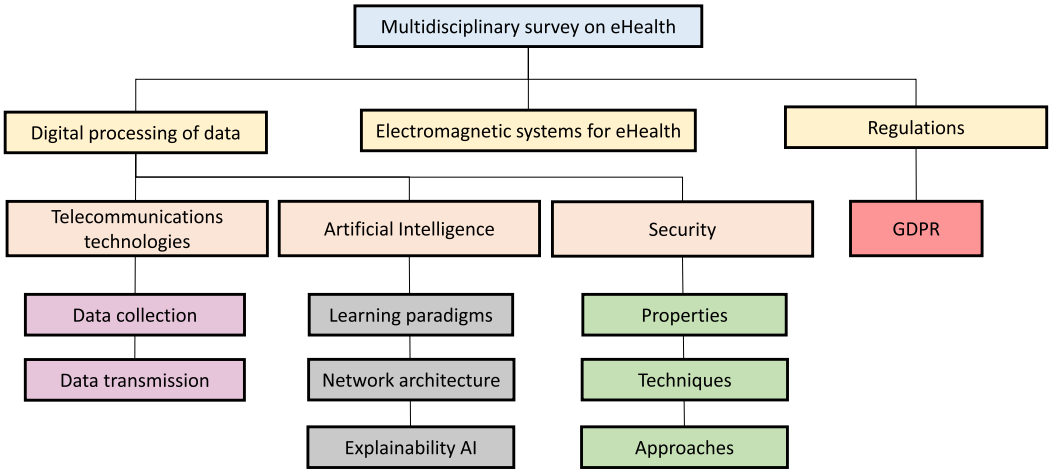


FIGURE 1. Taxonomy of the multidisciplinary survey on eHealth.

the three data processing steps. It can take on a high, medium, or low value based on how much we believe the rapid use of the technology/technique in eHealth is likely. Mainly, the study of the most recent literature and the knowledge of the mentioned paradigms are the basis for the RTA evaluation that will be discussed later.

2) The 6G technologies expected as enablers in health data processing are investigated, and a collection of diverse classifications related to IoMT devices in the literature is provided to demonstrate the heterogeneity of these devices.
3) AI techniques proposed in the literature for analyzing biological data are explored and given the telemedicine-focused focus of our review, AI clinical applications to evaluate their potential impact are also proposed.
4) The main security properties that an eHealth solution should guarantee are introduced. Furthermore, the leading techniques and approaches offering security features in the eHealth ecosystem are surveyed, showing how they can ensure the above security properties.
5) As an example of the application of the defined data processing paradigm (collection/elaboration/security), research proposals concerning innovative *electromagnetic systems* applied to the remote and safe monitoring of patient status are described.
6) An in-depth analysis of telemedicine-related regulations is provided, particularly dwelling on some specific articles of GDPR (this research work has been funded by the European Community). Besides, a critical discussion of the reliability that should legally be granted to machines and algorithms is addressed through an example based on the use of AI.

The paper is structured as follows. The next section introduces three technological perspectives on health data processing: collection and transmission, elaboration, and security. Section III discusses the applications of electromagnetic systems in eHealth. In Section IV, a juristic vision of the current challenges related to the healthcare sector is given. Open issues and future research directions are discussed in Section V. Finally, Section VI draws conclusions.

We summarize the meaning of all acronyms used in the paper in Table 2.

II. DIGITAL PROCESSING OF HEALTH DATA: A MULTISTEP METHOD

Nowadays, health data may be efficiently and securely collected, transmitted, and elaborated through the exploitation of ICT, thanks to recent technological advances. In this section, we analyze three different data processing steps (i.e., collection, elaboration, and security), focusing on the technological

and innovative tools in the literature that can help digitalize the operations to be accomplished so that the data can be detected on the patient and elaborated by the healthcare professionals in the best possible way. Table 3 collects all the technologies/techniques and works cited in this section grouped by data processing steps and reports the RTA value for each technology/technique.

A. COMMUNICATIONS PARADIGMS FOR DATA COLLECTION

The authors of [2] point out that digital healthcare applications will require increasingly stringent data rate, latency, and reliability requirements, thus making the support of pioneering technologies necessary. IoE, Device-to-Device (D2D), Edge Computing, AI, Digital Twin, Holography, Robotics, Tactile Internet, and Non-Terrestrial Networks (NTNs) are among the technologies that will play a pivotal role in the 6G era and can help in meeting the strict requirements of future applications. In the following, we discuss recent works in the literature that propose using some of these technologies to support the collection and transmission of data on 6G-oriented networks for eHealth services. For each cited technology, a description is provided supported by the advantages, disadvantages, and challenges deriving from its use in the eHealth context. Figure 2 provides a graphical representation of the mentioned technologies.

1) INTERNET OF EVERYTHING (IoE)

IoE is defined, in [18], as the paradigm able to enable the connection on a wireless channel of a plethora of heterogeneous devices, mostly portable and featuring low energy resources. According to [19], IoE belongs to the *revolutionary* tide of the fifth generation (5G) that includes the most innovative and forward-looking trends. Furthermore, the authors place telemedicine among the IoE applications that will foster the birth of 6G, whose hallmarks will be mainly set based on the performance requirements of IoE services, increasingly imposing in the panorama of current and future cellular networks. In [20], the origin of the term ''IoE'' is attributed to CISCO that, in 2012, defined it as a network of networks connecting *people, processes, data, and things*, thus being an evolution of the Internet of Things (IoT). To date, the IoT affects many of the most widespread everyday-life applications, and the IoE, as its evolution, will guarantee requirements never yet explored to the services expected for the future 6G cellular networks. Moreover, the cooperative use of IoE with other technologies, such as machine learning, could favor the emergence of new consumer services increasingly oriented towards improving the quality of life of the world population. Representing the evolution of the IoT, the IoE inherits some challenges, including the need to be combined with energy-saving techniques, as it will mainly affect portable and low-power devices; besides, being a revolutionary technology expected for 6G, the IoE is not fully utilized by the current generations of cellular networks, and only some of its ''subsets'' are.

TABLE 2. List of acronyms.

2D	Two-Dimensional
3GPP	3rd Generation Partnership Project
5G	Fifth Generation
6G	Sixth Generation
AI	Artificial Intelligence
ANNs	Artificial Neural Networks
ABE	Attribute-Based Encryption
CP-ABE	Cipher-Policy Attribute-Based Encryption
CP-ABPRE	Cipher-Policy Attribute-Based Proxy Re-Encryption
CNNs	Convolutional Neural Networks
DL	Deep Learning
D2D	Device-to-Device
ECG	Electrocardiogram
EEG	Electroencephalogram
eHealth	Digital Health
EHR	Electronic Health Record
eIDAS	electronic IDentification Authentication and Signature
EU	European Union
FC	Fully-Connected
GDPR	General Data Protection Regulation
IBE	Identity-Based Encryption
ICT	Information and Communication Technologies
IoE	Internet of Everything
IoMT	Internet of Medical Things
IoST	Internet of Space Things
IoT	Internet of Things
IPFS	Interplanetary File System
KP-ABE	Key-Policy Attribute-Based Encryption
LEO	Low-Earth Orbit
MAC	Message Authentication Code
MEC	Multi-access Edge Computing
NLP	Natural Language Processing
NTNs	Non-Terrestrial Networks
PDTs	Personal Digital Twins
PKG	Private Key Generator
PKI	Public Key Infrastructure
PPDP	Privacy-Preserving Data Publishing
RNNs	Recurrent Neural Networks
RTA	Readiness to Adopt
SVMs	Support Vector Machines
UAVs	Unmanned Aerial Vehicles
UV	Ultraviolet
xAI	explainable AI

For example, in the healthcare field, the IoMT paradigm has made its way, which consists of the use of ''medical things'' to collect and transmit biomedical signals over a network for monitoring patients' diseases [21]. Literature provides several classifications based on different criteria concerning the IoMT systems. As one of the contributions of this work, we have collected in Table 4 some of the most noteworthy IoMT-related taxonomies in the literature. The authors of [21] rank the different sensors that can be used in eHealth environments according to the type of remote monitoring that must be carried out, distinguishing between the five categories shown in Table 4. Two different classifications can be drawn from [22], both related to IoMT but one about the sensors and the other about the general smart healthcare systems: the first distinguishes categories based on the positioning of the sensors inside or outside the patient's body; the latter characterizes systems based on their purpose and function. The macro-categories that can be identified thanks to these classifications are illustrated in Table 4. IoMT devices are classified according to where they are used in [23]; Table 4 portrays the detected macro-categories. Also, in [24], two distinct criteria are considered to classify IoMT sensors, both reported in Table 4: one based on the operating principle of the sensor, the other on the type of medical application in which it is employed. The collection of these taxonomies presented in the literature mainly aims to demonstrate the growing importance that IoMT devices are

TABLE 3. References and readiness to adopt (RTA) value for technologies/techniques analyzed in each data processing steps.

Data processing step	Technologies/techniques	Literature	RTA
Data Collection	IoE	[18]–[24]	MEDIUM
	D2D	[1], [25]–[29]	HIGH
	Digital Twin	[30]–[34]	LOW
	Robotics	[32], [35]	HIGH
	NTNs, Space communications, and IoST	[36]–[38]	LOW
Data Elaboration	Image-based diagnosis	[39]–[42]	HIGH
	Genome interpretation	[43]–[45]	HIGH
	Biomarker discovery	[46]–[50]	HIGH
	Patient monitoring and clinical care prediction	[51]–[54]	MEDIUM
	Health assessment using wearable devices and AI	[55]–[57]	MEDIUM
	Autonomous robotic surgery	[58]–[62]	LOW
Data Security	k-anonymity, l-diversity, and t-closeness	[63]–[67]	LOW
	ABE and IBE	[68]–[74]	MEDIUM
	Blockchain and IPFS	[75]–[90]	HIGH

assuming in the panorama of wireless network applications, given the numerous criteria that can be used to classify them.

2) DEVICE-TO-DEVICE (D2D)

D2D communications enable data transmissions among devices in mutual proximity, thus bringing gains mostly in terms of high data rate and low latency [25]. In the literature, D2D falls within the enabling technologies for smart healthcare applications [26]. In particular, the telemonitoring service could significantly benefit from the exploitation of D2D. For example, IoMT devices can be employed to remotely detect medical parameters and vital signs (e.g., temperature, pressure, oxygen, pulse oximetry, and electrical biosignals) on patients. Personal wireless devices (e.g., smartphones) may receive the gathered data through D2D links (i.e., sidelinks) and forward them to the doctor via the cellular network. A similar application of D2D is presented in [27], where it is considered a valuable solution to support reliable healthcare monitoring services; the authors list enhancements in data rate, latency, coverage, and system capacity among the advantages that D2D could offer to eHealth services. A strong point of [27] is that the major research challenges of D2D communication in wireless networks are highlighted, among which security stands out. Although the more general aspects of the "security for eHealth data" topic will be treated later, in this section, we want to emphasize the key challenge of the security issues deriving from the use of D2D communications in healthcare. Thus, in the following, some research proposals introducing solutions for the security of D2D-aided eHealth systems are briefly described. In [28], an escrow-free identity-based aggregate signcryption scheme is proposed to secure a D2D communication protocol in a cloud-centric IoMT-enabled smart healthcare system. In [91], a lightweight and robust security-aware D2D-assist data transmission protocol exploiting a generalized signcryption technique without a certificate has been designed for health systems. Recently, in [1], a novel eHealth system architecture, integrating D2D communications and Multi-access Edge Computing (MEC) and supporting security mechanisms, has been introduced for handling sensitive health data gathered by IoMT devices.

3) DIGITAL TWIN

The digital twin is *a virtual representation of elements and dynamics of a physical system* [30] that, if exploited in future 6G networks, could help meet the requirements of upcoming applications (including healthcare). It could be considered as closely related to the IoE since it requires the deployment of several sensors to create a replica of the physical object.

The potential for utilizing the digital twin in eHealth and wellness applications has increased since its concept has been extended to *the reproduction of living and non-living entities* [31]. It is generally agreed that the realization of the digital twin requires the support of various sensing algorithms, communications technologies, data analysis techniques, and security paradigms to make the virtual copy a faithful and updated replica of the physical entity. In this regard, the great success that the use of wearables has recently enjoyed makes the adoption of the digital twin easier and more user-friendly in the health and well-being contexts [31]. For example, personal digital twins (PDTs) are mentioned in [32] as valid applications in healthcare for developing virtual replicas of human organs. According to the authors, PDTs can offer numerous profits in this field, among which self-generation of alerts, better personal awareness, quicker feedback, and faster triage emerge. The role of the digital twin as a game-changer in the healthcare field is investigated in [33], which introduces a framework for the predictions of heart anomalies through the analysis of electrocardiogram models. Three phases characterize the data collection process for monitoring the medical conditions of patients and for the early detection of anomalies: (1) processing and prediction, (2) monitoring and correction, and (3) comparison. Given the sensitivity of the data collected, the digital-twin-related problems highlighted by the authors mainly concern trust, security, and privacy, since the devices used to create and update the virtual replica can be vulnerable to attacks by

TABLE 4. IoMT-related classifications in the literature.

Paper	Differentiation Criterion	Classification
[21]	Type of executed remote monitoring	• Remote monitoring system for heart-related diseases • Remote monitoring system for brain and neurological diseases • Remote monitoring system for diabetic patients • Remote monitoring of fall detection of elderly people • Ingestible sensors
[22]	Positioning of the sensors	• Wearable sensors • Implanted sensors • Embedded sensors
	Purpose and function of smart healthcare systems	• Health monitoring • Medical automation
[23]	Place of use of devices	• On-Body • In-Home • Community • In-Clinic • In-Hospital
[24]	Operating principle of sensors	• Physical sensors • Electrochemical sensors • Optical sensors • Magnetic sensors
	Medical application of sensors	• Monitoring • Targeted Drug delivery • Detection • Point of care diagnostic • Surgery • Treatment • Therapy • Medical Images • Sleep diagnosis and treatment • Obstetrics

malicious actors. Despite the great potential, in [92], besides the problems related to data security, the novelty of technology, time and cost, lack of standards and regulations, and life-cycle mismatching are outlined as challenges to the digital twin implementation. Another aspect that emerges from [92] concerns the numerous definitions that in the literature refer to the same concept of the ''digital twin'', among which the ''virtual object'' lacks.

In fact, a noteworthy observation we want to bring out matters the correlation between the digital twin and virtual object concepts, whose distinction seems a bit fuzzy. An in-depth analysis of the virtualization of objects in the IoT world is provided in [34], where the virtual object is defined as the *digital counterpart of any real entity in the IoT*. The same authors dwell on the definitions and characteristics of the virtual object, pointing out that there is confusion about the use of the term ''virtual'', given the disproportionate use that has been made of it since the 70s. They claim that the functionalities obtainable through virtualization can change according to the considered architecture, except for some common ones and for the goals of the virtual object, which must offer benefits to improve consumers' quality of life. We believe this makes the distinction between the virtual object and digital twin unclear and opens the way for further study on the topic.

4) ROBOTICS

The potential of applying robotics to the healthcare sector has emerged especially following the outbreak of COVID-19. The authors of [35] collect and describe some compelling robot applications developed during the height of the pandemic emergency to help ensure the health system's resilience. In detail, robotics can be leveraged in favor of: *(i)* diagnostics, both by facilitating the automation of some equipment and by interacting with patients to measure vital parameters; *(ii)* interventions, since robots can be used to perform surgery procedures instead-of or together-with doctors; *(iii)* rehabilitation, which has shown promising results for some years now and could enable telerehabilitation, allowing patients to receive therapy from home; *(iv)* assistance to patients and healthcare professionals, to improve the well-being of the former and reduce the workload on the latter. It is worth underlining that some of the systems mentioned above are not yet mature enough to be adopted. However, they

represent outstanding solutions that could be implemented thanks to technological progress and the evolution of mobile networks towards 6G. Also, in [32], the role of robotics in the healthcare sector, particularly during public health emergencies, is handled. In addition to the previous functionalities, the authors cite disease prevention, for example, through the robotic ultraviolet (UV) disinfection of surfaces performed during COVID-19, and the use of drones and Unmanned Aerial Vehicles (UAVs), to reach patients in remote areas.

5) NON-TERRESTRIAL NETWORKS (NTNs)

Thanks to the implementation of eHealth services, the in-person meeting between patient and doctor can be avoided in all cases in which the latter deems it appropriate. People living in areas away from hospitals or clinics can prevent long travels if the requirements are in place to provide them with access to all the medical care they need. Space communications and the Internet of Space Things (IoST) can ensure the ubiquity of eHealth services by offering their availability anywhere and anytime [36]. NTN is considered one of the key technologies of 6G wireless systems since global connectivity can be achieved owing to the satellite's large footprint (i.e., coverage area) and/or thanks to the implementation of constellations of Low-Earth Orbit (LEO) satellites [37], [38], which can also provide eHealth services with low latency due to their low altitude. To sum up, reaching places unserved or under-served by the terrestrial network is feasible through the exploitation of NTN systems, which represent an excellent wireless component to access 6G eHealth services by meeting ubiquity and low latency requirements.

6) RTA EVALUATION

A MEDIUM RTA value is assigned to the IoE in Table 3 because, although IoMT is already widely used (e.g., for remote monitoring of patient's health conditions), IoE can not be considered highly ready to be adopted since it represents something more complex and broad in comparison to IoMT. 5G was supposed to be the enabler of the IoE; however, its actual application is currently far. 6G will represent the means to overcome the challenges related to the activation of heterogeneous IoE services since it will be designed to fulfill the performance requirements of IoE applications. Considering that the IoE has already been cited in the literature as a revolutionary 5G technology but that it needs 6G (expected to be released approximately in 2030) to be enabled [19], we believe that its RTA value is MEDIUM. Once implemented, the IoE will highly impact eHealth services, fostering personalized care, and continuity of care for chronic patients, improving their quality of life.

D2D technology was introduced in Release 12 of the 3rd Generation Partnership Project (3GPP), but it could have a notable impact on the efficiency of communications between future medical devices. One of the main challenges of using D2D in eHealth concerns communications security. As already discussed, many works in the literature propose possible solutions that, if applied, could allow the success of D2D technology in eHealth services. This justifies the HIGH RTA value we have attributed to the D2D in Table 3.

NASA provided the first definition of the digital twin around the 1960s to indicate a kind of living model in the Apollo missions. Nonetheless, the idea of the digital twin began to seem successful in several fields only with the growing importance gained by the virtualization trend [93]. As highlighted in [92], the digital twin is an emerging paradigm that could bring significant benefits to the healthcare industry but whose evolution is blocked by the current absence of technologies sufficiently advanced to support it; this is why it was assigned a LOW RTA value in Table 3.

Although the use of robotics to support medicine is not yet feasible for some specific applications, due to the technology immaturity, a HIGH RTA value can be assigned to its general employment in eHealth since several services already implement it [35].

Finally, NTNs could bring numerous benefits to eHealth services, especially in terms of connectivity extension. However, their application in this field is far away and is expected to be achieved only when 6G technologies will be widely used. Therefore, the RTA level of NTNs in eHealth is assessed as LOW.

B. ARTIFICIAL INTELLIGENCE FOR eHealth DATA

AI improves healthcare professionals' ability to catch better the day-to-day patterns and needs of the people they care for to optimize available resources and provide a higher quality of service and care to stay healthy. According to the authors of [4], [94], AI tools have revolutionized diagnostic methods in the healthcare system. AI algorithms employ mathematical-computational techniques to learn information directly from data, without mathematical models and predetermined equations [95]. In eHealth, a typical advantage of these algorithms is their flexibility to learn complex patterns that are often impossible to model with standard mathematical approaches (e.g., in identifying biomarkers in time series such as electroencephalograms or magnetic resonance images). Despite AI algorithms having gained impressive progress and far outstripped traditional approaches, biological data elaboration still represents an open challenge.

In this section, we investigate how AI, in particular DL, can play a key role in eHealth to meet the rigorous requirements and future demands of services. We explore the knowledge-learning methodology to train models from data. Comparative investigations of these tools from qualitative and quantitative perspectives are also provided. Finally, open research challenges in using DL for biological data mining are outlined and some possible future perspectives are proposed.

1) LEARNING PARADIGMS

AI techniques can be generally divided based on how a system learns from the data, namely supervised, unsupervised, and reinforcement approaches. The three learning paradigms

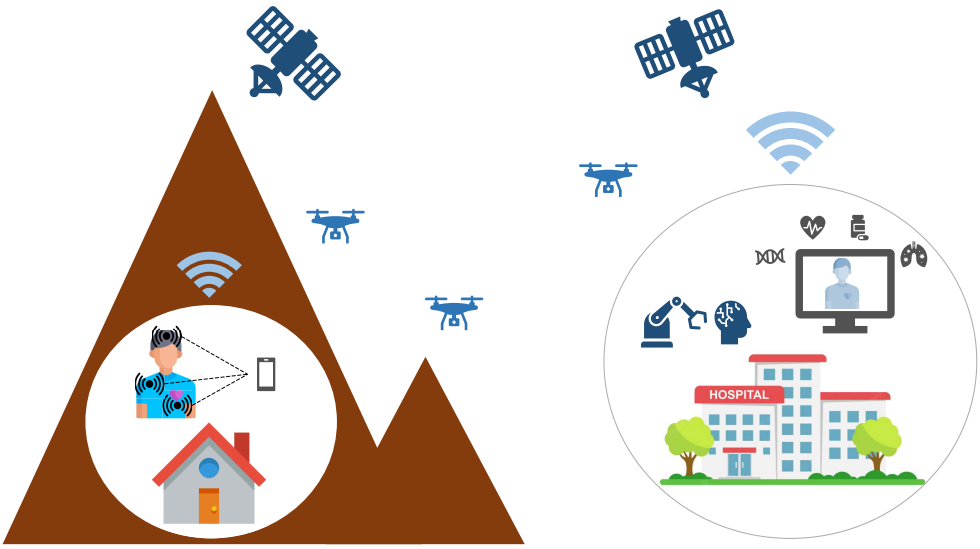


FIGURE 2. Use of the major 6G technologies in eHealth.

are the basis for training algorithms able to extract knowledge from data, exploitable for resilient eHealth solutions.

Supervised learning systems use pre-labeled data as a source of knowledge. The name recalls the idea of a 'supervisor' who instructs the learning system on the labels to be assigned to training instances [96]. Class labels are the possible classification outputs (i.e., diseases or specific associated conditions). Thanks to previous diagnoses made by doctors, it is possible to create well-structured datasets that are very useful for training new models. According to [4], this approach is the most widely used and will provide increasing help in eHealth. Many methods related to supervised learning have been proposed in recent years, including Artificial Neural Network [97], Convolutional Neural Networks [98], Recurrent Neural Network [99], Support Vector Machines [100], k-Nearest Neighbours [101], and Decision Trees [102].

Unsupervised learning is increasingly becoming a key paradigm for analyzing large amounts of biological data as it overcomes the complexity of annotating health datasets during or after collection, being laborious, time-consuming, and expensive [103]. It determines patterns among the entities in a dataset with unknown annotations or characteristics and applies the acquired knowledge to classify the leftover data [5]. In unsupervised learning, we only have input data without any expected output. The objective is to classify and organize a set of inputs that the computer system will reclassify based on common characteristics to make reasoning and predictions about the subsequent inputs. Therefore, unsupervised learning could be employed to overcome limitations and improve the efficiency of eHealth. The most popular unsupervised methods include: Autoencoders [104], Self-Organizing Maps [105], k-Means [106], and Density-based Clustering [107]. Several of these techniques have been employed to analyze data from numerous biological sources with great results.

Reinforcement learning systems can automatically discover interesting and useful patterns in data. It aims to find a solution to a problem by attempting and checking whether it produces the desired effect. If this occurs, the attempt constitutes a solution to the problem. Otherwise, a different attempt has to be done [108]. It is widely used in robotics; therefore, it could be used for telemedicine applications for remote surgery or home care assistance [109].

2) DEEP NETWORK ARCHITECTURES

Architectures that support biological data processing, including for potential eHealth applications, are now being investigated, especially those that can fully automate data-driven processes by learning directly from raw data.

According to [4], which offers an in-depth survey of the most important algorithms for different data, biological data can be classified into images, signals, and sequences; this classification can be graphically learned in Figure 3. Standard algorithms, such as support vector machines (SVMs), Linear classifiers, or random forests have achieved interesting results over the years; the authors of [110], [111], and [112] explore the literature on these algorithms. They can still be used, but we do not explore them in depth because they require manual extraction of characteristics, which is time-consuming and needs domain-specific know-how. As a result, we discuss the most widely used deep algorithms that solve the aforementioned problems.

- **Artificial neural networks (ANNs)** have a strong impact in the domain of eHealth. They consist of layers of nodes that include an input layer, one or more hidden layers, and an output layer. Hence, every node or artificial neuron links to another and has an associated weight and threshold. If the output of a node is higher than the specified threshold value, this node is activated, sending data to the next layer in the network. Otherwise, no data is transmitted to the next network layer [113]. There

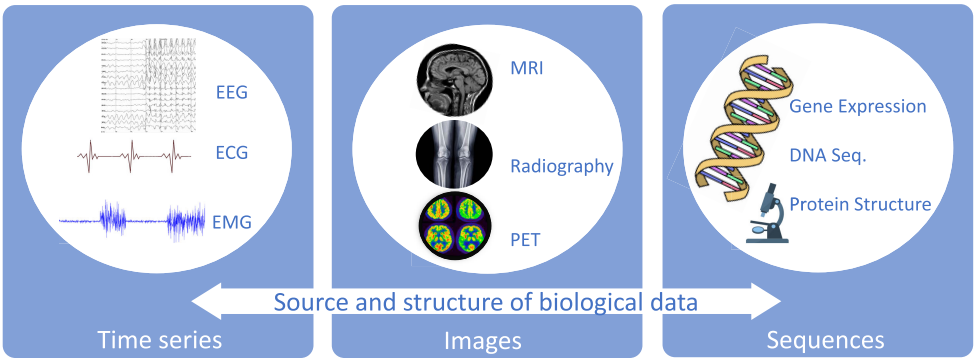


FIGURE 3. Different biological data categorized by structure.

are many clinical applications where ANNs are helpful, such as assisting physicians in medical image interpretation [39], [40], [41], [42], detection of Epilepsy [114], breast cancer [115], lung cancer [116], coronary artery disease [117], Alzheimer's disease [118], etc. The authors of [119] analyze how decisive ANNs have been in the exponential growth of data processing capabilities for present and future health applications. Several studies have been carried out in the literature with highly accurate results [120], [121], [122], [123]. Their remarkable flexibility in modeling complex problems gives more them advantages as compared to standard algorithms. The structures are directly based on studies of existing complex biological neural networks [124], [125], [126].

- **Convolutional neural networks (CNNs)** are the most widely used architectures with the greatest potential for automated Image-based diagnosis. The complexity of learnable patterns has increased significantly the fields of application providing excellent learning capabilities and enabling classification of challenging healthcare disorders, such as neurological disease [127], [128], [129], cardiac diseases [130], [131], [132], cancer [133], [134], [135], genetic diseases [136], [137], etc. Their architecture can be described as a series of feed-forward layers with convolutional filters that are intermixed with convolutional layers, pooling layers, and fully-connected layers. The first two levels provide an automated feature extraction. The third block is analogous to normal ANNs. The combination of these layers carries an unheard-of flexibility in the input. This is precisely why it is the most extensively used architecture for bio-signal analysis, as described above, of the huge variety in structure and complexity.
- **Recurrent neural networks (RNNs)** use training data to learn (supervised learning) and are distinguished by their 'memory' that take information from previous inputs to influence current input and output [138]. The output of RNNs depends on previous elements within the sequence, unlike feedforward neural networks (i.e., ANNs, CNNs) that assume input and output are independent of each other. RNNs can analyze time series data, as ordinal or temporal problems such as language translation, natural language processing (NLP), speech recognition, and image subtitling. They can be used in eHealth to analyze medical texts such as anamnesis, and they can be of great help, e.g., in scanning thousands of text documents and finding similarities to support a physician in diagnosing a disease. In general, RNNs can be used in clinical applications requiring time correlation, such as recognition of abnormalities in the electrocardiogram (ECG), electroencephalogram (EEG) monitoring, etc., [139], [140].

3) EXPLAINABILITY AI

AI, specifically DL, offers extraordinary opportunities in eHealth. However, its systematic application is hampered by the lack of trust in the decisions made due to the low interpretability of deep architectures, which represents a severe problem in the clinical field. The validation of models with explainable AI (xAI) tools helps quantify the generated output's resilience and improve security and confidence over black-box models. XAI helps users understand and trust machine learning models by describing how certain features used in the model contribute to its prediction. Furthermore, xAI can be used to validate extracted features, confirm heuristics, identify patient subgroups, and discover new biomarkers [141]. By identifying avenues for model performance improvement, xAI can support research conclusions and guide research advancement. For example, if a network model predicts a heart disease patient's health risk, a clinician would want to understand how strongly the patient's heart rate data influences that prediction [142]. To solve this problem, xAI has been developed to make models transparent. XAI describes the behavior of the neural network and the decision-making process. It involves two approaches:

- Globally, which aims at a general explanation of the behavior of the model. It identifies how data features collectively influence the result and provides an overview of the model.
- Locally, which identifies how features individually influence the result and independently evaluates each

instance and feature of the data (e.g., specific image pixels) [143].

Although this approach is very recent and has been a hot topic only in recent years, researchers have populated the literature to solve this decisive challenge that will transform the future of eHealth [144], [145], [146], [147].

4) RTA EVALUATION

Several AI technologies have been analyzed in detail so far, and their relevance in eHealth has been shown by citing the existing literature. In the following, an evaluation of the RTA of clinical applications exploiting some of these technologies is conducted to provide insight into the adoption rate of AI implementations in the medical field. The RTA values assigned to each application are summarized in Table 3. It is worth mentioning that some limitations to the implementation of the applications are not due to technological constraints but to regulatory limits or an incomplete integration of the technological platforms.

Automated Image-based diagnosis is the most successful and high-impact area of AI applications in the medical field [39], [40], [41], [42]. Indeed, image-based diagnoses are used in many medical specialties, including radiology, neurology, dermatology, and oncology; therefore, we believe that the RTA value of automated medical image diagnosis is HIGH. CNNs are the most successful architectures in automated Image-based diagnosis.

Genome interpretation allows scientists to understand how DNA changes between people and whether or not genetic variations play a role in the development of disease. According to [43], [44], and [45], high-performance algorithms, such as CNNs and RNNs, are decisive in analyzing high-throughput sequencing methods since they generate terabytes of complex raw data. In addition, this application enables accurate clinical interpretation of biological data, which is essential for recognizing the individual differences underlying precision medicine. We thus assigned a HIGH RTA value as it represents a mature technology already in use.

Biomarkers discovery is the building block of precision medicine. It is an emerging area of research and ANNs, CNNs, RNNs, according to [46], [47], [48], [49], and [50], are improving and expanding its diagnostic capabilities. Furthermore, clinicians can benefit from xAI by gaining insight into how the AI models reach solutions from clinical data. We assigned HIGH RTA value in Table 3 because the innovative AI tools of bio-informatics allow the interpretation of large amounts of data, moving the global scientific trend from assumption to data-driven approaches. This adds significant value in different medical fields, gaining insights into molecular pathological mechanisms of disease, identifying new drug targets, or designing emerging economic assays to improve diagnosis, prognosis, or response prediction, readily available for clinical application.

Patient monitoring and clinical care prediction are allowed by the exploitation of electronic health records that provide large amounts of data to predict the most efficient treatments (such as the classification of cancer patients with different responses to chemotherapy [148]) and post-operative prognosis [149] or mortality [150]. RNNs can provide much help to monitor the treatment or progress of medical history because they take information from previous inputs to influence current input and output. RNNs can detect clinically relevant predictors with good accuracy and lead physicians in finding an optimized treatment strategy [51], [52], [53], [54]. After an analysis of the existing adoption rate we have assigned a MEDIUM RTA value in Table 3.

Health assessment using wearable devices and AI algorithms has been the subject of numerous studies [55], [56], [57]. The accessibility of smartphones and wearable sensor technology is causing a rapid accumulation of human subject data. Machine learning and DL, in particular with CNNs, are emerging as techniques to map those data into medical predictions. Clinical decision-making may be directly impacted by such applications that could boost patient care quality while lowering costs. Although wearable devices record a plethora of biomedical signals, including heart rate, voice, tremor, limb movement, and saturation, in an extended recording time, they still lack medical certification or accurate performance. Despite wide margins for development we have assigned a MEDIUM RTA value in Table 3 for the above-mentioned reasons.

Autonomous robotic surgery promises improved safety, efficacy, and access to surgical procedures. Reinforcement learning in this field covers a key role as as an up-and-coming approach for simulating an autonomous agent. The ability to mimic human learning behaviors to maximize the long-term reward enables a robot to learn on its own and partially replicate the work of experts. The trial-and-error learning approach can use complex input data, such as text, image, and temporal data, in the decision-making process and recommends specific actions at predetermined intervals. Due to technological limitations, such as a lack of intelligent algorithms and vision systems that can recognize and track the target tissues in dynamic surgical environments to carry out complex surgical tasks, surgeries have not been completely performed autonomously [58], [59], [60], [61], [62]. Thanks to future developments in AI, robots could one day run the operating room, with surgeons supervising their movements but, to date, the development and adoption of autonomous robots in medical interventions have been remarkably slow. Therefore, a LOW RTA value has been assigned in Table 3.

C. PROPERTIES, TECHNIQUES, AND APPROACHES FOR DATA SECURITY

The quantity and variety of patients' health and wellness data reflect how, where, why, and by whom they are collected [151], [152]. The healthcare data domain involves diversified information related to the patient's life and their links with healthcare facilities and entities. The authors of [153] show how several kinds of data, such as demographic, clinical, wellness, and administrative attributes,

concur to create every patient's medical profile and the corresponding electronic health record (EHR). The collection, storage, processing, and sharing of EHRs are key performance indicators for developing and maintaining an efficient healthcare system. However, the attributes of the EHRs may reveal extremely sensitive information; this is the reason why dedicated security measures must be applied for the protection of data and users [154]. Furthermore, the GDPR [155] plays a crucial role in healthcare environments, indicating six principles that must be guaranteed on the data: *i*) lawfulness, fairness, and transparency; *ii*) purpose limitation; *iii*) data minimization; *iv*) accuracy; *v*) storage limitations; *vi*) integrity and confidentiality.

In this section, we focus on the security properties and measures investigated to protect data in the healthcare domain.

1) SECURITY PROPERTIES

In the following, the main security properties are presented as the starting point in individuating, developing, and maintaining a secure eHealth solution. These properties are shown in Figure 4.

FIGURE 4. Security properties in eHealth.

- **Anonymity.** The concept of anonymity is not absolute but depends on the domain. A well-consolidated definition, coming from the field of anonymous communications is provided in [156], which claims that *anonymity for a subject is the state of being not identifiable within a set of subjects*. In the healthcare domain, we particularly refer to the anonymity of users' data. In this context, a typical example is provided by the concept of k-anonymity [157]. Suppose we assume that we have a dataset containing clinical data on users. In that case, we can say that this dataset satisfies the k-anonymity property if the information associated with a user can not be distinguished from the information associated with other $k-1$ users.
- **Accountability.** This property refers to the possibility of identifying and attributing responsibility to an entity for a given action. For example, when a doctor draws up a medical report on a patient, this action should be notarized so that anyone can verify who the report's author is (even without knowing its content). An effective way to achieve accountability is the blockchain technology [158], [159].
- **Authentication.** Authentication proves that a given user owns the digital identity they claim. For example, before accessing medical reports, interested users must perform an authentication procedure proving their identities. This can be done using a well-consolidated framework such as electronic IDentification Authentication and Signature (eIDAS) [160].
- **Confidentiality.** It concerns that data must not be disclosed to not-authorized parties. Again, it is very important that a medical report containing sensitive data about a user can not be accessible by other users. Effective ways to achieve confidentiality are encryption [161], access control mechanisms [162], or a combination of both [163].
- **Integrity.** This property means that unauthorized parties must not alter the data. Indeed, if a user manages to alter another user's medical report, even if confidentiality is preserved, this can dramatically impact the victim. Like confidentiality, integrity can be achieved through encryption. However, more lightweight approaches exist, such as Message Authentication Code (MAC) [164]. The concept of Integrity is strictly related to that of **Immutability**, which is a stronger property. By guaranteeing integrity, we mean that even though the data can be altered, there is a public way to check this alteration. On the other hand, immutability requires just the impossibility to alter the data. This can be obtained, for example, by storing them on the blockchain.
- **Non Repudiation.** It is related to the accountability property and refers to the fact that an entity can not deny having performed a certain action. For example, when a doctor writes a medical report, everyone can verify this (accountability), but at the same time, the doctor can not repudiate the report. Again, blockchain represents the most effective way to achieve this property.
- **Revocability.** This property consists of the possibility to revoke some privileges or capabilities to some entities. For example, access to the clinical data of patients must be revoked for a doctor who is fired from a hospital upon dismissal. Achieving revocability can be a hard task that depends on the privilege to invalidate. Some specific solutions have been proposed in the literature when dealing with advanced access control methods [165].

2) SECURITY TECHNIQUES

The aforementioned properties should be guaranteed in any solution offering eHealth services to citizens and doctors.

However, in practice, it is challenging to offer *all* of them simultaneously.

Therefore, according to the specific eHealth service to provide and the needs of the involved actors, only a subset of the above properties usually is guaranteed. For example, a trade-off can exist between anonymity and accountability [166].

When dealing with EHR, achieving at least confidentiality is a necessary condition. Several solutions in the literature pursue this goal [12]. In the following, we briefly discuss the evolution of cryptographic approaches to obtain confidentiality by highlighting their limitations that lead to the introduction of new solutions.

Traditional approaches to ensure confidentiality are based on symmetric encryption or public-key encryption [167].

The main problem of the symmetric encryption schemes is that a key has to be preliminary exchanged between the two communicating actors. This makes these schemes impractical in eHealth environments, considering that a doctor can have many patients and should exchange a key with everyone; furthermore, other keys should be used to communicate between doctors.

Public-key encryption can solve this problem. Indeed, each actor owns a public and a private key, and anyone can encrypt the data by relying on the public key; only those who own the associated private key can decrypt the message. However, also public-key encryption is not conclusive. The public key is a sequence of bytes not associated with the identity of a user. If we assume that a patient wants to share their EHR with a particular doctor (whose identity is known), how can the patient be sure that a given public key belongs to the intended doctor?

Identity-based encryption (IBE) [168] can help in this situation since, in IBE, the public key is represented by some unique information associated with the user's identity (e.g., the e-mail address). This way, the patient can encrypt a message without requiring the public key to any external party, such as a Public Key Infrastructure (PKI) [169]. A price to pay for these benefits is represented by introducing a third-trusted party, called Private Key Generator (PKG), which manages and distributes to the users the private keys associated with the identities. Even though is possible to reduce the trust in the PKG by splitting its competence among multiple PKGs [170], the complete removal of the PKG is an open problem. More advanced IBE schemes allow obtaining confidentiality and anonymity by hiding the identity of the recipient [171], [172]. The advantages of the introduction of IBE in the healthcare domain are witnessed by several proposals in the literature [71], [72], [73], [74].

An IBE extension that can guarantee confidentiality and access control is based on attribute-based encryption (ABE), introduced for the first time in [173]. In ABE, the ciphertext and the key are associated with some attributes and a policy. If the attributes satisfy the policy, the decryption of the ciphertext is allowed.

In particular, in the Key-Policy attribute-based encryption (KP-ABE) [174], the policy is associated with the key, and the attributes are associated with the ciphertext. A user owning a given key can decrypt only those ciphertexts whose attributes match the policy associated with their key.

In Cipher-Policy attribute-based encryption (CP-ABE) [175], [176], the policy is associated with the ciphertext, and the attributes are associated with the key. In this case, which is also the most applied in the healthcare sector, a user has to own the right attributes to decrypt the ciphertext. IBE can be viewed as a particular case of ABE by treating the identity as an attribute.

CP-ABE can introduce several benefits in eHealth applications. Indeed, patients can encrypt their EHRs with a particular policy so that only authorized doctors can access them. For example, data about mental illness can be encrypted under a policy requiring that only Psychiatrists or Psychologists of a given hospital can decrypt them. Another benefit is that the patient does not need to know in advance the specific Psychiatrists and Psychologists (and then their public keys) who have access to the data. Similarly to IBE, a drawback of ABE is represented by the introduction of a PKG that manages and distributes to the users the private keys associated with the attributes or policies. In practical terms, the PKG releases the keys through the collaboration of some attribute providers certifying the ownership of the involved attributes.

An enhancement of CP-ABE is represented by Cipher-Policy attribute-based proxy re-encryption (CP-ABPRE) [177], [178]. In CP-ABPRE, an honest-but-curious proxy is introduced to reduce the computational workload on a user who wants to change the policy associated with a ciphertext. In particular, the proxy receives a re-encryption key from the user to replace the policy associated with a ciphertext with a new one. The advantage of this approach is that the proxy performs this transformation of the ciphertext without learning anything about the plaintext. To understand the benefits of CP-ABPRE in eHealth, we refer to the example reported in [68]. Suppose a user encrypts an EHR under a given policy P_1, satisfied by some doctors of a clinic C_1. Furthermore, suppose that the clinic C_1 needs the collaboration of other clinics with additional competencies to make a diagnosis. To do this, C_1 would decrypt the EHR and re-encrypt it with a new policy P_2, requiring further attributes. If several EHRs have to be translated from the policy P_1 to P_2, the computational effort required to C_1 may be high (many decryptions and encryptions). Then, it can take advantage of CP-ABPRE, delegating a proxy on the cloud, with high computational power, to re-encrypt all the ciphertexts encrypted under P_1 into new ciphertexts encrypted under P_2. This can be done by providing the proxy with a single re-encryption key from P_1 to P_2. It is worth underlining that the proxy can not access the content of the medical records. As a final remark about ABE, we want to observe that, in the eHealth setting, a revocation mechanism should be implemented in case of users lose ownership of some attributes. It is not a trivial task but ad-hoc solutions are available in the literature [69], [70].

As previously stated, the presented encryption techniques (e.g., IBE and ABE) are well-known for protecting EHRs in

the medical cloud or servers at a data storage phase. In addition, during the data processing phase, privacy-preserving data publishing (PPDP) approaches are highly required to conceal or obfuscate any sensitive data on the patients to limit their re-identification [63]. Each EHR typically is made of a number of distinct attributes classified as: *i*) *explicit identifier*, namely a set of attributes that uniquely identifies a patient (e.g., national ID, name and surname, mobile number); *ii*) *quasi-identifier*, which potentially can identify the patient with some additional information (e.g., gender, address, date of birth); *iii*) *sensitive attribute*, consisting of personal information that can reveal a particular state *iv*) *non-sensitive attribute*, which can not violate patient privacy if disclosed and that are not categorized in the previous groups [64].

In the literature, some privacy protection models have been proposed to handle the challenge of guaranteeing a certain level of anonymity. The technique called k-anonymity aims to make the tuple distinguishable from one another by assuring that each value in a given dataset is indistinct from a minimum of $k - 1$ records [179]. However, due to its simplicity, k-anonymity is vulnerable to several attacks such as Homogeneity attacks and Background knowledge-based attacks [63]. A different approach to reaching anonymity is l-diversity, which is an extension to k-anonymity given that it is based on the concept that attributes belonging to each relevant group, called equivalence classes, must be well-represented. Instead, the t-closeness introduces the concept of a threshold. Indeed, it is obtained when the sensitive attribute distance in an equivalence class is not greater than this threshold. These techniques have also been investigated in the healthcare sector to assure the privacy of patients' data by providing a suitable patient anonymity level. The authors of [65] analyze some security frameworks able to face the existing challenges of the healthcare industry. In [66] and [67], a clustering-based anonymization approach has been proposed for cloud healthcare users, while in [180], an anonymity-based solution is developed to generate anonymous tuples for both the client and server side.

3) EXISTING APPROACHES

The protection of EHRs is quite tricky since it needs a balance between privacy and utility: data need to be used and analyzed by several entities, but, at the same time, sensitive information must be kept away from unauthorized actors [181]. We have analyzed the most popular cryptography techniques in an eHealth scenario. Besides, some higher-level deployment approaches have been explored in the literature to manage and organize EHRs.

In [181], authors explore the cloud deployment models and divide the approaches into three categories: *i*) public cloud model, where the infrastructure is accessible to public users and participating entities (e.g., hospitals, pharmacies, laboratories); *ii*) private cloud model, an infrastructure administered by one healthcare organization; *iii*) hybrid cloud model, which is a unification of the previous models since the health organization exploits outsourced resources but controls the data. Each of these models needs to achieve privacy and secure the confidentiality of EHRs data.

Recently, the potentiality of blockchain technology has been harnessed to meet the urgent and strict security requirements in the eHealth environment. Thanks to its immutability, transparency, data integrity, and decentralized nature, blockchain technology can represent an effective approach to managing EHRs [75], [76], [77], [78], [79]. For example, in [80], the authors propose a blockchain-based system in which only authenticated participants can outsource data on the cloud. This way, their integrity is guaranteed also when the medical institution and the cloud collude. Here, Ethereum [81] has been selected as a public blockchain.

Other solutions that rely on consortium and/or private blockchain are available in the literature, like [82], [83], and [84]. Among these, [84] is a very recent proposal designed to exchange health information between different providers. It offers secure storage, rapid access and update of medical records. The system was implemented on Hyperledger Fabric [85].

When dealing with blockchain technology, the interplanetary file system (IPFS) [182] represents a reference solution to store data in a decentralized way. IPFS is a distributed file system in which data are stored and retrieved by content (instead of by location). Currently, a lot of healthcare solutions adopt blockchain in combination with IPFS [86], [87], [88], [89], [90]. Even though several differences (in scope and implementations) exist between these solutions, a common element is the reduction of the cost of storing data. Indeed, in traditional approaches, medical data are stored directly on the blockchain in an immutable way. Often, this results in prohibitive costs. On the other hand, IPFS does not introduce costs to store data and allows the owner to "unpin" them so that a garbage collector can remove them from the network. However, no guarantee is provided about removing data, for example, if a node previously hosting a file decides to re-host it. Currently, data removal from IPFS is an open issue. Then, data should be encrypted before being stored on IPFS.

4) RTA EVALUATION

To evaluate the applicability of the security approaches above mentioned, we group them into three categories as reported in Table 3. Before entering into the details, we want to highlight that the limitation of the adoption of these solutions is not necessarily due to technological lack. Indeed, often, security solutions may require an effort to be used that a user or operator is not available to spend. Therefore, to speed up their adoption, these solutions should be developed as transparently as possible for the users.

Concerning blockchain-based approaches, we classify their RTA as HIGH since this represents a mature technology already employed in real-life scenarios. For example, the Guardtime KSI Blockchain [183] adopted in Estonia stores the eHealth records of patients by guaranteeing integrity and privacy. Another interesting project with similar objectives is Medicalchain [184].

Concerning ABE/IBE-based solutions, we rate their RTA as MEDIUM. Indeed, even though their practical adoption in eHealth scenarios is limited (apart from research demonstrators [185]), a lot of cryptographic schemes are already available and ready to be adopted in real-life contexts. This is also witnessed by some ETSI standards (TS 103 458 and TS 103 532). Probably, a small gap to overcome is the presence of a fully trusted party, i.e., the PKG, that potentially may access data by colluding with other entities. The benefits introduced by these approaches have already been discussed in the previous section and concern mainly confidentiality and access control.

Finally, as regards the implementation of privacy-preserving methods in the healthcare domain, several challenges and pressing question marks are still unsolved, which made our choice of a LOW RTA. First, researchers and industries strive to find the proper trade-off between utility and privacy in their necessarily GDPR-compliant solutions [186]. The prominent drawback relates to the difficulty of applying these models to medical datasets [187]. Then, again, a downside and a possible research challenge is the absence of a clear standardization of policy compliance plan where the privacy models and protection level are indicated for the healthcare dataset [64].

To conclude, we would like to point out that even if the introduction of these security solutions does not have a direct impact in terms of data usability, it might have an indirect impact. Indeed, the ability to manage data in a privacy-preserving way may incentivize users to increase the amount of data shared (which can be used, for example, to develop AI algorithms).

III. INNOVATIVE ELECTROMAGNETIC SYSTEMS FOR HEALTHCARE AND ASSISTED LIVING SERVICES

The data processing paradigm illustrated in Section II can be applied to different eHealth scenarios and, therefore, to different data types. An example is described in this section, which concerns the application of the data collection/elaboration/security paradigm to monitor indoor patient status. One of the key points in chronic and old-age diseases is remote and safe monitoring of patient status and physiological parameters (e.g., temperature, heartbeat, and breath), without affecting their everyday life. In this respect, localization and tracking are of high interest, and several innovative electromagnetic systems and techniques have been proposed in literature [188], [189], [190].

Among the very many available *localization techniques*, active systems imply that the targets are equipped with a transmitting/receiving tag, and they actively contribute to the localization process [191]. However, active systems have some drawbacks related to cost issues. For this reason, passive systems have also been proposed, wherein the targets are device-free, and the localization techniques exploit their interaction with the transmitted signal. Several passive systems and approaches have been recently proposed, exploiting electromagnetic waves from optical frequencies to radiofrequency and sound waves [192]. Among them, radiofrequency detection techniques are usually based on the analysis of features such as the time of arrival, the direction of arrival, and the received signal's strength or the channel state information [193]. On the other hand, new non-cooperative device-free techniques for target tracking and localization in the radiofrequency regime exist, which take advantage of the peculiar feature of the electromagnetic waves to penetrate non-metallic objects and exploit inverse scattering approaches [194]. For instance, the main idea of [195] is to image the investigated area by measuring the scattered field generated by the interaction of the electromagnetic waves with the targets and by retrieving the electromagnetic properties by solving an inverse scattering problem [196].

As far as patient cardio-respiratory activities are concerned, the continuous *monitoring* of breathing and inhalation volumes is essential for diagnosing many respiratory systems, both during hospital confinement and in-home care. Microwave systems demonstrated their potentialities for non-invasive monitoring of vital signs such as heartbeat and breathing. In particular, these systems are usually based on continuous-wave doppler radar and can correctly identify the heartbeat and breathing rate with a reasonable degree of accuracy [197], [198], [199], [200]. For instance, in [201] a simple microwave interferometer capable of measuring displacements of wavelength fractions has also been proposed with an accuracy measurement of chest wall displacement less than $2mm$. On the other hand, ultra-wide band radars have also been proposed to quickly detect small movements of the chest wall while breathing [202], [203], [204], [205]. They are based on detecting ultra-wide band pulses reflected by the human body in the time domain. First, the radar transmits short impulses and are reflected by the human body. Then, amplitude variations as well as the time of arrival of the reflected pulse are used to evaluate the thorax and heart movements. These systems radars have some advantages with respect to continuous-wave radars, such as ability to work with low signal-to-noise ratio thus offering high performances in noisy environments, low transmission power, high performance in multipath channels, and simple transceiver architectures enabling low production costs [206].

IV. AN IN-DEPTH ANALYSIS ON THE REGULATIONS

Starting with the communication COM (2008) 689 of 4 November 2008 ''Telemedicine for the benefit of patients, health systems and society'' [207], European Commission has encouraged the Member States to increase their efforts in the field of eHealth, highlighting how telemedicine can be able to significantly improve healthcare efficiency as well as the quality of patient care. Definitely, the pandemic caused by COVID-19 has shown the potential of digital health, for the development of which a unitary regulatory framework is required, capable of harmonizing digital applications, in order to ensure the interoperability of the systems. Above all, the unitary regulatory framework must ensure a robust and

safe infrastructure to preserve the assets of patients' health data [208].

A. DATA SECURITY IN THE HEALTH SECTOR: CONSIDERATIONS ON ART. 9 GDPR

Pursuant art. 4 GDPR [209], the ''relative data health'' are personal data related to a natural person's physical or mental health, including the provision of healthcare services that reveal information regarding their state of health. The following art. 9 GDPR includes these data among the particular categories of personal data whose processing is prohibited, according to any limitations that the Member States may even implement [210].

Legislative Decree 10 August 2018, n. 101, issued for the adaptation of Italian legislation to the provisions of the GDPR, has inserted in the legislative decree 30 June 2003 n. 196 (Privacy Code), the art. 2-septies, titled ''Guarantee measures for the processing of genetic, biometric and related to health''. According to co. 1 and 2 of this article, health-related data can be subject to treatment in accordance with the guarantee measures arranged by the Guarantor for the protection of personal data, to be adopted taking into account not only the indications provided by the European Data Protection Board and Best Practice on the processing of personal data but also those pertaining to the scientific development and technology in the sector covered by the measures.

Pursuant the guarantee measures of paragraph 4 of art. 9 GDPR, they concern the precautions to be taken with respect to organizational and management profiles in the health sector and the communication methods directed to the person receiving the medical diagnosis. Pursuant the following paragraph 5 of art. 9 GDPR, it identifies the security measures, also from the technical point of view, the *minimization measures*, and the specific methods for the selective access to the data. There is a strong correlation between training safety and security of the conservation and circulation of health data [211]. Art. 9, par. 2, GDPR lists the cases in which the prohibition of treatment of health data does not apply, including that in which the interested party has given explicit consent to the processing pursuant lett. a) of the same article.

B. SECURITY IN THE FORMATION OF HEALTH DATA: AN ANALYSIS OF ART. 22 GDPR

The importance of informed consent in the health context is connected to the issues arising from the rules contained in art. 22 GDPR. Pursuant this article, the interested party has the right not to be subjected to a decision solely based on the automated processing, including profiling, that produces legal effects concerning them or that significantly affects them in a similar way on their person.

An exception to this rule consists in the fact that the decision ''is based on the explicit consent of the interested party'' (paragraph 2, letter a)). In this case ''the owner of the processing implements appropriate measures to protect freedoms and legitimate rights of the interested party, at least the right to obtain human intervention by the data controller, to express their opinion and to contest the outcome''. Therefore, deciding to produce legal effects based on such treatment is crucial. Moreover, this places the discipline in a more advanced security perspective [212]. These regulations concern a problematic issue that currently animates the debate among administrative law scholars, and that refers to the limits where it is possible to delegate the decision-making, in particular of nature, to a procedural or administrative algorithm. In this regard, there is a path traced by some recent rulings by the administrative judge of the first and second instance. However, not all Member States of the European Union (EU) have yet absorbed this path; for example, the Italian Digital Administration Code, despite its repeated changes and the spread of the phenomenon, has not yet done so. The Italian administrative jurisprudence [213] has highlighted the indispensability of the search for the technical rule that governs each algorithm, with a motivation focused on EU law and art. 22 GDPR. Since it is always possible to find a sort of Anthropomorphic principle, administrative discretion can not be delegated to the software, manifesting its persistent relevance when the technical rule is concretely elaborated and applied. There is no radical incompatibility between computerization and administrative discretion, since new technologies determine the redefinition and reallocation of discretion, not its disappearance. The decision entrusted to technology is a human decision: its innovation and creativity depend on human's ability to understand.

An analysis follows in which this concept is examined in detail by taking as a concrete example the application of AI to support the diagnosis. The starting question is: what is the concrete possibility of guaranteeing the transparency of the operation of AI systems? For example, it could be ensured by introducing suitable certification and control procedures with respect to their reliability. It is worth highlighting that AI is never mentioned in the GDPR, though many of the data processed by the AI-connected decision-making mechanisms are classifiable as personal and, therefore, attributable to the protection of the European regulations. Furthermore, as part of the European strategy for AI, the EU published on 21 April 2021, the proposal for a Regulation on the European approach, which resulted in the first European legal framework on AI. This proposal, in addition to prohibiting possible uses of some AI systems, such as those using subliminal techniques or exploiting an age-related vulnerability or a specific disability to distort a person's behaviour, provides for a specific regulation on ''high'' risk for AI systems used as security components of products are subject to evaluation by compliance according to European regulation, such as medical devices. The introduced rules include, in particular, the obligation to create and keep active a risk management system, the obligation to ensure that the AI systems can be supervised on the part of natural persons, the obligation to ensure the reliability, accuracy and safety of the same and specific transparency obligations towards users on the functioning of AI systems [214]. The progressive pervasiveness of algorithms is of great interest in the healthcare context.

In fact, it is connected to the increasing reduction of the role of the human in making decisions with significant consequences for the patient's health. In terms of data security [215], this question pertains not only to the circulation and conservation of health data but to its formation. It is about generating the formation of a relevant and safe decision for the patient's health. In the analysis focused on art. 22 GDPR, it is essential to clarify the meaning of the sentence ''decision solely based on processing automated'', since the term ''solely'' acts as a distinction between decisions eligible and not. The reasoning carried out in the light of the aforementioned administrative jurisprudence has led to assume that the human component can not be replaced by one presumed objectivity of the algorithms. Therefore, there is a reaffirmation of the centrality of the role that the human dimension retains even in the era of smart technologies. However, the majority doctrine assumes that in the case considered by art. 22 GDPR, there must be human intervention to review the results generated by the automated process. Therefore, the art. 22 GDPR could be interpreted in the sense of configuring the right for patients to be recipients of decisions also obtained thanks to the participation of the human component. There will be a difference between the visit carried out by a doctor opposed to confirming a decision made by an algorithm, compared to that performed by a doctor prepared to select the most suitable option to support the choices of the machine due to the lack of availability of information inherent to the huge amount of data that constituted the prerequisite for the decision of the machine. The authoritative doctrine has found that ''the automatic system tends, over time, to capture the decision itself'' [212]. This generates two consequences: first of all, the demonstration that an injurious decision is based only on an automated process represents a ''Probatio diabolica''; in addition, the excessive reliance that the doctor places on the results produced by intelligent machines leads to the so-called phenomenon of ''Professional deskilling'', i.e., the progressive reduction of the skills of health professionals, who can become so unfamiliar with analytics evaluation to be no longer able to detect errors more or less serious. Finally, the presence of explicit consent by the interested party introduces an exception to the rule established in art. 22, par. 1, GDPR. The key point consists in identifying the characteristics that the human intervention must have in terms of technical preparation, given that the data controller has to guarantee human intervention anyway. This will be even more relevant in the transition towards cutting-edge technologies, whose complex logic requires a technical evaluation, which is by its nature questionable.

V. OPEN ISSUES AND FUTURE RESEARCH DIRECTIONS

The outbreak of the COVID-19 pandemic has given rise to new needs related to the digitalization of various sectors globally. Although digital medicine seems a fairly widespread reality, several shortcomings have emerged in recent years, and the total absence of services remotely provided has weighed heavily on some countries, bringing attention to the Digital Divide issue. As our work shows, the challenges associated with the implementation of eHealth services are many and depend on plenty of factors.

Concerning the telecommunications sector, the technologies are not sufficiently mature for the fulfillment of the requirements of many eHealth services, in particular those relating to latency, connectivity availability, and transmission management of huge amounts of data. 6G is expected as the solution to the problem as it could guarantee the fulfillment of the most stringent requirements of eHealth services, also by leveraging the technologies mentioned in Section II-A. To provide some examples, in the next generation of eHealth, wearable devices are expected as useful means in the remote care of patients. The digital twin can help improve medical care, organizational systems, precision medicine, and advanced modeling of the human body. By exploiting NTNs, connectivity can be guaranteed even in the most remote and disadvantaged areas. Surgical and diagnostic robots can be used to support the human interventions of specialized doctors. These are just a few examples of what telecommunications can do to improve the way medicine will be used not only to ensure the survival of patients but also to improve their quality of life.

In the AI field, developments in algorithm processing capabilities can not keep pace with the evolution of eHealth services. Cloud systems generally lack sufficient processing capabilities for efficient data management, and the methods of storing significant amounts of health data often do not allow their adequate analysis by automated algorithms. In the next generation of eHealth, AI algorithms will provide advanced diagnoses in real time. The training of complex neural networks will be granted via cloud systems capable of handling large amounts of data and xAI techniques to ensure the reliability of results, both through the improvement of the models and the verification of the output.

Regarding security and privacy aspects, even though several technologies are already ready to be used, their adoption is struggling to take hold. This can be explained by two reasons. First, security and privacy risks are misperceived (and underestimated) by the users and eHealth operators. Second, often security comes at a price in terms of usability and/or efficiency. Therefore, two main challenges that we can identify are: (1) increasing the awareness about security risks through the education of users and eHealth operators and (2) developing new security solutions as much transparent as possible.

VI. CONCLUSION

In the next decade, innovative information and communication technologies will benefit various fields, such as the healthcare sector. In particular, eHealth could revolutionize the conventional methods to offer medical services to patients owing to the remote monitoring of diseases and provision of medical assistance, thus guaranteeing continuity and availability of care in every situation, including emergency times. This paper has investigated the literature related to different

approaches aimed at collecting, transmitting, elaborating, and protecting health data, being these operations functional to the innovation process towards eHealth. In particular, we survey the research proposals on the following aspects: the 6G technologies that can be leveraged to gather and transmit health data; the AI algorithms and applications useful for the elaboration of biological data; the approaches and techniques for the assurance of the security properties of such sensitive medical data; the application of innovative electromagnetic systems for healthcare and assisted living services; the European Commission's regulations for secure data treatment. The RTA metric for estimating the readiness to be adopted of the technologies and techniques analyzed in this survey has been introduced to highlight their application utility in eHealth. The multidisciplinary facet that characterizes this work has been developed thanks to the collaborations activated within the iCare project, which aims to the empowerment of research infrastructures and the improvement of health services management. By writing this paper, we want to convey that the success of telemedicine and the diffusion of eHealth paradigms could be achieved if heterogeneous-by-competence working groups collaborate to define the hallmarks of the future technologies and approaches. Most currently usable paradigms can not adequately support the digital transformation of healthcare. Furthermore, the knowledge of the current regulations can not be neglected since the diffusion and use of technologies in the daily life of citizens inevitably depend on it. This should also make the legislators think, as their decisions can promote or, on the contrary, thwart the digitalization of the health sector.

REFERENCES

[1] C. Suraci, S. Pizzi, A. Molinaro, and G. Araniti, "MEC and D2D as enabling technologies for a secure and lightweight 6G eHealth system," *IEEE Internet Things J.*, vol. 9, no. 13, pp. 11524–11532, Jul. 2022.

[2] C. D. Alwis, A. Kalla, Q. V. Pham, P. Kumar, K. Dev, W. J. Hwang, and M. Liyanage, "Survey on 6G frontiers: Trends, applications, requirements, technologies and future research," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 836–886, 2021.

[3] E. Esenogho, K. Djouani, and A. M. Kurien, "Integrating artificial intelligence Internet of Things and 5G for next-generation smartgrid: A survey of trends challenges and prospect," *IEEE Access*, vol. 10, pp. 4794–4831, 2022.

[4] M. Mahmud, M. S. Kaiser, and A. Hussain, "Deep learning in mining biological data," *Cogn. Comput.*, vol. 13, no. 1, pp. 1–33, Jan. 2021.

[5] Y. Li and L. Chen, "Big biological data: Challenges and opportunities," *Genomics, proteomics Bioinf.*, vol. 12, no. 5, p. 187, 2014.

[6] S. Zeadally, J. T. Isaac, and Z. Baig, "Security attacks and solutions in electronic health (E-health) systems," *J. Med. Syst.*, vol. 40, no. 12, pp. 1–12, Dec. 2016.

[7] H. L. Brian Horowitz. *Hackers Reportedly Breach Hospital Surveillance Cameras, Exposing the Security Risks of Connected Devices*. Accessed: Jun. 2022. [Online]. Available: https://www.fiercehealthcare.com/tech/hackers-breach-hospital-surveillance-cameras-exposing-risks-device-security

[8] H. Landi. *Healthcare Data Breaches Hit All-Time High in 2021, Impacting 45m People*. Accessed: Jun. 2022. [Online]. Available: https://www.fiercehealthcare.com/health-tech/healthcare-data-breaches-hit-all-time-high-2021-impacting-45m-people

[9] P. Doyle. *Healthcare Breaches on the Rise in 2022*. Accessed: Jun. 2022. [Online]. Available: https://www.techtarget.com/searchsecurity/news/252521771/Healthcare-breaches-on-the-rise

[10] G. Lofaro. (2022). *Surveys on the Validation of Telemedicine: Procedural Models and Management Simplification of the Platform*. [Online]. Available: https://www.osservatoriosullefonti.it/archivi/archivio-note-e-commenti/note-e-commenti-n-1-2022/1703-rilievi-sulla-validazione-della-telemedicina-modelli-procedimentali-e-semplificazione-gestionale-della-piattaforma

[11] G. Lofaro. (2022). *The Security of Health Data in Smart Technologies As a Realization Tool of the Right to Health Between Telemedicine and Artificial Intelligence*. [Online]. Available: https://dirittifondamentali.it/2022/06/16/la-sicurezza-dei-dati-sanitari-nelle-smart-technologies-quale-strumento-di-realizzazione-del-diritto-alla-salute-tra-telemedicina-ed-intelligenza-artificiale/

[12] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, "Security and privacy-preserving challenges of E-health solutions in cloud computing," *IEEE Access*, vol. 7, pp. 74361–74382, 2019.

[13] H. S. G. Pussewalage and V. A. Oleshchuk, "Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions," *Int. J. Inf. Manag.*, vol. 36, no. 6, pp. 1161–1173, Dec. 2016.

[14] A. Ahad, M. Tahir, and K.-L.-A. Yau, "5G-based smart healthcare network: Architecture, taxonomy, challenges and future research directions," *IEEE Access*, vol. 7, pp. 100747–100762, 2019.

[15] S. Nayak and R. Patgiri, "6G communication technology: A vision on intelligent healthcare," in *Health Informatics, A Computational Perspective in Healthcare*. Berlin, Germany: Springer, 2021, pp. 1–18.

[16] M. B. Janjua, A. E. Duranay, and H. Arslan, "Role of wireless communication in healthcare system to cater disaster situations under 6G vision," *Frontiers Commun. Netw.*, vol. 1, Dec. 2020, Art. no. 610879.

[17] K.-H. Yu, A. L. Beam, and I. S. Kohane, "Artificial intelligence in healthcare," *Nature Biomed. Eng.*, vol. 2, no. 10, pp. 719–731, Oct. 2018.

[18] H. Zhang, N. Shlezinger, F. Guidi, D. Dardari, M. F. Imani, and Y. C. Eldar, "Near-field wireless power transfer for 6G internet of everything mobile networks: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 60, no. 3, pp. 12–18, Mar. 2022.

[19] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May/Jun. 2020.

[20] V. C. F. D. Costa, L. Oliveira, and J. D. Souza, "Internet of everything (IoE) taxonomies: A survey and a novel knowledge-based taxonomy," *Sensors*, vol. 21, no. 2, p. 568, Jan. 2021.

[21] S. Vishnu, S. R. J. Ramson, and R. Jegan, "Internet of medical things (IoMT)—An overview," in *Proc. 5th Int. Conf. Devices, Circuits Syst. (ICDCS)*, Mar. 2020, pp. 101–104.

[22] A. O. Akmandor and N. K. Jha, "Smart health care: An edge-side computing perspective," *IEEE Consum. Electron. Mag.*, vol. 7, no. 1, pp. 29–37, Jan. 2018.

[23] A. Avinashiappan and B. Mayilsamy, "Internet of medical things: Security threats, security challenges, and potential solutions," in *Internet of Medical Things*. Cham, Switzerland: Springer, 2021, pp. 1–16.

[24] S. Javaid, S. Zeadally, H. Fahim, and B. He, "Medical sensors and their integration in wireless body area networks for pervasive healthcare delivery: A review," *IEEE Sensors J.*, vol. 22, no. 5, pp. 3860–3877, Mar. 2022.

[25] D. Zhang, J. J. P. C. Rodrigues, Y. Zhai, and T. Sato, "Design and implementation of 5G E-health systems: Technologies, use cases, and future challenges," *IEEE Commun. Mag.*, vol. 59, no. 9, pp. 80–85, Sep. 2021.

[26] S. Zhang, J. Liu, H. Guo, M. Qi, and N. Kato, "Envisioning device-to-device communications in 6G," *IEEE Netw.*, vol. 34, no. 3, pp. 86–91, Jun. 2020.

[27] C. Chakraborty and J. J. C. P. Rodrigues, "A comprehensive review on device-to-device communication paradigm: Trends, challenges and applications," *Wireless Pers. Commun.*, vol. 114, pp. 185–207, Sep. 2020.

[28] M. Kumar and S. Chand, "A secure and efficient cloud-centric internet-of-medical-things-enabled smart healthcare system with public verifiability," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10650–10659, Oct. 2020.

[29] A. P. G. Lopes and P. R. L. Gondim, "Mutual authentication protocol for D2D communications in a cloud-based E-health system," *Sensors*, vol. 20, no. 7, p. 2072, Apr. 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/7/2072

[30] L. U. Khan, W. Saad, D. Niyato, Z. Han, and C. S. Hong, "Digital-twin-enabled 6G: Vision, architectural trends, and future directions," *IEEE Commun. Mag.*, vol. 60, no. 1, pp. 74–80, Jan. 2022.

[31] F. Laamarti, H. F. Badawi, Y. Ding, F. Arafsha, B. Hafidh, and A. El Saddik, "An ISO/IEEE 11073 standardized digital twin framework for health and well-being in smart cities," *IEEE Access*, vol. 8, pp. 105950–105961, 2020.

[32] F. Firouzi, B. Farahani, M. Daneshmand, K. Grise, J. Song, R. Saracco, L. L. Wang, K. Lo, P. Angelov, E. Soares, and P. S. Loh, "Harnessing the power of smart and connected health to tackle COVID-19: IoT, AI, robotics, and blockchain for a better world," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12826–12846, Aug. 2021.

[33] H. Elayan, M. Aloqaily, and M. Guizani, "Digital twin for intelligent context-aware IoT healthcare systems," *IEEE Internet Things J.*, vol. 8, no. 23, pp. 16749–16757, Dec. 2021.

[34] M. Nitti, V. Pilloni, G. Colistra, and L. Atzori, "The virtual object as a major element of the Internet of Things: A survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1228–1240, 2nd Quart., 2015.

[35] K. Jovanovic, "Digital innovation hubs in health-care robotics fighting COVID-19: Novel support for patients and health-care workers across Europe," *IEEE Robot. Autom. Mag.*, vol. 28, no. 1, pp. 40–47, Mar. 2021.

[36] I. F. Akyildiz, A. Kak, and S. Nie, "6G and beyond: The future of wireless communications systems," *IEEE Access*, vol. 8, pp. 133995–134030, 2020.

[37] F. Rinaldi, H.-L. Maattanen, J. Torsner, S. Pizzi, S. Andreev, A. Iera, Y. Koucheryavy, and G. Araniti, "Non-terrestrial networks in 5G & beyond: A survey," *IEEE Access*, vol. 8, pp. 165178–165200, 2020.

[38] G. Araniti, A. Iera, S. Pizzi, and F. Rinaldi, "Toward 6G non-terrestrial networks," *IEEE Netw.*, vol. 36, no. 1, pp. 113–120, Jan. 2022.

[39] M. Montazeri, R. ZahediNasab, A. Farahani, H. Mohseni, and F. Ghasemian, "Machine learning models for image-based diagnosis and prognosis of COVID-19: Systematic review," *JMIR Med. Informat.*, vol. 9, no. 4, Apr. 2021, Art. no. e25181.

[40] C. Martin-Isla, V. M. Campello, C. Izquierdo, Z. Raisi-Estabragh, B. Baeßler, S. E. Petersen, and K. Lekadir, "Image-based cardiac diagnosis with machine learning: A review," *Frontiers Cardiovascular Med.*, vol. 7, p. 1, Jan. 2020.

[41] Z. Hu, J. Tang, Z. Wang, K. Zhang, L. Zhang, and Q. Sun, "Deep learning for image-based cancer detection and diagnosis—A survey," *Pattern Recognit.*, vol. 83, pp. 134–149, Nov. 2018.

[42] Y. Zheng, Y. Zheng, D. Suehiro, and S. Uchida, "Top-rank convolutional neural network and its application to medical image-based diagnosis," *Pattern Recognit.*, vol. 120, Dec. 2021, Art. no. 108138.

[43] R. Dias and A. Torkamani, "Artificial intelligence in clinical and genomic diagnostics," *Genome Med.*, vol. 11, no. 1, pp. 1–12, Dec. 2019.

[44] O. Alvarez-Machancoses, E. J. D. Galiana, A. Cernea, J. F. De La Vina, and J. L. Fernandez-Martinez, "On the role of artificial intelligence in genomics to enhance precision medicine," *Pharmacogenomics Personalized Med.*, vol. 13, p. 105, Mar. 2020.

[45] S. Quazi, "Artificial intelligence and machine learning in precision and genomic medicine," *Med. Oncol.*, vol. 39, no. 8, pp. 1–18, Jun. 2022.

[46] D. Ledesma, S. Symes, and S. Richards, "Advancements within modern machine learning methodology: Impacts and prospects in biomarker discovery," *Current Medicinal Chem.*, vol. 28, no. 32, pp. 6512–6531, Oct. 2021.

[47] Y. Xie, W.-Y. Meng, R.-Z. Li, Y.-W. Wang, X. Qian, C. Chan, Z.-F. Yu, X.-X. Fan, H.-D. Pan, C. Xie, Q.-B. Wu, P.-Y. Yan, L. Liu, Y.-J. Tang, X.-J. Yao, M.-F. Wang, and E. L.-H. Leung, "Early lung cancer diagnostic biomarker discovery by machine learning methods," *Transl. Oncol.*, vol. 14, no. 1, Jan. 2021, Art. no. 100907.

[48] M. Mann, C. Kumar, W.-F. Zeng, and M. T. Strauss, "Artificial intelligence for proteomics and biomarker discovery," *Cell Syst.*, vol. 12, no. 8, pp. 759–770, Aug. 2021.

[49] X. Li, N. C. Dvornek, Y. Zhou, J. Zhuang, P. Ventola, and J. S. Duncan, "Efficient interpretation of deep learning models using graph structure and cooperative game theory: Application to ASD biomarker discovery," in *Proc. Int. Conf. Inf. Process. Med. Imag.* Cham, Switzerland: Springer, 2019, pp. 718–730.

[50] J. Yao, S. Wang, X. Zhu, and J. Huang, "Imaging biomarker discovery for lung cancer survival prediction," in *Proc. Int. Conf. Med. Image Comput. Comput.-Assist. Intervent.* Cham, Switzerland: Springer, 2016, pp. 649–657.

[51] M. Makar, M. Ghassemi, D. M. Cutler, and Z. Obermeyer, "Short-term mortality prediction for elderly patients using medicare claims data," *Int. J. Mach. Learn. Comput.*, vol. 5, no. 3, p. 192, 2015.

[52] C. Guo, J. Wang, Y. Wang, X. Qu, Z. Shi, Y. Meng, J. Qiu, and K. Hua, "Novel artificial intelligence machine learning approaches to precisely predict survival and site-specific recurrence in cervical cancer: A multi-institutional study," *Transl. Oncol.*, vol. 14, no. 5, May 2021, Art. no. 101032.

[53] C. Díez-Sanmartín and A. S. Cabezuelo, "Application of artificial intelligence techniques to predict survival in kidney transplantation: A review," *J. Clin. Med.*, vol. 9, no. 2, p. 572, Feb. 2020.

[54] M. M. Churpek, T. C. Yuen, C. Winslow, A. A. Robicsek, D. O. Meltzer, R. D. Gibbons, and D. P. Edelson, "Multicenter development and validation of a risk stratification tool for ward patients," *Amer. J. Respiratory Crit. Care Med.*, vol. 190, no. 6, pp. 649–655, Sep. 2014.

[55] X. Li, J. Dunn, D. Salins, G. Zhou, W. Zhou, S. M. S. F. Rose, D. Perelman, E. Colbert, R. Runge, S. Rego, R. Sonecha, S. Datta, T. McLaughlin, and M. P. Snyder, "Digital health: Tracking physiomes and activity using wearable biosensors reveals useful health-related information," *PLOS Biol.*, vol. 15, no. 1, Jan. 2017, Art. no. e2001402.

[56] C. Y. Jin, "A review of AI technologies for wearable devices," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 688, no. 4, Nov. 2019, Art. no. 044072.

[57] V.-T. Tran, C. Riveros, and P. Ravaud, "Patients' views of wearable devices and AI in healthcare: Findings from the compare E-cohort," *Npj Digit. Med.*, vol. 2, no. 1, pp. 1–8, Jun. 2019.

[58] A. Shademan, R. S. Decker, J. D. Opfermann, S. Leonard, A. Krieger, and P. C. W. Kim, "Supervised autonomous robotic soft tissue surgery," *Sci. Transl. Med.*, vol. 8, no. 337, May 2016, Art. no. 337ra64.

[59] P. Gomes, "Surgical robotics: Reviewing the past, analysing the present, imagining the future," *Robot. Comput.-Integr. Manuf.*, vol. 27, no. 2, pp. 261–266, Apr. 2011.

[60] S. Panesar, Y. Cagle, D. Chander, J. Morey, J. Fernandez-Miranda, and M. Kliot, "Artificial intelligence and the future of surgical robotics," *Ann. Surgery*, vol. 270, no. 2, pp. 223–226, 2019.

[61] S. O'Sullivan, N. Nevejans, C. Allen, A. Blyth, S. Leonard, U. Pagallo, K. Holzinger, A. Holzinger, M. I. Sajid, and H. Ashrafian, "Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery," *Int. J. Med. Robot. Comput. Assist. Surgery*, vol. 15, no. 1, p. e1968, Feb. 2019.

[62] X.-Y. Zhou, Y. Guo, M. Shen, and G.-Z. Yang, "Application of artificial intelligence in surgery," *Frontiers Med.*, vol. 14, no. 4, pp. 417–430, 2020.

[63] K. Rajendran, M. Jayabalan, and M. E. Rana, "A study on K-anonymity, l-diversity, and T-closeness techniques," *IJCSNS*, vol. 17, no. 12, p. 172, 2017.

[64] K. M. Chong, "Privacy-preserving healthcare informatics: A review," in *Proc. ITM Web Conf.*, vol. 36, 2021, p. 04005.

[65] A. Shah, H. Abbas, W. Iqbal, and R. Latif, "Enhancing E-healthcare privacy preservation framework through L-diversity," in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2018, pp. 394–399.

[66] A. Abbasi and B. Mohammadi, "A clustering-based anonymization approach for privacy-preserving in the healthcare cloud," *Concurrency Comput., Pract. Exper.*, vol. 34, no. 1, p. e6487, Jan. 2022.

[67] K. Arava and S. Lingamgunta, "Adaptive K-anonymity approach for privacy preserving in cloud," *Arabian J. Sci. Eng.*, vol. 45, no. 4, pp. 2425–2432, Apr. 2020.

[68] K. Liang, L. Fang, W. Susilo, and D. S. Wong, "A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security," in *Proc. 5th Int. Conf. Intell. Netw. Collaborative Syst.*, Sep. 2013, pp. 552–559.

[69] K. Edemacu, B. Jang, and J. W. Kim, "Collaborative E-health privacy and security: An access control with attribute revocation based on OBDD access structure," *IEEE J. Biomed. Health Informat.*, vol. 24, no. 10, pp. 2960–2972, Oct. 2020.

[70] K. Edemacu, B. Jang, and J. W. Kim, "CESCR: CP-ABE for efficient and secure sharing of data in collaborative E-health with revocation and no dummy attribute," *PLoS ONE*, vol. 16, no. 5, May 2021, Art. no. e0250992.

[71] A. Sudarsono, M. Yuliana, and H. A. Darwito, "A secure data sharing using identity-based encryption scheme for E-healthcare system," in *Proc. 3rd Int. Conf. Sci. Inf. Technol. (ICSITech)*, Oct. 2017, pp. 429–434.

[72] P. Sharma, N. R. Moparthi, S. Namasudra, V. Shanmuganathan, and C. Hsu, "Blockchain-based IoT architecture to secure healthcare system using identity-based encryption," *Exp. Syst.*, vol. 39, no. 10, Dec. 2022, Art. no. e12915.

[73] Q. Huang, W. Yue, Y. He, and Y. Yang, "Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing," *IEEE Access*, vol. 6, pp. 36584–36594, 2018.

[74] L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker, "A type-and-identity-based proxy re-encryption scheme and its application in healthcare," in *Proc. Workshop Secure Data Manag.* Cham, Switzerland: Springer, 2008, pp. 185–198.

[75] M. Zhang and Y. Ji, "Blockchain for healthcare records: A data perspective," *PeerJ Preprints*, vol. 6, May 2018, Art. no. e26942v1.

[76] T. Benil and J. Jasper, "Cloud based security on outsourcing using blockchain in E-health systems," *Comput. Netw.*, vol. 178, Sep. 2020, Art. no. 107344.
[77] Q. Mamun, "Blockchain technology in the future of healthcare," *Smart Health*, vol. 23, Mar. 2022, Art. no. 100223.
[78] M. Attaran, "Blockchain technology in healthcare: Challenges and opportunities," *Int. J. Healthcare Manag.*, vol. 15, no. 1, pp. 70–83, Jan. 2022.
[79] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare: Medrec prototype for electronic health records and medical research data," in *Proc. IEEE Open Big Data Conf.*, vol. 13, Aug. 2016, p. 13.
[80] S. Cao, G. Zhang, P. Liu, X. Zhang, and F. Neri, "Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain," *Inf. Sci.*, vol. 485, pp. 427–440, Jun. 2019.
[81] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, Apr. 2017.
[82] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in E-health systems via consortium blockchain," *J. Med. Syst.*, vol. 42, no. 140, pp. 1–18, 2018.
[83] S. S. Minahil, K. Mahmood, S. Kumari, and C.-M. Chen, "A secure blockchain-based E-health records storage and sharing scheme," *J. Inf. Secur. Appl.*, vol. 55, Dec. 2020, Art. no. 102590. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212620307596
[84] U. Chelladurai and S. Pandian, "A novel blockchain based electronic health record automation system for healthcare," *J. Ambient Intell. Humanized Comput.*, vol. 13, no. 1, pp. 693–703, Jan. 2022.
[85] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, and S. Muralidharan, "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, 2018, pp. 1–15.
[86] R. Kumar, N. Marchang, and R. Tripathi, "Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and blockchain," in *Proc. Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2020, pp. 1–5.
[87] J. Jayabalan and N. Jeyanthi, "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy," *J. Parallel Distrib. Comput.*, vol. 164, pp. 152–167, Jun. 2022.
[88] K. Azbeg, O. Ouchetto, and S. J. Andaloussi, "BlockMedCare: A healthcare system based on IoT, blockchain and IPFS for data management security," *Egyptian Informat. J.*, vol. 23, no. 2, pp. 329–343, Jul. 2022.
[89] S. Kumar, A. K. Bharti, and R. Amin, "Decentralized secure storage of medical records using blockchain and IPFS : A comparative analysis with future directions," *Secur. Privacy*, vol. 4, no. 5, p. e162, Sep. 2021.
[90] R. Gupta, A. Shukla, and S. Tanwar, "AaYusH: A smart contract-based telesurgery system for healthcare 4.0," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2020, pp. 1–6.
[91] A. Zhang, L. Wang, X. Ye, and X. Lin, "Light-weight and robust security-aware D2D-assist data transmission protocol for mobil E-health systems," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 662–675, Mar. 2017.
[92] M. Singh, E. Fuenmayor, E. Hinchy, Y. Qiao, N. Murray, and D. Devine, "Digital twin: Origin to future," *Appl. Syst. Innov.*, vol. 4, no. 2, p. 36, May 2021.
[93] H. X. Nguyen, R. Trestian, D. To, and M. Tatipamula, "Digital twin for 5G and beyond," *IEEE Commun. Mag.*, vol. 59, no. 2, pp. 10–15, Feb. 2021.
[94] S. Pouyanfar, S. Sadiq, Y. Yan, H. Tian, Y. Tao, M. P. Reyes, M.-L. Shyu, S.-C. Chen, and S. S. Iyengar, "A survey on deep learning: Algorithms, techniques, and applications," *ACM Comput. Surveys (CSUR)*, vol. 51, no. 5, pp. 1–36, 2018.
[95] K. Liakos, P. Busato, D. Moshou, S. Pearson, and D. Bochtis, "Machine learning in agriculture: A review," *Sensors*, vol. 18, no. 8, p. 2674, 2018.
[96] R. Krishnan, P. Rajpurkar, and E. J. Topol, "Self-supervised learning in medicine and healthcare," *Nature Biomed. Eng.*, vol. 6, pp. 1–7, Aug. 2022.
[97] O. I. Abiodun, A. Jantan, A. E. Omolara, K. V. Dada, N. A. Mohamed, and H. Arshad, "State-of-the-art in artificial neural network applications: A survey," *Heliyon*, vol. 4, no. 11, Nov. 2018, Art. no. e00938.
[98] Z. Li, F. Liu, W. Yang, S. Peng, and J. Zhou, "A survey of convolutional neural networks: Analysis, applications, and prospects," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 33, no. 12, pp. 6999–7019, Dec. 2022.
[99] Y. Yu, X. Si, C. Hu, and Z. Jianxun, "A review of recurrent neural networks: LSTM cells and network architectures," *Neural Comput.*, vol. 31, no. 7, pp. 1235–1270, Jul. 2019.
[100] J. Cervantes, F. Garcia-Lamont, L. Rodríguez-Mazahua, and A. Lopez, "A comprehensive survey on support vector machine classification: Applications, challenges and trends," *Neurocomputing*, vol. 408, pp. 189–215, Sep. 2020.
[101] P. Cunningham and S. J. Delany, "K-nearest neighbour classifiers—A tutorial," *ACM Comput. Surveys*, vol. 54, no. 6, pp. 1–25, Jul. 2022.
[102] H. Sharma and S. Kumar, "A survey on decision tree algorithms of classification in data mining," *J. Sci. Res.*, vol. 5, no. 4, pp. 2094–2097, 2016.
[103] A. Glielmo, B. E. Husic, A. Rodriguez, C. Clementi, F. Noé, and A. Laio, "Unsupervised learning methods for molecular simulation data," *Chem. Rev.*, vol. 121, no. 16, pp. 9722–9758, Aug. 2021.
[104] D. Bank, N. Koenigstein, and R. Giryes, "Autoencoders," 2020, *arXiv:2003.05991*.
[105] M. Cottrell, M. Olteanu, F. Rossi, and N. Villa-Vialaneix, "Self-organizing maps, theory and applications," *Revista de Investigacion Operacional*, vol. 39, no. 1, pp. 1–22, 2018.
[106] M. Ahmed, R. Seraj, and S. M. S. Islam, "The K-means algorithm: A comprehensive survey and performance evaluation," *Electronics*, vol. 9, no. 8, p. 1295, Aug. 2020.
[107] P. Bhattacharjee and P. Mitra, "A survey of density based clustering algorithms," *Frontiers Comput. Sci.*, vol. 15, no. 1, pp. 1–27, Feb. 2021.
[108] M. E. Celebi and K. Aydin, *Unsupervised Learning Algorithms*. Berlin, Germany: Springer, 2016.
[109] N. Kalugina, "Diagnostics of the organism on biomedical signals based on reinforcement learning," in *Proc. 12th Russian-German Conf. Biomed. Eng.*, 2016, pp. 204–207.
[110] B. Mahesh, "Machine learning algorithms—A review," *Int. J. Sci. Res.*, vol. 9, pp. 381–386, Oct. 2020.
[111] M. Ghassemi, T. Naumann, P. Schulam, A. L. Beam, I. Y. Chen, and R. Ranganath, "A review of challenges and opportunities in machine learning for health," *AMIA Summits Transl. Sci. Proc.*, vol. 2020, p. 191, May 2020.
[112] R. Pillai, P. Oza, and P. Sharma, "Review of machine learning techniques in health care," in *Proc. ICRIC*. Cham, Switzerland: Springer, 2020, pp. 103–111.
[113] *Neural Networks*. Accessed: Jun. 2022. [Online]. Available: https://www.ibm.com/cloud/learn/neural-networks
[114] R. S. Shankar, C. Raminaidu, V. S. Raju, and J. Rajanikanth, "Detection of epilepsy based on EEG signals using PCA with ANN model," *J. Phys., Conf.*, vol. 2070, no. 1, Nov. 2021, Art. no. 012145.
[115] R. Jafari-Marandi, S. Davarzani, M. S. Gharibdousti, and B. K. Smith, "An optimum ANN-based breast cancer diagnosis: Bridging gaps between ANN learning and decision-making goals," *Appl. Soft Comput.*, vol. 72, pp. 108–120, Nov. 2018.
[116] I. M. Nasser and S. S. Abu-Naser, "Lung cancer detection using artificial neural network," *Int. J. Eng. Inf. Syst.*, vol. 3, no. 3, pp. 17–23, 2019.
[117] E. Shamsara, S. S. Soflaei, M. Tajfard, I. Yamshchikov, H. Esmaily, M. Saberi-Karimian, H. Ghazizadeh, S. R. Mirhafez, Z. Farjami, G. A. Ferns, and M. Ghayour-Mobarhan, "Artificial neural network models for coronary artery disease," *Current Bioinf.*, vol. 16, no. 4, pp. 610–623, Aug. 2021.
[118] D. Zafeiris, S. Rutella, and G. R. Ball, "An artificial neural network integrated pipeline for biomarker discovery using Alzheimer's disease as a case study," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 77–87, Jan. 2018.
[119] J. M. Haglin, G. Jimenez, and A. E. M. Eltorai, "Artificial neural networks in medicine," *Health Technol.*, vol. 9, no. 1, pp. 1–6, Jan. 2019.
[120] A. Vilamala, K. H. Madsen, and L. K. Hansen, "Deep convolutional neural networks for interpretable analysis of EEG sleep stage scoring," in *Proc. IEEE 27th Int. Workshop Mach. Learn. Signal Process. (MLSP)*, Sep. 2017, pp. 1–6.
[121] S. Roy, I. Kiral-Kornek, and S. Harrer, "Deep learning enabled automatic abnormal EEG identification," in *Proc. 40th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Jul. 2018, pp. 2756–2759.
[122] C. Ieracitano, N. Mammone, A. Bramanti, A. Hussain, and F. Morabit, "A convolutional neural network approach for classification of dementia stages based on 2D-spectral representation of EEG recordings," *Neurocomputing*, vol. 323, pp. 96–107, Jan. 2019.
[123] Z. Jiao, X. Gao, Y. Wang, J. Li, and H. Xu, "Deep convolutional neural networks for mental load classification based on EEG data," *Pattern Recognit.*, vol. 76, pp. 582–595, Apr. 2018.
[124] I. N. Da Silva, D. H. Spatti, R. A. Flauzino, L. H. B. Liboni, and S. F. D. R. Alves, *Artificial Neural Networks*, vol. 39. Cham, Switzerland: Springer, 2017.

[125] S. Walczak, "Artificial neural networks," in *Encyclopedia of Information Science and Technology*, D. B. A. M. Khosrow-Pour, Ed., 4th ed. Hershey, PA, USA: IGI Global, 2018, pp. 120–131.

[126] C. Koch, "Computation and the single neuron," *Nature*, vol. 385, no. 6613, pp. 207–210, 1997.

[127] F. C. Morabito, M. Campolo, C. Ieracitano, J. M. Ebadi, L. Bonanno, A. Bramanti, S. Desalvo, N. Mammone, and P. Bramanti, "Deep convolutional neural networks for classification of mild cognitive impaired and Alzheimer's disease patients from scalp EEG recordings," in *Proc. IEEE 2nd Int. Forum Res. Technol. Soc. Ind. Leveraging Better Tomorrow (RTSI)*, Sep. 2016, pp. 1–6.

[128] C. Ieracitano, N. Mammone, A. Hussain, and F. C. Morabito, "A novel multi-modal machine learning based approach for automatic classification of EEG recordings in dementia," *Neural Netw.*, vol. 123, pp. 176–190, Mar. 2020.

[129] M. Lo Giudice, G. Varone, C. Ieracitano, N. Mammone, G. G. Tripodi, E. Ferlazzo, S. Gasparini, U. Aguglia, and F. C. Morabito, "Permutation entropy-based interpretability of convolutional neural network models for interictal EEG discrimination of subjects with epileptic seizures vs. psychogenic non-epileptic seizures," *Entropy*, vol. 24, no. 1, p. 102, Jan. 2022. [Online]. Available: https://www.mdpi.com/1099-4300/24/1/102

[130] J. M. Wolterink, R. W. Van Hamersvelt, M. A. Viergever, T. Leiner, and I. Išgum, "Coronary artery centerline extraction in cardiac CT angiography using a CNN-based orientation classifier," *Med. Image Anal.*, vol. 51, pp. 46–60, Jan. 2019.

[131] B. Wu, Y. Fang, and X. Lai, "Left ventricle automatic segmentation in cardiac MRI using a combined CNN and U-Net approach," *Computerized Med. Imag. Graph.*, vol. 82, Jun. 2020, Art. no. 101719.

[132] D. Verma and S. Agarwal, "Cardiac arrhythmia detection from single-lead ECG using CNN and LSTM assisted by oversampling," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Sep. 2018, pp. 14–17.

[133] F. Gao, T. Wu, J. Li, B. Zheng, L. Ruan, D. Shang, and B. Patel, "SD-CNN: A shallow-deep CNN for improved breast cancer diagnosis," *Computerized Med. Imag. Graph.*, vol. 70, pp. 53–62, Dec. 2018.

[134] S. Dabeer, M. M. Khan, and S. Islam, "Cancer diagnosis in histopathological image: CNN based approach," *Informat. Med. Unlocked*, vol. 16, Jan. 2019, Art. no. 100231.

[135] W. Alakwaa, M. Nassef, and A. Badr, "Lung cancer detection and classification with 3D convolutional neural network (3D-CNN)," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 8, pp. 409–417, 2017.

[136] L. Xie and A. Yuille, "Genetic CNN," in *Proc. IEEE Int. Conf. Comput. Vis. (ICCV)*, Oct. 2017, pp. 1379–1388.

[137] Y. Sun, B. Xue, M. Zhang, G. G. Yen, and J. Lv, "Automatically designing CNN architectures using the genetic algorithm for image classification," *IEEE Trans. Cybern.*, vol. 50, no. 9, pp. 3840–3854, Sep. 2020.

[138] *Recurrent Neural Networks*. Accessed: 9, Jul. 2020. [Online]. Available: https://www.ibm.com/cloud/learn/recurrent-neural-networks

[139] F. Ma, R. Chitta, J. Zhou, Q. You, T. Sun, and J. Gao, "Dipole: Diagnosis prediction in healthcare via attention-based bidirectional recurrent neural networks," in *Proc. 23rd ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Aug. 2017, pp. 1903–1911.

[140] Y. Cheng, H. Zhu, J. Wu, and X. Shao, "Machine health monitoring using adaptive kernel spectral clustering and deep long short-term memory recurrent neural networks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 2, pp. 987–997, Feb. 2018.

[141] T. Makino, S. Jastrzebski, W. Oleszkiewicz, C. Chacko, R. Ehrenpreis, N. Samreen, C. Chhor, E. Kim, J. Lee, K. Pysarenko, and B. Reig, "Differences between human and machine perception in medical diagnosis," *Sci. Rep.*, vol. 12, no. 1, pp. 1–13, 2022.

[142] A. Zytek, I. Arnaldo, D. Liu, L. Berti-Equille, and K. Veeramachaneni, "The need for interpretable features: Motivation and taxonomy," 2022, *arXiv:2202.11748*.

[143] A. Das and P. Rad, "Opportunities and challenges in explainable artificial intelligence (XAI): A survey," 2020, *arXiv:2006.11371*.

[144] F. M. Janssen, K. K. H. Aben, B. L. Heesterman, Q. J. M. Voorham, P. A. Seegers, and A. Moncada-Torres, "Using explainable machine learning to explore the impact of synoptic reporting on prostate cancer," *Algorithms*, vol. 15, no. 2, p. 49, Jan. 2022. [Online]. Available: https://www.mdpi.com/1999-4893/15/2/49

[145] N. Burkart and M. F. Huber, "A survey on the explainability of supervised machine learning," *J. Artif. Intell. Res.*, vol. 70, pp. 245–317, Jan. 2021.

[146] S. Tonekaboni, S. Joshi, M. D. McCradden, and A. Goldenberg, "What clinicians want: Contextualizing explainable machine learning for clinical end use," in *Proc. Mach. Learn. Healthcare Conf.*, 2019, pp. 359–380.

[147] R. Guidotti, A. Monreale, S. Ruggieri, F. Turini, F. Giannotti, and D. Pedreschi, "A survey of methods for explaining black box models," *ACM Comput. Surveys (CSUR)*, vol. 51, no. 5, pp. 1–42, 2018.

[148] T. Ng, L. Chew, and C. W. Yap, "A clinical decision support tool to predict survival in cancer patients beyond 120 days after palliative chemotherapy," *J. Palliative Med.*, vol. 15, no. 8, pp. 863–869, Aug. 2012.

[149] Y. Kudo, Y. Shimada, J. Matsubayashi, Y. Kitamura, Y. Makino, S. Maehara, M. Hagiwara, J. Park, T. Yamada, S. Takeuchi, M. Kakihana, T. Nagao, T. Ohira, J. Masumoto, and N. Ikeda, "Artificial intelligence analysis of three-dimensional imaging data derives factors associated with postoperative recurrence in patients with radiologically solid-predominant small-sized lung cancers," *Eur. J. Cardio-Thoracic Surgery*, vol. 61, no. 4, pp. 751–760, Mar. 2022.

[150] R. Ramakrishnan, S. Rao, and J.-R. He, "Perinatal health predictors using artificial intelligence: A review," *Women's Health*, vol. 17, Jan. 2021, Art. no. 174550652110461.

[151] S.-R. Oh, Y.-D. Seo, E. Lee, and Y.-G. Kim, "A comprehensive survey on security and privacy for electronic health data," *Int. J. Environ. Res. Public Health*, vol. 18, no. 18, p. 9668, Sep. 2021.

[152] M. Karatas, L. Eriskin, M. Deveci, D. Pamucar, and H. Garg, "Big data for healthcare industry 4.0: Applications, challenges and future perspectives," *Exp. Syst. Appl.*, vol. 200, Aug. 2022, Art. no. 116912.

[153] K. Feldman, R. A. Johnson, and N. V. Chawla, "The state of data in healthcare: Path towards standardization," *J. Healthcare Informat. Res.*, vol. 2, no. 3, pp. 248–271, Sep. 2018.

[154] A. K. Singh, A. Anand, Z. Lv, H. Ko, and A. Mohan, "A survey on healthcare data: A security perspective," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 17, no. 2, pp. 1–26, May 2021.

[155] (2022). *GDPR Official Website*. Accessed: Jul. 3, 2022. [Online]. Available: https://eugdpr.org

[156] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," TU Dresden, Dresden, Germany, Tech. Rep. v.034, Aug. 2010. Accessed: Dec. 2022. [Online]. Available: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

[157] S. Ito and H. Kikuchi, "Estimation of cost of K–anonymity in the number of dummy records," *J. Ambient Intell. Humanized Comput.*, pp. 1–10, Mar. 2022.

[158] N. Deepa, Q.-V. Pham, D. C. Nguyen, S. Bhattacharya, B. Prabadevi, T. R. Gadekallu, P. K. R. Maddikunta, F. Fang, and P. N. Pathirana, "A survey on blockchain for big data: Approaches, opportunities, and future directions," *Future Gener. Comput. Syst.*, vol. 131, pp. 209–226, Jun. 2022.

[159] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: Opportunities, challenges, and future recommendations," *Neural Comput. Appl.*, vol. 34, no. 14, pp. 11475–11490, 2021.

[160] C. Cuijpers and J. Schroers, "eIDAS as guideline for the development of a pan European eID framework in futureID," in *Open Identity Summit 2014*, D. Hühnlein and H. Roßnagel, Eds. Bonn, Germany: Gesellschaft für Informatik e.V., pp. 23–38.

[161] K. Munjal and R. Bhatia, "A systematic review of homomorphic encryption and its contributions in healthcare industry," *Complex Intell. Syst.*, pp. 1–28, May 2022.

[162] S. Kern, T. Baumer, S. Groll, L. Fuchs, and G. Pernul, "Optimization of access control policies," *J. Inf. Secur. Appl.*, vol. 70, Nov. 2022, Art. no. 103301.

[163] P. S. K. Oberko, V.-H. K. S. Obeng, and H. Xiong, "A survey on multi-authority and decentralized attribute-based encryption," *J. Ambient Intell. Hum. Comput.*, vol. 13, no. 1, pp. 515–533, 2022.

[164] M. A. Simplicio, B. T. De Oliveira, C. B. Margi, P. S. L. M. Barreto, T. C. M. B. Carvalho, and M. Näslund, "Survey and comparison of message authentication solutions on wireless sensor networks," *Ad Hoc Netw.*, vol. 11, no. 3, pp. 1221–1236, May 2013.

[165] M. Pirretti, P. Traynor, and P. McDaniel, "Secure attribute-based systems," *J. Comput. Secur.*, vol. 18, no. 5, pp. 799–837, 2010.

[166] F. Buccafurri, V. De Angelis, and S. Lazzaro, "A blockchain-based framework to enhance anonymous services with accountability guarantees," *Future Internet*, vol. 14, no. 8, p. 243, Aug. 2022. [Online]. Available: https://www.mdpi.com/1999-5903/14/8/243

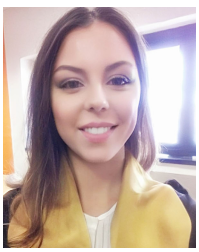
[167] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," in *Proc. Int. Conf. Eng. Technol. (ICET)*, Aug. 2017, pp. 1–7.

[168] C. Cai, X. Qin, T. H. Yuen, and S. M. Yiu, "Tight leakage-resilient identity-based encryption under multi-challenge setting," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, May 2022, pp. 42–53.
[169] T. Saleem, M. U. Janjua, M. Hassan, T. Ahmad, F. Tariq, K. Hafeez, M. A. Salal, and M. D. Bilal, "ProofChain: An X. 509-compatible blockchain-based PKI framework with decentralized trust," *Comput. Netw.*, vol. 213, Jan. 2022, Art. no. 109069.
[170] Z. Zhao, G. Wu, W. Susilo, F. Guo, B. Wang, and Y. Hu, "Accountable identity-based encryption with distributed private key generators," *Inf. Sci.*, vol. 505, pp. 352–366, Dec. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0020025519307054
[171] A. D. Caro, V. Iovino, and G. Persiano, "Fully secure anonymous HIBE and secret-key anonymous IBE with short ciphertexts," in *Proc. Int. Conf. Pairing-Based Cryptogr.* Cham, Switzerland: Springer, 2010, pp. 347–366.
[172] Z. Brakerski, A. Lombardi, G. Segev, and V. Vaikuntanathan, "Anonymous IBE, leakage resilience and circular security from new assumptions," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Cham, Switzerland: Springer, 2018, pp. 535–564.
[173] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Cham, Switzerland: Springer, 2005, pp. 457–473.
[174] C.-J. Wang and J.-F. Luo, "A key-policy attribute-based encryption scheme with constant size ciphertext," in *Proc. 8th Int. Conf. Comput. Intell. Secur.*, Nov. 2012, pp. 447–451.
[175] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2007, pp. 321–334.
[176] S. Deng, G. Yang, W. Dong, and M. Xia, "Flexible revocation in ciphertext-policy attribute-based encryption with verifiable ciphertext delegation," *Multimedia Tools Appl.*, pp. 1–24, Aug. 2022.
[177] X. Liang, Z. Cao, H. Lin, and J. Shao, "Attribute based proxy re-encryption with delegating capabilities," in *Proc. 4th Int. Symp. Inf., Comput., Commun. Secur. (ASIACCS)*, 2009, pp. 276–286.
[178] J. Li, C. Ma, and K. Zhang, "A novel lattice-based CP-ABPRE scheme for cloud sharing," *Symmetry*, vol. 11, no. 10, p. 1262, Oct. 2019.
[179] P. Samarati, "Protecting respondents identities in microdata release," *IEEE Trans. Knowl. Data Eng.*, vol. 13, no. 6, pp. 1010–1027, Nov./Dec. 2001.
[180] H. Li, F. Guo, W. Zhang, J. Wang, and J. Xing, "(a,k)-anonymous scheme for privacy-preserving data collection in IoT-based healthcare services systems," *J. Med. Syst.*, vol. 42, no. 3, pp. 1–9, Mar. 2018.
[181] T. Kanwal, A. Anjum, and A. Khan, "Privacy preservation in E-health cloud: Taxonomy, privacy requirements, feasibility analysis, and opportunities," *Cluster Comput.*, vol. 24, no. 1, pp. 293–317, Mar. 2021.
[182] E. Daniel and F. Tschorsch, "IPFS and friends: A qualitative comparison of next generation peer-to-peer data networks," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 31–52, 1st Quart., 2022.
[183] A. Aaviksoo, "Building blockchain powered trusted digital health services. Estonia," *Blockchain Healthcare Today*, Dec. 2019.
[184] *Medicalchain, Medicalchain Whitepaper 2.1. Tech. Rep. Medicalchain*, Medicalchain, London, U.K., 2018.
[185] M. Ambrosin, A. Anzanpour, M. Conti, T. Dargahi, S. R. Moosavi, A. M. Rahmani, and P. Liljeberg, "On the feasibility of attribute-based encryption on Internet of Things devices," *IEEE Micro*, vol. 36, no. 6, pp. 25–35, Nov. 2016.
[186] I. E. Olatunji, J. Rauch, M. Katzensteiner, and M. Khosla, "A review of anonymization for healthcare data," *Big Data*, Mar. 2022.
[187] J. Jayapradha and M. Prakash, "An efficient privacy-preserving data publishing in health care records with multiple sensitive attributes," in *Proc. 6th Int. Conf. Inventive Comput. Technol. (ICICT)*, Jan. 2021, pp. 623–629.
[188] A. Kiourti, A. M. Abbosh, M. Athanasiou, T. Bjorninen, A. Eid, C. Furse, K. Ito, G. Lazzi, M. Manoufali, M. Pastorino, M. M. Tentzeris, K. Tisdale, E. Topsakal, L. Ukkonen, W. G. Whittow, H. Zhang, and K. S. Nikita, "Next-generation healthcare: Enabling technologies for emerging bio-electromagnetics applications," *IEEE Open J. Antennas Propag.*, vol. 3, pp. 363–390, 2022.
[189] S. Palipana, B. Pietropaoli, and D. Pesch, "Recent advances in RF-based passive device-free localisation for indoor applications," *Ad Hoc Netw.*, vol. 64, pp. 80–98, Sep. 2017.
[190] C. Li, L. Mo, and D. Zhang, "Review on UHF RFID localization methods," *IEEE J. Radio Freq. Identificat.*, vol. 3, no. 4, pp. 205–215, Dec. 2019.
[191] N. Li, G. Calis, and B. Becerik-Gerber, "Measuring and monitoring occupancy with an RFID based system for demand-driven HVAC operations," *Autom. Construct.*, vol. 24, pp. 89–99, Jul. 2012.
[192] R. M. Buehrer, C. R. Anderson, R. K. Martin, N. Patwari, and M. G. Rabbat, "Introduction to the special issue on non-cooperative localization networks," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 1, pp. 2–4, Feb. 2014.
[193] F. Viani, P. Rocca, G. Oliveri, D. Trinchero, and A. Massa, "Localization, tracking, and imaging of targets in wireless sensor networks: An invited review," *Radio Sci.*, vol. 46, no. 5, pp. 1–12, Oct. 2011.
[194] J. Wilson and N. Patwari, "Radio tomographic imaging with wireless networks," *IEEE Trans. Mobile Comput.*, vol. 9, no. 5, pp. 621–632, May 2010.
[195] R. Palmeri, M. T. Bevacqua, A. F. Morabito, and T. Isernia, "Noncooperative localization and tracking through the factorization method," *IEEE Geosci. Remote Sens. Lett.*, vol. 16, no. 8, pp. 1205–1209, Aug. 2019.
[196] D. Colton and R. Kress, *Inverse Acoustic and Electromagnetic Scattering Theory*. Berlin, Germany: Springer-Verlag, 1992.
[197] M. Donelli and F. Viani, "Life signals detection system based on a continuous-wave X-band radar," *Electron. Lett.*, vol. 52, no. 23, pp. 1903–1904, Nov. 2016.
[198] Z. Park, C. Li, and J. Lin, "A broadband microstrip antenna with improved gain for noncontact vital sign radar detection," *IEEE Antennas Wireless Propag. Lett.*, vol. 8, pp. 939–942, 2009.
[199] Z. Peng, J. M. Muñoz-Ferreras, Y. Tang, C. Liu, R. Gómez-García, L. Ran, and C. Li, "A portable FMCW interferometry radar with programmable low-IF architecture for localization, ISAR imaging, and vital sign tracking," *IEEE Trans. Microw. Theory Techn.*, vol. 65, no. 4, pp. 1334–1344, Apr. 2017.
[200] C.-H. Tseng and Y.-H. Lin, "24-GHz self-injection-locked vital-sign radar sensor with CMOS injection-locked frequency divider based on push–push oscillator topology," *IEEE Microw. Wireless Compon. Lett.*, vol. 28, no. 11, pp. 1053–1055, Nov. 2018.
[201] M. Donelli, M. Manekiya, D. Cunial, L. Cristoforetti, and F. Fracchiolla, "A microwave interferometer for human breath monitoring in proton therapy applications," *Microw. Opt. Technol. Lett.*, vol. 62, no. 2, pp. 589–591, Feb. 2020.
[202] S. Pisa, P. Bernardi, M. Cavagnaro, E. Pittella, and E. Piuzzi, "A circuit model of an ultra wideband impulse radar system for breath-activity monitoring," *Int. J. Numer. Model., Electron. Netw., Devices Fields*, vol. 25, no. 1, pp. 46–63, Jan. 2012.
[203] G. Varotto and E. M. Staderini, "On the UWB medical radars working principles," *Int. J. UltraWideband Commun. Syst.*, vol. 2, no. 1, pp. 83–93, 2011.
[204] Y. Nijsure, W. P. Tay, E. Gunawan, F. Wen, Z. Yang, Y. L. Guan, and A. P. Chua, "An impulse radio ultrawideband system for contactless noninvasive respiratory monitoring," *IEEE Trans. Biomed. Eng.*, vol. 60, no. 6, pp. 1509–1517, Jun. 2013.
[205] Ø. Aardal, Y. Paichard, S. Brovoll, T. Berger, T. S. Lande, and S.-E. Hamran, "Physical working principles of medical radar," *IEEE Trans. Biomed. Eng.*, vol. 60, no. 4, pp. 1142–1149, Apr. 2013.
[206] E. Pittella, S. Pisa, and M. Cavagnaro, "Breath activity monitoring with wearable UWB radars: Measurement and analysis of the pulses reflected by the human body," *IEEE Trans. Biomed. Eng.*, vol. 63, no. 7, pp. 1447–1454, Jul. 2016.
[207] Commission of the European Communities. (Jul. 2022). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*. [Online]. Available: https://eur-lex.europa.eu/legal-content/ENG/TXT/PDF/?uri=CELEX:52008DC0689&from=ENG/
[208] R. Somolinos, A. Munoz, M. E. Hernando, M. Pascual, J. Caceres, R. Sanchez-De-Madariaga, J. A. Fragua, P. Serrano, and C. H. Salvador, "Service for the pseudonymization of electronic healthcare records based on ISO/EN 13606 for the secondary use of information," *IEEE J. Biomed. Health Informat.*, vol. 19, no. 6, pp. 1937–1944, Nov. 2015.
[209] M. L. Rustad and T. H. Koenig, "Towards a global data privacy standard," *Fla. L. Rev.*, vol. 71, p. 365, Jan. 2019.
[210] *Article 9 GDPR*. Accessed: Dec. 2022. [Online]. Available: https://privacy-regulation.eu/it/9.htm
[211] F. T. Jaigirdar, C. Rudolph, and C. Bain, "Risk and compliance in IoT—Health data propagation: A security-aware provenance based approach," in *Proc. IEEE Int. Conf. Digit. Health (ICDH)*, Sep. 2021, pp. 27–37.

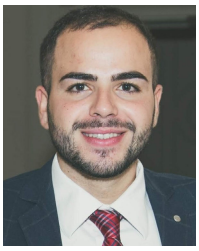
[212] P. Lombardi, "Sicurezza dei dati in ambito sanitario ed evoluzione tecnologica tra passato, presente e futuro," *Diritto Dell'economia*, vol. 3, pp. 49–82, Jan. 2021.
[213] C. Di Stato. (Apr. 8, 2019). *Sezione VI, N 2270*. [Online]. Available: www.giustizia-amministrativa.it
[214] (2022). *Temi in Evidenza*. Accessed: Jul. 27, 2022. [Online]. Available: https://temi.camera.it
[215] J. Ahmed, T. N. Nguyen, B. Ali, A. Javed, and J. Mirza, "On the physical layer security of federated learning based IoMT networks," *IEEE J. Biomed. Health Informat.*, early access, May 10, 2022, doi: 10.1109/JBHI.2022.3173947.

CHIARA SURACI received the M.Sc. degree in telecommunications engineering and the Ph.D. degree in information engineering from the University Mediterranea of Reggio Calabria, Italy, in 2018 and 2022, respectively. She is currently a Postdoctoral Researcher with the Department of Information, Infrastructure and Sustainable Energy (DIIES), University Mediterranea of Reggio Calabria. Her current research interests include 5G/6G networks, device-to-device (D2D) communications, network security, virtualization technologies, and eHealth services.

VINCENZO DE ANGELIS received the B.S. degree in information engineering and the master's degree in telecommunication engineering, in 2017 and 2019, respectively. He is currently pursuing the Ph.D. degree in information engineering with the University Mediterranea of Reggio Calabria, Italy. He is the author of a number of papers published in international journals and conference proceedings. His research interests include information security, blockchain, cloud, and applied cryptography. He was a PC member of a number of conferences and a guest editor of a special issue in an international journals.



GIUSEPPINA LOFARO received the degree (cum laude) in law, in 2008. She received the Ph.D. degree in law and economics, curriculum public economic law, in 2020. Since 2010, she has been a Specialist for the Legal Professions. Since 2012, she has been a Lawyer. In 2017, she was a Technical-Legislative Innovator at the Chamber of Deputies on University, Research, and Health. She is currently a Research Fellow in administrative law with the Department of Information, Infrastructure and Sustainable Energy (DIIES), Mediterranean University of Reggio Calabria. She has authored on Anvur Class A Scientific Journals on: *Administrative Procedures and Processes*, health law, publicly owned companies, federalism, and sustainable development. She is a member of the editorial board of scientific journals and a speaker at academic conferences.



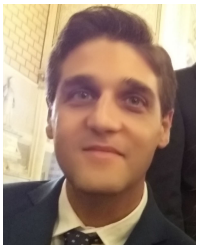
MICHELE LO GIUDICE received the B.S. degree in information engineering and the master's degree in telecommunication engineering, in 2017 and 2019, respectively. He is currently pursuing the Ph.D. degree in biomarkers of chronic and complex diseases with the Department of Medical and Surgical Sciences, University of Catanzaro. He is currently working with the iCare Project, Department of Information, Infrastructure and Sustainable Energy (DIIES), University Mediterranea of Reggio Calabria, for the implementation of a eHealth platform. Recently, he was a Visiting Ph.D. Fellow at the Imperial College London, U.K., under the supervision of Prof. D. Mandic. His current research interests include machine learning, deep learning, and biomedical signal processing, especially EEG signals analysis of patients affected by neural disorders.

GIUSEPPE MARRARA received the Laurea degree (cum laude) in civil engineering and the Ph.D. degree in environmental engineering from the Mediterranean University of Reggio Calabria, Italy, in 1999 and 2005, respectively. He worked for 20 years in the eHealth field in the role of product and sales manager, gaining an in-depth experience in clinical and biomedical engineering. He is currently a Research Fellow with the Department of Information, Infrastructure and Sustainable Energy (DIIES), University Mediterranea of Reggio Calabria. His research interests include digital health, the IoMT, and eHealth platform and applications.

FEDERICA RINALDI received the Ph.D. degree in information engineering, in 2021. She is currently a Research Fellow with the University Mediterranea of Reggio Calabria, Italy. In 2019, she spent six months at Ericsson Research, Finland, where she worked on satellite and non-terrestrial networks (NTNs) in 5G and beyond technology. Her current research interests include NTNs, radio resource management, device-to-device (D2D) communications, and multimedia broadcast/multicast service in 5G/6G networks. She received the 2022 Scott Helt Award for the Best Paper published in the IEEE TRANSACTIONS ON BROADCASTING.

ANTONIA RUSSO received the Ph.D. degree in information engineering from the University Mediterranea of Reggio Calabria, in 2022. She is currently a Postdoctoral Researcher with the University Mediterranea of Reggio Calabria. Her research interests include security, privacy, access control, and social network analysis.

MARTINA TERESA BEVACQUA was born in Reggio Calabria, Italy, in 1988. She received the Laurea degree (M.S. equivalent) (summa cum laude) in electronic engineering and the Ph.D. degree in information engineering from the University Mediterranea of Reggio Calabria, Italy, in July 2012 and May 2016, respectively. She is currently working as an Assistant Professor with the University Mediterranea of Reggio di Calabria within a tenure track position. Her research activity mainly concerns electromagnetic inverse problems, with particular interest in: 1) inverse scattering problems from both a theoretical and applicative point of view; 2) field intensity focusing and shaping in non-homogeneous and unknown scenario, in the framework of hyperthermia treatment planning, wireless power transfer and MRI shimming. She was a recipient of the G. Barzilai Award from the Italian Electromagnetics Society, in 2014, while in March 2016, she received the Honorable Mention from IEEE-Antennas and Propagation Society (Central and Southern Italy Chapter) in the Best Student Member Paper Competition. Moreover, she was also a recipient of the URSI Young Scientist Award, in 2018.



GIANLUCA LAX (Member, IEEE) received the Ph.D. degree in computer science from the University of Calabria, in 2005. In 2018, he got the Habilitation as a Full Professor of computer science. Since 2018, he has been the Coordinator of a master's degree in information technologies for telecommunications engineering. He is currently an Associate Professor of computer science with the University Mediterranea of Reggio Calabria, Italy. He is the author of more than 150 papers published in leading international journals and conference proceedings. His research interests include privacy, information security, and social network analysis.

NADIA MAMMONE received the Laurea degree (M.S. equivalent) in electronic engineering and the Ph.D. degree in informatics, biomedical, and telecommunications engineering from the Mediterranea University of Reggio Calabria, in 2003 and 2007, respectively, with a dissertation that was awarded the Caianiello Prize from the Italian Neural Networks Society (SIREN). From 2014 to 2018, she was a Principal Investigator at the IRCCS Centro Neurolesi Bonino-Pulejo, Messina, Italy, of a research project on advanced EEG processing, funded by the Italian Ministry of Health. Formerly, she was a Postdoctoral Fellow in biomedical and electrical engineering at the Department of Civil Engineering, Energy, Environment and Materials (DICEAM), Mediterranea University of Reggio Calabria. She was a Visiting Ph.D. Fellow at the Computational NeuroEngineering Laboratory (CNEL), University of Florida, Gainesville, FL, USA, in 2005 and 2008, and a Visiting Postdoctoral Fellow at the Communication and Signal Processing Research Group, Department of Electrical and Electronic Engineering, Imperial College, London, U.K., in 2015. She is currently an Assistant Professor with the DICEAM Department, Mediterranea University of Reggio Calabria. Her research interests include deep learning, brain–computer interfaces, neural and adaptive systems, biomedical signal processing, and information and complex network theory. In 2022, she received the Hojjat Adeli Award for Outstanding Contributions in Neural Systems, awarded annually by the World Scientific Publishing to the most innovative scientific research published in the previous year. She is currently an Associate Editor of *Frontiers in Neuroscience-Neural Technology*.

ANTONINO MAZZA LABOCCETTA graduated in law from the University of Rome La Sapienza. He received the Ph.D. degree in administrative law from the University of Catania. He was a Researcher of administrative law. He is currently a Lawyer, an Associate Professor of administrative law, and a Lecturer in public contract law and town planning law with the Department of Law, Economics and Human Sciences, University of Mediterranean Studies of Reggio Calabria. He is the author of publications, including monographs, articles, sentence notes, essays in collateral volumes. He was awarded by the President of the Republic Oscar Luigi Scalfaro for his university commitment.

FRANCESCO CARLO MORABITO (Senior Member, IEEE) is currently a Full Professor of electrical engineering and neural engineering with the University Mediterranea of Reggio Calabria, Italy. He has served as the Dean of the Faculty of Engineering, from 2001 to 2008, a Vice-Rector for Internationalization from 2013 to 2022, and the Deputy Rector from 2017 to 2018. He has authored or coauthored over 400 papers in international journals/conference proceedings in various fields of engineering (machine/deep learning, biomedical signal processing, radar data processing, nuclear fusion, nondestructive testing and evaluation, and computational intelligence). He has coauthored less than 20 international books (mostly focused on neural networks and machine learning) and held five international patents. He has been a Foreign Member of the Royal Academy of Doctors, Spain, since 2004. Since 2017, he has also been a member of the Institute of Spain, Barcelona Economic Network. He is a Senior Member of INNS, in 2006. He serves as a Governor of the International Neural Network Society (INNS), from 2022 to 2024, and earlier for 12 years, from 2000 to 2012. He is an Editorial Board Member for various international journals, including the *International Journal of Neural Systems*, *Neural Networks*, *International Journal of Information Acquisition*, *Sensors*, *Clinical EEG and Neuroscience*, and *Renewable Energy*. He has served as the President of the Italian Neural Network Society (SIREN), from 2008 to 2014. He is the Co-Chair of the Italian Conference on Neural Networks (WIRN).

GIUSEPPE ARANITI (Senior Member, IEEE) received the Laurea and Ph.D. degrees in electronic engineering from the University Mediterranea of Reggio Calabria, Italy, in 2000 and 2004, respectively. He is currently an Associate Professor of telecommunications with the University Mediterranea of Reggio Calabria. His major research interests include 5G/6G networks and it includes personal communications, enhanced wireless and satellite systems, traffic and radio resource management, multicast and broadcast services, device-to-device (D2D), and machine-type communications (M2M/MTC).