Computer Science Review 45 (2022) 100494

Contents lists available at ScienceDirect

Computer Science Review

journal homepage: www.elsevier.com/locate/cosrev

Review article

The future of computing paradigms for medical and emergency applications

Daria Alekseeva [a], Aleksandr Ometov [a,*], Otso Arponen [b,c], Elena Simona Lohan [a]

[a] Electrical Engineering Unit, Tampere University, Tampere 33720, Finland
[b] Department of Radiology, Tampere University Hospital, 33520 Tampere, Finland
[c] Department of Radiology, School of Clinical Medicine, University of Cambridge, Hills Rd, Cambridge CB2 0SP, United Kingdom

ARTICLE INFO

Article history:
Received 7 January 2022
Received in revised form 4 July 2022
Accepted 13 July 2022
Available online 5 August 2022

Keywords:
Computing paradigms
Medical and emergency services
Wireless communications
Electronic healthcare
Smart healthcare
Standardization

ABSTRACT

Healthcare is of particular importance in everyone's life, and keeping the advancement of it on a good pace is a priority of any country, as it highly influences the overall well-being of its citizens. Each government strives to build a modern, intelligent medical system that provides maximum population coverage with high-quality medical services. The development of Information and Communication Technologies (ICT) significantly improves the accessibility and effectiveness of the healthcare system by forming the eHealth environment, thus, providing an opportunity to enhance the quality of patient care and significantly speed up the work of medical experts and reduce costs for medical services. Shifting medical services to digital and remote operations requires a lot of computational capabilities. Implementing new computing paradigms is prominent — remote services face new requirements due to the increasing data and demand for new computing solutions. Computing paradigms, e.g., Cloud, Edge, Mobile Edge Computing, besides others, are used to process the collected medical data, improving patient healthcare quality. This paper focuses on computing solutions for medical use cases by offering a comprehensive survey on standardization aspects, use cases, applicable computing paradigms, security limitations, and design considerations within the ICT usages for medical applications. Finally, it outlines the most critical integration challenges and solutions from the literature.

Contents

[*] Correspondence to: Tampere University, P.O. Box 1001, FI-33014, Finland.
E-mail address: aleksandr.ometov@tuni.fi (A. Ometov).

https://doi.org/10.1016/j.cosrev.2022.100494

1. Introduction

Health is one of the most valuable assets in each person's life. Modernizing the eHealth services in line with the current technology developments might bring many benefits to society. Research advances in noninvasive health monitoring are based on the newly emerged computing solution, e.g., body computing [1]. The development of computing paradigms is expected to improve Quality of Service (QoS) and provide on-demand service in any place on Earth, even in hard-to-reach areas.

Most countries are aiming to build an intelligent eHealth system that enables high-quality medical service and, at the same time, optimizes the medical staff's work. Naturally, it is necessary to develop the eHealth network applications to meet future healthcare needs. In 2020, F. Froes introduced a new term for mankind – 2020-nMan [2] being a person who prefers remote health care to personal visits in a hospital even after the COVID-19 pandemic [3]. With the COVID-19 pandemic, people have realized all the advantages and potential shortcomings of telemedicine and the possibility of providing medical health care remotely. This worldwide situation has shifted the human perspective on medical services. Now, a quick response from the doctors and getting the laboratory testing with minimal human interaction is prioritized as never before.

Due to the pandemic of 2020–2022, many organizations have been forced to operate remotely, which increased the popularity of digital services. To keep the health-providing organizations afloat, the product owners and governments have been in demand of new Information and Communication Technology (ICT)-based services. In turn, it has pushed health organizations to scale their digital capabilities significantly by, i.e., harnessing Cloud solutions. One of the Cloud benefits is rapid scalability on-demand, making it relatively easy to adapt and promoting cost savings [4].

Simultaneously, the number of wearable devices by the end of the second decade of XXI century reached 237 million, according to the estimation of International Data Corporation (IDC) [5]. Experts forecast even more growth of Internet of Things (IoT) devices in the oncoming years [6]. The winning solution of effective data operation is the deployment of Edge and Cloud computing architectures, which is another reason why offloading data to the Cloud (i.e., processing the data outside the device) is a promising direction.

The apparent advantage of a Cloud Computing (CC), or Cloud, is the enormous computing capacity due to the potent use of various Data Centers. Paradigms, where computing provides a short processing delay to the user, are mostly applicable for delay-sensitive scenarios. Edge and Mobile-Edge Computing (MEC) perform computational tasks at the edge of the network (closer to the end-consumer user), while Fog works with a group of Cloud-like servers still deeper in the infrastructure but as close as it could be to the user [7]. A prerequisite approach for modern computing paradigms is mobility support, which is inherent in Mobile Cloud Computing (MCC) or MEC. Since the mobile or IoT devices have a limited battery life, MCC computes in the cloud rather than on the mobile device itself [8].

The average response time of the computing paradigms consists of a few main component namely the time spent for the communication and computing time itself [9]. The computing time depends on the infrastructure energy and computing capacity. Cloud paradigm is so far the winning paradigm among existing ones in terms of computational power because it can use computing powers at levels not affordable on the user device or at the edge network. Nonetheless, the Cloud paradigm loses delay sensitivity overall end-to-end latencies to paradigms with close-to-user infrastructure, which happens because the time spent to the communication is shorter in Edge/Fog computing paradigms than in the Cloud. Therefore, optimizing the communication time will highly influence the system latency. That is why the communication part is crucial to be taken into consideration and optimized while designing new computing architectures.

The development of the communication systems plays a significant role in emergency services as well. The probability of preventing the death of a patient in need of urgent care depends on the journey distance to the hospital or nearest emergency unit [10]. By providing reliable communication to the first responders, such as ambulances, firefighters, police, their quality of service can be improved, which, in turn, correlates to the number of saved lives, see Fig. 1. The following communication technologies provide a quick and qualified response to emergencies, competing in coverage, bit rate, reliability, and latency. PMR technologies based on digital Narrowband (NB) standards such as Trans-European Trunked Radio (TETRA), TETRAPOL, TETRA Enhanced Data Service (TEDS), Project 25/Project 34 (P25/P34), or Digital Mobile Radio (DMR) [11]. Each country has set its Public Protection and Disaster Relief (PPDR) standard for PMR technologies, e.g., DMR (Europe), Next Generation Digital Network system (NXDN) (Japan), Broadband Trunking Communication (B-TrunC) (China), and others.

The quick and extremely high growth of mobile devices supported by broadband with high-speed internet access will require the development of the PMR standards for broadband operations. High-resolution videos are becoming increasingly critical for real-time local awareness and intelligence-driven decisions.

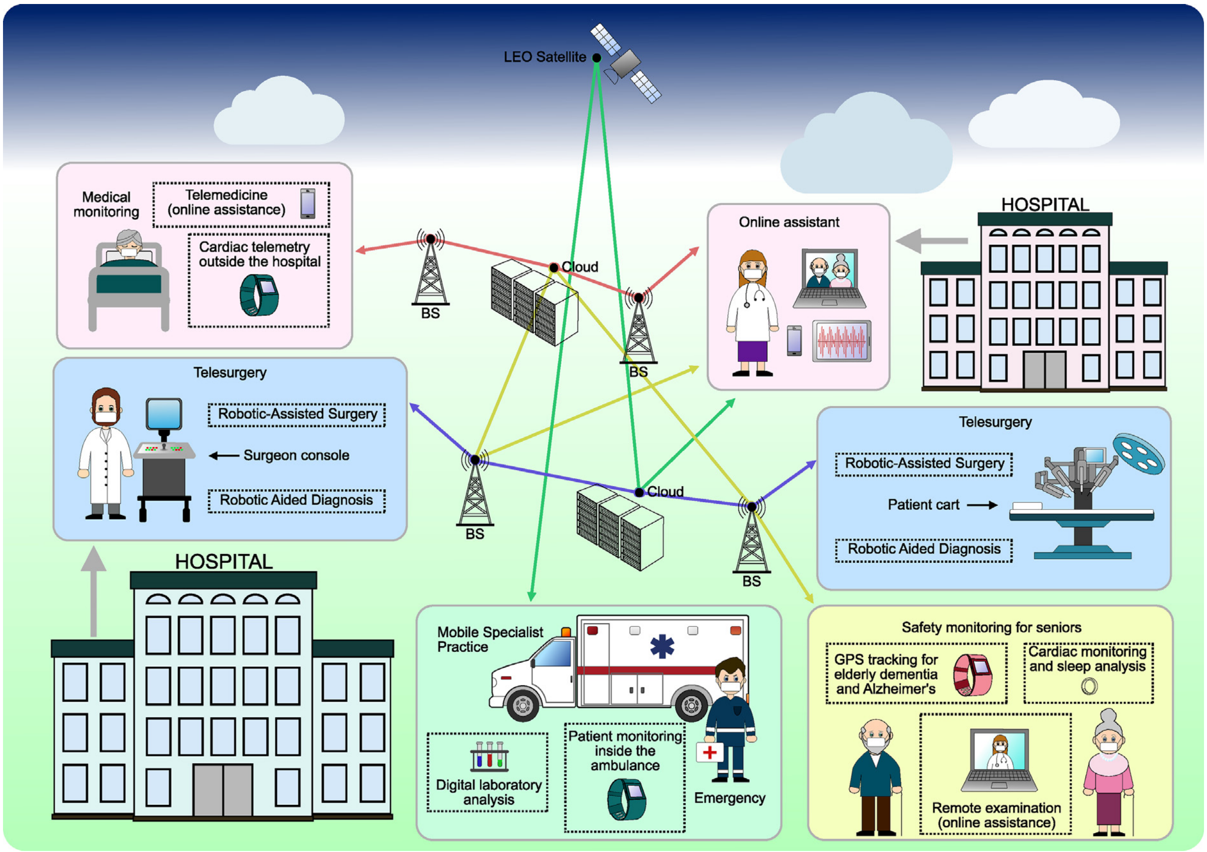

LEO Satellite
Medical monitoring
Telemedicine (online assistance)
Cardiac telemetry outside the hospital
BS
Cloud
BS
Online assistant
HOSPITAL
Telesurgery
Robotic-Assisted Surgery
Surgeon console
Robotic Aided Diagnosis
BS
Cloud
BS
Telesurgery
Robotic-Assisted Surgery
Patient cart
Robotic Aided Diagnosis
HOSPITAL
Mobile Specialist Practice
Digital laboratory analysis
Patient monitoring inside the ambulance
Emergency
Safety monitoring for seniors
GPS tracking for elderly dementia and Alzheimer's
Cardiac monitoring and sleep analysis
Remote examination (online assistance)

Fig. 1. The computing ecosystem suitable for modern and future medical applications.

Long-Term Evolution (LTE) might be qualified to support the emergency applications that are requiring high-resolution photos and video imaging. 5th Generation Network (5G) currently provides the best services for IoT devices, which is also successfully utilized in the medical sphere. The declared parameters support the energy-efficient connection of a large number of devices and provide a high traffic capacity, communication with very low latency below 1 ms, and ultra-high reliability [12].

There are various standardization organizations determining the upcoming technological development directions: Digital Imaging and Communications in Medicine (DICOM), Third Generation Partnership Project (3GPP), European Telecommunications Standards Institute (ETSI), International Telecommunication Union (ITU), etc. Specifically, DICOM is specialized in required quality digital images for medical devices. ITU's main purpose is to facilitate international connectivity. It determines the requirements for PPDR technologies. 3GPP is a partnership project between seven standardization organizations aiming to provide specifications for cellular communications, e.g., on-going 5G developments and future 6th Generation Network (6G) design. ETSI is a European standardization body that provides communication and networking standards in Europe. ETSI standardized TETRA, TEDS, DMR.

This article surveys the literature over the period 2010–2022 on the computational offloading strategies and related wireless technologies used for medical and emergency healthcare services as well as briefly touches the related information security aspects. We are addressing, in a comprehensive manner and for the first time in the literature, to the best of the Authors' knowledge, the following three research questions (RQs):

RQ1: What are the technical requirements for the medical and emergency-service use cases in terms of computing paradigms and architectures?
RQ2: Where to locate the computing resources to achieve the best performance, by considering multi-dimensional target optimization criteria, of remote medical use cases?
RQ3: What are the promising technological directions for mobile/remote eHealth services in the long-term future?

To answer the research questions thoroughly, we have identified the following steps:

- To identify the requirements for the medical use cases through the standardization outlook.
- To identify existing computing paradigms and map the use cases to those.
- To identify and compare the advantages and disadvantages of each computing paradigm.
- To highlight the main challenges and overview the potential solutions found in the literature.
- To offer a long-term outlook on the most promising computing paradigms for the healthcare domain.

The paper's novelty comes from three main directions: (i) offering a unified and comprehensive survey of computing paradigms applicable in the healthcare domain and emergency services; (ii) offering a structured view of the standardization efforts of ICT usages in the medical field domain; and (iii) providing a long-term future outlook of ICT architectures and computing paradigms for medical and emergency services.

The paper is structured as follows. Section 2 provides the standardization outlook as the motivation of this work. It gives a brief description of the existing specifications and technical reports, covering the requirements for emergency services and medical use cases, identified in the corresponding documents. Next, Section 3 surveys the existing computing paradigms and their applicability to medical and emergency use cases as well as in the case of disaster relief, which is closely related to emergencies. Further, Section 4 focuses on the communication outlook for emergency response. Further, Section 5 provides the outlook on Cloud-, Edge-, and Fog-like systems security and data privacy aspects of related computing systems. Finally, Section 6 identifies major challenges and limitations related to computing paradigms, and discusses the potential future directions that could be improved in the nearest decades. The last section outlines the summary of this paper's main findings and takeaways.

2. Standardization outlook

This section provides a review of specifications & regulations and collects the main technical recommendations for various medical applications and emergency services. The normative documents have been declared by ETSI, ITU, 3GPP, DICOM, European Committee for Standardization (CEN), and National Health Service, England (NHS). Next paragraphs provide a few sentences about each of the standardization bodies.

ETSI is an European Standards Organization (ESO), whose standards also recognized as European Standards (ES) in telecommunication, broadcasting, and networking. Established in 1987, nowadays ETSI is a primary recognized regional standards body in Europe, which supports the EU legislation and regulations through the building of Harmonised European Standards [13].

ITU is a United Nations agency that was founded in 1865 and is specialized on developing the technical standards for international connectivity in communications networks [14].

3GPP was initially aimed to develop technical specifications for 3rd Generation Network (3G), cellular telecommunications, and Universal Mobile Telecommunications System (UMTS) [15]. 3GPP partners are seven standardization bodies from Asia, Europe, and North America. They are Association of Radio Industries and Businesses, Japan (ARIB) [16], Alliance for Telecommunications Industry Solutions, USA (ATIS) [17], Telecommunications Standards Development Society, India (TSDSI) [18], Telecommunications Technology Association, Korea (TTA) [19], Telecommunication Technology Committee, Japan (TTC) [20], ETSI [13], China Communications Standards Association (CCSA) [21].

DICOM is the international standard for the required quality medical images and is implemented in different medical devices. DICOM revolutionized medicine by replacing the X-ray film with digital imaging in 1993 [22].

CEN is a wide network of technical experts both from industry and academia that represents European organizations, associations, governmental bodies, and other authorities to provide a target level of quality, and it closely collaborates with International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) [23]. ES and EU regulations of the European Parliament must be followed in their entirety across the EU.

The following subsections elaborate on the standards related to the medical domain, while Table 1 compactly lists these documents and provides their brief description.

2.1. Overview on 3GPP standards

3GPP TS 22.104 specifies the requirements for suitable support of various use cases of cyber–physical control applications (or so-called vertical applications) [24]. Those require a high level of communication service availability and low end-to-end latency. The conventional wireless communication technology for vertical applications was real-time Ethernet. The specification provides the communication service performance requirements for industrial wireless sensors. Implementation of 5G in the medical industry is stated to allow access to highly professional medical services remotely from different locations, e.g., Robotic Aided Surgery or Robotic Aided Diagnosis.

3GPP TS 22.261 outlines the recommendations for the system Key Performance Indicator (KPI) [25]. 5G system provides better performance of various excited and new services and heterogeneous traffic than former cellular systems such as 2nd Generation Network (2G) – 4th Generation Network (4G). 5G services include managing Unmanned Aerial Vehicle (UAV), Augmented Reality (AR)/Virtual Reality (VR), the control of critical medical automation, and enhancement Mobile Broadband (MBB) that are require to support huge data rates. A 5G system should also be able to provide the Low Earth Orbit (LEO) satellite access with the following service requirements: the end-to-end latency is 35 ms maximum with the 99.99% of communication service availability. In the medical domain, health monitoring requires highly-available IoT traffic. This specification shows that the Narrowband-IoT (NB-IoT) requires 2 kb/s, Downlink (DL) and 10 kb/s, Uplink (UL) data rate for the moving device with speed to 100 km/h. Public safety scenarios require 3.5 Mb/s, DL/UL data rate for the moving equipment with the same speed.

3GPP TS 22.263 gives requirements to professional audio, video, and imaging applications [26]. The high-quality video performance gives a significant advantage in the surgery, minimizing the invasiveness of the operation. It is expected that all equipment inside the Operating Room (OR) will be synchronized and perform the allowed latency according to the 5G system recommendations. There are two possible scenarios of the medical team and patient distribution: first, when the patient and medical specialists are located in the same room, and second when they are located in different places, e.g., telesurgery. In the first use case, communication services are delivered by a 5G system over Non-Public Network (NPN), while in the second case — over Public Land Mobile Network (PLMN). Both scenarios have their requirements that are written in [26].

3GPP TS 23.167 describes the emergency services in the IP Multimedia Core Network Subsystem (IMS) [27]. There are expectations on the IP Connectivity Access Network (IP-CAN) for IMS emergency services. Among the requirements, we mention: the prioritization of emergency services traffic, the free-of-charge emergency-service support, and the access granting of the emergency numbers to the User Equipment (UE). *ETSI TS 123 167* is similar to the *3GPP TS 23.167* and it provides the same IMS requirements [28].

3GPP TS 23.401 sheds light the Mobility and Access Restrictions for Emergency Services, Policy and Charging Control (PCC), and Reachability Management for UE [29]. Local regulations require an emergency connection to the end device in an accident or disaster. They also require emergency sessions to be provided regardless of mobility or access restrictions. When the E-UTRAN Radio Access Bearer (E-RAB) for emergency unidirectional links is set, the Allocation and Retention Priority (ARP) value for emergency unidirectional services indicates the use of emergency services for the Evolved Universal Terrestrial Radio Access Network (E-UTRAN).

3GPP TR 22.826 mainly focuses on critical medical applications [42]. Implementing a 5G system is aimed to improve the

Table 1
Overview of regulations and normative documents applicable to the emergency cases.

Ref.	Official title	The first release	Main contents of the documentation
[30]	Rep. ITU-R M.2014-3 digital land mobile systems for dispatch traffic	January 1998	Characteristics (technical and operational) for spectrum-efficient digital dispatch systems
[31]	CEN/TC 239 EN 1789:2006 Medical vehicles and their equipment. Road ambulances	October 1999	Requirements related to road ambulances (for the transport and care of patients), in terms of design, testing, performance, and equipment
[32]	ETSI TS 102 164 V1.3.1 (2006-09) Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Emergency Location Protocols	April 2003	Protocol specifications for local emergency operators to obtain the positioning information
[33]	ETSI TR 102 299 V1.3.1 (2013-07) Emergency Communications (EMTEL); Collection of European Regulatory Texts and orientations	April 2004	The regulatory principles applicable to Emergency Communications
[27]	3GPP TS 23.167 V17.0.0 (2021-03) IP Multimedia Subsystem (IMS) emergency sessions (Release 17)	October 2005	Emergency services description for the IMS, including the supporting elements for IMS emergency services and IMS emergency services for eCall
[34]	ETSI TS 102 181 V1.2.1 (2008-02) Emergency Communications (EMTEL); Requirements for communication between authorities/organizations during emergencies	November 2005	The requirements for communications between the authorized units involved in the emergency responses/actions
[29]	3GPP TS 23.401 V17.0.0 (2021-03) General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 17)	December 2006	Mobility requirements between cellular radio access technologies, e.g., E-UTRAN and pre-E-UTRAN 3GPP, as well as policy control/charging and authentication mechanisms
[35]	ITU-T E.107 (02/2007) Emergency Telecommunications Service (ETS) and interconnection framework for national implementations of ETS	February 2007	Definition of the Emergency Telecommunications Service (ETS) needed to enable ETS wireless communications between authorized units
[36]	ETSI TR 102 476 V1.1.1 (2008-07) Emergency Communications (EMTEL); Emergency calls and VoIP: possible short and long term solutions and standardization activities	August 2008	Focus on standardization activities and methods for Voice over IP (VoIP) providers to deliver wireless emergency services
[37]	ETSI TR 102 764 V1.1.1 (2009-02) eHEALTH; Architecture; Analysis of user service models, technologies and applications supporting eHealth	February 2009	User service models in eHealth for the identification of interoperable solutions for healthcare data transmission and storage
[28]	ETSI TS 123 167 V9.4.0 (2010-03) Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Subsystem (IMS) emergency sessions	January 2010	The description of the emergency services in the IMS, including the elements necessary to support IP Multimedia (IM) emergency services
[38]	ETSI EN 302 663 V1.2.1 (2013-05) Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band	January 2010	The protocol stack for supporting Vehicle-to-Vehicle Communication (V2V) in an ad hoc network to be used at the 5.9 GHz frequency band
[39]	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016	April 2016	The regulation on the protection of natural persons concerning the processing of personal data and the free movement of such data
[25]	3GPP TS 22.261 V18.2.0 (2021-03) Service requirements for the 5G system (Release 18)	August 2016	The requirements that define a 5G system, such as support for multiple access technologies, scalability, resource efficiency, availability, latency, reliability, etc.
[40]	ETSI TR 103 394 V1.1.1 (2018-01) Smart Body Area Networks (SmartBAN); System Description	January 2018	The Smart Body Area Network (SmartBAN) system description
[24]	3GPP TS 22.104 V18.0.0 (2021-03) Service requirements for cyber–physical control applications in vertical domains (Release 18)	August 2018	The real-time Ethernet requirements for 5G vertical applications
[41]	NHS National ambulance vehicle specification for English NHS ambulance trusts	October 2018	The national ambulance vehicle specification for English NHS ambulance trusts
[42]	3GPP TR 22.826 V17.2.0 (2021-03) Study on Communication Services for Critical Medical Applications	November 2018	Recommendations on 5G services targeting the critical medical applications and enabling wireless connectivity between those applications and medical devices
[26]	3GPP TS 22.263 V17.3.0 (2020-12) Service requirements for video, imaging, and audio for professional applications (VIAPA) (Release 17)	August 2019	The service and performance requirements for the professional video, audio, and imaging applications via a 5G system
[43]	DICOM Standards Committee Supplement 202: Real-time video	September 2019	Recommendations for the transport of real-time video, audio, and other medical-related data
[44]	3GPP TR 22.839 V0.2.0 (2021-03) Study on Vehicle-Mounted Relays (Release 18)	November 2020	The new requirements for 5G support of mobile base station relays mounted on vehicles

healthcare delivery models and to shift to outpatient services to reduce administrative and supply costs. The [42] document presents the performance requirements for the communication, security, clock synchronization, and network services. In addition, the document identifies four modalities of medical scenarios based on the distance between the patient and the patient and the speed of moving the equipment. These are discussed in more detail further in Section 2.4.

3GPP TR 22.839 shows the potential new requirements for 5G support of mobile Base Station (BS) relays mounted on vehicles, using 5G New Radio (5G NR) over the radio links towards UE and macro Radio Access Network (RAN) [44]. The high-level deployment scenario includes moving vehicles equipped with a small on-board BS relays providing 5G coverage and communication to UE (inside the vehicle or in its vicinity) and connected in a wireless manner to the 5G network via macro RAN (donor) nodes. One of the use cases is the optimization of the relay for medical devices in an ambulance. For devices in ambulances, where UE could be pre-installed or have a fixed location, the exact position inside the vehicle, relative to the BS relay, can also be identified. The 5G system will support mechanisms to optimize mobility, e.g., re-selection or handover, and energy efficiency for a UE camped or connected via a vehicle mobile BS relay, e.g., for UE located inside a vehicle, equipped with a BS relay.

2.2. Overview on ETSI standards

ETSI TS 102 181 describes the requirements for communications between the authorized bodies operating in the emergency situation [34]. The rapid interaction of authorized representatives is directly related to the number of lives saved during a disaster. The number of authorized representatives directly depends on the nature of the emergency. Crisis teams or temporary headquarters will be organized in some cases. Additional resources will allow the organization of a mass event and, if necessary, include several centers' help or additional levels of third-party units in the rescue plan (such as administrative bodies and associations or private operators).

ETSI TS 102 164 discusses the application-level protocol design to obtain mobile stations location independently of the location-awareness technology and bearer for emergency location information services [32]. The document does not provide the details about the operation of the existing network but rather the general procedures for higher levels of abstraction.

ETSI TR 102 476 summarizes different methods for VoIP providers to offer emergency communication services [36]. Over time, the quantity of broadband mobile phones has significantly increased. A circuit-switched network is not able to handle a massive amount of calls, unlike a packet-switched network, a fact also reflected by the transition to full packet-switched operation in cellular systems starting with 4G as well as transition to new possibilities of the routing from Internet Protocol (IP) networks. The IP networks met new requirements to support the Emergency Services. For example, it is essential to define the IP interface for Public Safety Answering Points (PSAP).

ETSI TR 103 394 describes the SmartBAN system level, also defines possible use cases for SmartBAN [40]. SmartBAN is a network of actors performing some health monitoring through, for example, wireless wearable devices. The modern health equipment needs to meet strict technical requirements in energy efficiency, co-existence with other systems, QoS, short-time access. Among the potential use cases for SmartBAN are safety and fall monitoring (an alert signal reports to care workers if the patient feels physically sick), sleep/apnea monitoring, stress monitoring, monitoring of the blood pressure fluctuations or abnormal cardiac rhythms, and monitoring of sports activities.

ETSI TR 102 299 provides the executive summary of Emergency Communications (EMTEL) relevant data from EU normative documents [33]. The rapid development of the market in Europe and the emergence of new decentralized communication technologies require a revision of the regulations in the communications sector in the EU. It brings many new challenges that relate to the need for a high level of support from emergency communications systems and the continuous improvement of the efficiency of the responsible authorities in such situations. The purpose of the [33] document is to contribute to a stricter standardization in this field by bringing together various standardization rules in the EU.

ETSI TR 102 764 describes several eHealth user service models to identify compatible solutions for collecting and storing health-monitored data [37]. It defines the requirements for the security and reliability of the entire e-health system and supporting ICT technologies. The document indicates where further standardization is needed in ICT to support eHealth.

ETSI EN 302 663 highlights the physical and the link layer in the protocol stack for V2V in the 5.9 GHz band in the European ad-hoc network [38]. The technology defined for the access layer is referred to as Intelligent Transportation System (ITS)-G5. The ITS-G5 standard uses existing communication standards, which is based on IEEE 802.11.

2.3. Overview on other standards

Report *ITU-R M.2014-3* consists of the digital dispatch systems technical characteristics [30]. The development of the spectrally-efficient radio technologies using digital modulation is relevant to meet the high demand for PMR technologies and new demands for communications services, such as high-speed data service in response to PMR. The [30] document provides the description and core characteristics of TETRA, TEDS, P25/P34, TETRAPOL, Digital Integrated Mobile Radio Service (DIMRS), Frequency Hopping Multiple Access system (FHMA), Code-Division Multiple Access (CDMA)-Public Access Mobile Radio (PAMR), B-TrunC, Global open Trunking architecture (GoTa), and Enhanced Digital Access Communication System (EDACS).

ITU-T E.107 gives recommendations for the international cooperation authorities' work in the case when disaster geographically occupied the territories of different countries [35]. There is a potential that countries may enter into multilateral agreements for the emergency systems interconnection.

DICOM Standards Committee Supplement 202: Real-Time Vide describes several new DICOM IODs and associated transfer syntax for transferring real-time video, audio, and other associated medical data [43]. The corresponding supplement also specifies a new IP-based DICOM service for the broadcasting of real-time video to subscribers with a quality of service which is compatible with the communication inside the OR.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 is based on the claim that the protection of personal data is a fundamental right [39]. It gives the regulation in personal data protection, EU controllers administrations, defines the restriction personal data processing methods, etc., which has always been relevant and remains one of the most challenging tasks being critical in the medical domain. Sensors and wearables that record personal health data should stay private and safe.

CEN/TC 239 EN 1789:2006 "Medical vehicles and their equipment. Road ambulances" defines the requirements for equipping ambulances for transporting and monitoring injured or ill patients [31]. The mobile intensive care engine must be fully equipped to provide advanced medical treatment and pre-hospital care. The requirement states that all ambulances should be equipped with a mobile radio transceiver and internal communication between driver and patient compartment.

NHS National ambulance vehicle specification for English NHS ambulance trusts is a national medical vehicle specification that all defines the system for providing evidence in any collision [41]. The document also provides the requirement for designing, testing, and equipping ambulances at the national level for English NHS ambulances. The vehicle demands to be equipped with a channel recorder that can record vehicle Global Positioning System (GPS) speed and to provide a 4G/Wireless Fidelity (Wi-Fi) connection to view live images and download recorded footage.

Table 1 provides a summary at-a-glance of the discussed regulations and normative documents applicable to emergency and medical-domain use cases. The documents are sorted in chronological order, and the last column summarizes the main scope of each document. Nonetheless, Table 2 depicts a systematic representation of the main covered topics covered in every regulation.

2.4. Identified use cases and applications

Implementation of ICT in the healthcare domain is one of the results of global growth, improving the treatments and holding economical potential [45]. ICT-enabled healthcare services are expected to reduce geographic disparities in access to the medical care providers and improve the efficiency of the healthcare delivery. Shifting medical treatment to the digital and remote way of operation requires high communication reliability, channel capacity, and a lot of computational capabilities. Interconnection of a large number of various medical devices makes the communication architecture even more complex. Implementing new computing paradigms is prominent — remote services face new requirements due to increasing data and demand for giant computing capabilities.

The motivation for creating this subsection was to define scenarios for which the requirements are standardized in the paragraphs above (see Sections 2.1, 2.2, 2.3). The present section provides an overview of some of the integrated medical use cases in the healthcare system. The executed requirements for the medical use cases have been reviewed and summarized at-a-glance in Table 3. There are four scenarios, defined as: "static – local", "moving – local", "static – remote", and "moving – remote" [42]. The first two ("local") modalities cover use cases when the medical team and patients are collocated (e.g., OR, AR Assisted Surgery, Robotic Aided Surgery, cardiac telemetry inside the hospital). The other two ("remote") modalities refer to the situations when medical staff and patients are located in different places, e.g., first pre-hospital help in the ambulances, telesurgery, mobile specialist practice equipment, monitoring/providing continuous care to injured patients in a moving ambulance, cardiac telemetry outside the hospital. "Static" modalities indicate scenarios where the equipment does not change location over time, e.g., Robotic Aided Surgery. In contrast, "moving" modalities cover use cases where the equipment is mobile, i.e., wearable IoT devices for cardiac telemetry inside/outside the hospital.

Notably, Table 4 reviews some of the integrated examples of ICT in healthcare. These examples are successfully used in international medical practice nowadays or analyzed by researchers as promising oncoming ones. After analyzing those, it could be concluded that we are currently knocking at the door of future eHealth, as there is already an opportunity to identify the major driving use-cases, i.e., remote patient monitoring, robotic assisted surgery, telemedicine, and many others, being already integrated in different countries.

Nowadays, Wearable Health Devices (WHD) have become very common in healthcare facilities [46]. Remote monitoring of the patient's health is an emerging wireless technology for collecting the patient's vital signs in real-time and transmitting the collected data to the attending physician or representative to monitor the patient's physical condition [47]. For this purpose, WHD is being used to obtain/measure e.g., temperature, Electrocardiogram (ECG), Respiratory Rate (RR), Blood Pressure (BP), Blood Glucose (BG) and Oxygen Saturation (SpO_2) [48]. In hospitals, vital signs monitoring is essential for, e.g., heart failure care and faster recovery [46,49]. In senior homes, where residents have memory problems and other chronic diseases, monitoring the person's location is critical. For this, bracelets with built-in geo-positioning are used [50,51]. In addition, wireless electronics can alert the attendant of a senior's sleep disturbance, feelings of unwellness, and alert of the falls of an elderly resident [52]. A significant advantage of using wearables to control the BG is found in people with diabetes mellitus. The standard method of blood glucose monitoring includes invasive blood extraction. Non-invasive blood glucose monitoring has become a reality with the rapid development of WHD and biosensors [53,54]. Less-invasive glucose measurements for persons with diabetes significantly improve their life quality [55].

The ICT implementation and the robotic systems' development in the surgical field allow an operation to be carried from a further distance. The first and only complete telesurgery, also known as remote surgery, was conducted in 2001 with the patient based in Strasbourg, France, and a robotic console in New York, USA using ZEUS-TS surgical system [56]. The robotic setup lasted 16 min, and the surgery was performed in 54 min. The distance between the patient and surgeon's robotic console was more than 14,000 km, and the transmission latency during the procedure was 155 ms which is imperceptible to the human eye [57]. It was a milestone that clarified the global advantage of telemedicine — anyone could receive the appropriate high-quality medical service in any place in the world [58]. Robotic-assisted surgery, where the surgeon controls the robotic arms sitting by a console away from the patient and the operating table, is an important method in multiple surgical disciplines, including thoracic surgery [59], urology [60], and gynecology [61], as it allows improved dexterity in comparison to Conventional Laparoscopy (CL) and 3D visualization instead of CL's 2D visualization [62]. Robots have a massive benefit in the surgical process, as their less invasive approach requires smaller cuts, and they are also able to pass through narrow canals to reach the diseased organ [63].

Off-site teleradiology, i.e., remote interpretation of radiological images outside of the imaging unit, has the promise of improved quality of care and services by lessening the geographic and temporal discrepancies in imaging care [64–66]. Another similar use case is the remote ultrasound examination, which provides real-time, high-quality images obtained under the guidance of a remote expert [67,68].

These, and other examples of the integrated use cases, are presented in Table 4. The further section discusses the most appropriate computing paradigm, e.g., Cloud, Edge, Fog, etc., for each of the medical scenarios.

3. Computing outlook

This section discusses various computing paradigms and computing solutions for medical scenarios. The idea to compute data remotely has reshaped the computing world.

The middle of the 20th century marked the beginning of the Cloud era. At first, people used terminals – a massive device that consisted of a monitor and keyboard, to connect to the heavy mainframe shared by many users. After that, computers became much more powerful and gave enough resources to satisfy users' daily work. Also, the technological developments reached the level when the local networks allowed multiple computers to connect, which started the Internet era. The idea that users could utilize remote resources through the Internet connection aligned with the development of distributed systems. This new concept allowed users to increase the computing power and storage resource, which brought many advantages in using remote applications.

Cloud paradigm has shifted the Internet industry and has provided all available resources on the Internet in a scalable and simple way which has brought the researchers to investigate new concepts based on the idea of on-demand remote services [95]. Two of the first and most successful examples are Salesforce, where a customer runs software remotely using the provider's infrastructure (Software-as-a-Service (SaaS)), and Amazon Web

Table 2
Overview of aspects from the regulations and normative documents related to the emergency cases.

Ref.	Specification	Comms. Sync.	Latency	Security and privacy	Positioning	Real-time video	Application reqs.	Multicast reqs.	QoS	5G reqs.	Energy-efficiency	Emergency calls	Vehicle reqs.	UAV reqs.	Wireless ITS infrastructure	Satellite access	BAN reqs.
[24]	3GPP TS 22.104 V18.0.0	✓	✓		✓				✓		✓						
[25]	3GPP TS 22.261 V18.2.0		✓					✓	✓	✓				✓		✓	
[26]	3GPP TS 22.263 V17.3.0					✓				✓							
[27]	3GPP TS 23.167 V17.0.0											✓					
[29]	3GPP TS 23.401 V17.0.0	✓						✓				✓					
[42]	3GPP TR 22.826 V17.2.0		✓	✓		✓	✓	✓		✓							
[44]	3GPP TR 22.839 V0.2.0				✓												
[34]	ETSI TS 102 181 V1.2.1		✓	✓									✓				
[32]	ETSI TS 102 164 V1.3.1																
[28]	ETSI TS 123 167 V9.4.0											✓					
[33]	ETSI TR 102 299 V1.3.1											✓					
[36]	ETSI TR 102 476 V1.1.1											✓					
[40]	ETSI TR 103 394 V1.1.1																✓
[37]	ETSI TR 102 764 V1.1.1	✓		✓													
[38]	ETSI EN 302 663 V1.2.1	✓													✓		
[30]	Rep. ITU-R M.2014–3	✓															
[35]	ITU-T E.107											✓					
[39]	EU REG. 2016/679			✓													
[31]	CEN/TC 239 EN 1789:2006												✓				
[41]	NHS vehicle specification												✓				

Table 3
Performance requirements.

	Use case	Ref.	Characteristic parameter					Influence quantity					Computing location
			Availability [%]	Reliability/lifetime	Latency [ms]	Bit rate	Direction	Message size [byte]	Survival time [ms]	UE speed [km/h]	Number of UE	Service area	
Static – local	Duplicating video on additional monitors	[42]	>99.99999	>1 year	<1	120 Gbits/s	UL	∼1500 – ∼9000	8	0	1	100 m^2	Network edge
	UHD medical video over NPN	[26]	>99.99999	>1 year	<1	<50 Gbit/s	UL; DL	∼1500 – ∼9000	∼8	0	1	100 m^2	N/A
	AR Assisted surgery	[42]	>99.99999	>1 year	<0.75	30 Gbits/s; 12 Gbits/s	UL	∼1500 – ∼9000	8	0	1	100 m^2	Short network distance from the operating room.
	Robotic aided surgery	[42]	>99.99999	>1 year	<2	240 Gbits/s	UL; DL	∼1500 – ∼9000	8	0	1	100 m^2	Short network distance from the operating room.
		[24]	>99.999999	>10 years	<2	2–16 Mbit/s	UL; DL	250 – 2000	1	0	1	Room	Edge or Cloud
Moving – local	Cardiac telemetry inside hospital/care facility (body-worn IoT device)	[42]	99.99999	>1 year	<100	0.5 Mbit/s	N/A	≤1000	100	≤5 km/h	≤1000 per 1 km^2	Hospital (incl. elevators)	N/A
Static – remote	Emergency care — Ultrasound examination and remote interventional support	[42]	99.99	>1 month	<20	25 Mbits/s	UL	∼1500	∼100	0	<20 per 100 km^2	<50 km	N/A
	Mobile specialist practice	[42]	99.99	>1 month	<250	2 Gbit/s	UL	∼1500 – 9000	∼16	0	<20 per 100 km^2	∼0.1 km	N/A
	Telesurgery	[24]	>99.9999	>1 year	<20	2–16 Mbit/s	UL; DL	250 – 2000	1	0	<2 per 1000 km^2	National	Edge or Cloud
		[42]	>99.9999	>1 year	<20	2 – 16 Mbit/s	UL; DL	250 – ∼2000	∼1	0	<2 per 1000 km^2	<400 km	Cloud
	Ultra-High-Definition (UHD) video for telesurgery over PLMN	[26]	>99.9999	>1 year	<20	<6 Gbit/s	UL; DL	∼1500 – ∼9000	∼16	0	<2 per 1000 km^2	<400 km	N/A
	Robotic aided diagnosis	[24]	>99.999	>1 year	<20	2–16 Mbit/s	N/A	80	1	0	20 per 100 km^2	<50 km	Edge or Cloud
	UHD video for medical examination over PLMN	[26]	>99.99	>1 month	<20	<4 Gbit/s	UL; DL	∼1500 – 9000	∼16	0	<20 per 100 km^2	<50 km	N/A
Moving – remote	Patient monitoring inside ambulances	[42]	99.99	>1 month	<100	25 Mbits/s	UL	∼1500	∼100	150	<20 per 100 km^2	<50 km	N/A
	Cardiac telemetry outside the hospital (body-worn IoT device)	[42]	99.9999	>1 year	<100	0.5 Mbit/s	N/A	≤1000	<1000	≤500	Hospital: 1000 per 1 km^2; Suburban: 10 per 1 km^2	Country wide	Hospital cloud
	General medical/safety monitoring	[25]	>99.9999	>1 year	<100	<1 Mbit/s	UL	∼1000	50	<500	10 – 1000 per 1 km^2	Country wide	N/A
		[40]	N/A	N/A	10	640 bps – 16 kbps	UL	N/A	N/A	N/A	N/A	Country wide	N/A

UL — Uplink DL — Downlink N/A — not available in the corresponding document.

Table 4
Examples of integrated scenarios with a relation to ones discussed in the standardization documents.

Scenario	Country	Description	Ref.
Monitoring health status	Canada	The remote guided examination and mentor control	[67,68]
	United Kingdom	Ultrasound imaging across network of hospitals	[69]
	Australia	ECG, RR, SpO_2 monitoring while the patient remains active without the restriction of being attached to a bedside cardiac monitor	[70]
	Finland	Remote cardiac monitoring by detecting, recording and wirelessly transmitting the full recorded ECG information to the internet	[48]
	United Kingdom	Wear of wristband on every admitted to hospital patient	[71]
	USA, Bulgary, Canada	BioSigns ambulance telemonitoring in the most urgent conditions	[72]
	USA	Equipping ambulances with medical monitors, pulse oximeters, and anesthesia machines for when emergency anesthesia needs to be administered before arrival to the hospital	[73]
	United Kingdom	Advanced telemetry systems: transport monitor for all intra-hospital transport needs, wireless patient bedside monitoring system, tools to visualize alarm workflows and manage clinical data, etc.	[74]
	USA	Remote monitor health status that includes remote evaluation and diagnosis of sleep disorders, record client's heart rate and activity such as steps walked, monitor chronic or post-discharge conditions	[47]
	Finland	Using wearable safety devices at senior houses for real-time wellbeing monitoring and automatic calling for help	[52]
Robotic assisted surgery	China	Minimally invasive surgery for removing kidney due to the cancer	[75]
	Russia	Endoscopic surgery of joints	[76]
	USA	Minimally invasive bariatric surgery	[77]
	USA	Comprehensive surgical services	[78]
	United Kingdom	Open heart surgery	[79]
	Korea	The use of Robot-Assisted Laparoscopic Radical Prostatectomy (RALRP)	[80]
	Korea	Laparoscopic robotic surgery performed by Revo-i	[81,82]
	Germany	Tumor therapy, kidney transplantation, and plastic reconstructive urology	[83]
	Japan	Artificial joint replacement	[84]
Robotic aided remote diagnosis	Canada	Remote examination thought AR (Google Glass)	[85,86]
Telemedicine (online assistant)	New Zealand	Virtual patient consultations via video	[87]
	Japan	Remote consultations via telephone or video link	[88]
	Malaysia	Online solutions reachable via chat or phone	[89,90]
GPS tracking	USA	GPS tracker for Elderly, Dementia, and Alzheimer's	[50,51]
AR/VR systems to patient care and rehabilitation	Russia	VR systems (high motivating, challenging movement rehabilitation in a virtual environment presented by screen or head-mounted display)	[91]
	USA	AR system (Google Glass and Augmedix software) to improve patient care, enhance physician workflow and reduce physician burnout	[92]
Digital labs	Germany	Environments allowing for fostering the digital health community to stimulate new innovation projects; mentoring/coaching; supporting the launch and growth of digital health spin-offs in cooperation with partners	[93]
	United Kingdom	CaRi-Heart® Technology to detect underlying risks of possible heart disease using Artificial Intelligence (AI)	[94]

Services (AWS) [96]. In 2006, Amazon announced a web service named Amazon Elastic Compute Cloud (Amazon EC2) that provides quick scale compute capacity in Amazon's environment on an as-needed basis and at-commodity prices [97]. CC was presented at the conference in the same year by Google [98]. Other companies, such as Microsoft and IBM, started to announce Cloud services.

3.1. Primordial computing paradigms

In 2011, the National Institute of Standards and Technology, USA (NIST) published an official paper where Cloud was defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [4]. Thus, Cloud was defined as a powerful data center consisting of several nodes connected with a high-speed channel. The Cloud hierarchy consists of two levels: the end-user and the data center (user-Cloud), where the main requirement is to have a stable connection with the Internet. The main goal for the Cloud service providers is to allocate the node for the user's task computation to be completed, and the data remains safe.

The physical layer in the Cloud architecture consists of servers, network equipment, and storage devices. The lowest layer of the Cloud operating system consists of physical infrastructure drivers and cloud drivers for communication with the hardware and connecting to other external clouds. The core of the Cloud Operating System (OS) consists of a virtual machine manager, a network manager, a storage manager, etc [99]. The top of the OS system includes various management tools — administrator tools, service manager, scheduler, cloud interfaces. The client is connecting to the server through this Cloud interface.

Table 5
Main aspects of computing paradigms and related medical scenarios.

Comp. paradigm	Organizational structure	Comp. location	Comp. latency	Comm. latency	Most suitable medical applications	Ref.
Cloud	Centralized	Data center	Very low	Very high	Robotic aided surgery, robotic aided diagnoses, cardiac telemetry inside/outside the hospital	[100]
Edge	Centralized	Closest power-independent network edge node	Varying	Low	AR assisted surgery, robotic aided surgery, robotic aided diagnoses	[104,105]
Fog	Highly decentralized	Distributed collaborating Cloud-like nodes	Low	Varying	AR assisted surgery, robotic aided surgery, robotic aided diagnoses, patient monitoring, telemetry	[106,107]
MCC	Centralized	Data center	Very low	Very high	Cardiac telemetry inside/outside the hospital	[8,108]
Mobile ad-hoc Cloud Computing (MACC)	Decentralized	Group of devices	Low	Varying	Robotic telesurgery, mobile specialist practice in disaster relief, group live video streaming, UAV	[109]
MEC	Centralized	Edge of the network	Varying	Low	Robotic aided surgery, ultra-sound examination, patient monitoring	[110,111]
LEO network's Edge Computing (LEC)	Decentralized	LEO satellite	Varying	Very high	Robotic telesurgery, mobile specialist practice in disaster relief or in a hard-reach areas	[112]
Dew Computing (DC)	Decentralized	Close to end-device (IoT)	Very low	Very low	Cardiac telemetry, medical monitoring	[113,114]

The primary idea of the first computing paradigm was to forward data to the Cloud for analysis. For example, the IoT-Cloud platform was primarily used for voice pathology monitoring. The information collected from local sensors is sent to the Cloud, which is processed efficiently. The Machine Learning (ML) algorithms detect voice pathology, which is sent back to the doctor and patient [100]. Karaca et al. proposed to use the Cloud concept for the Stroke Healthcare System due to the limited mobile phone parameters [101]. Cloud supports Big Data analyses, accessibility from any platform, and fast computational speed because of the high computational power. With the rapid rise of the wearables, sensors, and IoT devices, requirements have become stricter and stricter in terms of mobility support, geo-distribution, location-awareness, and latency [7]. Therefore, the computational core has been shifted in new paradigms, e.g., Edge and Fog computing, to reduce the distance between the end device and the server.

Fog Computing (FC) is a distributed computing infrastructure that runs the computational capabilities close to the user yet still in the Cloud-like manner, and this allows to store and process data with lower latency, better location-awareness, and with higher QoS than Cloud paradigm for real-time applications [102].

Edge Computing is a paradigm aimed at the data center to be located at the "edge" of the network, i.e., in close proximity to the user, and it provides computing offloading, data storage, and data processing services [103].

Technically, these two paradigms are relatively similar with some definition disagreements between FC and Edge in terms of processing location and types of used hardware [115]. Both FC and Edge bring data processing nodes closer to the user, with the only difference being that the Edge device should be the first node in the Internet network. In contrast, the FC node proximity depends on the available servers. The Edge hardware includes devices that generate and receive data, e.g., sensors, smartphones, servers, while FC's hardware is only server-based. Edge provides the computation on the end network servers, while Fog processes the data at the local-area network-level computing.

Table 5 shows the main aspects of the mentioned Computing paradigms. CC provides a centralized computation on the remote server (or the Data Center) with a clear focus on the client and can process an enormous amount of data. Edge and FC are decentralized paradigms where the computation is shifted closer to the ground: edge servers in the Edge paradigm and the local-area servers in the Fog. Fig. 2 illustrates the connection scheme of and principle differences of them. There are similar concepts such as MCC, MEC, and MACC, which have overlap with Cloud, Fog, and Edge computing with the difference that the end device should have full mobility.

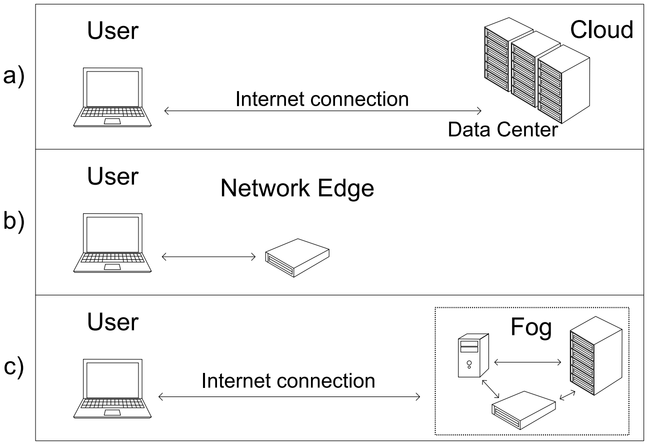


Fig. 2. Most common task offloading models.

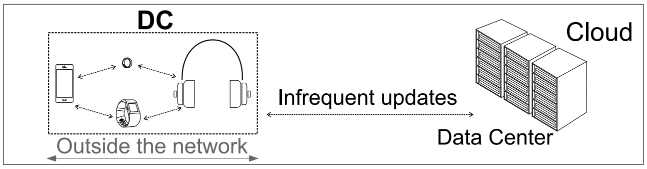


Fig. 3. Dew Computing – computation on wearables outside the network.

Shifting the computing even closer to the end-user emerged the new post-cloud paradigm, named DC or Personal Cloud [116].

The concept of DC is to locate the computation in closer proximity than Edge and Fog when it is out of the Internet network (outside the "edge") illustrated in Fig. 3. Even though, the DC architecture assumes to be outside of the Internet, it can collaborate with the Cloud [113]. New characteristics of DC are synchronization with servers on higher layers, and independent servers work in the higher architecture layers since the link to them is not constant [117]. The proposed by Brezany P. et al. automatic analysis framework for breath gas analysis and brain damage restoration is based on Cloud-Dew architecture [118]. The activity analysis could continue even if some of the Cloud nodes fail to be considered the main advantage of the DC approach, and leads us to the next group of the paradigms.

3.2. Computing for mobile devices

The interest in computing on mobile devices has grown exponentially originated due to the increasing number of smartphones and mobile devices. Concepts of mobile computing-like MCC, MACC, and MEC are similar to the Cloud, FC, and Edge paradigms, with the main difference that it performs on moving devices.

Seemingly, the most accessible and most affordable way is to provide computing on the device itself. High mobility and high security are maintained with local execution because this is the only equipment required. Nonetheless, the main drawback is the limit of battery and computing resources. In addition, local data processing is not suitable for real-time applications that require low latency, processing, and storage of large amounts of data. One possible solution is to process Big Data on a remote server with minimal device power consumption by introducing offloading techniques, e.g., MCC, where the computation is performed in the Cloud outside the mobile device.

Migrating the application from the mobile device benefits energy and storage capacity, thus, optimizing the execution process [119]. Data processing is performed on a remote resource-rich server, while the mobile device is connecting through wireless mobile communications [8]. In MCC, the resource-constrained mobile devices can leverage resource-rich cloud services which make the benefit of applications include crowdsourcing, healthcare, sensor data processing, and task offloading. Compared to the computing on the device, the MCC has an advantage in running heavy applications and increasing the energy efficiency of mobile devices. The worldwide ability of connection to the Internet makes the MCC have high availability. MCC complements mobile healthcare and emergency applications because of its advantages in reliability, scalability, and privacy [108,120].

MACC is a new type of MCC, mostly reminded of the FC paradigm. It is a mix of existing paradigms for the special purpose where the application is required high availability, high velocity, and the emergence of Big Data computation. Due to the lack of network infrastructure in the MACC paradigm, MACC mobile devices are responsible for routing traffic among themselves. MACC performs heavy computations by connecting several available mobile resources through an ad-hoc network for the creation of a supercomputing node. While MCC is tightly connected to the Cloud and requires data centers for computation, MACC performs data processing on networked mobile devices. MACC is suitable for disaster scenarios, group live video streaming or unmanned vehicles operation & control [109].

MEC is a paradigm where the server is running at the network edge (commonly, the network BS), applying the concepts of CC at a close distance to mobile users [110]. Benefits of MEC are the ability to run isolated from the rest of the network, access to local resources, short distance to a client, low latency, location awareness, and network data in real-time.

MEC is successfully used in latency-sensitive applications as it allows task overload to a nearby edge server and offloads from local devices. In this way, MEC expands the capabilities of Internet of Medical Things (IoMT) by providing sufficient computing resources. Ning Z. et al. designed a MEC-enabled 5G eHealth monitoring system for IoMT minimizing the system-wide cost, which depends on the medical criticality [111].

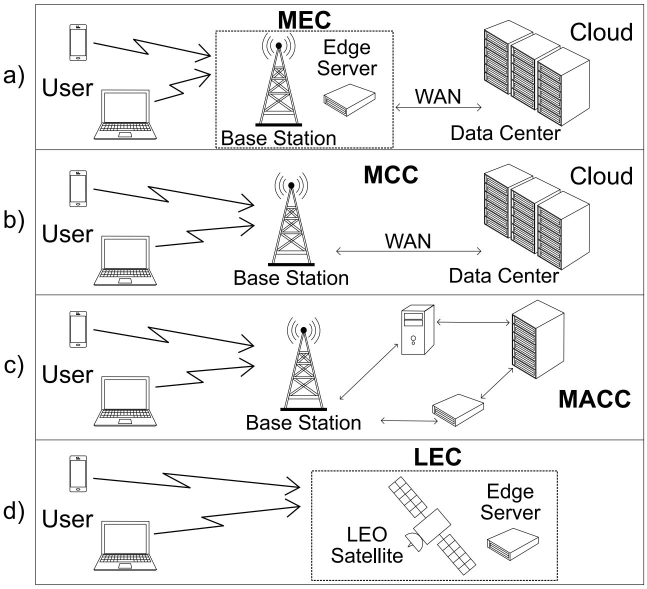


Fig. 4. Mobile computing paradigms.

With an increasing research interest in satellites, Li et al. proposed to integrate the Edge into LEO satellite network [112]. To name this new computing paradigm, the authors proposed a new term – LEC. Benefits of deployment Edge computing resource on LEO satellite, i.e., LEC, are reducing the number of inter-satellite links, wide bandwidth, and reducing the data processing delay compared to the Edge deployed in the ground. The proposed solution may help to relieve bandwidth in the LEO network but it anticipates several drawbacks. First, there is a need to integrate all the satellites' resources to provide satisfactory service because of the environment and limited satellite parameters. Second, there is a handover challenge caused by the high speed of satellites, and the devices often switch from one satellite to another. One of the possible solutions is to find an effective allocation scheme for computing resources implemented on the satellites [121]. Despite this, it is ideal for complex emergency scenarios, e.g., in the sea or high-mountains, where there are no base stations, and line-of-sight is poor.

This section discusses the concepts of various computing paradigms and their architecture, see Fig. 4. They have different characteristics that are shown in Table 5. The following subsection discusses the concepts of computing paradigms in medical applications. The subsection gives their prospects in the medical domain and discusses the upcoming challenges in this area.

3.3. Potential interoperability framework for computing paradigms and medical applications

Healthcare quality improvements are related to preventing medical errors, improved administration management, and affordable health care. Applications for the eHealth delivery in the emergency medical system are critical. In this paper, we made an effort to analyze and combine the work of different standard organizations. Therefore, we present a potential framework (see Fig. 5) and recommendations (see Fig. 6) for the application of

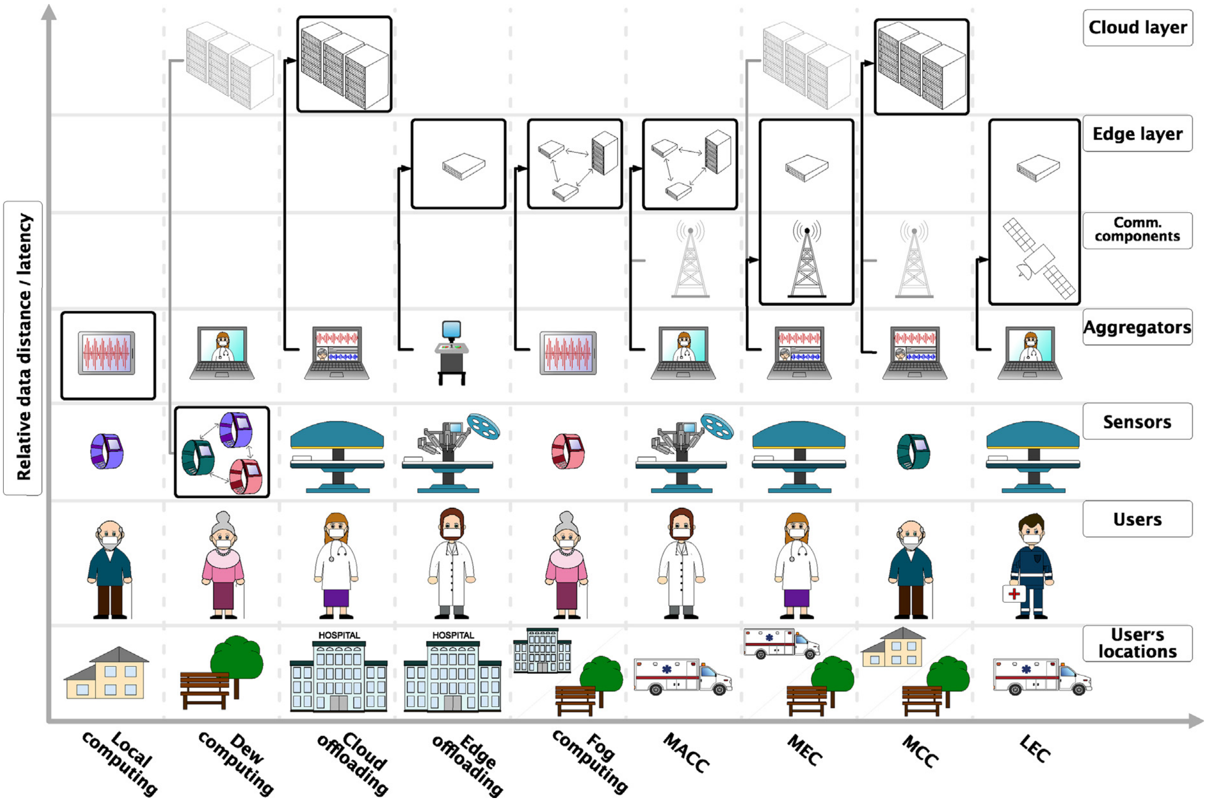
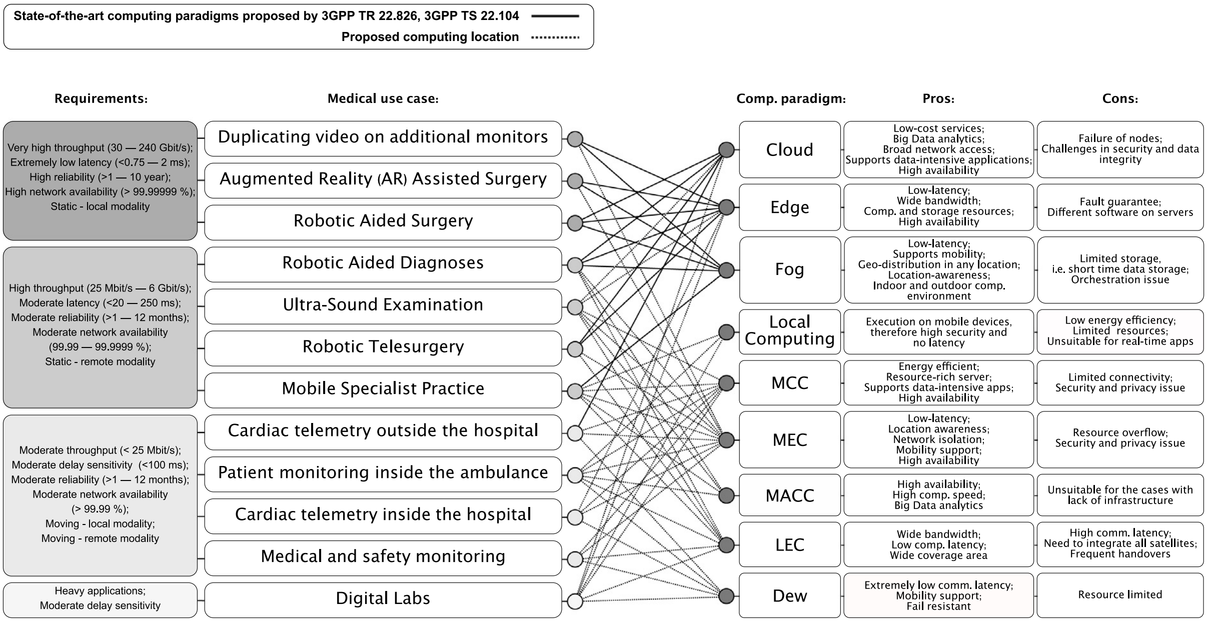


Fig. 5. Outlook on potential heterogeneous offloading framework in healthcare domain.


State-of-the-art computing paradigms proposed by 3GPP TR 22.826, 3GPP TS 22.104
Proposed computing location
Requirements:
Very high throughput (30 — 240 Gbit/s); Extremely low latency (<0.75 — 2 ms); High reliability (>1 — 10 year); High network availability (> 99.99999 %); Static - local modality
High throughput (25 Mbit/s — 6 Gbit/s); Moderate latency (<20 — 250 ms); Moderate reliability (>1 — 12 months); Moderate network availability (99.99 — 99.9999 %); Static - remote modality
Moderate throughput (< 25 Mbit/s); Moderate delay sensitivity (<100 ms); Moderate reliability (>1 — 12 months); Moderate network availability (> 99.99 %); Moving - local modality; Moving - remote modality
Heavy applications; Moderate delay sensitivity
Medical use case:
Duplicating video on additional monitors
Augmented Reality (AR) Assisted Surgery
Robotic Aided Surgery
Robotic Aided Diagnoses
Ultra-Sound Examination
Robotic Telesurgery
Mobile Specialist Practice
Cardiac telemetry outside the hospital
Patient monitoring inside the ambulance
Cardiac telemetry inside the hospital
Medical and safety monitoring
Digital Labs

Comp. paradigm:	Pros:	Cons:

Cloud	Low-cost services;
	Big Data analytics;
	Broad network access;
	Supports data-intensive applications;
	High availability
		Failure of nodes;
		Challenges in security and data integrity

Edge	Low-latency;
	Wide bandwidth;
	Comp. and storage resources;
	High availability
		Fault guarantee;
		Different software on servers

Fog	Low-latency;
	Supports mobility;
	Geo-distribution in any location;
	Location-awareness;
	Indoor and outdoor comp. environment
		Limited storage,
		i.e. short time data storage;
		Orchestration issue

Local Computing	Execution on mobile devices, therefore high security and no latency	Low energy efficiency;
		Limited resources;
		Unsuitable for real-time apps

MCC	Energy efficient;
	Resource-rich server;
	Supports data-intensive apps;
	High availability
		Limited connectivity;
		Security and privacy issue

MEC	Low-latency;
	Location awareness;
	Network isolation;
	Mobility support;
	High availability
		Resource overflow;
		Security and privacy issue

MACC	High availability;
	High comp. speed;
	Big Data analytics
		Unsuitable for the cases with lack of infrastructure

LEC	Wide bandwidth;
	Low comp. latency;
	Wide coverage area
		High comm. latency;
		Need to integrate all satellites;
		Frequent handovers

Dew	Extremely low comm. latency;
	Mobility support;
	Fail resistant
		Resource limited

Fig. 6. Potential computing paradigms in the medical domain..

computational paradigms in digital medicine. Fig. 5 shows a potential interoperability framework where computing paradigms are presented in components. Users, locations, and devices are taken as examples from the identified medical use cases, which are described above in Section 2.

Overall, Fig. 6 illustrates nine computing paradigms related to the various medical scenarios offering different benefits and disadvantages. The comprehensive list of medical use cases are divided into four according to the requirements. Solid lines connect the use case with the computing paradigm recommended or standardized by 3GPP. In the graphics, the dotted lines show the proposed computing locations for the use case according to the standards outlook and related literature.

Due to historical reasons, Cloud has a great potential to be utilized by emergency bodies making it easier for authorized persons to access relevant information wherever and whenever they need it [122]. CC has been used to create a flexible and scalable system that supports data-intensive applications. To all of the above, using the Cloud as online storage for Big Data with enormous computing power and ML implementation help to find complex diseases [100]. Cloud components consist of powerful Data Centers offering Big Data analysis, broad network access, and supporting data-intensive applications, providing broad network access with low-cost services. To summarize, proceeding data in Cloud is specified for the following medical use cases: Robotic Aided Surgery, Robotic Aided Diagnoses, cardiac telemetry outside the hospital, and Robotic Telesurgery.

Further, Edge significantly reduces storage requirements, maintenance costs, and energy consumption in the Cloud due to offloading. Since Edge is closer to the user, this paradigm provides a low latency service, wide bandwidth, and high availability. Edge computing consists of servers close to the users' location. Also, it uses devices on the network's edge that could generate and receive data, such as smartphones, servers, and sensors. Edge is recommended as the computing location in the case of duplicating video on additional monitors, AR surgery, Robotic Aided Surgery, Robotic Aided Diagnostics, and Robotic Telesurgery.

Like Edge computing, Fog shifts computational power closer to the user with the difference that it could be not only at the Edge. Fog provides computing at the local-area network on server-based devices. Fog Computing has benefits in low latency, mobility support, geo-distribution in any location, and location awareness. Moreover, reduced storage reduces the complexity of Big Data analysis and provides Cloud offloading, which may be still limited for Fog [107].

The newly emerged MCC is an extension of computing resources through the Cloud for mobile devices. MCC has benefits in supporting mobility and data-intensive applications, providing high network availability, rich resource servers, and energy efficiency [8,108]. MEC is a promising technology for future networks, where the computing location is pushed closer to the radio access. MEC supports mobility, delay-sensitive data provides location awareness and high-bandwidth access. It is suitable for use cases that could be defined as throughput-hungry, low latency or etwork availability demanding [110,111]. MACC is a mix of existing paradigms useful for applications requiring high availability, high velocity, and big data analysis [109]. It is suitable for the emergency scenarios such as disaster relief.

As for the most recent paradigms, LEC is Edge computing deployed on LEO satellites. Yet, LEC has several advantages: wide coverage, wide bandwidth, and fast computing possibilities. Nevertheless, the high cost of deployment as it requires integrating all satellites, high communication latency, and high risk of handovers because there is a need to often switch between satellites are this computing solution's drawbacks [112]. This paradigm could be applied to the use cases with a lack of terrestrial infrastructure, e.g., in the ocean or the emergency scenarios of a big disaster.

The number of IoT devices increases annually, affecting the amount of generated tasks and traffic itself. IoMT devices have limited computing and storage capacity, so the data could not be computed on the device. It became necessary to integrate Cloud with medical IoT. Integration DC, defined as computing closely to the IoT device, and Cloud could be applied in healthcare because this concept allows the hospital staff to monitor patient devices in remote with higher redundancy [118].

A detailed description of the system/framework for intelligent joint computing paradigms operation for providing qualified patient care is still foreseen as the major task of the standardization organizations. Thus, the goals of this paper are not to provide the framework as such, but a set of recommendations for the companies developing healthcare-related solutions based on offloading algorithms and, preferably, for further work of the authorities. The following section discusses an equally important part of the system — an overview of communication technologies.

4. Communication outlook

Efficient communication is critical to emergency management to provide quick response and save people's lives [123]. It is vital for remote work and disaster relief to provide a reliable and safe channel for the authorities offering the connectivity everywhere at any time. Traditional analog radio technologies can no longer satisfy the operational requirements, so digital mobile radio changed professional communication.

Initially, PMR was developed for private users to keep contact in short distances with a dispatcher at the same time became widely used by police, firefighters, ambulances, and other emergency bodies. The essential emergency digital services are divided into three types: teleservices, bearer services, and supplementary services, and each of them meets different communication requirements [30]. PMR teleservices offer the user a full range of options from secure calling and telephony to videotext and telex. Bearer services provide the capacity needed to transmit appropriate signals between two nodes, a minimum of 7.2 kb/s and 4.8 kb/s for unprotected and protected data, respectively. Supplementary services are other PMR technologies that provide priority calls, calls authorized by a dispatcher, ambiance listening, discreet listening, etc.

Traditional PMR communication systems are based on such standards as TETRA, TEDS, P25/P34, and other similar technologies. Table 6 shows the PMR technologies core parameters, such as carrier frequencies, carrier spacing, modulation, access method, and throughput. Presented in Table technologies use one of the following access methods: Frequency-Division Multiple Access (FDMA), Time-Division Multiple Access (TDMA), CDMA, FHMA.

4.1. Conventional PMR technologies

TETRA is an open standard for public safety telecommunication system developed by ETSI and operating on 25 kHz channelization in the bandwidth below 1 GHz [30]. TETRA is a virtual private network technology on the existing physical network shares among several emergency authorities. TETRA was designed to provide a high level of security, confidentiality, and privacy. It protects against the unauthorized reading of transmitted information, proving the true identity of the communicating parties and the network, permitting authorized monitoring of communications, uninhibited by the security mechanisms. The advantage of TETRA is that if the cellular network becomes unavailabe due to, e.g., the network overload, the dedicated communications may still be executed separately. TETRA has unique PMR services like Direct Mode Operation (DMO), high-level voice encryption for safety conversation, and full-duplex voice for PABX and PSTN telephony communications [124]. Nevertheless, TETRA has a considerable disadvantage in limited data rate.

P25/P34, or APCO-25, is a PMR standard for two-way radio communication developed in North America [127]. A key element of the P25/P34 technology is its ability to coexist with operational analog systems, enabling a graceful migration from analog to digital while maintaining an emphasis on interoperability and compatibility among conventional and trunked system implementations [30]. The main difference P25/P34 with TETRA is the wider area coverage with low population density.

TETRAPOL is a digital PMR technology for mission-critical public safety systems. TETRAPOL gives better protection against eavesdropping and offers better voice quality compared with analog PMR systems [125]. Also, it has the same advantage as TETRA over 2G/Global System for Mobile Communications (GSM), 3G/UMTS, 4G/LTE, 5G as they can collapse in a disaster because all base stations will be overloaded. TETRAPOL became the primary technology of communication for the federal and

Table 6
PMR technologies core parameters.

PMR technology	Carrier frequencies [MHz]	Carrier spacing [kHz]	Modulation	Access method	Throughput [kbit/s]	Ref.

TETRA	380–390/390–400;
	410–420/420–430;
	450–460/460–470;
	870–888/915–933
		25	π/4-DQPSK	TDMA	36	[30,124]

TETRAPOL	70–520; 746–870; 870–888/915–933	10; 12.5	GMSK	FDMA	8	[30,125]

TEDS	380–390/390–400;
	410–420/420–430;
	450–460/460–470;
	870–888/915–933
		25; 50; 100; 150	π/4-DQPSK;
			π/8-DQPSK; 4-QAM;
			16-QAM; 64-QAM
				TDMA	150	[30,126]

P25/P34	136–200; 360–520; 746–870	12.5; 6.25	C4FM; CQPSK; QPSK; 16-QAM; 64-QAM	FDMA	9.6	[30,127]
DMR	30–1000	12.5; 20; 25	4FSK	TDMA	9.6	[128,129]
DIMRS	806–821/851–866	25	M16-QAM ($M = 4$)	TDMA	64	[30]

EDACS	136–174; 380–512;
	806–821/851–866;
	896–901/935–940
		25; 12.5	GFSK	FDMA	9.6	[30]

GoTa	410–415/420–425;
	452–457.5/462–467.5;
	806–821/851–866;
	824–849/869–894;
	1850–1910/1930–1990;
	1920–1980/2110–2170
		1230; 1250	QPSK; 8-PSK; 16-QAM	CDMA	9.6–153.6	[30]

NXDN	136–174; 380–512;
	806–821/851–866;
	896–901/935–940
		12.5/6.25	4FSK	FDMA	4.8/9.6	[30,130]

B-TrunC	1447–1467; 1785–1805;
	450–470;
	806–821/851–866
		15	QPSK; 16-QAM; 64-QAM	FDMA	25000/50000	[30]

FHMA	806–821/851–866; 896–901/935–940	25	π/4-SQPSK	FHMA	36.9	[30]

CDMA-PAMR	410–420/420–430;
	450–460/460–470;
	870–876/915–921
		1250	BPSK, QPSK, 8-PSK,
			16-QAM
				CDMA	1800/3100	[30]

state police forces to ensure security at the 2014 Fifa World Cup in Brazil [131].

TEDS is technology integrated with TETRA and developed by ETSI. It brings mostly the same core parameters as TETRA but with an advantage in a higher transmission rate (beyond 500 kb/s). The packet data throughput that is achieved for TEDS is based on the level of Quadrature Amplitude Modulation (QAM) modulation and the bandwidth. The initial bandwidth being offered by manufacturers is 50 kHz. The expected capabilities from TEDS were with the highest level of 64-QAM and throughput about 150 kb/s. It is not likely to be practicable and more likely giving a data rate of about 100 kb/s [126].

DMR is an open standard developed by ETSI for professional, commercial, and private radio users defining as a direct digital replacement for analog PMR. DMR uses the TDMA channel access method and 4FSK modulation scheme to provide a flexible and low-cost network for transmitting voice messages. DMR's implementation of TDMA offers 6.25 kHz spectrum efficiency per channel and provides the ability to deliver advanced features that professional users require [128].

Many countries have developed their implementations of PMR technology. DIMRS is one of the methods being used in North America to provide integrated dispatch services and increase spectrum efficiency. CDMA-PAMR is a digital Land Mobile Radio (LMR) technology utilizes VoIP developed by Telecommunications Industry Association, USA (TIA-US). This technology meets the demand for digital terrestrial communications services, including high-speed data and voice services, and offers significant opportunities for ad-hoc communications and public safety requirements. EDACS is two-way trunked radio standard carried by TIA-US and working in Very High Frequency (30 MHz–300 MHz) (VHF) and Ultra High Frequency (300 MHz–3 GHz) (UHF) frequency bands. It provides various capabilities from digital voice and digital data to encryption of digitized voice for emergency and civil calls. EDACS provides parameters that satisfy the requirements needs for public safety. GoTa is a professional trunking system developed by CCSA. It provides high voice quality and performance for professional and public access mobile radio services and offers a broad range of applications to satisfy public safety needs. B-TrunC is a professional trunking system developed in China that can be used PMR system supporting emergency call, voice group call, video group call, private voice call, private video call, etc. It operates in the bandwidths from 20 MHz down to 1.4 MHz. NXDN is an open standard for digital land mobile radio system developed in Japan in 2005. It is a narrowband digital radio system operating on 12.5 kHz or 6.25 kHz channel bandwidths in 800 MHz and 900 MHz frequency bands. Typical teleservices of NXDN system include individual call, group call, broadcast call, and interconnect call. FHMA is a system developed in Israel where the prime incentive for developing has been spectral efficiency. The achieved spectral efficiency makes it suitable for the PMR [30].

Integrating PMR with broadband systems becomes a solution for full connectivity in the disaster between emergency authorities, e.g., the complete interconnection between emergency teams and a wide range of providing teleservices [132]. Broadband access technologies are needed to achieve the target performance for emergency and medical services applications that

Table 7
Broadband technologies core parameters for medical communications.

Technology	Carrier frequencies [GHz]	Carrier spacing [MHz]	Supported modulation	Channel access methods	Achievable throughput	Target applications	Ref.
4G/LTE (3GPP Rel.8)	0.60–0.85; 1.7–2.6	5–20	π/2-BPSK, BPSK, QPSK, 16-QAM, 64-QAM	OFDMA, SC-FDMA	100–300 Mbit/s	Public safety, emergency calls	[55,134, 135]
5G (3GPP Rel.16)	<52	>100 MHz for <6 GHz, >400 MHz for >6 GHz;	π/2-BPSK, BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM	OFDMA, NOMA	10 Gbit/s	eHealth, public safety, transport services	[25,55, 135,136]
IEEE 802.11ac (Wi-Fi-5)	5	20, 40, 80, 160	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, OFDM	SDMA, CSMA/CA	6.9 Gbit/s	Ambulance management, transport services	[137]
IEEE 802.11ax (Wi-Fi-6)	2.4; 5	20, 40, 80, 160	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM	OFDMA	9.6 Gbit/s	Ambulance management, transport services	[137]
IEEE 802.11p (ITS-G5)	5.9	10	BPSK, QPSK, 16-QAM, 64-QAM	OFDMA	3; 6; 12 Mbit/s	Transport management, V2V	[38]

require real-time video, remote data access, and location awareness. Broadband wireless technologies for emergency and medical use cases are described in the following section.

4.2. Broadband wireless technologies for medical communications

The simultaneous operation of several multimedia applications is only possible due to increased bandwidth and high-speed data transmission capacity. For transferring high-resolution photos and videos, a high bit rate is required. High peak data rates, extended coverage, and localized coverage open up limitless new possibilities for broadband medical applications. Broadband access is also required to process data collected from a high-density sensor network and quickly update location information that meets the emergency application needs [132].

Due to the current massive advancement in LTE technology, it is considered as an up-and-coming candidate to serve the striving, tightly-constrained needs of Public Safety Network (PSN). LTE is capable of supporting the emergency services that require a high-quality photo, live video streaming, sensing, and tracking [133]. LTE is advanced in high-speed radio access for IP, but some standards developed to meet the PMR needs. There are some of them: development of secure algorithms, development of the standard for group communications including multicast voice and data, standardization of the voice quality that is compatible with TETRA, TETRAPOL, and P25/P34, standardization of access control and priority management, standardization of interworking with and providing TETRA, TEDS, P25/P34, and TETRAPOL PMR voice and data services over LTE, and others. Moreover, the development of a PMR standard for broadband operations will be required, including adopting LTE reference points for infrastructure, interoperability support, and standardization of Application Programming Interface (API) for control rooms [126].

At the state-of-the-art technology advancement 5G spectrum is divided into three broad bands: high-frequency band (mmWave), which support the highest 5G speeds; medium bands (1–10 GHz), which offer a good mix of coverage and capacity, and bands of up to 1 GHz, which help to provide reliable coverage over large areas and inside buildings [136]. 5G meets higher requirements than 4G in data rates, traffic density, user mobility, security, scalability, low latency, etc. All from the above expands the capabilities of different types of applications in more complex scenarios, including support of emergency calls and first responder operations, logistics, eHealth, Massive Internet of Things (mIoT), and aerial systems [138]. Under the development of next-generation 6G networks, the planning process is expected to be significantly faster and meet even more high requirements [139].

A group of standards *IEEE 802.11* defines the requirements for wireless technology known under the brand of Wi-Fi. One of the latest releases, *IEEE 802.11ac*, a.k.a., Wi-Fi-5 uses Orthogonal Frequency-Division Multiplexing (OFDM) access method in combination with Multi-user – Multiple Input Multiple Output (MU-MIMO) technology benefits to support multiple spatially separated clients, what was a breakthrough technology for 2013. In 2021, a successor of Wi-Fi-5 was approved being *IEEE 802.11ax* or Wi-Fi-6, which advantages higher network efficiency and reduced latency [137]. In combination with MU-MIMO and Beamforming technology, Wi-Fi-6 enable to exchange information up to 8 UE both UL and DL. Here, MU-MIMO and Orthogonal Frequency-Division Multiple Access (OFDMA) complement each other allowing one to work with applications with different throughput requirements. Later, this was standard amended and named Wi-Fi-6e, which is also working on 6 GHz. This frequency is not in Industrial, Scientific and Medical Radio Band (ICM radio band) in many countries, and therefore, this standard only operates in the USA as of today. Devices supporting Wi-Fi-6 are also applicable for the Wi-Fi-6e. Another Wi-Fi standard *IEEE 802.11p* offers the protocol stack for medical V2V communications in the 5.9 GHz that is referred to the *ETSI EN 302 663*, also known as the ITS-G5 [38].

Implementation of the broadband communication for an emergency is expected not to replace but extend the existing PMR capabilities. Future medical services will enable secure access in an interoperable manner of the existing technologies, ensure a required allocation of the network capacity to users, and provide a wide and reliable spectrum for medical applications [140]. The core parameters (carrier frequencies, carrier spacing, modulation, access method, and throughput) of the broadband wireless technologies described above that are used for disaster rescue and people's safety is presented in Table 7.

5G and beyond must support intelligent healthcare applications to fulfill high bandwidth and high energy efficiency requirements. Predictive analysis based on AI in healthcare can help

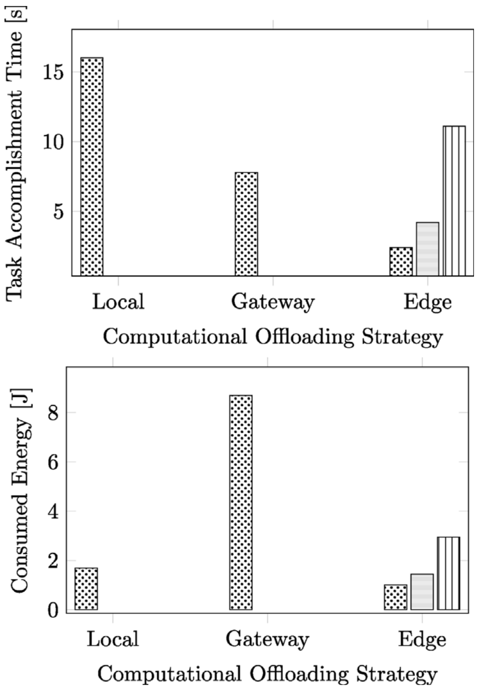


Fig. 7. Comparison of the offloading-originated metrics (Bars for Edge scenario correspond to distances [100, 300, 600] m).

physicians and medical experts make intelligent and effective decisions [141]. For example, a monitoring system capable of analyzing data from diabetic patients and sending emergency notifications based on 5G technology and ML algorithms will be helpful to doctors to track the patient's current status [55]. Implementation of ML is essential to achieve optimal routing for ambulances and provide a quick emergency response. Reliable communication between emergency authorities improves their management, optimizes safety operations, and improves the quality of their work. For example, using ML in the transport system may speed up the delivery of ambulances to the scene of the accident. AI algorithms based on the current state of traffic jams could find the most optimal and fastest route [142,143].

Interestingly, but there are no universal tools for modeling such complex systems. The majority of the analyzed works are mainly focused on either standalone systems analysis [144] while some authors attempt to utilize more general analytical approaches to understand the scenario with task or traffic saturation [145]. In the latter one, the authors propose to use the analytical system-level model to validate the assumption that MEC may perform better under computational-hungry task, e.g., offloading a video stream processing from the AR device to either more powerful mobile gateway or the network Edge. The communications from the end-device to the gateway are executed over IEEE 802.11n, while the communications from the gateway to the Edge/Cloud are done over the cellular link.

The energy consumption and task execution time analysis is executed for a fixed distance from the end-device to the gateway but varies for the Edge as the user is assumed to be mobile, see Fig. 7. Interestingly, the authors identify that offloading is always beneficial from the execution time perspective but may vary tremendously due to the propagation conditions. Therefore, the question of the efficient wireless technology enabler (as the major factor affecting the resource-constrained device energy consumption) remains an open prospect.

5. Security outlook in brief

As a standalone means to seamlessly integrate various medical computing paradigms, cloud providers' security and privacy concerns have become a major topic for storing and processing large amounts of data and critical applications while sharing those with their customers [146]. Currently, every paradigm of offloaded computation focuses on achieving a high level of the user privacy and preventing various attacks as well as maintaining the integrity of the data [147–149].[1]

From the privacy perspective, medical data has plenty of concerns due to its nature as the majority of the data collected through smart devices are personally-identifiable [150]. The major medical data privacy-related aspects are related to integrity, especially while malicious node or individual can directly influence the data processor or originator by means of infected hardware or software. As the built-in sensors in various medical devices collect personal information, the processing of data must comply with the privacy policy that should be standardized. Countries around the world have specific laws aiming at achieving the desired level of the citizens' data privacy. As of today in Europe, the main set of rules related to information security and privacy is General Data Protection Regulation (GDPR), thus, also covering the aspects of biomedical and personal data.

5.1. Cloud-related aspects

Most of today's medical systems are heavily focused on remote data storage and are leaning towards CC-related technologies due to various GDPR oriented issues. One of the special requirements of the CC is that services always provide a maintained level of consistency and reliability or up to 99.999% and beyond. Therefore, the main reason why medical centers are not rushing to support the rapid shift to the CC (and its various forms described in Section 3) lies in the data privacy and information security domains [151].

From the information security point of view, general CC uses different distributed models based on their specific requirements. That is one of the reasons why CC security and privacy threats vary tremendously depending on the infrastructure hosted in the Cloud or locally in, e.g., hospitals and medical centers. Information leaks, Denial of Service (DoS) attacks and Advanced Persistent Threats (APT) are the top regular threats for said domain based on Cloud Security Alliance (CSA) [152].

Adequate security of the Cloud infrastructure depends largely on the established protection technologies with many layers. Therefore, customizing an Intrusion Detection System (IDS) is important to intelligently analyze and identify potential threats and attempt to decrease the probability of the attacks across a any computing environment [153].

The presence of medical data service providers and customers also plays a role in the deployment & integration plan [154]. The need to establish related mutual agreements raises questions from the domain of service level negotiation, sensitive data transfer, and especially data processing policies [155].

When the medical data is stored or processed in the public Cloud, it is exposed to a wide variety of privacy threats, although these threats differ depending on the CC model options. Some concerns relate to information dissemination, malicious use by unauthorized persons, and lack of customer control [156]. Privacy risks are viewed from different perspectives, such as access control, cloud system specifics, client application and information

[1] Note, the main purpose of this survey is not in the field of information security but in the field of computing and communications, so the following section is included in brief to keep the interested readership informed.

provider devices, as well as the stored information [157]. One of the main obstacles preventing major hospitals from moving to the Cloud is the fear of losing sensitive data due to information leaks, which is especially important when working with medical data [158].

Nonetheless, the trust aspect is directly related to the disclosure of a person's or organization's data, which is considered a breach of confidentiality [159]. Nonetheless, the direction of access control reveals that CC has serious problems that an unauthorized person or group of individuals can gain access to if the trust issues are not addressed properly [160]. The majority of those could be, to some extent, eliminated in CC by applying the traditional data encryption that must be strong enough to keep the client's files confidential [160].

5.2. Edge-related aspects

Today 5G networks cover many areas and operations of daily human activities, including those related to the medical field [111]. Edge (and its variations) is undoubtedly at the core of all these changes, as it is part of the 5G network, making it crucial regarding small battery-dependent devices and their communication capabilities. Edge computing demonstrates how to connect to heterogeneous devices from various verticals and multiple spanning networks. With the data processing at the edge node, new privacy and security considerations would come to light that still needs ongoing improvement [161].

In Edge, the probability of imminent threats is very high due to the non-centralized nature of the offloading environment, although the information analysis at the nodes provides a certain level of security and privacy protection themselves [162]. As of today, the Edge computing framework cannot adequately support security and information protection mechanisms as the architectural specifics of the Edge node make the information flow relatively open, therefore, difficult to protect from various insider attacks [163].

The evolution of Edge-like systems paces the way in a developing manner, yet, the aspects of security and privacy remain an ongoing and problematic research process, and explains why there is not much research as the majority of activities are executed "in-house", thus, limiting the integrates from keeping up with the speed.

At present, it remains difficult to find practical work on the broad computational offloading security and privacy research fields, as scholars mainly focus on the CC [164] paradigm or perhaps the FC [165] paradigm. The main goal of information security in Edge-like computing is to provide enables for secure, reliable yet fast data transfers and, simultaneously, reduce the potential overheads brought by a heavy common model with an uninterruptible operation. By these means, end-users and remote sites are developing acceptable general information security tools and simplified designs.

In addition to the previously mentioned aspects, the following important Edge-specific items should be considered. Please note that cloud issues often apply to edge scenarios as well.

In particular, works [166,167] highlight the disadvantages associated with Edge computing privacy and demonstrate the very high risk associated with unauthorized access by service providers, especially, during the data transmission throughout the distributed network [168].

Edge systems can seamlessly interoperate with node hosting applications to provide most standard services. The edge node may incorporate a harsh environment with an insufficient security guarantee, thus, the performance can be significantly impacted when threats are poorly managed and/or spread to another edge node. Therefore, finding a "quick fix" can be difficult due to the weight of the threat spreading through the edge nodes. In addition, there are additional costs to find the original cause of the problem, and even recovery can take some time [169].

5.3. Fog-related aspects

Of course, CC platforms offer a plethora of well-centralized systems, albeit with some disadvantages [170,171]. CC nodes and their end-users may experience higher latencies or time-critical applications [172]. Correspondingly high risk exists in a situation in which the information structure fails and between networked systems. A possible violation here is the potential disclosure of privacy. To mitigate this problem, the FC model was introduced to improve computing, latency, security, and privacy, currently leading and the most recommended computing service [173].

Nevertheless, FC was recognized as the most viable approach due to the feature of interconnecting more heterogeneous devices, services, as well as peripheral devices. As proven by the IoT domain, said relationship may be affected by major privacy and security breaches, e.g., location data disclosure, confidential documents leaks, and compromisation of personal records. Considering FC surfaces as an alternative to the local Cloud offers great help from latency, QoS, and positioning data distribution [174]. Yet, FC services are foreseen as widely percepted as a virtualized system and has associated vulnerabilities [175].

Notably, it is important to develop the Threat Intelligence Platform (TIP) in FC to provide protection for the architecture on the required level [176]. Intelligent hardware and data gathering nodes are to be deployed to decrease the level of threat. Naturally, the function distribution of the FC nodes will feature affects the security implementation of CC infrastructures in FC systems.

In the medical field, the FC architecture has multiple nodes that may have some vulnerabilities, including unauthorized access to information while it is stored or in transit, unscrupulous insiders, and systemic dissemination of information. The anti-"fog" system sequentially receives data transmitted by sensors of medical devices over a wired or wireless network. Falsification of patient identity, integrity, and device availability is evident and can occur when communication systems and sensors are compromised. Some end-to-end channels like DoS can be easily implemented due to vulnerabilities found in wireless networks. On the other hand, the lack of proper structures to control access to FC nodes that process sensitive information can put information at risk due to leakage due to account theft, unauthorized access, and possibly some unsafe passage. These problems can be mitigated with careful analysis and strict rules and regulations to establish standard controls such as personal systems, selective (limited) encryption, and mutual authentication [177].

In general, FC has similar problems to Edge-like systems but combines them with a decentralized and distributed environment in a more sophisticated manner.

Protecting the privacy of individuals and organizations is often a major challenge for the FC paradigm. As of today, more hands-on research is needed to understand privacy issues better and implement state-of-the-art privacy solutions for FC [178]. Sensitive information is expected to be leaked more often, even when end users never reveal their information [179].

5.4. Identified security and privacy vulnerabilities in brief

Notably, it is necessary to consider several developed models to protect the offloaded computation system, and, thus, will help create a joint force out of many models of reliable defensive mechanisms that could coexist on a higher abstraction level in the healthcare system [180].

Table 8 provides a list of threats of the generalized computing models based on a specific layer of the Open Systems Interconnection (OSI) model. Those are mapped to the identified in the literature countermeasures. In some situations, the same countermeasures to one paradigm can be applied to others. However,

Table 8
Main computing aspects of privacy and security [149].

	Attack	Specifics of Paradigm/Main Proposed Countermeasures		
		Cloud-like	Edge-like	Fog-like
Application	HTTP flood	Runtime monitoring, WAF, privacy management [181]	Filtering mechanisms and intrusion detection [182]	HTTP-Redirect scheme [183]
	SQL injection	SQL injection detection using adaptive deep learning [184]	Random noise, constant execution path code, balancing Hamming weights [185]	SQL injection detection with Elastic-pooling [186]
	Malware	Use of Antivirus Software [181]	Signature-based and behavior-based detection [187]	Botnet detection [183]
Session/Presentation	Data leakage	Encrypt stored data/use secured transmission medium, Virtual Firewall [188]	Homomorphic Encryption [189]	Data isolation, location-based access control [190]
	VM-Based	Anti-viruses, the guest OS events' mobitoring [191]	Identity and Authentication systems, IBE [189]	Intrusion detection, anomaly detection, behavioral assessment, and ML approach in classifying [183]
Transport	TCP Flood	Firewalls, proprietary caching strategies [192]	Sophisticated cookies [193]	Integrated Firewalls [194]
	UDP Flood	Novel design for secure communication [195]	Response rate for UDP packets to be reduced/limited [194]	
	Session hijacking	AES-GCM symmetric encryption [195]	Light-weight authentication algorithm [193]	Multi-purpose authentication [177]
Network	DoS attack	IDS [196], Access Security	Network Authentication mechanisms	Deployment of routing security and behavioral monitoring [197]
	MITM	Data Encryption [181]	Time stamps, stronger encryption [185]	Authentication are a must [190]
	Spoofing attacks	Identity Authentication [181]	Secure trust schemes [198]	Secured identification and stronger authentication [198]
PHY/MAC	Eavesdropping	Encryption, Cryptography [199]	Data Encryption using asymmetric AES scheme [185]	Protection of identity by use of IBC [200]
	Tampering	Detection of behavioral pattern	Observe manner of behavior [199]	PKI-based solutions [165]
	Replay attack	Dynamic identity-based authentication model [201]	Stronger authentication mechanisms [202]	Key generation approach [202]

deploying a single countermeasure is difficult due to architectural specifics of every standalone paradigm.

Currently, the end-devices operating in various computing environments do not have established the standardized security measures. It could be explained by both heterogeneities of the systems and the lack/outdating of appropriate standardization activities. Vulnerability analysis must be comprehensive and thorough, examining attacks and their aspects and taking the results to the higher bodies [203]. We can conclude that vulnerabilities should be identified and protected separately at each layer and, thus, differently in each computing system. This ensures that the baseline security requirements are met.

Security and privacy are considered major stopping factors that prevent some institutions and organizations from using compute offload technology. As mentioned, these paradigms are subject to various privacy and security issues, but the most serious of these are DoS/DDoS attacks, e.g., CC clients can be severely affected when attackers temporarily compromise CC services and resources. CC systems face high latency and high communication and storage costs. These problems arise from the centralization of the CC and its geographical distance from the data provider nodes. To address these deficiencies in the CC, edge computing was introduced as an extension of CC.

In conclusion, while FC generally provides better security and privacy services for endpoints, some architectural details of FC are still vulnerable to various threats compared to non-shared CC. Unfortunately, the highly effective security and privacy measures of the CC paradigm cannot be directly implemented in the FC paradigm due to the aforementioned features and the need for appropriate standardization. Thus, FC-based solutions still require significant research and tools to solve the problems listed above. New methods and mechanisms suitable for the functions of the FC paradigm, and possibly cross-platform countermeasures, are still being developed.

6. Challenges and future perspectives

The development of the integrated eHealth system is a complex procedure – a lot of conflicting factors are required to be considered for the reconfiguration of medical services. The utilization of computing offloading schemes can improve the performance of the system, but it also adds other difficulties. Computing paradigms face a tremendous number of challenges in the design and implementation phases. They are highlighted in Table 9 and described in further paragraphs.

Table 9
Major identified challenges and limitations related to computing paradigms.

Challenge	Description	Paradigm	Potential solution or research direction
Lack of interoperability enablers	Various services and different wireless access technologies, etc	All	The scalable platform for a managing number of connected UE [204]
Policy issues	The implementation of the ICT in the government level	All	Development of state regulations and implementation frame [205]
			The worldwide standardization of regulations based on evidences with possibility to medical experts to influence the legalization of regulations [66]
Security and privacy issues	Protection of the personal and medical information	All	Implementation of AI, Blockchain (BC), ML, and Quantum Computing (QC) for secure biomedical data acquisition [206]
			Ensuring access to the data only by authorized bodies [42]
			Deploy a trusted platform in the edge data center to prevent the location-based services use data [103]
			To improve the authentication with trusted authentication mechanisms based on Public Key Infrastructure [207]
			Implementation of the BC technology to improve the security of the system [208]
Large communication delay	The delay is a consequence of the computing location at a large distance from the end-user	CC	Deploy a hybrid computing paradigm to provide the data processing closer to the user when required, e.g., the Edge-Cloud model [209]
High system overhead and costing model	Reducing the cost of the computation process itself does not make it cheaper to use the entire system	CC	Cloud is significantly reducing the infrastructure cost, but not the cost of data communication, which can be solved with negotiations with the Internet providers and operators or deployment of the new cost-efficient communication technologies [210]
			The implementation of fuzzy c-means clustering method to reducing the Cloud overhead [211]
		LEC	How to reduce the cost of the server implementation to the satellite is an open issue
Need to control the use of computing resources	Guarantees from providers on service, and user responsibilities	CC	Different Service Level Agreement (SLA) for various services, e.g., Infrastructure-as-a-Service (IaaS), SaaS, Platform-as-a-Service (PaaS) [212]
Data overloading	There is a need of the load balancing between computing nodes when the computing capacity of one node reaches its limit	CC	To deploy a hybrid computing architecture with spare nodes [209,213]
		EC	Data offloading schemes for the equally distributing load between devices [103]
			Implementation of path computing paradigm that supports data storage and data processing on a progression of the data centers deployed on the path from user to Cloud [214]
Energy consumption optimization	Optimizing the use of energy for the computing	EC	Deploy Edge based IoMT platform and adopt hierarchical multi-stage clustering techniques [215]
		FC	Leverage new orchestration mechanisms that, based on workloads, have a complex effect on system power consumption [216]
		DC, MEC, MCC	Choose the optimal computing location using the Lyapunov optimization technique [9]
		MCC	Optimizing the response time and energy consumption by migrating an application [119]
			Proposed JointDNN engine for collaborative and efficient computing between the ser device and Cloud [217]
Designing of new naming mechanisms	The need for new naming mechanisms that are flexible to serve the dynamic network	EC	Applying new naming mechanisms to the Edge, e.g., Named Data Network (NDN) mechanism [218]
Orchestration problem and resource management	Managing the efficient work of the system	CC	Use of the efficient task scheduling algorithm [219]
		EC	Provide service model by analogy with Cloud (SaaS, PaaS, IaaS) [220]
		FC	Employment of the control layer in the framework [221]
			The heuristic approach in making real-time forwarding decisions [222]
		MEC	Need to develop an optimized solution to enhance performance of the resources [103]
		MCC	Stochastic Game-Theoretic Approach for smart offloading decision process under dynamic environment [223]
		MACC	Heterogeneity-aware solution that enable the controller to make an intelligent decision of task allocation [109]
			Incentive mechanism for effective resource sharing [224]
		LEC	Due to the limited size of the satellite plus the rigid space environment need an intelligent allocation of resources and cooperative computation offloading strategy to meet the requirements of multi-users [121]

(*continued on next page*)

Table 9 (*continued*).

Challenge	Description	Paradigm	Potential solution or research direction
		LEC	The algorithm for failure recovery via computation task migration and computation task re-creation for cases of handover issues [121]
		DC	Design of the new ecosystems that manage the collaborate feature [113,116]
Synchronization issue	Complexity of the integrity with Cloud with the increasing number of data and restoring data in case of the failure	DC	The local computer must process data all the time to provide the synchronization, which leads to the energy consumption challenge [113]
Not guaranteed Quality of Experience (QoE)	While some user requirements could be met, e.g., latency, other could not be guaranteed, e.g., low energy consumption	LEC	Need to find the possible trades off and mitigation strategies based on, e.g., statistical analysis or ML [121]

CC — Cloud Computing EC — Edge Computing; FC — Fog Computing; MACC – Mobile ad-hoc Cloud Computing; MEC – Mobile-Edge Computing; MCC – Mobile Cloud Computing; LEC – LEO network's Edge Computing; DC – Dew Computing

6.1. State legalization

Implementation of the eHealth system brings many benefits, especially, for mobile scenarios. The traditional transportation system is getting a fundamental change as it requires effective managing of traffic load. One of the possible solutions is the application of ML techniques in complement with the computing solutions to improve emergency transportation [142]. Hence, replacing the current transportation system with the Autonomous Transportation System (ATS) aims to make the road use more efficient and optimized to provide a more coordinated, fast, and budget emergency service response.

Another example is the use of UAV to enable aid in hard-to-reach areas. There are complex situations where it is impossible to deliver first aid quickly. Drones are successfully applied to reach remote areas [225]. This solution faces another issue in lack of documentation. Future work requires the standardization of UAV and/or its relation to the cellular networks [226].

Robotic aided surgery or AR surgery requires a system for the delay-sensitive data. The emergency disaster information attends to the delay-sensitive data as any minute could be crucial for life-saving operations. The data collected from the sensor mounted in the UAV is transmitted by LEO satellite network due to its ability to send data to Earth with minimal latency. Supplementing existing technologies with LEO satellite communications and implementation of the LEC reduce the blind spot and provide ubiquitous coverage, wide bandwidth while maintaining high signal strength [112,227,228].

Unfortunately, researchers face boundaries at the implementation level even with reasonable experimental results. The level of the integrated technologies varies from one country to another. The ubiquitous ICT integration in the medical sphere is controlled by internal regulations and should be checked by the governmental authorities. A thorough check takes a long time, which makes the whole process energy- and time-consuming, thus, challenging.

Difficulties in integrating the wireless technologies into eHealth systems also relate to the absence of authorized bodies. There is a lack of state regulations, frame of implementation, authority bodies, and leaders who will implement the telemedicine program [205]. There is a need for technologies standardization and designing the interfaces between them to make a fully digital integrated healthcare system [42,226].

6.2. Protection of personal and biomedical data

Speaking about the medical domain, healthcare organizations and medical authorities value and protect the medical information of each individual. The security and privacy challenge is an important aspect of computing paradigms that operate with private data, which appears to be not a primary challenge for Fog or DC as they process data locally before sharing it to third-party servers [229]. Nevertheless, the importance of this aspect could not be neglected.

Confidentiality. Keeping confidentiality of patients' personal information and health status is an ethical issue that the medical staff learns from the beginning of their professional careers. Medical members have a professional responsibility to keep private information, which becomes even more significant for eHealth [230]. Provenance information could be used for various purposes, such as traceback and history-based access control. On the other side, it is vital to save the confidentiality of the customer and keep a balance between data protection and user privacy. Collecting and retaining personal data in information systems is an essential domain for ICT's successful implementation as is highlighted by various leading organizations (including the GDPR by the EU).

Authentication. Privacy in terms of biomedical data means which will access personal information and under what conditions. The security of biomedical data is determined by the authentication of the medical staff as well. Authentication mechanisms play a major role in verifying the user's identity and accessing the computing service. Access to the data only by authorized parties is the leading solution for personal data protection. Most of the existing authorizing protocols are not suitable in cases with limited connectivity to the central authentication server. Weak password-based authentication could be improved with trusted authentication mechanisms based on public keys or the Lightweight Directory Access Protocol [207].

Secure data transfer to the server. Security and privacy in computing paradigms is an important challenge. Implementation of the computing paradigms in the medical scenarios benefits fast and accurate medical decisions and performance and provides information security risks. Luh et al. urge stakeholders to reprioritize and consider changes in investment strategies, government policies, and medical business partnerships to improve cybersecurity in healthcare [206]. The implications of stolen medical information are evident and may affect patients' confidence in medical institutions. To secure biomedical data acquisition could be improved by implementation of AI, BC, ML, and QC.

6.3. Lack of interoperability enablers

A number of different kinds of services, as well as a large number of mobile and static devices that are utilizing various types of communication technologies, such as 4G, 5G, Wi-Fi, etc., caused the network heterogeneity. This issue and the domains' diverse access requirements in computing environments demand fine-grained access control policies. It is essential to take into account the network heterogeneity and data interoperability to ensure the troubleproof of the computing operations [204]. It becomes crucial to employ a scalable and easily managed computing paradigm, which privilege distribution is administered efficiently. This challenge applies to all computing paradigms.

6.4. Issues related to the cloud paradigm

Cloud is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared computing resource [4]. It has a great benefit with the computing resources and storage capabilities. Still, it falls behind in terms of communication delay, overloading, costing model, and the need for a agreement to guarantee the service delivery.

Task scheduling in Cloud is a critical issue in terms of efficient resource management. The number of Cloud users is increasing, and the number of utilized services, so scheduling becomes more difficult. Arunarani et al. provide an overview of scheduling algorithms to improve the computing performance [219], e.g., multi-processor-based scheduling, fuzzy-based scheduling, Genetic algorithm-based task scheduling, and other algorithms.

The main advantage of CC is to migrate the data processing out of the device, bringing resource availability to the device and significantly reducing the infrastructure cost. On the other hand, it raises the cost of data communication, i.e., transferring data between user and Cloud. The cost per unit of computing resource used is likely to be higher. The implementation of the clustering method assists to reduce the overhead in the Cloud. Wang et al. proposed the clustering algorithm that reduces computational complexity [211].

SLA between the cloud provider and user has gained significant attention in designing the trust model in cloud computing. SLA is a part of a service contract between the user and provider of the service that formally defines the level of service. For consumers, SLA is a guarantee from providers on service delivery. Different cloud services, e.g., IaaS, SaaS, paas, will define different SLA specifications. It records a common understanding of services, priorities, responsibilities, guarantees, and warranties. In computing, SLA are necessary to control the use of the computing resources.

6.5. Issues related to the edge computing

Edge computing is a paradigm where the computing performs in one (or two) hop from the end device, in other words — the "edge" of the network [231]. The proximity to the user benefits in terms of communication latency and reliability. Anyway, among the disadvantages are data overloading, energy efficiency, and efficient naming.

Edge servers suffer the limitations of the storage capabilities that bring the challenge of adding more computing resources and providing intelligent resource management. Mortazavi et al. came up with the solution of implementing the path computing paradigm that processes data along the path from the user to Cloud datacenter [214]. While the traditional Edge is a two-tier framework, path computing has a multi-tier topology that supports the application execution on a progression of datacenters. This opportunity has its drawbacks in handovers, cost of serving, computing managing, and the need to partition the provider's server-side functionality.

Nowadays, there are a significant number of IoT applications where each of them has its structure. The naming scheme is the principal for programming, addressing, identification, and data communication. However, an efficient naming mechanism for the Edge has not been built and standardized yet [231]. Traditional naming mechanisms are not flexible enough to serve the dynamic network. Zhang at al. proposed to apply the NDN mechanism to the Edge [218]. NDN provides a hierarchically structured name for content/data-centric network, and it is human-friendly for service management and provides good elasticity.

6.6. Issues related to the fog computing

Bonomi et al. used the term Fog computing to introduce the new decentralized computing infrastructure, which defines as a highly virtualized platform that provides compute, storage, and networking services between end devices and Data Center [102]. Fog paradigm provides a computing resource with high QoS for real-time and delay-intolerant applications. The main drawbacks of this model are application offloading issues, high energy consumption, efficient resource management, or orchestration problem.

To manage the interconnection between nodes successfully is an open issue for researchers. The increasing popularity of the hybrid computing paradigms that include various middle nodes and different types of hardware need an implementation of the control layer into the architecture [221]. This aspect is more relevant for the computing that connects the devices into the group and choosing the main node that will orchestrate the operation when it is a demand to proceed with the computation.

The Fog architecture considers multiple computing nodes. It is essential to select the source and destination node and orchestrate the computing process. Mahmud et al. propose a new management policy based on the heuristic approach of making the task allocation decision [222]. Researchers propose to identify highly-occupied and under-occupied allocated resources and making a decision based on these results.

6.7. Issues related to MEC

MEC is a server running at the BS within the RAN close to mobile users [110]. Benefits of MEC are the ability to run isolated from the rest of the network, maintain access to local resources, have a short distance to a client, low latency, location awareness, and network data in real-time. Naturally, there are drawbacks to efficient resource management, energy efficiency, etc.

The limited capabilities by the server of the computing resources in such paradigms as Edge, or MEC, might force new solutions to manage the resources effectively. The solution was found in the Cloud paradigm, which provides services according to the demand. Cloud allows to run the application remotely (SaaS), use the virtual operation system (PaaS), or offer the entire server for the private purpose (IaaS). Tran et al. introduced such approaches as MEC-as-a-Service [220].

Improving the energy efficiency of the data centers and servers is an important task for environmental health. Jain et al. propose different ways to reduce power consumption. Among them, to reduce CPU dissipation, use advanced Clock gating, use energy-efficient processors and storage, reduce cooling requirements [232]. To satisfy the application needs in the high technologies scenarios, it is important to stay environmental-friendly.

6.8. Issues related to MCC

MCC is a Cloud extension on mobile devices. It runs the application on the remote rich server outside the mobile device [8]. MCC meets such problems as data management, resource allocation, and synchronization issue.

The intelligent resource allocation and offloading schemes help reach energy-efficient and effective application execution. Jianchao Zheng et al. developed a stochastic learning algorithm to evaluate MCC performance under dynamic environment [223]. Researchers formulated the stochastic game for the computing paradigm with a guaranteed convergence rate. Eshratifar et al. discussed a JointDNN engine that provides energy- and performance-efficient method for querying on the mobile side and reducing the amount of workload in the Cloud [217].

6.9. Issues related to MACC

MACC performs on a group of computing devices that share their resources [233]. It is a paradigm for the special purpose where the application is required high availability, high mobility, and the emergence of Big Data computation. This paradigm is challenged with long execution time and limited computing power.

Zhang et al. proposed the method of improving the performance of the overall system by encouraging mobile devices to share their idle resources [224]. The authors designed a real-time distributed algorithm based on utility maximization. Yaqoob et al. proposed a solution that shorter execution time and reduces the energy consumption in MACC [234]. Researchers developed multi-threaded matrix multiplication and infinite loop execution of compute-intensive applications.

6.10. Issues related to computing on satellites

LEO satellite computing architecture is a promising direction in the future network. LEC benefits in coverage due to high altitudes. The main drawback is frequent handovers due to the high satellite speed. Medical use cases require high or very high network availability [24,26,42]. The computing system should fulfill the standardized requirement. In computing paradigms, resource availability is dictated by the server computing capacity and communication reliability [204]. LEC has limited resources caused by the size and weight of a satellite being natural for the space environment.

6.11. Issues related to DC

As of today, computing paradigms mostly require an Internet connection. The benefit of the DC is computing that processes on the wearable devices out of the network. Drawbacks of DC connected to the limit of the device resources and synchronization issue.

In implementing new computing paradigms, it is crucial to determine the correct strategy for each scenario. Regulatory documents do not provide precise guidance or recommendations in all cases. Finding solutions for the optimization problems, e.g., the Lyapunov optimization technique and new orchestration methods, may improve the computing performance in response time and energy consumption [9].

7. Summary and main takeaway points

The effectiveness of the general healthcare system is determined by the quality of patient care, fast and accurate work of medical specialists, and the availability of eHealth services for all patients independently of their wealth and a variety of other factors. As a supportive point, the development of eHealth mechanisms could ensure the high availability of medical services. For example, remote monitoring of the patient's health status can detect diseases at the early stages and would inevitably notify the corresponding medical specialists. Remote services require suitable and efficient computing solutions, and they typically also need a significant amount of computing power to meet the quality requirements of various services based on multimodal data, such as video and audio streaming.

Modern eHealth/medical use cases are currently divided by the standardization bodies into four modalities, according to the equipment location and the distance between the medical team and patient. "Static-local" use cases define where the equipment is not moving, and the medical team and patient are located in the same room. Examples of this modality are duplicating video for the additional monitor, AR assistance, robotic-assisted surgery, etc. This use case requires the service operation and communications high accuracy and high reliability to provide minimum invasive surgery, and all kinds of delays might be fatal (below 0.75 ms and the availability of over 99.99999%). In this modality, we recommend that the computing be performed close to the user, i.e., in the Edge, to reach the required parameters. The wired network is winning in terms of reliability to the current state of communication development. The second modality is "Static-remote" and covers all use cases where the operation is performed at a distance without moving, e.g., remote ultrasound examination, mobile specialists practice, robotic-aided diagnosis, etc. These use cases are not so strict concerning the latency (e.g., they tolerate up to 20 ms latency) and availability 99.999%. The computation could be performed at the Edge of the network to meet the strict requirements for robotic telesurgery and robotic aided diagnoses. Mobile specialist practice and ultrasound examination have moderate requirements in terms of reliability and latency. They mainly suit to provide computation in the MEC or MCC server.

The third and fourth modalities are "moving-local" and "moving-remote", e.g., cardiac monitoring inside the hospital (IoT wearables) and medical monitoring outside the hospital/inside the ambulance, respectively. These use cases are delay-tolerant, but they demand more significant storage and computing capacity to analyze the data from sensors. Paradigms such as Fog, MCC, or DC are well suited for use cases where user mobility and data processing are required, but latency values are not critical. In an emergency, when the base stations are destroyed or overloaded, Fog or MACC could be a cost-effective solution. In the most challenging scenarios, e.g., a catastrophe in the sea or in the mountains, where there is not enough communication enablers available, the only operational solution is to provide computing on the satellites, i.e., LEC paradigm.

From the security perspective, while the FC paradigm provides better security and privacy services for endpoints in general, some features of the FC paradigm, such as decentralization, resource constraints, homogeneity, and virtualized systems, are still vulnerable to a vast variety of security and privacy issues compared to conventional CC that is centralized. Due to the lack of standardization regarding countermeasures, highly effective security and data protection measures in the majority of computing paradigms paradigm cannot be yet applied and integrated directly in the healthcare domain.

The development of communications is prominent for enabling fast and effective computing. Even with the high computing capacity, the communication latency might be challenging for many use cases. The minimal required latency for medical scenarios is below 1 ms, which is not covered by such technology as conventional 3G. 5G networks and beyond provide throughput up to 10 Gbps and offer bandwidth up to 47 GHz. The new Wi-Fi standards specified by *IEEE 802.11* family work on the new OFDMA access method that enables transferring data simultaneously from many users with a high bit rate.

There are a lot of cultural, organizational, and technical challenges in involving ICT in the medical domain. For example, new devices need wider bandwidth, provide delay-sensitive data, data security, resolve privacy issues, improve energy efficiency, fill the gap of universal interfaces for the medical equipment, and standardize the medical device requirements issue. Implementation of computing paradigms to medical emergency use cases brings more challenges. They are the secure transfer of medical data, ability to operate in a heterogeneous network, optimization of the energy consumption, resource management, resource availability, and challenges related to policy and the legal aspects of implementation. This paper provides a discussion on the challenges from above.

CRediT authorship contribution statement

Daria Alekseeva: Writing – original draft, Visualization. **Aleksandr Ometov:** Writing – original draft, Methodology, Supervision, Project administration, Funding acquisition. **Otso Arponen:** Writing review & editing, Formal analysis. **Elena Simona Lohan:** Writing – review & editing, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was partly supported by the Academy of Finland, under the project ULTRA (328226, 328214), and by the doctoral grants of the Information Technology and Communications Science Faculty at Tampere University, Finland.

References

[1] Y. Lin, M. Bariya, A. Javey, Wearable biosensors for body computing, Adv. Funct. Mater. 31 (39) (2021) 2008087.
[2] F. Froes, And now for something completely different: From 2019-nCoV and COVID-19 to 2020-nMan, Pulmonology 26 (2) (2020) 114.
[3] R. Latifi, C.R. Doarn, Perspective on COVID-19: Finally, telemedicine at center stage, Telemed. E-Health 26 (9) (2020) 1106–1109.
[4] T.G. Peter Mell, The NIST definition of cloud computing, in: Recommendations of the National Institute of Standards and Technology, Special Publication 800-145, Computer Security Division, Information Technology Laboratory, National ..., 2011.
[5] M. Mukherjee, L. Shu, D. Wang, Survey of fog computing: Fundamental, network applications, and research challenges, IEEE Commun. Surv. Tutor. 20 (3) (2018) 1826–1857.
[6] Worldwide global datasphere IoT device and data forecast, 2021–2025, 2022, https://www.idc.com/getdoc.jsp?containerId=US48087621 (Accessed August 4, 2022).
[7] I. Stojmenovic, S. Wen, The fog computing paradigm: Scenarios and security issues, in: Proc. of Federated Conference on Computer Science and Information Systems, IEEE, 2014, pp. 1–8.
[8] N. Fernando, S.W. Loke, W. Rahayu, Mobile cloud computing: A survey, Future Gener. Comput. Syst. 29 (1) (2013) 84–106.
[9] H. Wu, K. Wolter, P. Jiao, Y. Deng, Y. Zhao, M. Xu, EEDTO: an energy-efficient dynamic task offloading algorithm for blockchain-enabled IoT-edge-cloud orchestrated computing, IEEE Internet Things J. 8 (4) (2020) 2163–2176.
[10] J. Nicholl, J. West, S. Goodacre, J. Turner, The relationship between distance to hospital and patient mortality in emergencies: an observational study, Emerg. Med. J. 24 (9) (2007) 665–668.
[11] C. Gruet, L. Martinod, P. Mège, X. Pons-Masbernat, Broadband private mobile radio (PMR)/public protection and disaster relief (PPDR) services evolution, in: Orthogonal Waveforms and Filter Banks for Future Communication Systems, Elsevier, 2017, pp. 53–71.
[12] H. Holma, A. Toskala, T. Nakamura, 5G Technology: 3GPP New Radio, John Wiley & Sons, 2020.
[13] About ETSI, 2022, https://www.etsi.org/about (Accessed August 4, 2022).
[14] About international telecommunication union (ITU), 2022, https://www.itu.int/en/about/Pages/default.aspx (Accessed August 4, 2022).
[15] A global initiative 3GPP – Partners, 2022, https://www.3gpp.org/about-3gpp/partners (Accessed August 4, 2022).
[16] The association of radio industries and businesses (ARIB), 2022, https://www.arib.or.jp (Accessed August 4, 2022).
[17] The alliance for telecommunications industry solutions (ATIS), 2022, https://www.atis.org (Accessed August 4, 2022).
[18] TSDSI – India's telecom SDO, 2022, https://tsdsi.in (Accessed August 4, 2022).
[19] Telecommunications technology association (TTA), 2022, http://www.tta.or.kr (Accessed August 4, 2022).
[20] Telecommunication technology committee (TTC), 2022, https://www.ttc.or.jp (Accessed August 4, 2022).
[21] China communications standards association, 2022, http://www.ccsa.org.cn (Accessed August 4, 2022).
[22] About DICOM: Overview, 2022, https://www.dicomstandard.org/about-home (Accessed August 4, 2022).
[23] European standardization: CEN and CENELEC, 2022, https://www.cencenelec.eu/european-standardization/cen-and-cenelec/ (Accessed August 4, 2022).
[24] G.T.. V18.0.0, Service Requirements for Cyber-Physical Control Applications in Vertical Domains, Rel. 18, 2021.
[25] G.T.. V18.2.0, Service Requirements for the 5G System, Rel. 18, 2021.
[26] 3GPP TS 22.263 V17.3.0, Service Requirements for Video, Imaging and Audio for Professional Applications (VIAPA), Rel. 17, 2020.
[27] 3GPP TS 23.167 V17.0.0, IP Multimedia Subsystem (IMS) Emergency Sessions, Rel. 17, 2021.
[28] ETSI TS 123 167 V9.4.0, Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Subsystem (IMS) Emergency Sessions, 2010.
[29] 3GPP TS 23.401 V17.0.0, Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access, Rel. 17, 2021.
[30] Report ITU-R M.2014-3, Digital Land Mobile Systems for Dispatch Traffic; Mobile, Radiodetermination, Amateur and Related Satellite Services, 2016.
[31] CEN/TC 239 EN 1789:2006, Medical Vehicles and Their Equipment. Road Ambulances, 2006.
[32] ETSI TS 102 164 V1.3.1, Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Emergency Location Protocols, 2006.
[33] ETSI TR 102 299 V1.3.1, Emergency Communications (EMTEL); Collection of European Regulatory Texts and Orientations, 2013.
[34] ETSI TS 102 181 V1.2.1, Emergency Communications (EMTEL); Requirements for Communication Between Authorities/Organizations During Emergencies, 2008.
[35] ITU-T E.107, Emergency Telecommunications Service (ETS) and Interconnection Framework for National Implementations of ETS, 2007.
[36] ETSI TR 102 476 V1.1.1, Emergency Communications (EMTEL); Emergency Calls and VoIP: Possible Short and Long Term Solutions and Standardization Activities, 2008.
[37] ETSI TR 102 764 V1.1.1, eHEALTH; Architecture; Analysis of User Service Models, Technologies and Applications Supporting eHealth, 2009.
[38] ETSI EN 302 663 V1.2.1, Intelligent Transport Systems (ITS); Access Layer Specification for Intelligent Transport Systems Operating in the 5 GHz Frequency Band, 2013.
[39] REGULATION (EU) 2016/679, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016.
[40] ETSI TR 103 394 V1.1.1, Smart Body Area Networks (SmartBAN); System Description, 2018.
[41] NHS, National Ambulance Vehicle Specification for English NHS Ambulance Trusts, 2018.
[42] 3GPP TR 22.826 V17.2.0, Study on Communication Services for Critical Medical Applications, Rel. 17, 2021.
[43] DICOM Supplement 202: Real-Time Video, Digital Imaging and Communications in Medicine (DICOM) Supplement 202: Real-Time Video, 2019.
[44] 3GPP TR 22.839 V0.2.0, Study on Vehicle-Mounted Relays, Rel. 18, 2021.
[45] J.E. Hollander, B.G. Carr, Virtually perfect? Telemedicine for COVID-19, N. Engl. J. Med. 382 (18) (2020) 1679–1681.
[46] D. Dias, J. Paulo Silva Cunha, Wearable health devices – Vital sign monitoring, systems and technologies, Sensors 18 (8) (2018) 2414.
[47] Northern light health: Telemonitoring, 2022, https://northernlighthealth.org/Services/Telehealth/Telemonitoring (Accessed August 4, 2022).
[48] Bittium. Cardiac monitoring, 2022, https://www.bittium.com/medical/cardiology (Accessed August 4, 2022).
[49] A.D. DeVore, J. Wosik, A.F. Hernandez, The future of wearables in heart failure patients, JACC: Heart Fail. 7 (11) (2019) 922–932.
[50] GPS tracker for elderly, dementia, and alzheimer's, 2022, https://www.angelsense.com/gps-tracker-for-elderly/ (Accessed August 4, 2022).
[51] What is GPS SmartSole?, 2022, https://gpssmartsole.com/gpssmartsole/ (Accessed August 4, 2022).
[52] Vivago: Pioneer in personal health care technology, 2022, https://www.vivago.com/company/ (Accessed August 4, 2022).
[53] M. Tierney, J. Tamada, R. Potts, L. Jovanovic, S. Garg, C.R. Team, et al., Clinical evaluation of the GlucoWatch® biographer: a continual, non-invasive glucose monitor for patients with diabetes, Biosens. Bioelectron. 16 (9–12) (2001) 621–629.
[54] W. Villena Gonzales, A.T. Mobashsher, A. Abbosh, The progress of glucose monitoring – A review of invasive to minimally and non-invasive techniques, devices and sensors, Sensors 19 (4) (2019) 800.

[55] A. Rghioui, J. Lloret, S. Sendra, A. Oumnad, A smart architecture for diabetic patient monitoring using machine learning algorithms, in: Healthcare, Vol. 8, Multidisciplinary Digital Publishing Institute, 2020, p. 348.

[56] J. Marescaux, J. Leroy, F. Rubino, M. Smith, M. Vix, M. Simone, D. Mutter, Transcontinental robot-assisted remote telesurgery: Feasibility and potential applications, Ann. Surg. 235 (4) (2002) 487.

[57] E.I. George, C.T.C. Brand, et al., Origins of robotic surgery: From skepticism to standard of care, JSLS: J. Soc. Laparoendosc. Surg. 22 (4) (2018).

[58] J.W. Collins, R. Ma, Y. Beaulieu, A.J. Hung, Telementoring for minimally invasive surgery, in: Digital Surgery, Springer, 2021, pp. 361–378.

[59] R.M. Terra, P.H.C. Leite, A.J.M.D. Vega, Global status of the robotic thoracic surgery, J. Thorac. Dis. 13 (10) (2021) 6123.

[60] S. Scarcella, D. Castellani, P. Piazza, C. Giulioni, L. Sarchi, M. Amato, C.A. Bravi, M.P. Lores, R. Farinha, S. Knipper, et al., Concomitant robot-assisted laparoscopic surgeries for upper and lower urinary tract malignancies: a comprehensive literature review, J. Robot. Surg. (2021) 1–15.

[61] A.S. Moon, J. Garofalo, P. Koirala, M.-L.T. Vu, L. Chuang, Robotic surgery in gynecology, Surg. Clin. 100 (2) (2020) 445–460.

[62] A.R. Lanfranco, A.E. Castellanos, J.P. Desai, W.C. Meyers, Robotic surgery: A current perspective, Ann. Surg. 239 (1) (2004) 14.

[63] H. Haapiainen, T.J. Murtola, M. Raitanen, 3D laparoscopic prostatectomy: A prospective single-surgeon learning curve in the first 200 cases with oncologic and functional results, Scand. J. Urol. (2021) 1–7.

[64] W.G. Bradley Jr., Off-site teleradiology: The pros, Radiology 248 (2) (2008) 337–341.

[65] J.H. Thrall, Teleradiology part II. Limitations, risks, and opportunities, Radiology 244 (2) (2007) 325–328.

[66] T.N. Hanna, S.D. Steenburg, A.B. Rosenkrantz, R.S. Pyatt Jr., R. Duszak Jr., E.B. Friedberg, Emerging challenges and opportunities in the evolution of teleradiology, Am. J. Roentgenol. 215 (6) (2020) 1411–1416.

[67] D. Dyer, J. Cusden, C. Turner, J. Boyd, R. Hall, D. Lautner, D.R. Hamilton, L. Shepherd, M. Dunham, A. Bigras, et al., The clinical and technical evaluation of a remote telementored telesonography system during the acute resuscitation and transfer of the injured patient, J. Trauma Acute Care Surg. 65 (6) (2008) 1209–1216.

[68] N. Biegler, P.B. McBeth, C. Tiruta, D.R. Hamilton, Z. Xiao, I. Crawford, M. Tevez-Molina, N. Miletic, C.G. Ball, L. Pian, et al., The feasibility of nurse practitioner-performed, telementored lung telesonography with remote physician guidance-'a remote virtual mentor', Crit. Ultrasound J. 5 (1) (2013) 1–8.

[69] HCA healthcare UK: Ultrasound imaging, 2022, https://www.hcahealthcare.co.uk/our-services/tests/ultrasound-imaging (Accessed August 4, 2022).

[70] The royal children's hospital melbourne: Cardiac telemetry, 2022, https://www.rch.org.au/rchcpg/hospital_clinical_guideline_index/Cardiac_telemetry/ (Accessed August 4, 2022).

[71] The countess of chester hospital: Patient wristbands. What, who, when, where and why, 2022, https://asl-uk.co.uk/blog/patient-wristbands/ (Accessed August 4, 2022).

[72] Biosigns: Patient's heart at your fingertips, 2022, http://www.biosigns.com/s_applications_ambulances.html (Accessed August 4, 2022).

[73] Mobile medical monitor technology for ambulances and emergency vehicles from infinium medical, 2022, https://www.infiniummedical.com/mobile-medical-monitor-technology.html (Accessed August 4, 2022).

[74] ApexPro telemetry system, 2022, https://www.gehealthcare.co.uk/products/patient-monitoring/wireless-networks/apexpro-telemetry-system (Accessed August 4, 2022).

[75] Renji hospital: Doctors remove 93-year-old woman's kidney to treat cancer, 2022, https://www.renji.com/default.php?mod=article&do=detail&tid=9036 (Accessed August 4, 2022).

[76] Russian scientific research institute of traumatology and orthopedics named after R.R. Vreden: Clinical work, 2022, https://www.rniito.org/eng/r/clinicalwork/ (Accessed August 4, 2022).

[77] The froedtert and the medical college of wisconsin: Bariatric surgery, 2022, https://www.froedtert.com/bariatric-surgery (Accessed August 4, 2022).

[78] Horizon health: Comprehensive surgical services, 2022, https://www.myhorizonhealth.org/services/surgical-services/ (Accessed August 4, 2022).

[79] About the wellington cardiac unit, 2022, https://www.hcahealthcare.co.uk/facilities/the-wellington-hospital/our-centres/the-wellington-hospital-cardiac-unit (Accessed August 4, 2022).

[80] I.Y. Seo, Urologic robotic surgery in Korea: Past and present, Korean J. Urol. 56 (8) (2015) 546–552.

[81] Revo. Surgical solution, 2022, http://revosurgical.com/#/main.html (Accessed August 4, 2022).

[82] Gibbeum hospital: Non-mesh hernia center, 2022, http://gibbeum.com/main/main.php (Accessed August 4, 2022).

[83] The charité center, 2022, https://www.charite.de/en/charite/charitecenters/surgery/ (Accessed August 4, 2022).

[84] The university of Tokyo hospital: Orthopaedic surgery and spinal surgery, 2022, https://www.h.u-tokyo.ac.jp/english/centers-services/clinical-divisions/orthopaedic-surgery-and-spinal-surgery/index.html (Accessed August 4, 2022).

[85] The university of saskatchewan: Health care, anywhere, 2022, https://news.usask.ca/articles/research/2017/health-care-anywhere.php (Accessed August 4, 2022).

[86] Discover glass enterprise edition, 2022, https://www.google.com/glass/start/ (Accessed August 4, 2022).

[87] About telehealth: Video consultation, 2022, https://www.telehealth.org.nz/health-provider/what-is-telehealth/video-consultation/ (Accessed August 4, 2022).

[88] Tokyo medical and surgical clinic: Telehealth, 2022, https://tmsc.jp/telehealth (Accessed August 4, 2022).

[89] Sunway medical centre: Telemedicine command centre, 2022, https://www.sunwaymedical.com/telemedicine-command-centre/ (Accessed August 4, 2022).

[90] Pantai hospital: ehealth, 2022, https://www.pantai.com.my/ehealth/penang (Accessed August 4, 2022).

[91] Neurology and neurosurgery clinic: Rehabilitation methods, 2022, https://www.neurology.ru/o-centre/neurology-and-neurosurgery-clinic (Accessed August 4, 2022).

[92] TriHealth, TriHealth expanding use of glass enterprise edition technology, 2017, https://www.trihealth.com/dailyhealthwire/news/trihealth-expanding-use-of-glass-enterprise-edition-technology (Accessed August 4, 2022), Last Updated: July 27, 2017.

[93] The charité center: Digital labs, 2022, https://technologietransfer.charite.de/en/services/bhi_digital_labs/ (Accessed August 4, 2022).

[94] CaRi-heart® technology, 2022, https://www.hcahealthcare.co.uk/facilities/the-harley-street-clinic/cari-heart (Accessed August 4, 2022).

[95] J. Voas, J. Zhang, Cloud computing: New wine or just a new bottle? IT Prof. 11 (2) (2009) 15–17.

[96] S. Garfinkel, An evaluation of amazon's grid computing services: EC2, S3, and SQS, 2007.

[97] Announcing amazon elastic compute cloud (Amazon EC2) – Beta, 2022, https://aws.amazon.com/about-aws/whats-new/2006/08/24/announcing-amazon-elastic-compute-cloud-amazon-ec2---beta/ (Accessed August 4, 2022).

[98] Who coined cloud computing? by antonio regalado MIT technology review, 2022, https://www.technologyreview.com/2011/10/31/257406/who-coined-cloud-computing/ (Accessed August 4, 2022).

[99] Y. Lin, L. Shao, Z. Zhu, Q. Wang, R.K. Sabhikhi, Wireless network cloud: Architecture and system requirements, IBM J. Res. Dev. 54 (1) (2010) 1–12.

[100] G. Muhammad, S.M.M. Rahman, A. Alelaiwi, A. Alamri, Smart health solution integrating IoT and cloud: A case study of voice pathology monitoring, IEEE Commun. Mag. 55 (1) (2017) 69–73.

[101] Y. Karaca, M. Moonis, Y.-D. Zhang, C. Gezgez, Mobile cloud computing based stroke healthcare system, Int. J. Inf. Manage. 45 (2019) 250–261.

[102] F. Bonomi, R. Milito, J. Zhu, S. Addepalli, Fog computing and its role in the internet of things, in: Proc. of the First Edition of the MCC Workshop on Mobile Cloud Computing, 2012, pp. 13–16.

[103] T. Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman, D.O. Wu, Edge computing in industrial internet of things: Architecture, advances and challenges, IEEE Commun. Surv. Tutor. 22 (4) (2020) 2462–2488.

[104] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, W. Lv, Edge computing security: State of the art and challenges, Proc. IEEE 107 (8) (2019) 1608–1631.

[105] S. Dash, S. Biswas, D. Banerjee, A.U. Rahman, Edge and fog computing in healthcare–A review, Scalable Comput.: Pract. Exp. 20 (2) (2019) 191–206.

[106] T.-A.N. Abdali, R. Hassan, A.H.M. Aman, Q.N. Nguyen, Fog computing advancement: Concept, architecture, applications, advantages, and open issues, IEEE Access 9 (2021) 75961–75980, http://dx.doi.org/10.1109/ACCESS.2021.3081770.

[107] H. Dubey, A. Monteiro, N. Constant, M. Abtahi, D. Borthakur, L. Mahler, Y. Sun, Q. Yang, U. Akbar, K. Mankodiya, Fog computing in Medical Internet-of-Things: Architecture, implementation, and applications, in: Handbook of Large-Scale Distributed Computing in Smart Healthcare, Springer, 2017, pp. 281–321.

[108] A. Nirabi, S.A. Hameed, Mobile cloud computing for emergency healthcare model: Framework, in: Proc. of 7th International Conference on Computer and Communication Engineering (ICCCE), IEEE, 2018, pp. 375–379.

[109] S.C. Shah, A mobile ad hoc cloud computing and networking infrastructure for automated video surveillance system, 2018, arXiv preprint arXiv:1810.07338.

[110] Y.C. Hu, M. Patel, D. Sabella, N. Sprecher, V. Young, Mobile edge computing—A key technology towards 5G, ETSI White Paper 11 (11) (2015) 1–16.

[111] Z. Ning, P. Dong, X. Wang, X. Hu, L. Guo, B. Hu, Y. Guo, T. Qiu, R.Y. Kwok, Mobile edge computing enabled 5G health monitoring for internet of medical things: A decentralized game theoretic approach, IEEE J. Sel. Areas Commun. 39 (2) (2020) 463–478.

[112] C. Li, Y. Zhang, R. Xie, X. Hao, T. Huang, Integrating edge computing into low earth orbit satellite networks: Architecture and prototype, IEEE Access 9 (2021) 39126–39137, http://dx.doi.org/10.1109/ACCESS.2021.3064397.

[113] H.M. Patel, R.R. Chaudhari, K.R. Prajapati, A.A. Patel, The interdependent part of cloud computing: Dew computing, in: Intelligent Communication and Computational Technologies, Springer, 2018, pp. 345–355.

[114] P.P. Ray, An introduction to dew computing: Definition, concept and implications, IEEE Access 6 (2017) 723–737.

[115] V. Prokhorenko, M.A. Babar, Architectural resilience in cloud, fog and edge systems: A survey, IEEE Access 8 (2020) 28078–28095.

[116] N. Mäkitalo, D. Flores-Martin, J. Berrocal, J. Garcia-Alonso, P. Ihantola, A. Ometov, J.M. Murillo, T. Mikkonen, The internet of bodies needs a human data model, IEEE Internet Comput. 24 (5) (2020) 28–37.

[117] M. Gusev, What makes dew computing more than edge computing for internet of things, in: Proc. of IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), IEEE, 2021, pp. 1795–1800.

[118] P. Brezany, T. Ludescher, T. Feilhauer, Cloud-dew computing support for automatic data analysis in life sciences, in: Proc. of 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), IEEE, 2017, pp. 365–370.

[119] B.-G. Chun, S. Ihm, P. Maniatis, M. Naik, A. Patti, CloneCloud: Elastic execution between mobile device and cloud, in: Proc. of 6th Conference on Computer Systems, 2011, pp. 301–314.

[120] T.H. Noor, S. Zeadally, A. Alfazi, Q.Z. Sheng, Mobile cloud computing: Challenges and future research directions, J. Netw. Comput. Appl. 115 (2018) 70–85.

[121] R. Xie, Q. Tang, Q. Wang, X. Liu, F.R. Yu, T. Huang, Satellite-terrestrial integrated edge computing networks: Architecture, challenges, and open issues, IEEE Netw. 34 (3) (2020) 224–231.

[122] V. Koufi, F. Malamateniou, G. Vassilacopoulos, Ubiquitous access to cloud emergency medical services, in: Proc. of the 10th IEEE International Conference on Information Technology and Applications in Biomedicine, IEEE, 2010, pp. 1–4.

[123] L. Zhang, H. Li, K. Chen, Effective risk communication for public health emergency: Reflection on the COVID-19 (2019-nCoV) outbreak in Wuhan, China, in: Healthcare, Vol. 8, Multidisciplinary Digital Publishing Institute, 2020, p. 64.

[124] ETSI TETRA standards page, 2022, https://www.etsi.org/technologies/tetra (Accessed August 4, 2022).

[125] Why is TETRAPOL?, 2022, https://www.tetrapol.com/technology/why_tetrapol/ (Accessed August 4, 2022).

[126] ETSI TR 102 022-1 V1.1.1, User Requirement Specification; Mission Critical Broadband Communication Requirements, Rel. 17, 2012.

[127] P25 Standards page, 2022, https://www.apcointl.org/spectrum-management/spectrum-management-resources/interoperability/p25/ (Accessed August 4, 2022).

[128] ETSI TR 102 398 V1.4.1, Electromagnetic Compatibility and Radio Spectrum Matters (ERM); Digital Mobile Radio (DMR) General System Design, 2018.

[129] DMR association (DMR standard), 2022, https://www.dmrassociation.org/dmr-standards.html (Accessed August 4, 2022).

[130] NXDN forum, 2022, http://www.nxdn-forum.com/what-is-nxdn/nxdn-a-brief-overview/ (Accessed August 4, 2022).

[131] Tetrapol technology underpins security at Brazil world cup, 2022, https://www.policeprofessional.com/news/tetrapol-technology-underpins-security-at-brazil-world-cup/ (Accessed August 4, 2022).

[132] A. Durantini, M. Petracca, F. Vatalaro, A. Civardi, F. Ananasso, Integration of broadband wireless technologies and PMR systems for professional communications, in: Proc. of 4th International Conference on Networking and Services (ICNS 2008), IEEE, 2008, pp. 84–89.

[133] A. Jarwan, A. Sabbah, M. Ibnkahla, O. Issa, LTE-based public safety networks: A survey, IEEE Commun. Surv. Tutor. 21 (2) (2019) 1165–1187.

[134] S. Avgousti, Mobile Video Tele-Echography Robotic Platform Over 4G-LTE Network, University of Orleans France, 2016.

[135] Ready to test 5G data throughput?, 2022, https://www.microwavejournal.com/articles/print/29477-ready-to-test-5g-data-throughput (Accessed August 4, 2022).

[136] GSMA, 5G spectrum GSMA public policy position, 2021, https://www.gsma.com/spectrum/wp-content/uploads/2021/04/5G-Spectrum-Positions.pdf (Accessed August 4, 2022).

[137] D. López-Pérez, A. Garcia-Rodriguez, L. Galati-Giordano, M. Kasslin, K. Doppler, IEEE 802.11 be extremely high throughput: the next generation of wi-fi technology beyond 802.11 ax, IEEE Commun. Mag. 57 (9) (2019) 113–119.

[138] 3GPP TR 21.915 V15.0.0, Release 15 Description; Summary of Rel-15 Work Items (Release 15), 2019.

[139] T.S. Rappaport, Y. Xing, O. Kanhere, S. Ju, A. Madanayake, S. Mandal, A. Alkhateeb, G.C. Trichopoulos, Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond, IEEE Access 7 (2019) 78729–78757.

[140] R. Ferrus, O. Sallent, G. Baldini, L. Goratti, LTE: the technology driver for future public safety communications, IEEE Commun. Mag. 51 (10) (2013) 154–161.

[141] N. Stepanov, A. Veprev, A. Sharapova, D. Alekseeva, M. Komarov, E.S. Lohan, A. Ometov, On machine learning applicability to transaction time prediction for time-critical C-ITS applications, in: 2021 44th International Conference on Telecommunications and Signal Processing (TSP), 2021, pp. 408–413, http://dx.doi.org/10.1109/TSP52935.2021.9522629.

[142] M. Khalid, M. Awais, N. Singh, S. Khan, M. Raza, Q.B. Malik, M. Imran, Autonomous transportation in emergency healthcare services: Framework, challenges, and future work, IEEE Internet Things Mag. 4 (1) (2021) 28–33.

[143] N. Stepanov, D. Alekseeva, A. Ometov, E.S. Lohan, Applying machine learning to LTE traffic prediction: Comparison of bagging, random forest, and SVM, in: Proc. of 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2020, pp. 119–123, http://dx.doi.org/10.1109/ICUMT51630.2020.9222418.

[144] W.B. Qaim, A. Ometov, A. Molinaro, I. Lener, C. Campolo, E.S. Lohan, J. Nurmi, Towards energy efficiency in the internet of wearable things: A systematic review, IEEE Access 8 (2020) 175412–175435.

[145] W.B. Qaim, A. Ometov, C. Campolo, A. Molinaro, E.S. Lohan, J. Nurmi, Understanding the performance of task offloading for wearables in a two-tier edge architecture, in: Proc. of 13th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), IEEE, 2021, pp. 1–9.

[146] P. Ranaweera, A.D. Jurcut, M. Liyanage, Survey on multi-access edge computing security and privacy, IEEE Commun. Surv. Tutor. 23 (2) (2021) 1078–1124.

[147] A. Alhroob, V.W. Samawi, Privacy in cloud computing: Intelligent approach, in: Proc. of International Conference on High Performance Computing Simulation (HPCS), 2018, pp. 1063–1065.

[148] S. Parikh, D. Dave, R. Patel, N. Doshi, Security and privacy issues in cloud, fog and edge computing, Procedia Comput. Sci. 160 (2019) 734–739.

[149] A. Ometov, O.L. Molua, M. Komarov, J. Nurmi, A survey of security in cloud, edge, and fog computing, Sensors 22 (3) (2022) 927.

[150] M. Nguyen, M.O. Gani, V. Raychoudhury, Yours truly? Survey on accessibility of our personal data in the connected world, in: Proc. of IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), IEEE, 2019, pp. 292–297.

[151] K. Lee, Security threats in cloud computing environments, Int. J. Secur. Appl. 6 (4) (2012) 25–32.

[152] Cloud Security Alliance, The Treacherous Twelve-Cloud Computing Top Threats in 2016, 2016.

[153] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, M. Rajarajan, A survey of intrusion detection techniques in cloud, J. Netw. Comput. Appl. 36 (1) (2013) 42–57.

[154] V. Chang, M. Ramachandran, Towards achieving data security with the cloud computing adoption framework, IEEE Trans. Serv. Comput. 9 (1) (2016) 138–151.

[155] A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, et al., Above the Clouds: A Berkeley View of Cloud Computing, Vol. 28, Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS, 2009, p. 2009, (13).

[156] S. Pearson, A. Benameur, Privacy, security and trust issues arising from cloud computing, in: Proc. of IEEE Second International Conference on Cloud Computing Technology and Science, IEEE, 2010, pp. 693–702.

[157] S.D.C. Di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, P. Samarati, Over-encryption: Management of access control evolution on outsourced data, in: Proc. of 33rd International Conference on Very Large Data Bases, 2007, pp. 123–134.

[158] A. Mills, Protecting your data: Cloud security alliance, CIO (Jul/Aug 2012) (2012).

[159] A.K. Tyagi, S. Niladhuri, R. Priya, Never trust anyone: Trust-privacy trade-offs in vehicular ad-hoc networks, J. Adv. Math. Comput. Sci. (2016) 1–23.

[160] P.J. Sun, Privacy protection and data security in cloud computing: A survey, challenges, and solutions, IEEE Access 7 (2019) 147420–147452.

[161] R.P. França, Y. Iano, A.C.B. Monteiro, R. Arthur, Lower memory consumption for data transmission in smart cloud environments with CBEDE methodology, in: Smart Systems Design, Applications, and Challenges, IGI Global, 2020, pp. 216–237.

[162] N. Mäkitalo, A. Ometov, J. Kannisto, S. Andreev, Y. Koucheryavy, T. Mikkonen, Safe, secure executions at the network edge: Coordinating cloud, edge, and fog computing, IEEE Softw. 35 (1) (2017) 30–37.

[163] X. Xu, X. Liu, Z. Xu, C. Wang, S. Wan, X. Yang, Joint optimization of resource utilization and load balance with privacy preservation for edge services in 5G networks, Mob. Netw. Appl. 25 (2) (2020) 713–724.

[164] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Gener. Comput. Syst. 28 (3) (2012) 583–592.

[165] I. Stojmenovic, S. Wen, The fog computing paradigm: Scenarios and security issues, in: Proc. of Federated Conference on Computer Science and Information Systems, IEEE, 2014, pp. 1–8.

[166] A.N. Khan, M. Ali, A.u.R. Khan, F.G. Khan, I.A. Khan, W. Jadoon, S. Shamshirband, A.T. Chronopoulos, A comparative study and workload distribution model for re-encryption schemes in a mobile cloud computing environment, Int. J. Commun. Syst. 30 (16) (2017) e3308.

[167] M. Du, K. Wang, Y. Chen, X. Wang, Y. Sun, Big data privacy preserving in multi-access edge computing for heterogeneous internet of things, IEEE Commun. Mag. 56 (8) (2018) 62–67.

[168] Y. Hou, S. Garg, L. Hui, D.N.K. Jayakody, R. Jin, M.S. Hossain, A data security enhanced access control mechanism in mobile edge computing, IEEE Access 8 (2020) 136119–136130.

[169] H. Zeyu, X. Geming, W. Zhaohang, Y. Sen, Survey on edge computing security, in: Proc. of International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), 2020, pp. 96–105.

[170] K. Wang, M. Du, D. Yang, C. Zhu, J. Shen, Y. Zhang, Game-theory-based active defense for intrusion detection in cyber-physical embedded systems, 2016.

[171] W. Shi, L. Zhang, C. Wu, Z. Li, F.C. Lau, An online auction framework for dynamic resource provisioning in cloud computing, ACM SIGMETRICS Perform. Eval. Rev. 42 (1) (2014) 71–83.

[172] F. Ma, X. Luo, E. Litvinov, Cloud computing for power system simulations at ISO new England—Experiences and challenges, IEEE Trans. Smart Grid 7 (6) (2016) 2596–2603.

[173] X. Chen, L. Jiao, W. Li, X. Fu, Efficient multi-user computation offloading for mobile-edge cloud computing, IEEE/ACM Trans. Netw. 24 (5) (2015) 2795–2808.

[174] F. Bonomi, R. Milito, J. Zhu, S. Addepalli, Fog computing and its role in the internet of things, in: Proc. of 1st MCC Workshop on Mobile Cloud Computing, 2012, pp. 13–16.

[175] M. Aazam, E.-N. Huh, Fog computing: The cloud-IoT\IoE middleware paradigm, IEEE Potentials 35 (3) (2016) 40–44.

[176] H. El-Sayed, S. Sankar, M. Prasad, D. Puthal, A. Gupta, M. Mohanty, C.-T. Lin, Edge of things: The big picture on the integration of edge, IoT and the cloud in a distributed computing environment, IEEE Access 6 (2017) 1706–1717.

[177] S. Khan, S. Parkinson, Y. Qin, Fog computing security: A review of current applications and security solutions, J. Cloud Comput. 6 (1) (2017) 1–22.

[178] H.F. Atlam, R.J. Walters, G.B. Wills, Fog computing and the internet of things: A review, Big Data Cogn. Comput. 2 (2018).

[179] J. Ni, K. Zhang, X. Lin, X. Shen, Securing fog computing for internet of things applications: Challenges and solutions, IEEE Commun. Surv. Tutor. 20 (1) (2018) 601–628.

[180] O. Alkadi, N. Moustafa, B. Turnbull, A review of intrusion detection and blockchain applications in the cloud: Approaches, challenges and solutions, IEEE Access 8 (2020) 104893–104917.

[181] A. Ara, M. Al-Rodhaan, Y. Tian, A. Al-Dhelaan, A secure service provisioning framework for cyber physical cloud computing systems, 2015, arXiv preprint arXiv:1611.00374.

[182] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, W. Lv, Edge computing security: State of the art and challenges, Proc. IEEE 107 (8) (2019) 1608–1631.

[183] P. Krishnan, S. Duttagupta, K. Achuthan, SDN/NFV security framework for fog-to-things computing infrastructure, Softw. - Pract. Exp. 50 (2020) 757–800.

[184] Q. Li, W. Li, J. Wang, M. Cheng, A SQL injection detection method based on adaptive deep forest, IEEE Access 7 (2019) 145385–145394.

[185] A. Alwarafy, K.A. Al-Thelaya, M. Abdallah, J. Schneider, M. Hamdi, A survey on security and privacy issues in edge-computing-assisted internet of things, IEEE Internet Things J. 8 (6) (2021) 4004–4022.

[186] X. Xie, C. Ren, Y. Fu, J. Xu, J. Guo, SQL injection detection for web applications based on elastic-pooling CNN, IEEE Access 7 (2019) 151475–151481.

[187] N. Soni, R. Malekian, A. Thakur, Edge computing in transportation: Security issues and challenges, 2020, ArXiv abs/2012.11206.

[188] N.M. Almutairy, K.H. Al-Shqeerat, A survey on security challenges of virtualization technology in cloud computing, Int. J. Comput. Sci. Inf. Technol. (IJCSIT) 11 (2019).

[189] Z. Tao, Q. Xia, Z. Hao, C. Li, L. Ma, S. Yi, Q. Li, A survey of virtual machine management in edge computing, Proc. IEEE 107 (8) (2019) 1482–1499.

[190] T. Veerraju, K.K. Kumar, A survey on fog computing: Research challenges in security and privacy issues, Int. J. Eng. Technol. 7 (2.7) (2018) 335–340.

[191] M. Kazim, S.Y. Zhu, Virtualization security in cloud computing, in: Guide to Security Assurance for Cloud Computing, Springer, 2015, pp. 51–63.

[192] S. Kumarasamy, A. Gowrishankar, An active defense mechanism for TCP syn flooding attacks, 2022, ArXiv abs/1201.2103.

[193] I. Butun, P. Österberg, H. Song, Security of the internet of things: Vulnerabilities, attacks, and countermeasures, IEEE Commun. Surv. Tutor. 22 (1) (2020) 616–644.

[194] P. Sinha, V.K. Jha, A.K. Rai, B. Bhushan, Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey, in: Proc. of International Conference on Signal Processing and Communication (ICSPC), 2017, pp. 288–293.

[195] A. Faisal, M. Zulkernine, A secure architecture for TCP/UDP-based cloud communications, Int. J. Inf. Secur. 20 (2) (2021) 161–179.

[196] O.H. Younis, S.E. Essa, E.-S. Ayman, A survey on security attacks/defenses in mobile ad-hoc networks, Commun. Appl. Electron. 6 (2017) 1–9.

[197] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen, M. Chai, The impact of rank attack on network topology of routing protocol for low-power and lossy networks, IEEE Sens. J. 13 (10) (2013) 3685–3692.

[198] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications, IEEE Internet Things J. 4 (5) (2017) 1125–1142.

[199] F. Pan, Z. Pang, M. Luvisotto, M. Xiao, H. Wen, Physical-layer security for industrial wireless control systems: Basics and future directions, IEEE Ind. Electron. Mag. 12 (4) (2018) 18–27.

[200] S. Echeverría, D. Klinedinst, K. Williams, G.A. Lewis, Establishing trusted identities in disconnected edge environments, in: Proc. of IEEE/ACM Symposium on Edge Computing (SEC), IEEE, 2016, pp. 51–63.

[201] C.-T. Li, C.-C. Lee, C.-Y. Weng, A dynamic identity-based user authentication scheme for remote login systems, Sec. Commun. Netw. 8 (18) (2015) 3372–3382.

[202] D. Wang, B. Bai, K. Lei, W. Zhao, Y. Yang, Z. Han, Enhancing information security via physical layer approaches in heterogeneous IoT with multiple access mobile edge computing in smart city, IEEE Access 7 (2019) 54508–54521.

[203] B.D. Davis, J.C. Mason, M. Anwar, Vulnerability studies and security postures of IoT devices: A smart home case study, IEEE Internet Things J. 7 (10) (2020) 10102–10110.

[204] S. Shahzadi, M. Iqbal, T. Dagiuklas, Z.U. Qayyum, Multi-access edge computing: Open issues, challenges and future perspectives, J. Cloud Comput. 6 (1) (2017) 1–13.

[205] S. Bali, Barriers to development of telemedicine in developing countries, in: Telehealth, IntechOpen, 2018.

[206] F. Luh, Y. Yen, Cybersecurity in science and medicine: Threats and challenges, Trends Biotechnol. 38 (8) (2020) 825–828.

[207] R. Moreno-Vozmediano, R.S. Montero, I.M. Llorente, Key challenges in cloud computing: Enabling the future internet of services, IEEE Internet Comput. 17 (4) (2012) 18–25.

[208] K. Gai, J. Guo, L. Zhu, S. Yu, Blockchain meets cloud computing: A survey, IEEE Commun. Surv. Tutor. 22 (3) (2020) 2009–2030.

[209] O. Chukhno, N. Chukhno, G. Araniti, C. Campolo, A. Iera, A. Molinaro, Optimal placement of social digital twins in edge IoT networks, Sensors 20 (21) (2020) 6181.

[210] X. Xia, F. Chen, Q. He, J.C. Grundy, M. Abdelrazek, H. Jin, Cost-effective app data distribution in edge computing, IEEE Trans. Parallel Distrib. Syst. 32 (1) (2020) 31–44.

[211] Y. Wang, J. Li, H.H. Wang, Cluster and cloud computing famework for scientific metrology in flow control, Cluster Comput. 22 (1) (2019) 1189–1198.

[212] A. Bonadio, F. Chiti, R. Fantacci, Performance analysis of an edge computing saas system for mobile users, IEEE Trans. Veh. Technol. 69 (2) (2019) 2049–2057.

[213] C. Li, M. Song, M. Zhang, Y. Luo, Effective replica management for improving reliability and availability in edge-cloud computing environment, J. Parallel Distrib. Comput. 143 (2020) 107–128.

[214] S.H. Mortazavi, M. Salehe, C.S. Gomes, C. Phillips, E. De Lara, Cloudpath: A multi-tier cloud computing framework, in: Proceedings of the Second ACM/IEEE Symposium on Edge Computing, 2017, pp. 1–13.

[215] T. Han, L. Zhang, S. Pirbhulal, W. Wu, V.H.C. de Albuquerque, A novel cluster head selection technique for edge-computing based iomt systems, Comput. Netw. 158 (2019) 114–122.

[216] D. Lindsay, S.S. Gill, D. Smirnova, P. Garraghan, The evolution of distributed computing systems: From fundamental to new frontiers, Computing (2021) 1–20.

[217] A.E. Eshratifar, M.S. Abrishami, M. Pedram, JointDNN: An efficient training and inference engine for intelligent mobile cloud computing services, IEEE Trans. Mob. Comput. (2019).

[218] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J.D. Thornton, D.K. Smetters, B. Zhang, G. Tsudik, D. Massey, C. Papadopoulos, et al., Named data networking (NDN) project, in: Relatório Técnico NDN-0001, Xerox Palo Alto Research Center-PARC, Vol. 157, 2010, p. 158.
[219] A. Arunarani, D. Manjula, V. Sugumaran, Task scheduling techniques in cloud computing: A literature survey, Future Gener. Comput. Syst. 91 (2019) 407–415.
[220] T.X. Tran, A. Hajisami, P. Pandey, D. Pompili, Collaborative mobile edge computing in 5G networks: New paradigms, scenarios, and challenges, IEEE Commun. Mag. 55 (4) (2017) 54–61.
[221] Y. Jiang, Z. Huang, D.H. Tsang, Challenges and solutions in fog computing orchestration, IEEE Netw. 32 (3) (2017) 122–129.
[222] R. Mahmud, K. Ramamohanarao, R. Buyya, Latency-aware application module management for fog computing environments, ACM Trans. Internet Technol. (TOIT) 19 (1) (2018) 1–21.
[223] J. Zheng, Y. Cai, Y. Wu, X. Shen, Dynamic computation offloading for mobile cloud computing: A stochastic game-theoretic approach, IEEE Trans. Mob. Comput. 18 (4) (2018) 771–786.
[224] F. Zhang, R. Deng, H. Liang, An optimal real-time distributed algorithm for utility maximization of mobile ad hoc cloud, IEEE Commun. Lett. 22 (4) (2018) 824–827.
[225] Fresh approach to patient care takes flight, 2022, https://www.albertahealthservices.ca/news/Page15580.aspx (Accessed August 4, 2022).
[226] Y. Gao, J. Cao, P. Wang, J. Wang, M. Zhao, S. Cheng, S. Hu, W. Lu, UAV based 5G wireless networks: A practical solution for emergency communications, in: Proc of XXXIIIrd General Assembly and Scientific Symposium of the International Union of Radio Science, IEEE, pp. 1–4.
[227] Z. Jia, M. Sheng, J. Li, D. Niyato, Z. Han, LEO satellite-assisted UAV: Joint trajectory and data collection for internet of remote things in 6G aerial access networks, IEEE Internet Things J. (2020).
[228] Q. Zhu, F. Sun, Z. Hua, Research on hybrid network communication scheme of high and low orbit satellites for power application, in: 2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), Vol. 9, IEEE, 2020, pp. 460–466.
[229] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, Fog computing for healthcare 4.0 environment: Opportunities and challenges, Comput. Electr. Eng. 72 (2018) 1–13.
[230] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop, J. Rodriguez, D. Lymberopoulos, A survey on security threats and countermeasures in internet of medical things (IoMT), Trans. Emerg. Telecommun. Technol. (2020) e4049.
[231] W. Shi, J. Cao, Q. Zhang, Y. Li, L. Xu, Edge computing: Vision and challenges, IEEE Internet Things J. 3 (5) (2016) 637–646.
[232] A. Jain, M. Mishra, S.K. Peddoju, N. Jain, Energy efficient computing-green cloud computing, in: 2013 International Conference on Energy Efficient Technologies for Sustainability, IEEE, 2013, pp. 978–982.
[233] I. Yaqoob, E. Ahmed, A. Gani, S. Mokhtar, M. Imran, S. Guizani, Mobile ad hoc cloud: A survey, Wirel. Commun. Mob. Comput. 16 (16) (2016) 2572–2589.
[234] I. Yaqoob, E. Ahmed, A. Gani, S. Mokhtar, M. Imran, Heterogeneity-aware task allocation in mobile ad hoc cloud, IEEE Access 5 (2017) 1779–1795.

Daria Alekseeva received the B.Sc. and M.Sc. degrees in info-communication technologies and networks from the Saint-Petersburg State University of Telecommunications (SUT) in 2017 and 2019, respectively. She is currently pursuing the Ph.D. degree with Tampere University (TAU), Finland. Her research interests include wireless communications, network security, computing paradigms, and neural network technologies.

Aleksandr Ometov received the M.Sc. degree in information technology and the D.Sc. (Tech.) degree in communications engineering from the Tampere University of Technology (TUT), Finland, in 2016 and 2018, respectively. He also holds the Specialist degree in information security from the Saint Petersburg State University of Aerospace Instrumentation (SUAI) from 2013. He is a Postdoctoral Research Fellow at Tampere University (TAU), Finland. He is working on EU H2020 MCSA A-WEAR and APROPOS projects. His research interests include wireless communications, information security, computing paradigms, blockchain technology, and wearable applications.

Otso Arponen is a resident doctor and a post-doctoral researcher in the Department of Radiology at Tampere University Hospital in Finland. He earned his Licentiate and Ph.D. degrees in Medicine from the University of Eastern Finland in 2017 and 2020, respectively. In June 2022, he joined the Department of Radiology at the University of Cambridge, UK, as a visiting researcher. His main research interests include clinical oncological imaging, the clinical applications of novel magnetic resonance imaging sequences, and the utilization radiological services Dr. Arponen supervises 15 Ph.D. students and four M.D. thesis students. He is continually looking for his next travel destination and enjoys reading and going to the gym.

Elena Simona Lohan received the M.Sc. degree in electrical engineering from the Polytechnic University of Bucharest, Romania, in 1997, the D.E.A. degree (French equivalent of master) in econometrics from Ecole Polytechnique, Paris, France, in 1998, and the Ph.D. degree in telecommunications from the Tampere University of Technology, in 2003. She is currently a Professor at the Electrical Engineering Unit, Tampere University (TAU), Finland, and the Coordinator of the MSCA EU A-WEAR Network. Her current research interests include wireless location techniques, wearable computing, and privacy-aware positioning solutions.