1. Future Wireless Communication Systems to enable IoMT Services and Applications

Francisco Falcone
https://orcid.org/0000-0002-4911-9753
José Javier Astrain
https://orcid.org/0000-0002-7792-6317
Idoia Aguirre
Jesús Daniel Trigo
https://orcid.org/0000-0003-2916-4052
Luis Serrano
https://orcid.org/0000-0002-7072-4464

Abstract
In this chapter, we will describe the framework for IoMT evolution, from current LPWAN/5G connectivity to future B5G systems, focusing on sub THz (mainly in the 100 GHz to 300 GHz frequency range) and THz bands (up to 10 THz). The requirements in terms of device integration, node density, interference and energy handling will be described. The specific requirements in terms of wearable devices, considering intra-body, on-body and off-body communication links will be described. Coverage/capacity estimations for different case uses considering different communication link types will be presented. Different application scenarios, such as the evolution of current IoMT applications towards sensing networks will be discussed. Security as well as interoperability and standardization aspects within the IoMT communication framework will also be described.

1.1 Wireless Communication Systems

The IoMT market has grown exponentially from double-digit values, approximately $41.2 billion, during the past decade to three figures, $ 158.1 billion, in the present decade [1]. This growth can have its pillars in two aspects. On the one hand, a new idea of the patient-empowerment given that daily clinical practice can spin around them with IoMT. This concept can include not only common medical devices equipped with connectivity but also wearable devices, as well as apps connected to the Hospital Information System, even including more complex devices such as drones or AI and Augmented Reality algorithms [2-4]. On the other hand, the availability of technology and the past, present and future scenario of COVID-19 have led to the deployment of Health Services based on IoMT where the efficiency of the system and the safety of both patients and Health workers and, therefore, security in the provision of these “new” Health Services prevail. We are all aware that this daily clinical practice based on IoMT has come to stay. This evolution requires to consider additional implementation aspects, such as seamless/continuous connectivity, data/system interoperability, availability of distributed data/cloud handling infrastructure as well as user/data security and privacy.

One of the key aspects in order to enable the required interactivity levels that define context aware scenarios and their related applications are communication systems, as a part of the information and communication technology framework. In this sense, communication networks have experienced a sustained evolution towards network convergence, with the goal of providing the most adequate resource allocation given quality of service/quality of

experience metrics [5-7]. Wireless communication systems are largely employed within general IoT and more specific IoMT applications, owing to their ease of deployment, ubiquity, mobility and scalability. There are multiple wireless communication systems that can be employed, given coverage/capacity requirements (i.e., maximum transmission rate for given receiver sensitivity values), as well as by constraints such as limited energy availability, ergonomics, form factor or low cost, among others. Moreover, in the case of IoMT applications, there can be inherent requirements in relation with node/sensor location within the user, requiring intra-body or inter-body communication capabilities.

Wireless communication systems can be classified depending on there coverage range, as well as their mobility level, into the following categories:

- Wide area networks (WAN): provides worldwide coverage levels, with high mobility. Public Land Mobile Networks (PLMN) and Satellite Communication Networks (SatCom) are the main WAN types. Current PLMN networks provide heterogeneous operation (given by variable cell size as well as by network exchange via hand over mechanisms), co-existing legacy 3G networks, mature 4G networks and 5G networks in rollout phase. The evolution of 5G networks give rise to the concept of beyond 5G (B5G) and future 6G networks, which are expected to be a reality by 2030. PLMN usually operate below the 6 GHz frequency range (mainly in 900 to 3600 MHz range), whereas SatCom usually operate in X-band. 5G networks have opened the path to the use of millimetre wave spectrum, mainly in the 26-28GHz bands, whereas future 6G systems are exploring more intensive use of sub THz frequencies, particularly up to 300 GHz frequency range [7].
- Low Power Wide Area Networks (LPWAN): provide coverage levels of up to several km with respect to the corresponding gateway. LPWAN have gained popularity, as a natural evolution of wireless sensor networks, focusing on providing extended battery life (up to 10 years, taking advantage of energy harvesting techniques, such as photo-electric cells, thermo-electric effects, piezo-electric effects or electromagnetic energy scavenging via rectenna elements, among others). Within LPWANs different systems have been developed mainly within the framework of the 802.15 standard, such as LoRa/LoRaWAN, SigFox, ZigBee or eNocean, among others. PLMN based networks oriented towards telementry/sensor networks can also be considered part of LPWANs, including systems such as NB-IoT or LTE Cat M. Transmission rates are in general below 250 kbps, operating in frequency bands in the 400Mhz to 2400MHz frequency range.
- Wireless Local Area Networks (WLAN): developed in the late 90s as the wireless evolution of Ethernet 802.3 standard, it has become one of the most employed access networks, providing coverage levels usually below the km range. WLANs are developed within the IEEE 802.11 standards framework, providing transmission rates that vary from 1 Mbps to over 10 Gbps in the case of 802.11ax (referred as Wi-Fi 6 standard). WLANs frequency bands have been allocated from sub 1 GHz bands (in the case of 802.11ah, focused on IoT applications, in the 900MHz band) up to millimetre waves (60 GHz band in the case of 802.11ad). The most employed currently are in the 2.4 GHz and 5.5GHz to 5.9 GHz frequency ranges (being the upper band of the later reserved mainly for vehicular communications).
- Personal Area Networks (PAN): also developed within the framework of 802.15 (mainly 802.15.4), they provide short range communications (below 100m) usually for limited time, enabling connectivity of multiple types of devices, such as wearables to mobile gateways, such as smartphones. Examples of PAN are Bluetooth and Bluetooth Low

Energy, operating in the 2.4 GHz frequency, with transmission rates usually in the 1-2Mbps range as well as Ultrawideband (UWB) technology, which operate in the 4 GHz and 6 GHz frequency bands.

A schematic view of the coverage/capacity relations provided by wireless communication systems, spanning from PAN, LPWAN, WLAN and WAN is depicted in figure 1.

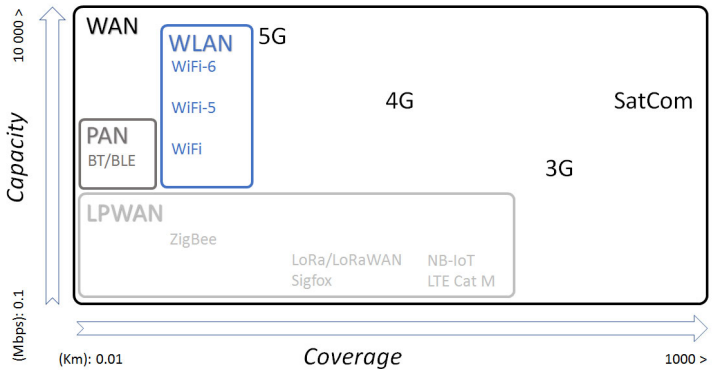


Figure 1. Schematic overview of coverage/capacity relations for different wireless systems, from LPWAN to WAN networks.

In order to analyse deployment requirements of wireless communication systems and hence the feasibility of employing one class of system or another, it is necessary to obtain the maximum transmission link distance as a function of receiver sensitivity thresholds, which gives rise to coverage/capacity relations. In this way, a simplified analytical approach can be followed, given by the following expressions:

$$P_{RX} \geq SENS_{RX} \quad (1)$$

$$P_{RX} = P_{TX} - L_{cable-feed\,TX} + G_{Ant\,TX} - L_{prop} + G_{Ant\,RX} - L_{cable-feed\,RX} \quad (2)$$

where:

- P_{RX}: Power level at receiver end of communication link in log scale
- $SENS_{RX}$: receiver sensitivity threshold, which depends on parameters such as binary transmission rate, modulation and coding schemes and transceiver specifications (such as amplifier noise factors or device phase noise)
- P_{TX}: Transmission power level in log scale. Varies depending parameters such as power control mechanisms and terminal class, among others
- $L_{cable\text{-}feed\ TX}$- $L_{cable\text{-}feed\ RX}$: losses corresponding to the transmission lines and cables employed for the feeding network, antenna matching circuits, power divider, power coupling and diplexer filters, at the transmitter/receiver side, respectively.
- $G_{Ant\ TX}$- $G_{Ant\ RX}$: Gain of transmitter/receiver antenna, which depends on the radiation diagram of the corresponding antenna element. Effects such as human body presence, which produces impedance mismatch, frequency shift and modification in radiation diagram need to be considered.
- L_{prop}: propagation losses, accounting the different physical phenomena related with the interaction of electromagnetic waves with the surrounding environment, as well as to inherent propagation mechanisms.

The highest variability and usually the most limiting factor in coverage/capacity relations is given by the propagation losses experienced by wireless links. The mechanisms that influence these losses are the following:

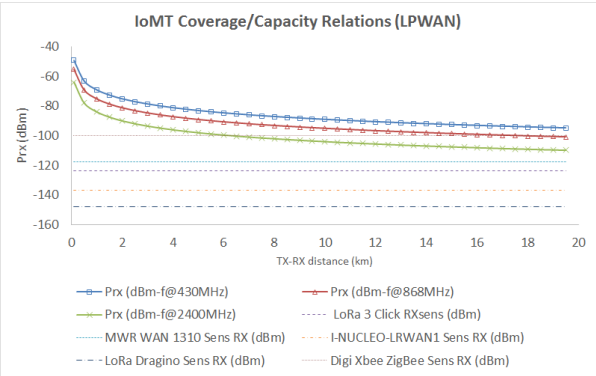
- Free space losses, exhibiting higher losses as distance between transmitter and receiver increases, as well as frequency dependence.
- Atmospheric losses: given by the interaction of electromagnetic waves with gases as well as hydrometeors in the atmosphere (mainly at the troposphere level). Losses increase with frequency, particularly in the millimetre wave range, with different absorption peaks given by the presence of different gases such forms of H_2O, CO_X, NO_x or N_2 among others. In the case of IoMT applications, usually frequency bands in the sub 6 GHz range are considered, which exhibit low atmospheric losses. The future use of millimetre wave frequencies gives rise to short transmission ranges, especially in the case of considering human body interaction (owing to additional body losses, later described), which leads mainly to body area network applications.
- Interaction with material objects: the presence of different elements in the wireless communication path derives into situations in which the propagating waves interact with these elements (e.g., furnishings, vegetation, presence of human bodies, etc.). This results in reflected, refracted, diffracted and scattered waves, being the main consequence the increase in the losses experienced by the propagating electromagnetic waves, decreasing the effective coverage radius. The effect of these interactions is described by deriving the corresponding transmission and reflection coefficients by application of Fresnel equations, which depend on the frequency, polarization, conductivity, dielectric constant and loss tangent of the different material elements within the scenarios under analysis. Diffraction losses are given by the presence of elements such as corners, edges or wedges, which by means of Huygens law, re-radiates new diffracted wave fronts, which are strongly dependent on the shape and material of the diffraction region. This will be usually the case with the presence objects with sharp edges, such as building corners or in the case of indoor environments, furniture or infrastructure elements. Additionally, the presence of non-homogeneous and rough surfaces gives rise to diffuse scattering, in which besides the corresponding reflected wave, a set of randomly disposed reflected wave components of small amplitude are generated, leading to an effective decrease in the received power levels and hence, reduces overall coverage. The main elements for diffuse scattering are given by building facades/walls and vegetation. There is also increased interest in the effect of diffused scattering caused by human body interaction, which is a variable to consider in the case of IoMT, particularly in the case of taking advantage of wearable transceivers.
- Human body presence: IoMT applications are in many cases user-centric, making use of wearable devices in stand alone or in a body area network configuration. Therefore, interaction of electromagnetic waves with the body of the users is unavoidable. The human body can be considered as an object present in the scenario under analysis in which wireless communication systems operate, requiring specific considerations [8-9]. On the one hand, the human body is composed of multiple tissues, with variable (but usually high) water content and different dielectric constant, loss tangent and conductivity values. This gives rise to losses in the case of intrabody propagation, as well as losses owing to off-body propagation mechanisms. The later is also given by the fact that the presence of the human body (as well other elements, such as garmets worn by the users) produce additional effects, such as changes in antenna impedance and variation in radiation diagram characteristics, which can limit the performance of wireless links. Other considerations must also be taken into account, such as the need for low profile, ergonomic and conformable devices, which again limit the performance. Different approaches have been proposed for the integration of

wireless transceivers in wearables, such as the use of flexible electronics (implemented with techniques such as inkjet or screen printing), miniaturized chip antennas or embedded conductive textiles, among others.

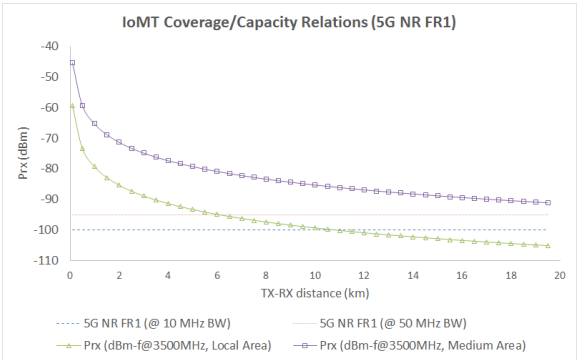
IoMT applications can span from social sensor network parameters to monitor user behaviour (e.g., presence sensors, accelerometers to monitor vertical/horizontal positions and hence, emergency situations owing to falls, pressure sensor in beds, etc.), continuous monitoring of biophysical signals (e.g., ECG, EEG, EMG, temperature, oxygen saturation level, etc.), real time transmission of audio/video signals for remote assistance or AR/VR information for medical diagnosis/training/procedures, just to name a few. These applications have different QoS/QoE parameters, with transmission bit rates in the range of 1Kbps to over 1Gbps or delay tolerance from 5 ms (e.g., remote robotic surgery) to several seconds (for device telemetry). On top of the application requirements, the impact of interference must also be considered, as this will degrade receiver performance. Interference sources can arise either from neighbouring users of our wireless communication system (intra-system interference), from other wireless communication systems (inter-system) or they can be generated by other external sources, such as brush motors, inductive arch welding, etc. [9-10]. Therefore, coverage/capacity analysis can provide insight in relation with the capabilities in network deployment as a function of the different available wireless communication systems. With this in mind, different results have been obtained and are presented in figure 2 related with coverage/capacity estimations, as a function of the employed frequency band and wireless system.

As it can be seen, depending on the frequency of operation, wireless system parameters and receiver sensitivity thresholds, communication link ranges can vary from meters to over several kilometres. It can be seen that if QoS parameters become more stringent, such as an increase in required transmission bit rate, in general coverage radius will decrease. Moreover, as interference values increase within the operating scenarios of the IoMT wireless systems, this will limit receiver performance (i.e., equivalent to degradation in receiver sensitivity value) which in turn will also reduce maximum wireless link distance. The values obtained consider in general line of sight conditions, therefore, if partial line of sight or non-line of sight conditions take place, expected coverage distances will be further reduced.

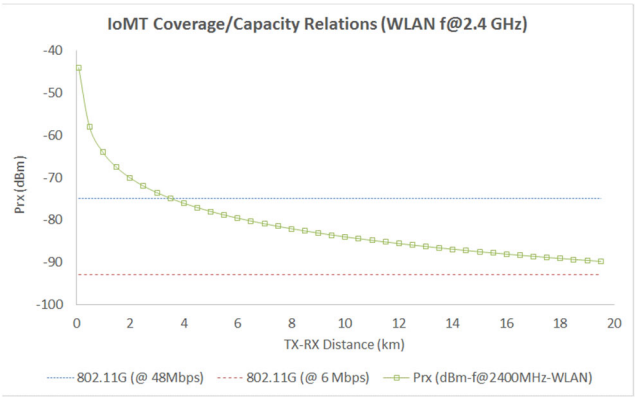
Once that the impact of wireless channel behaviour in terms of coverage/capacity considerations has been described, we will now discuss the impact in communication system within IoMT applications given by interoperability, distributed computing resources and related security issues.



a)



b)



c)

Figure 2: Estimation of coverage/capacity relations for a) LPWAN systems operating in 433 MHz, 868MHz and 2.4 GHz, b) 5G NR FR1 systems operating in 3.5 GHz, c) WLAN (f@2.4 GHz) systems, considering urban scenarios in predominant LOS link conditions.

1.2 Data standardization and interoperability in IoMT architectures

Data governance and management is crucial for ensuring data quality in current and future IoT and IoMT frameworks. In this context, interoperability and standardization are regarded as strategic enablers for versatile, seamless integration. The state of affairs of the Information and Communication Technologies (ICT) in the healthcare environment includes a gradually rising number of government policies and initiatives as well as a wide variety of standardization bodies and entities. In this subsection of the book chapter, an in-depth overview of the most relevant actors, organizations, standards and norms related to IoT and, particularly, IoMT will be described. A structured table summarizing all related acronyms of this subsection is provided below (see Table 1). Although platitudinous enough, IoT solutions, as inherently conveyed by the "I" in the acronym, are based on the Internet. Therefore, web and internet communications standards are the core foundation which IoT and IoMT systems are built with. There is a broad range of efforts related to IoT, ranging from physical protocols, such as Bluetooth Low Energy (BLE) or Narrow Band IoT (NB-IoT), to higher-level formats, such as JavaScript Object Notation (JSON). In this group of internet-related protocols, we could include several recent IoT protocols, designed to deliver lightweight machine-to-machine communications. Examples thereof are the Constrained Application Protocol (CoAP) [11], the Message Queuing Telemetry Transport (MQTT) [12], the Advanced Message Queuing Protocol (AMQP) [13], or the Data Distribution Service (DDS) [14]. A number of organizations work towards the development of novel and comprehensive norms expected to pave the way for enhanced interoperability. A Standards Development Organization (SDO) is an entity whose prime activity is to define, coordinate and/or promote consensus standards relevant for the related industry. In fact, they are usually proposed by the very stakeholders, in need for a formal stability within their domain. At the moment of writing, the principal organizations coordinating the development of medical informatics standards, applicable to IoMT scenarios, are presented as follows. The International Organization for Standardization (ISO) [15] is a body for defining international standards. However, ISO also publishes Technical Reports, Technical Specifications, Publicly Available Specifications, Technical Corrigenda, and Guides. The European Committee for Standardization (CEN, from French "*Committee European of Normalization*") [16] is the foremost organization in this field located in Europe. Moreover, in every country, there is usually a national organization acting as a CEN

mirror, in charge of coordinating the national activities. For example, in the case of Spain (where the authors of this book chapter are from), the national CEN mirror is the Spanish Normalization Association (AENOR, form Spanish "*Asociación Española de Normalización y Certificación*"). There are different subgroups working on standardization in the field of Health ICT. The most pertinent ones for this field are Technical Committee 251 (CEN/TC 251) and Technical Committee 139 (AEN/CTN 139), respectively. At a technical level, the Institute of Electrical and Electronics Engineers (IEEE) [17] is an international non-for-profit association engaged with standards development at a wide scope, including electrical and electronic engineering, telecommunications, informatics, cybersecurity and health, among others.

Acronym	Stands for
	GENERIC INTERNET-RELATED ACRONYMS
ICT	Information and Communication Technologies
IoT	Internet Of Things
IoMT	Internet Of Medical Things
HTTP	Hypertext Transfer Protocol
API	Application Programing Interface
TIPPSS	Trust, Identity, Privacy, Protection, Safety, Security
ETL	Extract, Transform and Load
	GENERIC IoT-RELATED PROTOCOLS
BLE	Bluetooth Low Energy
NB-IoT	Narrow Band IoT
JSON	JavaScript Object Notation
XMPP	eXtensible Messaging and Presence Protocol
CoAP	Constrained Application Protocol
MQTT	Message Queuing Telemetry Transport
AMQP	Advanced Message Queuing Protocol
DDS	Data Distribution Service
	TECHNICAL ORGANIZATIONS
SDO	Standards Development Organization
ISO	The International Organization for Standardization
CEN	European Committee for Standardization
AENOR	Spanish Normalization Association
IEEE	Institute of Electrical and Electronics Engineers
	TECHNICAL ORGANIZATIONS IN THE MEDICAL DOMAIN
HL7	Health Level Seven
IHE	Integrating the Healthcare Enterprise
PCHA	Personal Connected Health Alliance
HIMSS	Healthcare Information and Management Systems Society
	MEDICAL-RELATED STANDARDIZATION ACRONYMS
SNOMED	Systematized Nomenclature of Medicine
LOINC	Logical Observation Identifiers Names and Codes
FHIR	Fast Healthcare Interoperability Resources
EHR	Electronic Health Records
HIS	Health Information Systems
PoC	Point of Care
PHD	Personal Health Devices

DIM	Domain Information Model
ACOM	Abstract COntent Model
HIS	Healthcare Information Systems

Table 1. List of acronyms related to data standardization and interoperability in IoMT architectures

Diving more specifically into the healthcare context, a number of standards development organizations are active in this field. For example, Health Level Seven (HL7) International [18], which is a well-known developer of health data interoperability standards or Integrating the Healthcare Enterprise (IHE) [19], an organization that leverages health interoperability standards to propose profiles for improved health data governance. Continua Health Alliance, now part of the Personal Connected Health Alliance (PCHA) [20], was created by various stakeholders (that is to say, academia, healthcare professionals, medical device manufacturers and technology firms) to encourage the coordinated use of these standards. The PCHA is a membership-based company of the Healthcare Information and Management Systems Society (HIMSS) [21], an organization aimed at enhancing the quality and access to healthcare by means of an adequate use of information technology and health management systems.
IEEE, while aiming at a broader scope, is also dedicating ongoing effort to defining IoT standards. Among the various initiatives, we could emphasize the following four, since they are closely related to IoT and, therefore, to IoMT scenarios. First, the IEEE 2413-2019 [22] is a document that promotes a standardized architectural framework for IoT. Such architecture framework description is driven by concerns usually shared by stakeholders of IoT systems across multiple domains. In this document, an abstract foundation for the notion of "things" in the IoT is provided. It also elaborates a compendium of architecture viewpoints stemmed from the shared concerns mentioned above in order to create the core of the framework described in this document. Second, the IEEE P2510 [23] copes with sensors, which are crucial for an IoT ecosystem. More specifically, it aims at establishing quality of data sensor parameters in the IoT environment. This document therefore provides a shared framework for sensor-related issues (such as units, terminology, limits, etc.). Third, the IEEE P1451-99 [24] is a document devoted to the harmonization and security of IoT devices and systems. This standard aims at defining a way for sharing data, taking into account the interoperability and security of the messages over the network, independently of the specific communication technology underneath. The backend would be based on the eXtensible Messaging and Presence Protocol (XMPP), thus providing features such as globally authenticated identities, authorization, presence, life cycle management, interoperable communication, IoT discovery and provisioning. Finally, the IEEE P2733 [25], which promotes IoT data and device interoperability, but enforcing Trust, Identity, Privacy, Protection, Safety, Security (TIPPSS). The main purpose is to enable secured data sharing in connected healthcare while protecting patient privacy and security. Within the IoT field, there are multiple domains, such as smart manufacturing, industry 4.0, smart grid, smart cities, or smart logistics, to name only a few. One of the most complex scenarios is arguably the smart healthcare domain, due to the intricate data models inherent to this context. Some of the first to arrive were the terminologies, such as the Systematized Nomenclature of Medicine (SNOMED) [26] or Logical Observation Identifiers Names and Codes (LOINC) [27], whose main aim is to provide a reliable, comprehensive way to index and identify all health related terms there exist. On top of that, sophisticated protocols appear, such as the CEN/ISO 13606 standard [28] or the openEHR norm [29], both initiatives devoted to the interoperable exchange of Electronic Health Records

(EHR). The main objective of the CEN/ISO 13606 standard is to define a detailed and stable information architecture for communicating part or all of EHR of a patient between different EHR systems, or between an EHR system and other Health Information Systems (HIS). openEHR is a compound of open specifications, clinical models and software aimed to create medical standards and build interoperable information solutions in the healthcare domain. CEN/ISO 13606and openEHR share a common objective and structure. Indeed, the fundamental shareable specifications of clinical information (called archetypes) could be mutually transcoded. A simpler, more lightweight approach was established by version 4 of the HL7 standard, commonly referred to as Fast Healthcare Interoperability Resources (FHIR) [30]. This standard provides an Hypertext Transfer Protocol (HTTP)-based RESTful Application Programing Interface (API) for interoperable health data exchange. Related to all these are the ontologies, which provide formal representation of shared concepts and the relationships among them within the medical domain. In this context, a noteworthy initiative is ISO/IEEE 11073, a standard for medical device interoperability that has been evolving throughout the last years. First, it aimed at the Point of Care (PoC) [31], that is, typically bigger devices close to hospital beds. In parallel, the nomenclature was defined by means of the IEEE 11073-10101 document. Second, it evolved towards Personal Health Devices (PHD) [32], covering smaller medical devices in home scenarios with a local manager capable of handling all of them simultaneously. The core document of this version of the standard was the ISO/IEEE 11073-20601, referred to as the Optimized Exchange Protocol. This document defined a Domain Information Model (DIM), a service model and a communication model. The PHD version also defined several device specialization profiles (ISO/IEEE 11073-104zz), one for each sensor to be modelled, e.g. the pulse oximeter (ISO/IEEE 11073-10404), the blood pressure monitor (ISO/IEEE 11073-10407), or the electrocardiogram (ISO/IEEE 11073-10406). Along with that, the Continua Health Alliance proposed design and implementation guidelines to promote the global adoption of this standard [33]. However, such guidelines, despite continuous improvement, have had relative success so far. The main concerns are the inevitability of defining and implementing one profile per device type, the complexity of sending measurements directly to the cloud and the limited (albeit feasible) transcoding to HL7 FHIR, which arguably is the reference standard in current mobile health applications. Thus, in order to overcome these issues, a new Abstract COntent Model (ACOM) for PHDs is currently under development, with reference name project IEEE P11073-10206 [34]. It aims at defining an abstract model for devices based on the DIM and nomenclature previously defined for PHDs. The main advantages would be the straightforward binary representation of HL7 FHIR resources, the possibility of deploying direct-to-cloud architectures (there is an ongoing effort by IHE and PCHA), and the definition of a generic health sensor model for all types of sensors (being currently developed by the Bluetooth special interest group), simplifying thereby the implementation of scenarios with multiple sensors.

1.2.1 Data standardization and interoperability in IoMT architectures

The incorporation of IoT and IoMT standards to IoMT architectures provides several advantages and disadvantages. Among the advantages, we could name the following. First, it would provide enhanced interoperability and integration among the different healthcare actors involved. Second, the Extract, Transform and Load (ETL) operations would become simpler, since they operate consistently, even though when incorporating new devices to the ecosystem. Third, the definition of precise health data models open the door to effective reasoning over

the data, which could help to find patients at risk by means of software algorithms or artificial intelligence. Fourth, it would make it easier for individuals to become co-producers of health, since the medical data could be straightforwardly sent and integrated to EHRs. Fifth, this also would benefit patients, who would be able to access, download and inspect (with open source software applications) their own data, typically stored today at the hospital servers, often unavailable to patients. Finally, the Healthcare Information Systems (HIS) of the hospitals would become easier to develop and maintain.

On the other hand, there are some disadvantages to the standardization of IoMT architectures. In the following lines, the most relevant are named. First, as manifestly shown in this section of the chapter, the standardization arena is rather fragmented, moreover taking into account that this section provides a rather comprehensive but incomplete overview, limited to the most relevant efforts. This situation is problematic for developers, architects and health information systems managers. Second, some standards are excessively complex to implement, which hurdles wider adoption. Third, there is a cost attached to the incorporation of standards to the devices or architectures, in several terms, such as economic, temporal and/or human resources terms. This naturally increment the price of the solution at the end. Finally, there is also an additional information-related cost, in terms of memory and computing time, which directly affects the battery life, critical in IoMT devices. As a result, the interoperability and standardization arena in IoMT is a complex environment. A plethora of IoT and IoMT formats, protocols and standards have been proposed, but the seamless application thereof to IoMT ecosystems requires further research. In general, as a final reflection on this matter, the incorporation of standards to IoMT architectures poses a delicate trade-off between advanced interoperability and different costs.

1.3 Distributed and Cloud Computing Capabilities

An Internet of Healthcare Things system needs, as any other information system does, to collect, process, store, share and present information. In this case, the information to be handled has some special features that must be taken into account. The information reflects patients' medical data, which is protected by different regulations (in the case of the European Union by the GPDR) and must be treated in a special way. This implies a need for encryption and anonymization of the information, so that the information is unbundled from any data that would allow a third party to find out to which patient the information corresponds. This can be done by hash functions, by temporary identifiers that expire in short periods of time, or other solutions or combinations of them. IoT devices send patient information to an aggregator node (fog) located in the patient's immediate environment (patient's home) to which they are univocally linked via wireless networks (BLE or similar). This minimizes the risk of compromising patient information, as the aggregator takes care of the proper encryption of the information before it is sent to the information system located in the cloud. Furthermore, it reduces the communication latency. This secure transmission will guarantee both the integrity of the messages and the authenticity of the sender and receiver. The aggregator is responsible for negotiating with the information system the management of temporary identifiers and the encryption mechanism. Figure 5 shows a classical schema of computing and storage organization with three layers: edge, fog and cloud layers. IoT devices are located at the edge layer, and have a limited capacity of both computing and storage. At the fog layer, aggregators have greater computing, storage and communication capacity. This ensures a secure communication with the next level, and in case of communication interruption, allows the temporary storage of the information collected by the IoT network until it can be transmitted

to the cloud level. Finally, the cloud layer hosts the healthcare information system. This cloud may be either a public or a private solution according to the privacy and security requirements of each organization, or even a hybrid solution. When greater control of information is required and sufficient resources are available, a private cloud is often chosen over the alternative of a public cloud, which requires fewer resources on the part of the organization, but implies less control over the data.

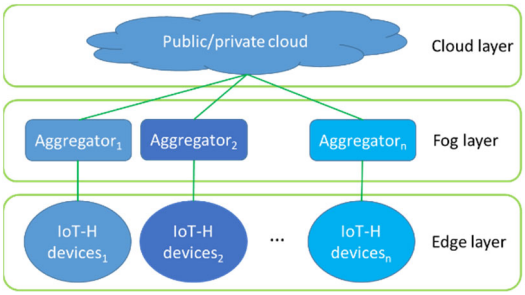


Figure 5 A classical schema of computing and storage organization: edge, fog and cloud layers.

Healthcare IoT-cloud based proposals are neither new nor novel [35, 36], although new proposals for patient (with chronical diseases) monitoring using narrowband IoT technologies are currently being put forward [37, 38]. The main drawback of these technologies is the latency introduced, which makes them unsuitable for real-time monitoring of vital signs. This is further aggravated when IoT devices communicate directly over a cloud-based information system, without using an edge/fog solution. Security is a key aspect, so both patient anonymity and communication encryption must be guaranteed but, in addition, the information must also be stored dissociated from any data that could allow an unauthorized identification of the patient, regardless of the computing and storage architecture chosen (cloud/fog/edge). Many proposals have addressed these issues, as [39-45] and there are sure to be more proposals that will continue to be formulated, since these are issues that have not yet been solved.

Data exchange between IoT monitoring devices and the information system is also a relevant issue to be considered. Different markup languages as XML and JSON (or even YAML) can be considered, as occurs with FHIR, so healthcare information systems (HIS) should natively support both interchange formats. HIS, either because they directly implement HL7, or because they use service buses to implement data ingestion from the IoT networks, must to deal with XML/JSON messages. NextGen Connect[1] (previously known as Mirt Connect) is an example of service bus, a cross-platform interface engine used to grant bi-directional sending/receiving of many types of messages, in this case to ensure the semantic interoperability of the data collected with the HL7 messaging standard. HIS implementations may concern a unique instance, but this is not the norm. For reasons of redundancy, but also of scalability, cloud solutions that leverage hyper-converged solutions are often used by the providers of these solutions. In this scenario, data ingestion from IoT devices is often performed at the aggregators side, which communicate directly by means of HL7 messages with the HIS hosted at the cloud side. The use of some elements of HL7 as Clinical Document Architecture (CDA), Continuity of Care Record (CCR), Continuity of Care Document (CCD) and Consolidated Clinical Document Architecture (CCDA) allow an easy customization of any HIS system to the corresponding language, which is an important aspect when opting for cloud-based systems.

[1] NextGen Connect, https://www.nextgen.com/products-and-services/integration-engine

This is especially important when the same HIS must support interaction in different languages, or when the same provider supports different customers. The latter case is particularly sensitive when it comes to ensuring the protection of medical record data. Opting for cloud solutions (public or private) helps to reduce HIS implementation and operating costs [46], mainly due to the dynamic scalability provided by virtualization. Performing system snapshots is really simple and fast, allowing for quick and efficient system recovery in case of failure. From the point of view of system integration, the use of archetypes and ontologies greatly facilitates the interoperability of HIS with legacy systems. This is possible through cloud systems by publishing web services or by using programming APIs. In any case, it is an issue to be considered by those responsible for healthcare management.

Currently, these systems are betting heavily on the ability to learn and recognize patterns and patterns [47-51]. This implies the use of machine learning techniques, for which it is not only necessary to have adequate computing capabilities (GPU), but it is just as important, if not more, to have enough learning samples to make such learning possible. In such context, the use of informed machine learning [52] by integrating prior knowledge into the training process may aid to avoid this issue. However, the biggest evolution in this field seems to come from digital twins (DT). Some authors, as [53], consider that DT technology "has the potential to transform healthcare in a variety of ways – improving the diagnosis and treatment of patients, streamlining preventative care and facilitating new approaches for hospital planning". DTs seem to be pervasively used to digitalize any assets of a health organization [54, 55] but they will also be used to provide personalized medicine [56, 57], to reproduce patients' previous pathologies before surgery, and even more. A DT of any vital organ may represent the physical behaviour (electrical, mechanical, biochemical…). This allows not only to know the behaviour of this organ in the patient, but also to study the best way to address their pathologies both at the surgical level as well as at any other level. In this context, the ability to use DT technology to reconstruct all or part of a patient's organs in order to provide real and effective personalized medicine will be crucial. This can be done with on premise proprietary solutions developed specifically for each hospital or even as a service (Digital Twin as a Service, DTaaS).

1.4 Security

The IoMT is already shaping healthcare with significant benefits for patients, clinicians, and medical device providers. The emergence of new and additional connectivity technologies in IoMT is enabling more and better remote collection and transmission of data from users and their environments. At the same time, such connectivity is considered a risk from a cybersecurity point of view.

Nowadays, cyberattacks are a complex, constantly evolving global threat. Cybersecurity vulnerabilities can emerge in any medical device that can be connected to another electronic device or network, disrupting its function and compromising the data security. In addition, vulnerable medical devices may be harnessed as part of a botnet to launch attacks on other targets; as a back channel to breach the security of hospital or clinic networks; to extract ransoms; to harm a patient or user of the device and to inflict other financial or reputational damages onto device manufacturers, clinics and patients [58, 59]. It is worth highlighting that, in healthcare services and environments, privacy of personal data in transit (e.g. managed on a health care cloud, transmitted across networks etc.) needs to offer a high level of assurance. Furthermore, confidentiality and integrity of data is of utmost importance, so emphasis should also be placed on data storage and processing.

With a large number of IoMT devices on the rise in the healthcare ecosystem, the need for strong security measures is essential. Two complementary strategies are presented below, with the aim of guaranteeing the security of IoMT devices and their compliance with current standards in the field of cybersecurity and medical devices development: IEC 62443, IEC 62304 and ISO 13485.

1.4.1 Risk-based cybersecurity management

The first step in the process is to develop a holistic risk-based cybersecurity plan that addresses overall vulnerability issues related to safety, security, privacy, software and design. Within this plan, medical device manufacturers should make provisions to ensure that device design will be simple and easy to update, while adhering to regulatory best practices. Also, manufacturers should plan vulnerability management processes to ensure that fixes can be rapidly developed and deployed to their products. At the same time, they will need to define processes and protocols to handle security breaches that could arise with the setup and maintenance of IoMT devices. In IEC 62443 standard, Risk is defined as the result of the equation:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequence} \quad (3)$$

Considering:

- *Threat:* Potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm
- *Vulnerability*: Flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy
- *Consequences:* Flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy

According IEC 62443 standard, cybersecurity related risks should be identified, classified and mitigation actions should be defined in order to achieve desired security levels. This methodologic approach allows device hardening to improve their ability withstand a cyberattack. Table 2 summarizes security Level (SL) coupled with a characterization of the type of attacker.

In order to empower the use of IoT in the medical health care domain, it is necessary to recognize and examine specific qualities of IoMT including security requirements, vulnerabilities, and countermeasures, as well as their implications from the health care perspective. A good risk assessment should provide a risk profile, highest severity consequences threats, vulnerabilities leading to the highest risks and Target security levels (SL) for de assessed devices. Table 3 shows some typical attacks in terms of effects and suggested mitigation actions [60-63]. Some actions would be applied on the device and others in the service architecture.

Security Level	**Target**	**Skills**	**Motivation**	**Means**	**Resources**
SL1	Casual or coincidental violations	No Attack Skills	Mistakes	Non-intentional	Individual
SL2	Cybercrime, Hacker	Generic	Low	Simple	Low (Isolated Individual)
SL3	Hacktivist, Terrorist	Specific	Moderate	Sophisticated (Attack)	Moderate (Hacker Group)

SL4	Nation State	Specific	High	Sophisticated (Campaign)	Extended (Multidisciplinary Teams)

Table 2 – Security Levels defined in IEC 62443

Attack	**Effect**	**Mitigation**
Denial of Service (DoS)	Distributed attack affects availability of system services.	Early intrusion detection
Routing Attack	Change route information	Continuous Route Monitoring
Sensor Attack	Data modification	Node Failure and Replacement Detection
Replay Attack	Drop data packets	Data freshness techniques

Table 3 – Typical attacks in smart health

1.4.2 Security by Design

Countering cyber-attacks starts by incorporating secure measures from the beginning of a device or app development, to mitigate threats. Security is a crucial objective at all stages of product creation and deployment. It addresses the challenge that, in many historic hardware deployments and instances of IoT design, security considerations were often included late in the design and prototyping phase, provoking serious security breaches. Security by design is a methodology that ensures security and privacy by design and by default. Accordingly, an effective and proactive means to reduce the number and severity of vulnerabilities in IoT is to develop applications in a secure manner, making use of secure Software Development Life Cycle (sSDLC) principles and developers trained in secure coding [64]. Several securities challenges of the IoT, can be addressed by establishing a set of secure development guidelines, such as checking for security vulnerabilities, secure deployment, ensuring continuity of secure development in cases of integrators, continuous delivery etc.

Figure 6 Secure SDLC [7]

Several securities challenges of the IoMT can be addressed by establishing a set of specific security considerations and guidelines to be taken into account during IoMT entire Development Life Cycle. See Table 4

Consideration	Description
Security Requirements	Identification and specification of explicit security requirements according to data classification, application requirements and regulatory or standardisation compliance objectives.
Hardware limitations	Alignment of security requirements with hardware limitations: processing capability, low power consumption
Protocols	Identification of the appropriate protocols for the solution, taking into account its security features and the IoMT solution's security requirements.
Threat modelling	Application of threat modelling methodologies to identify the threats and the associated countermeasures to mitigate them
Attack surface analysis	Identification of the IoMT solution's attack surface by taking into consideration architecture aspects and utilising security user stories
Secure design	Use / application of secure design patterns and principles during the architecture definition.
Security requirement tests	Performance of security tests to ensure that software is free of known vulnerabilities and to detect risks related to security requirements.
Penetration tests	Testing to identify potential vulnerabilities that could exist in IoMT solutions and could be exploited by an attacker.
Remote maintenance	Delivery management to push new versions of software in a remote environment securely when it is necessary to apply an update, either to add new functionalities or to mitigate vulnerabilities.
External checks	Use third-party cybersecurity testing services that employ trained security researchers who can conduct mock cyber-attacks to evaluate for weaknesses.

Table 4 – Security considerations during Development Life Cycle

1.5 Considerations for an IoMT deployed Use Case.

Patient-centered use cases for the provision of Health Services based on IoMT can be found in each of the medical scenarios. In the case of public health systems such as in Spain, the greatest efficiency of the system is found in patients with chronic diseases, such as diabetes, high blood pressure, respiratory failure, asthma, etc. Also of great interest are use cases based on screening of patients with asymptomatic pathologies such as cancer (Breast, colon, etc.) as well as other pathologies such as those associated with diabetes, aging, etc.. In short, there are many fronts in which to innovate both at a technological level, such as human resources (new professions) and management of health processes, etc. An innovation that must be carried out from a holistic point of view and not just only technological. In our closest environment, both screening strategies and Clinical Trials spin around patients as Home Hospitalization of mild or moderate covid-19 patients, generally asymptomatic, fundus screening, etc. have been addressed [65]. Without going into depth in the deployment of these Health Services based on IoMT describing in detail the medical devices and communications used, standardization and security, as well as the processing of the data itself, aspects that have been valued in other parts of this chapter, it seems appropriate to describe briefly those aspects that arise from the deployment itself. One example for a practical case study is given by eye fundus screening. The prevalence of diabetic patients can be around 10% in first world countries. As an example, in the region of Navarra,

Spain, around 7%, approx. 50,000 patients, according annual reports. Given these figures, a fundus screening strategy in order to prevent retinal pathologies such as RD, AMD, etc., is compulsory. The implementation of an eye fundus diagnosis and monitoring system is feasible following IoMT paradigms. The necessary technology is mature and integrates the following elements:

- Non-Mydriatic Fundus Camera: with mobility, with internet connection (wired or wireless), with medical image transmission standards such as DICOM
- HIS: Hospital Information Systems including appointment management (RIS), worklist management, electronic presciption, Electronic Health Record, PACS Servers, etc.
- Mature Artificial Intelligence algorithms for Medical Image Processing with a very high sensitivity and specificity in order not to generate long waiting lists.
- Other support elements: customized mobility for transport (vans, small lorries, etc.) including the medical devices needed (Non-Mydriatic Fundus Camera, OCT, Tonometer, etc.) as well as the necessary stays for patients. Likewise, it should have high speed wireless communication, Servers, etc.

In relation to the necessary professionals, the following can be distinguished:

- Non-Sanitary or Basic Sanitary Personnel (Van drivers), who could have the necessary skills to handle the Non-Midriatic fundus camera, take the photographs, as well as their subsequent transmission to the PACS, always with close collaboration with the Healthcare personnel, could manage the patients appropriately.
- Physician specialized in Ophthalmology, who are the main responsible for the operation of the Service, as well as for making decisions about the pathology, medical prescription, etc. In short, the main actors of this strategy.

The successful integration of this eye fundus diagnosis and analysis systems requires the definition and implementation of a process model that can be included within the general hospital complex procedures. In this case, the process model considers the following stages.

1. Patients are regularly cited, based on current medical evidence and in accordance with the evolution of medical knowledge. This appointment management is carried out automatically using the HIS and with the appropriate periodicity, always based on the medical evidence of the moment.
2. Patient-centric: Where are patients cited? Based on the Public health system in Spain, patients are cited at their local health center or its area of influence where the necessary room is available for an adequate location of mobility to carry out the tests, as well as for the usual waiting of the patient.
3. The mobility device (van or small lorries) equipped with the necessary medical and communication technology, travels to the health centers where the patients have been cited. These trips must be based on good route management using current technologies in order to minimize distance and maximize the number of daily or weekly patients cited depending on the needs of the system.

From a technological point of view, the technology is mature (HIS, Medical devices, Communications, Apps, AI algorithms for both Signal and Image processing; Maps, etc.) it is working perfectly, sometimes in isolation, but it may be a good time for its integration. From a human resources point of view, the rise of other types of multidisciplinary professions (drivers, non-specialized health personnel, biomedical engineers, etc.) could also be positive. The so-called digitization of Health Services entails this multidisciplinary approach between different fields of knowledge and new professions. The problems could come from the

regulatory point of view, but, it is true, that there is an evolution towards patient-centered health services, so these initiatives that seek efficiency in the management of resources should always be valued public, as well as in the adequate provision of health services. It is not difficult to imagine that this redesign could be used to include another type of IoMT technology for the provision of other Health Services (Electrocardiography, Echocardiography, etc.) in a way that makes intensive and efficient use of said technology, for the sake of system efficiency and thinking about the provision of patient-centered digital Health Services.

Acknowledgments

We would like to thank the collaboration of the health personnel of the Navarra Health Service-Osasunbidea, in particular, Dr. José Andonegui, Head of the Ophthalmology Service, Hospital Complex of Navarra, and the engineering team developing the AI strategies for DR screening.

Reference list

1. Reimagining Patient-Centric Clinical Trials with the IoMT. Last Access: July, 31st, 2021
2. Q. Qi, X. Chen, C. Zhong and Z. Zhang, "Integrated Sensing, Computation and Communication in B5G Cellular Internet of Things," in IEEE Transactions on Wireless Communications, vol. 20, no. 1, pp. 332-344, Jan. 2021
3. S. Forrest, K. Baker and M. Ketel, "Internet of Medical Things: Enabling Key Technologies," SoutheastCon 2021, pp. 1-5
4. J. D. Trigo et al., "Patient Tracking in a Multi-Building, Tunnel-Connected Hospital Complex," in IEEE Sensors Journal, vol. 20, no. 23, pp. 14453-14464, 1 Dec.1, 2020
5. B. Qian, H. Zhou, T. Ma, K. Yu, Q. Yu and X. Shen, "Multi-Operator Spectrum Sharing for Massive IoT Coexisting in 5G/B5G Wireless Networks," in IEEE Journal on Selected Areas in Communications, vol. 39, no. 3, pp. 881-895, March 2021
6. S. Sakib, T. Tazrin, M. M. Fouda, Z. M. Fadlullah and N. Nasser, "An Efficient and Lightweight Predictive Channel Assignment Scheme for Multiband B5G-Enabled Massive IoT: A Deep Learning Approach," in IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5285-5297, 1 April1, 2021
7. X. Chen, D. W. K. Ng, W. Yu, E. G. Larsson, N. Al-Dhahir and R. Schober, "Massive Access for 5G and Beyond," in IEEE Journal on Selected Areas in Communications, vol. 39, no. 3, pp. 615-637, March 2021
8. P. S. Hall, Y. Hao, “Antennas and Propagation for Body-Centric Wireless Communications”, 2nd Edition, 2012, Artech House, Norwood, MA, USA
9. J. Wang, Q. Wang, “Body Area Communications. Channel Modelling, Communication Systems, and EMC”, 2013, John Wiley and Sons, Singapore
10. M. U. A. Siddiqui, F. Qamar, F. Ahmed, Q. N. Nguyen and R. Hassan, "Interference Management in 5G and Beyond Network: Requirements, Challenges and Future Directions," in IEEE Access, vol. 9, pp. 68932-68965, 2021
11. Z. Shelby, "Constrained Application Protocol (CoAP)", *IETF Internet draft*, Oct. 2011.
12. MQTT. Message Queuing Telemetry Transport. Available: http://mqtt.org/. Last accessed: July, 2021
13. AMPQ. Advanced Message Queuing Protocol. Available: http://amqp.org/. Last accessed: July, 2021
14. DDS. Data Distribution Service. Available: https://www.omg.org/omg-dds-portal/. Last accessed: July, 2021
15. ISO. International Organization for Standardization. Available: https://www.iso.org/. Last accessed: July, 2021

16. CEN. Comiteé European Normalisation. Available: https://www.cen.eu/. Last accessed: July, 2021
17. IEEE. Institute of Electrical and Electronics Engineering. Available: http://www.ieee.org/. Last accessed: July, 2021
18. HL7. Health Level Seven. Available: http://www.hl7.org. Last accessed: July, 2021
19. IHE. Integrating the Healthcare Enterprise. Available: http://www.ihe.net/. Last accessed: July, 2021
20. Continua Health Alliance / Personal Connected Health Alliance. Available: https://www.pchalliance.org/. Last accessed: July, 2021
21. HIMSS. Healthcare Information and Management Systems Society. Available: http://www.himss.org/. Last accessed: July, 2021
22. IEEE 2413-2019 - IEEE Standard for an Architectural Framework for the Internet of Things (IoT). Available: https://standards.ieee.org/standard/2413-2019.html. Last accessed: July, 2021
23. IEEE P2510 - Standard for Establishing Quality of Data Sensor Parameters in the Internet of Things Environment. Available: https://standards.ieee.org/project/2510.html. Last accessed: July, 2021
24. IEEE P1451-99 - Standard for Harmonization of Internet of Things (IoT) Devices and Systems. Available: https://standards.ieee.org/project/1451-99.html. Last accessed: July, 2021
25. IEEE P2733 - Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS (Trust, Identity, Privacy, Protection, Safety, Security). Available: https://standards.ieee.org/project/2733.html. Last accessed: July, 2021
26. SNOMED. Systematized Nomenclature of Medicine. Available: https://www.snomed.org/. Last accessed: July, 2021
27. LOINC. Logical Observation Identifiers Names and Codes. Available: https://www.loinc.org/. Last accessed: July, 2021
28. CEN/ISO 13606, "Electronic Healthcare Record (EHR) Communication. Standard Parts 1-5," 2004 (1st Ed.).
29. openEHR. Available: http:///www.openehr.org. Last accessed: July, 2021
30. HL7 Fast Healthcare Interoperability Resources (FHIR). Available: https://www.hl7.org/fhir/. Last accessed: July, 2021
31. ISO/IEEE 11073, Health informatics. Point-of-care medical device communication. Parts: 1. MD Data Language (MDDL), 2. MD Application Profiles (MDAP), 3. Transport and Physical Layers.
32. ISO/IEEE 11073, Health informatics. Personal Health Devices communication. Parts: 11073-00103 Technical report - Overview, 11073-104zz Device Specializations, 11073-20601 Application profile-Optimized Exchange Protocol
33. Continua/PCHA Design Guidelines. Available: https://www.pchalliance.org/continua-design-guidelines. Last accessed: July, 2021
34. IEEE P11073-10206 - IEEE Draft Standard - Health informatics -- Device interoperability -- Part 10206: Personal health device communication -- Abstract information content model. Available: https://standards.ieee.org/project/11073-10206.html. Last accessed: July, 2021

35. V. P. Darcini S., D. P. Isravel and S. Silas, "A Comprehensive Review on the Emerging IoT-Cloud based Technologies for Smart Healthcare," 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), 2020, pp. 606-611
36. R. Hegde, S. Ranjana and C. D. Divya, "Survey on Development of Smart Healthcare Monitoring System in IoT Environment," 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), 2021, pp. 395-399
37. S. K. Routray and S. Anand, "Narrowband IoT for healthcare," 2017 International Conference on Information Communication and Embedded Systems (ICICES), 2017, pp. 1-4, doi: 10.1109/ICICES.2017.8070747.
38. S. Anand and S. K. Routray, "Issues and challenges in healthcare narrowband IoT," 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT), 2017, pp. 486-489.
39. M. Suguna, M. G. Ramalakshmi, J. Cynthia and D. Prakash, "A Survey on Cloud and Internet of Things Based Healthcare Diagnosis," 2018 4th International Conference on Computing Communication and Automation (ICCCA), 2018, pp. 1-4.
40. Y. Shi, G. Ding, H. Wang, H. E. Roman and S. Lu, "The fog computing service for healthcare," 2015 2nd International Symposium on Future Information and Communication Technologies for Ubiquitous HealthCare (Ubi-HealthTech), 2015, pp. 1-5, doi: 10.1109/Ubi-HealthTech.2015.7203325.
41. O. Bibani et al., "A Demo of IoT Healthcare Application Provisioning in Hybrid Cloud/Fog Environment," 2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), 2016, pp. 472-475, doi: 10.1109/CloudCom.2016.0081.
42. S. El Kafhali, K. Salah and S. Ben Alla, "Performance Evaluation of IoT-Fog-Cloud Deployment for Healthcare Services," 2018 4th International Conference on Cloud Computing Technologies and Applications (Cloudtech), 2018, pp. 1-6.
43. S. Ahmed, M. Saqib, M. Adil, T. Ali and A. Ishtiaq, "Integration of cloud computing with Internet of Things and wireless body area network for effective healthcare," 2017 International Symposium on Wireless Systems and Networks (ISWSN), 2017, pp. 1-6.
44. P. Kanchanadevi, D. Selvapandian, L. Raja and R. Dhanapal, "Cloud-based Protection and Performance Improvement in the E-Health Management Framework," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2020, pp. 268-270, doi: 10.1109/I-SMAC49090.2020.9243419.
45. J. Hong, P. Morris and J. Seo, "Interconnected Personal Health Record Ecosystem Using IoT Cloud Platform and HL7 FHIR," 2017 IEEE International Conference on Healthcare Informatics (ICHI), 2017, pp. 362-367, doi: 10.1109/ICHI.2017.82.
46. F. Sadoughi, L. Erfannia, “Health Information System in a Cloud Computing Context,” *Studies in health technology and informatics*, 2017, no. 236, pp. 290-297.
47. T. Karatekin *et al*., "Interpretable Machine Learning in Healthcare through Generalized Additive Model with Pairwise Interactions (GA2M): Predicting Severe Retinopathy of Prematurity," *2019 International Conference on Deep Learning and Machine Learning in Emerging Applications (Deep-ML)*, 2019, pp. 61-66, doi: 10.1109/Deep-ML.2019.00020.
48. S. Durga, R. Nag and E. Daniel, "Survey on Machine Learning and Deep Learning Algorithms used in Internet of Things (IoT) Healthcare," *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, 2019, pp. 1018-1022, doi: 10.1109/ICCMC.2019.8819806.

49. K. Yazhini and D. Loganathan, "A State of Art Approaches on Deep Learning Models in Healthcare: An Application Perspective," *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, 2019, pp. 195-200.
50. P. Sujatha and K. Mahalakshmi, "Performance Evaluation of Supervised Machine Learning Algorithms in Prediction of Heart Disease," *2020 IEEE International Conference for Innovation in Technology (INOCON)*, 2020, pp. 1-7.
51. V. Manimegalai, A. Gayathri, V. Mohanapriya, C. Gowtham, C. A. Kumar and S. D. Kanna, "Spruce Fitness Observation Method using IoT and Machine Learning," *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, 2021, pp. 384-388, doi: 10.1109/ICICCS51141.2021.9432297.
52. L. von Rueden *et al*., "Informed Machine Learning - A Taxonomy and Survey of Integrating Prior Knowledge into Learning Systems," in *IEEE Transactions on Knowledge and Data Engineering*, doi: 10.1109/TKDE.2021.3079836.
53. L. James, "Digital twins will revolutionise healthcare: Digital twin technology has the potential to transform healthcare in a variety of ways – improving the diagnosis and treatment of patients, streamlining preventative care and facilitating new approaches for hospital planning," in *Engineering & Technology*, vol. 16, no. 2, pp. 50-53, March 2021.
54. Ricci, A. Croatti and S. Montagna, "Pervasive and Connected Digital Twins – A Vision for Digital Health," in IEEE Internet Computing, doi: 10.1109/MIC.2021.3052039.
55. H. Elayan, M. Aloqaily and M. Guizani, "Digital Twin for Intelligent Context-Aware IoT Healthcare Systems," in *IEEE Internet of Things Journal*.
56. N. Wickramasinghe *et al*., "A Vision for Leveraging the Concept of Digital Twins to Support the Provision of Personalised Cancer Care," in *IEEE Internet Computing*.
57. R. Martinez-Velazquez, R. Gamez and A. E. Saddik, "Cardio Twin: A Digital Twin of the human heart running on the edge," *2019 IEEE International Symposium on Medical Measurements and Applications (MeMeA)*, 2019, pp. 1-6.
58. Sara Alromaihi, Wael Elmedany ,Chitra Balakrishna, *"Cyber Security Challenges of Deploying IoT in Smart Cities for Healthcare Applications",* DOI: 10.1109/W-FiCloud.2018.00028
59. Shariq Aziz Butt, Arshad Ali "IoT Smart Health Security Threats" 2019 19th International Conference on Computational Science and Its Applications (ICCSA)
60. Muhammad Aminu Lawal Riaz Ahmed Shaikh Syed Raheel Hassan "A DDoS Attack Mitigation Framework for IoT Networks using Fog Computing", DOI: https://doi.org/10.1016/j.procs.2021.02.003
61. Huraj, L.; Horak, T.; Strelec,P.; Tanuska, P. "Mitigation against DDoS Attacks on an IoT-Based Production Line Using Machine Learning". Appl. Sci. 2021, 11, 1847.
62. Cansu Eken, Hanım Eken "Security Threats and Recommendation in IoT Healthcare" 9th EUROSIM Congress on Modelling and Simulation, DOI: 10.3384/ecp17142369
63. Khadim R., Ennaciri A., Erritali M., Maaden A. (2017) "Impact of Location Data Freshness on Routing in Wireless Sensor NetworksAdvances in Intelligent Systems and Computing, vol 520. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-46568-5_38
64. "Good Practices for Security of IoT - Secure Software Development Lifecycle", ENISA, 2019. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1
65. J, Andonegui, et al, "Evaluation of a Telemedicine Model to Follow Up Patients with Exudative Age-Related Macular Degeneration", Retina: February 2016 - Volume 36 - Issue 2 - p 279-284. doi: 10.1097/IAE.0000000000000729