Computer Methods and Programs in Biomedicine 208 (2021) 106231

Contents lists available at ScienceDirect

Computer Methods and Programs in Biomedicine

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

Internet of things in health: Requirements, issues, and gaps

Jorge Calvillo-Arbizu[a,b,*], Isabel Román-Martínez[b], Javier Reina-Tosina[a,c]

[a] *Grupo de Ingeniería Biomédica, Universidad de Sevilla, Sevilla 41092, Spain*
[b] *Departamento de Ingeniería Telemática, Universidad de Sevilla, Spain*
[c] *Departamento de Teoría de la Señal y las Comunicaciones, Universidad de Sevilla, Spain*

ARTICLE INFO

Article history:
Received 14 December 2020
Accepted 2 June 2021

Keywords:
Internet of Things (IoT)
Healthcare
Requirements
Security
Data lifecycle

ABSTRACT

Background and objectives: The Internet of Things (IoT) paradigm has been extensively applied to several sectors in the last years, ranging from industry to smart cities. In the health domain, IoT makes possible new scenarios of healthcare delivery as well as collecting and processing health data in real time from sensors in order to make informed decisions. However, this domain is complex and presents several technological challenges. Despite the extensive literature about this topic, the application of IoT in healthcare scarcely covers requirements of this sector.

Methods: A literature review from January 2010 to February 2021 was performed resulting in 12,108 articles. After filtering by title, abstract, and content, 86 were eligible and examined according to three requirement themes: data lifecycle; trust, security, and privacy; and human-related issues.

Results: The analysis of the reviewed literature shows that most approaches consider IoT application in healthcare merely as in any other domain (industry, smart cities…), with no regard of the specific requirements of this domain.

Conclusions: Future efforts in this matter should be aligned with the specific requirements and needs of the health domain, so that exploiting the capabilities of the IoT paradigm may represent a meaningful step forward in the application of this technology in healthcare.

1. Introduction

Internet of Things (IoT) is gaining momentum as a disruptive paradigm to provide new capabilities and services in different sectors such as Smart-City, Industry 4.0, Smart-Energy or Connected Car [1]. Currently, IoT is one of the most popular technological trends in healthcare [2] for Ambient-Assisted Living (AAL), remote health monitoring, chronic disease management, elderly care as well as fitness programs [3]. Fig. 1 shows an overview of current technologies, services, and applications of healthcare IoT.

Most IoT-enabling technologies are general purposed and need to be adapted to comply with the specific requirements of each sector [4]. Hence, any technological solution in healthcare should observe requirements such as maximum availability of information resources (to support healthcare anytime), critical security of health information, persistence of large data volume, variability of data and processes, integration with legacy systems, etc. [5]. Nevertheless, these requirements are often neglected on health IoT-driven solutions and there is no systematic review analysing the growing literature from this viewpoint [6]. Therefore, the aim of this work is to analyse how the health sector complexity is being addressed by IoT solutions, identifying current issues and missing gaps. A literature review is performed by considering only design and development requirements.

Several reviews can be found in the literature, although with aims different from what motivates this work. Table 1 shows a non-exhaustive list of literature reviews on IoT applications in health. Most of them summarize enabling technologies, current research, and use cases on this domain. The variety of focus and findings is wide hence emphasizing the heterogeneity of health IoT solutions. All reviews point out challenges persisting over the years such as security and privacy, energy limitation of IoT devices, drawbacks of Cloud in health, etc. Whereas reviews analyse health IoT literature in order to describe the state of the art and find unsolved challenges, our approach is quite the opposite.

This emerges from the consideration that the health domain requirements should drive the design and development of IoT in

[*] Corresponding author at: Escuela Técnica Superior de Ingeniería, C. de los Descubrimientos, s/n 41092, Sevilla, Spain.
E-mail address: jcalvillo@us.es (J. Calvillo-Arbizu).

https://doi.org/10.1016/j.cmpb.2021.106231

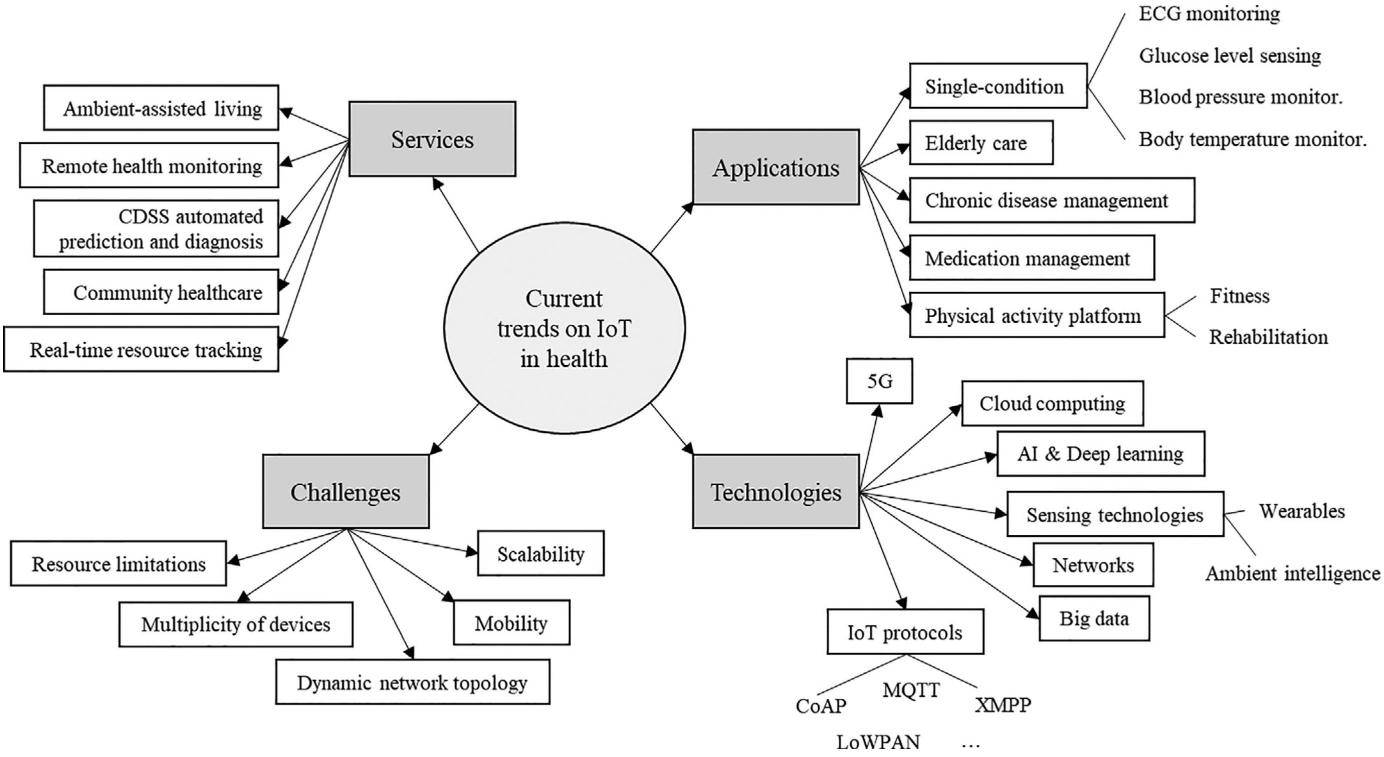

Fig. 1. Overview of current trends on healthcare IoT.

Table 1
Literature reviews on IoT applications in health.

Authors	Year	Focus	Findings	Challenges
Qi et al. [6]	2017	Existing research and case studies in IoT enabled personalized healthcare systems	Key enabling technologies: sensing technologies and data processing techniques	• Cost effective and non-obtrusive sensing • Effective data validation • Data processing & analytics
Islam et al. [7]	2015	Features of IoT-based health research (network topologies, use cases, services…)	Analysis of security requirements in IoT	• Standardization and cost-analysis • Low-power protocols • Continuous monitoring
Yuehong et al. [8]	2016	Enabling technologies and devices	Implementation strategies and methodologies	• Self-learning and self-improvement • Hardware integration and standardization • Security & privacy
de Morais and de Aquino [9]	2017	IoT-based applications in health	Non-/functional requirements Patterns and protocols	• Interoperability • Data mining for knowledge extraction • Security & privacy
Ahmadi et al. [10]	2019	Application areas of IoT in health	IoT technologies and protocols	• Security: hardware, network, application • Interoperability
Aceto, Persico, and Pescapé [11]	2020	Healthcare 4.0 application scenarios	Lessons learned from literature review	• Scalability & availability • Cloud challenges • Expectations on patients' experience
Greco et al. [12]	2020	IoT solutions on health monitoring	Use of fog computing Combination IoT and machine learning	–
Singh et al. [13]	2020	IoT applications for COVID-19 pandemic	Potential benefits for infected cases	• Security & privacy • Data aggregation
Swayamsiddha and Mohanty [14]	2020	Cognitive IoT applications for COVID-19	Effective applicability of cognitive IoT for COVID-19	• Security & privacy • Energy efficiency
Habibzadeh et al. [15]	2020	State-of-the-art in IoT on clinical applications	Requirements and conceptual IoT architecture	• Legal accountability • Regulatory requirements • Ethnographic challenges
Gardaševic et al. [16]	2020	Foundations of health IoT applications	Security techniques Standards and technologies	• Massive data management • Interoperability • Security and privacy
Butpheng, Yeh, and Xiong [17]	2020	Integration IoT-Cloud	Security & privacy solutions for IoT-Cloud health systems	• Energy constraints • Cloud limitations and scalability • Privacy by design
Shah, Bhat, and Khan [18]	2021	Cloud IoT-based healthcare integration components	Conceptual architecture and scenarios of healthcare Security issues and threats	• Energy efficient sensors • Low-power protocols • Latency and privacy protection on Cloud

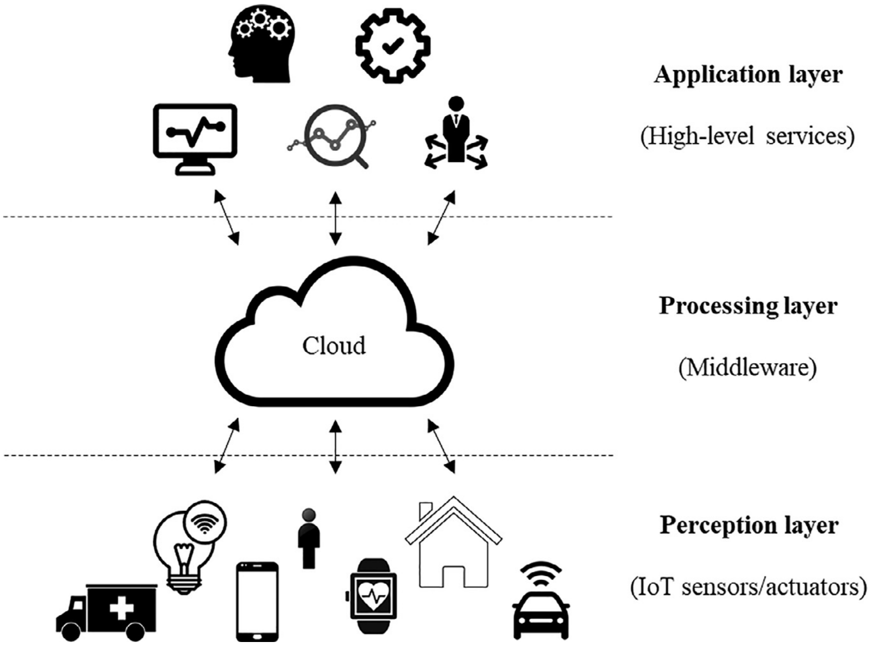

Fig. 2. An illustration of the IoT paradigm levels.

health. Thus, we put the spotlight on its specific requirements (some stated by those reviews and others do not) and analyse in which extent current approaches fulfil them, identifying trends and gaps. Since to the best of our knowledge, there is no such review, our work aims to fill such missing gap.

The remainder of the paper is structured as follows. Section 2 presents the IoT paradigm and describes major requirements of the health domain and the research method used for literature review. Results are showed in Section 3 and discussed in Section 4, giving a glance of findings, open issues, and missing gaps. Conclusions and future research hints are given in Section 5.

2. Methods

2.1. The IoT paradigm

IoT enhances pervasive computing by means of a network of objects or "things" uniquely addressable, which are capable of interacting and cooperating with each other to reach common goals [6,8,19]. Fig. 2 shows a general layered model of IoT.

The Perception layer is composed of things, understood as devices, that can interact with the surrounding world, usually as sensors or actuators. The middle level (i.e., IoT middleware) is responsible for distributing, processing, and storing data by employing cloud computing and providing a set of general capabilities such as service management, composition, orchestration, trust, privacy, and security management. The highest level contains specific software entities delivering advanced smart services through varied functionality (e.g., making decisions driven by data representing physical conditions).

One of the most relevant features of IoT in the health domain is enabling the provision of real-time information about patient health signs for remote follow-up or decision-making. Indeed, sensor devices can be applied both in-patient and out-patient care. Beyond gathering data from the point of care, IoT software entities may deploy machine learning algorithms, for example, to infer the risk of patient health deterioration [20]. Furthermore, combining information from Electronic Health Record (EHR) systems with patient's daily life data gathered through "things" (e.g., wearables or mobile devices) can improve healthcare delivery and contribute to build comprehensive views of each citizen.

2.2. Requirements of the health domain

Healthcare is a complex and heterogeneous sector involving extensive and specialized clinical knowledge, multimodal health information, variety of patients and potential conditions, relevance of health information over time, patient-centric paradigm, heterogeneous stakeholders, national and international regulations, etc. Thus, any IoT-driven solutions require a thorough analysis of requirements. In this work, three requirement themes have been identified: data lifecycle, security, and human-related issues (Fig. 3).

2.2.1. Theme 1: data lifecycle

Since IoT is a data-centric paradigm, efficient data management is a major requirement in any domain. Healthcare imposes several challenges due to variety, volume, and velocity of health data. Firstly, health data may be presented in multiple forms (e.g., numeric measures, unstructured data, images, codes…) and come from different sources or organizations. Thus, all potential health data sources should be considered and linked in order to maintain a comprehensive view of patient condition. Beyond ad-hoc solutions, interoperability should be addressed to guarantee meaningful data exchange and integration. Standards of medical devices, health information exchange, or coding (e.g., ISO 11073, ISO 13606, HL7 FHIR, SNOMED, LOINC) might ease the fulfilment of this requirement.

Secondly, IoT sensors may regularly generate big volumes of data that, additionally, if related to health, have long-term relevance. For instance, daily monitoring data of chronic conditions should be stored or linked to the patient's EHR, disregarding size or where they are generated. Consequently, storage systems should be versatile enough to receive/link and manage such amount of heterogeneous data. Furthermore, huge collections of integrated data (e.g., thousands of patients' records) require tools such as big data analytics to manage and exploit them in order to generate cross-domain knowledge, unreachable by working with each data source separately. Hence, health IoT-driven solutions should consider how data generated by sensors are going to be processed, stored, and exploited [18].

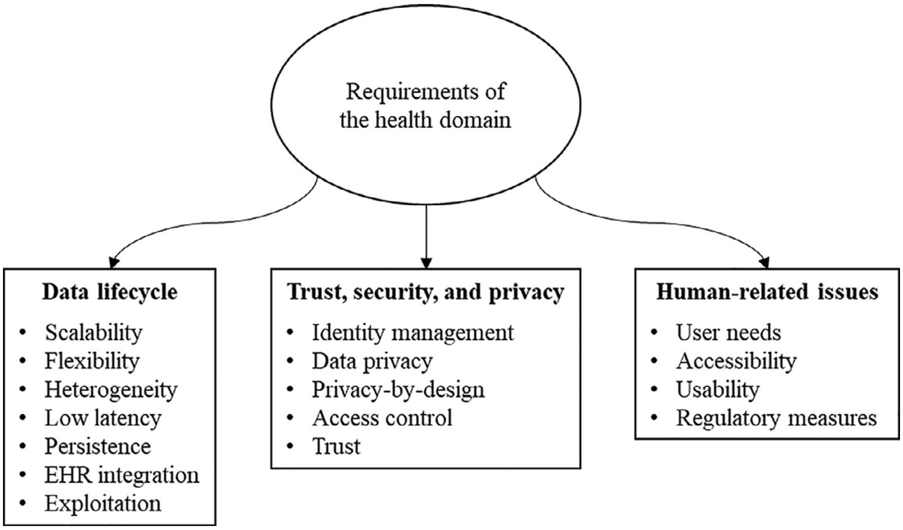

Fig. 3. Themes and requirements of the health domain.

Finally, IoT systems should optimize the reception and processing of data from several sources in real time in order not to lose data or overwhelm systems with data flooding.

2.2.2. Theme 2: trust, security, and privacy

Security and privacy of data and communications are of uttermost importance in health. This theme covers a wide spectrum of requirements such as authentication and authorization, encryption and confidentiality, integrity, non-repudiation, user safety, etc. Furthermore, 'security by design' and 'security by default' are key concepts upon which national and international regulations (such as EU General Data Protection Regulation -GDPR- or USA Health Insurance Portability and Accountability Act -HIPAA-) define their requirements.

IoT introduces additional security challenges. For instance, connected healthcare (wearable) devices could be hacked [7]. Hence, a secure uniqueness management and authentication is required. Furthermore, health actuators could influence health condition of patients, so trust is a capital requirement for this kind of solutions.

2.2.3. Theme 3: human-related issues

Health IoT-driven solutions should cope with both end-users and organizations where are applied. Firstly, if users may interact with IoT devices or services through interfaces, usability and accessibility must be boosted. Secondly, evaluating different needs and capabilities of users (e.g., patients, informal caregivers, health professionals, stakeholders…) is a requirement in order to achieve a rich alignment between solutions and users. Finally, governments and health organizations may impose regulatory measures (i.e., legislation, policies, and ethics principles) to protect patients and provide an efficient and ethic healthcare delivery. Any kind of tool involved in the healthcare process is subjected to such regulatory measures. Normative compliance depends on the specific environment (organization, region, setting…) where technology is applied.

2.3. Research method

Due to the variety of IoT definitions, this review particularly focuses on IoT-driven solutions that:

- deploy patient-centred care through sensor networks,
- combine sensor devices and cloud computing infrastructures for health data collection and processing, and/or
- apply the IoT paradigm for solving continuity of care issues.

Table 2
Search strings for extracting works from databases.

Keywords OR title OR abstract
('Internet of things' OR 'IoT') AND
(health OR healthcare OR mhealth OR 'mobile healthcare' OR 'pervasive healthcare')
'Internet of health things' OR 'IoHT'
'Internet of medical things' OR 'IoMT'
'pervasive computing' AND health

Scientific literature out of the scope of this review includes:

- development of sensors for health monitoring with no regard of transmission to or integration with health information systems,
- IoT solutions not directly related to patient care (e.g., logistics and resource tracking, health organization governance),
- development of protocols and technologies of IoT applied to the health domain as use case, and
- literature reviews or theoretical discussions of IoT in health.

Studies were collected by using IEEE Xplore, ScienceDirect, PubMed and Scopus databases. The initial inclusion criteria were English language, article or conference, and publication from January 2010 to February 2021. Four search string were used (Table 2). Titles, abstracts and contents were analysed by two peers in parallel to determine eligibility for further review.

3. Results

Databases searches resulted in 12,108 articles (Fig. 4). After excluding duplicates (3,602), papers were filtered by title (5,934 excluded) and abstract (2,376 excluded). The content of resulting papers was analysed in order to identify those works laying outside the target scope. Finally, 86 articles were eligible and examined [21–106].

4. Discussion

The papers finally included in the review show an increasing rate of publication and different approaches (e.g., blockchain, edge/fog computing, interoperability) (Fig. 5). The great impact of the IoT model in healthcare will come through the provision of health services everywhere anytime [107]. But this simple assertion implies a set of requirements not only related to distribution and mobility, but also to availability, interoperability, and se-

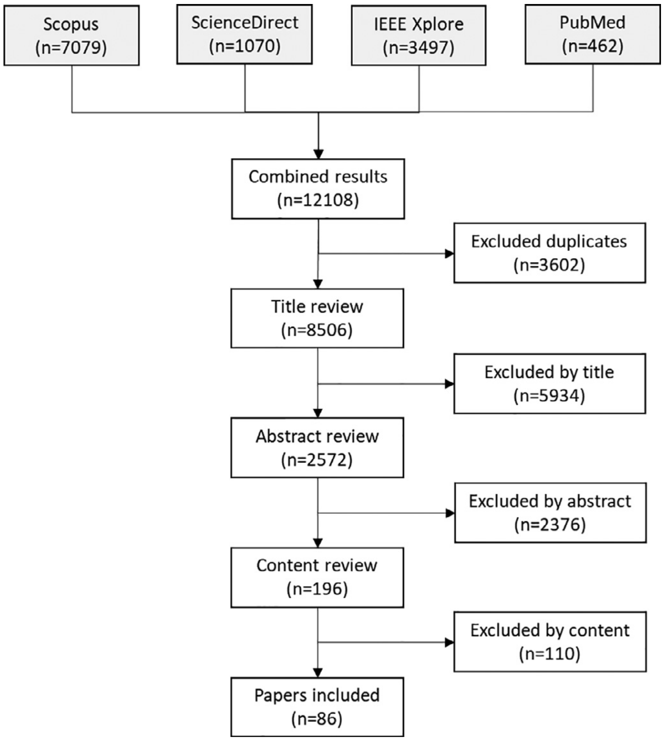

Fig. 4. Stages of the study selection process.

curity. Next, we discuss these requirements regarding each aforementioned theme and the literature review.

4.1. Theme 1: data lifecycle

Health IoT platforms allow to collect data from sensors distributed across locations of interest (e.g., patient home, ICU, nursing homes, outdoors worn by the patient). Table 3 shows the main requirements and trends of the topic of data lifecycle.

Regarding a massive application of health services, IoT platforms are likely to support hundreds of sensors sending data from dozens of locations. Furthermore, points of care are dynamic and may be deployed according to care needs. Hence, scalability and flexibility are major requirements that IoT solutions should address in order to adapt themselves to dynamic sets of sensors (sending data) and services (consuming data). Most reviewed papers deploy ad-hoc IoT platforms covering a limited number of sensors and services, and scalability is scarcely considered. Those taking healthcare demand flexibility into account follow one of two main approaches: decoupling of sensors and services through message-orientated middlewares [44,55,95] or using cloud virtualization capabilities. On the one hand, when there is not a "hard" connection between data generators and consumers, it is easier to adapt to variations on the number of sensors, points of care, or health services consuming data. On the other hand, the elastic nature of cloud infrastructure allows increasing/decreasing the pool of servers supporting a service or platform according to the current demand [32,94].

Beyond the number of sensors, their heterogeneity becomes another burden to the success of IoT solutions. Admitting heterogeneous devices means to share different data schemas or, in a more efficient way, to adopt standards. Thus, sensor data standards such as ISO/IEEE 11073 [108] or ontologies [109] may reduce the burden of covering wide spectra of sensors; nonetheless, their adoption is scarce ([45,79,92,96] are the only examples of standard adoption).

Ad-hoc solutions covering limited sets of use cases are prevailing in the current literature. However, IoT platforms focused on one specific scenario are hard to be reused or adapted to different contexts, what hinders the adoption of healthcare requirements such as openness and extensibility. In our review, only a few papers consider a wide spectrum of different types of data (even undetermined a priori) [21,53,54,56,67].

As it has been described above, cloud computing is widely combined with IoT solutions, providing a bunch of different services. Nevertheless, this paradigm shows some weaknesses. Beyond security concerns (addressed below), unpredictable latency may harm delay-sensitive services [110]. This latency may arise by poor network performance or massive communications between sensors and cloud services, negatively impacting on QoS [111]. In order to overcome this challenge, some papers introduce different data processing layers (i.e., fog and mist/edge computing levels) between sensors and the Cloud, providing services nearer to the point of care (Fig. 6). Thus, advanced devices such as smart-

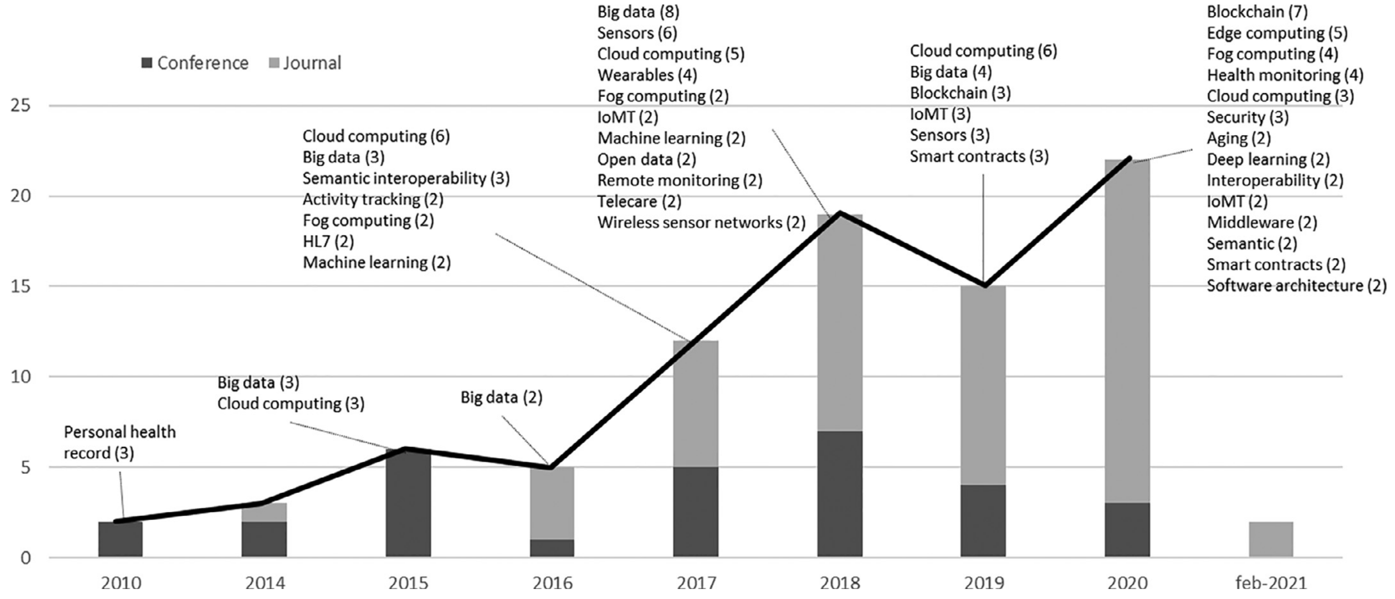

Fig. 5. Distribution of publications and most used keywords by year.

Table 3
Overview of theme 1 requirements, challenges, and trends.

Theme 1: Data lifecycle			
Health domain issues	Requirements	Challenges	Trends (examples)
Data gathering and performance			
Multiple sensors and locations	Scalability	Decoupling sensors/services	Message-orientated middleware [44,55,81,119]
Dynamic scenarios according needs	Flexibility	Increased number of participants	
		Elastic services demand	Cloud virtualization [32,94]
Heterogeneity (data, sensors…)	Openness	Sharing different schemas	Standards [45,79,96]
	Extensibility	Achieve common understanding	Semantic technologies [92]
Delay-sensitive services	Low latency	Unpredictable latency	Services nearer to the point of care
	QoS maintenance	Poor network performance	Fog computing [50,100,102]
			Mist/Edge computing [22,87]
Persistence and integration			
Storage of huge amounts of data	Long-term preservation	Balanced speed-consistency	NoSQL [33,39,77,85]
	Different storage possibilities	Data heterogeneity	Hybrid storage (on-/off-chain) [82,99,104]
Support for continuity of care	EHR integration	Open data silos	EHR standards [38,57,95,98]
		Integrate data from heterogeneous sources	Semantic technologies [30,47,55] Semantic Web of Things [113]
		Lack of EHR standards adoption	
Exploitation			
From raw data to knowledge	Knowledge generation	Massive data management	Machine and deep learning [88,96]
		Extract/discover patterns	Big data analytics [36,46,55,91]

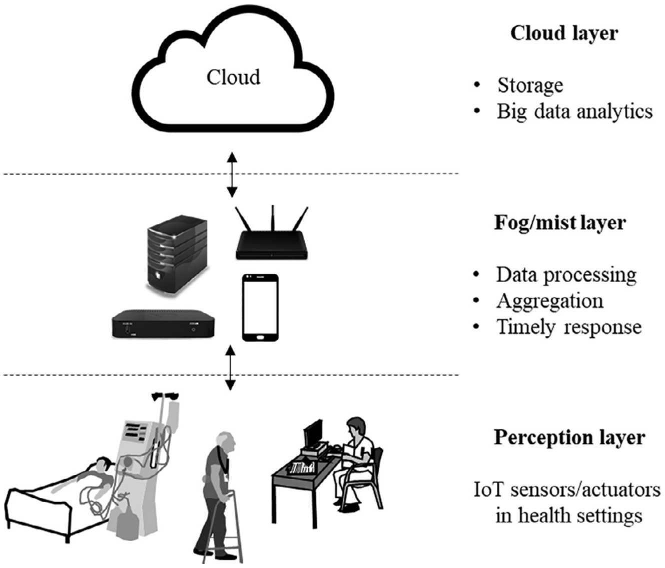

Fig. 6. Overview of different computing layers applied to healthcare.

phones or gateways may perform initial stages of data processing in order to detect events requiring a timely response, whereas cloud-based services are devoted to data storage and big data analytics. Such data management in layers is a major trend (e.g., [22,28,50,60,87,100,102]).

In the literature review, some works use commercial clouds (Amazon, Microsoft, etc.) [29,31,85], but most papers do not indicate which one is in use. While public clouds mean an increase of health data vulnerability, the economic cost of using private clouds for health IoT solutions has not been described yet.

Storage and persistence of health data are conditioned by the heterogeneity and the potential size of gathered data, and the mandatory requirement of long-term preservation for continued healthcare, legal purposes, or retrospective studies. Persistence is often approached by using NoSQL databases providing mechanisms for storage and retrieval of data that are modelled in other means than tabular relations used in relational databases. NoSQL databases (e.g., the Hadoop distributed file system, HDFS) are commonly adopted in big data scenarios since they allow to store high volumes of data in a timely manner [33,39,77,85]. The main drawback of NoSQL databases is that they enhance speed over consistency, what should be avoidable mostly in health data management. Then, adopting NoSQL and/or SQL databases should be conditioned by the use case, balancing between speed and consistency. A recent trend for data persistence is using blockchain and a hybrid storage model with some data stored on-chain and the rest off-chain [82,99,104].

In addition to transmission and persistence, raw sensor data must be included or linked to the patient's EHR. However, EHR data collected from sensors and systems often have different structures, semantics, and coding mechanisms, and data integration is a major challenge, the lack of which leads to the proliferation of data silos. Common standards such as HL7 v2, v3, openEHR, DICOM, or HL7 FHIR have been proposed, but there is still a major lack of adoption [112]. For instance, only two papers in our literature review adopt and discuss data standards for easing integration [38,57,95,98]. Other approaches use semantic tools (e.g., annotations and ontologies) for integration. Both public ontologies (such as SensorML or UMLS) or ad-hoc developments have been found in the reviewed literature [30,47,55]. Semantic Web of Things (SWoT) has also been proposed to enable a wide-scale integration by annotating semantics to the representation of the things [113].

The last stage of health data lifecycle is exploitation, i.e., knowledge generation. Big data management and analytics tools (including algorithms, machine learning or data mining techniques) are the most suitable option to deal with massive amounts of data and generate knowledge. While most works in our literature review do not describe in detail which actual platforms or tools they are using for big data (e.g., [88,96]), Apache Spark, Mahout, and Hadoop are the tools selected by others [36,46,55,91]. These provide machine learning algorithms and data processing engines that ease big data management. Big data tools are frequently deployed in the Cloud due to its virtually unlimited storage and processing capabilities [111]. Nevertheless, as was mentioned above, Cloud shortcomings related to delay and security may require the adoption of complementary solutions, e.g., fog computing.

4.2. Theme 2: trust, security, and privacy

This theme covers a wide set of requirements, challenges, and trends (Table 4). Despite the criticality of security requirements in managing personal health data, they are neglected in most re-

Table 4
Overview of theme 2 requirements, challenges, and trends.

Theme 2: Trust, security, and privacy			
Health domain issues	Requirements	Challenges	Trends (examples)
Identity management	Proper identification of users, sensors, and services	Distributed environments	Identity federation [56,72,93] Single sign-on
Confidentiality	Only authorized access to personal health data	Cross-organizational and multi-policy settings Extensive set of users, capabilities, and resources	Standards: OAuth, SAML, XACML [56] Blockchain [65]
Data privacy	Protect personal health data Secure transmission	Network vulnerability Man-in-the-middle attack Heterogeneity of IoT solutions	Anonymization [74] Encryption [37,60,77,97,106] Secure communication protocols [28,84] Blockchain [82]
Trust	Building trustable settings	Cross-organizational and distributed environments	Blockchain for consent management [90,120]
Device vulnerability	Protect devices from attack	No solutions for health	Adaptation of general-purpose solutions to the health domain
Integrity	Data accuracy and completeness		
Availability	Guaranteeing 24/7 availability		
Normative compliance	Compliance with HIPAA, GDPR...		

Table 5
Overview of theme 3 requirements, challenges, and trends.

Theme 3: Human-related issues			
Health domain issues	Requirements	Challenges	**Trends (examples)**
User interaction	Addressing user needs	Wide variety of users with different profiles and needs	User-centred methodologies [83] Multi-user solutions [30,67,75,77,85,95]
Accessibility	Conformity with user expectations, understandability, limitations...	Provide accessible interfaces and content	Standards [117,118]
Usability	Effectiveness & efficiency Satisfaction	User experience (UX) by design	
Regulatory measures	Compliance with FDA, CE, HIPAA, GDPR...	Obtain certifications as a guarantee of validity and reliability of devices	HIPAA and GDPR observation [57,70]

viewed papers. Indeed, no included article considers the specific security vulnerabilities of IoT in health settings such as constrained resources, heterogeneity, and ubiquity [113]. Firstly, health data are highly sensitive; hence, IoT-based platforms should address security issues covering not only authentication and authorization, but also confidentiality, integrity, availability, and normative compliance. Secondly, IoT devices involve an extension of vulnerabilities and an increased risk level (since they can be hackable), whereas their constrained resources lead to adopt simple security techniques. Stored data in public Cloud also represents a threat that may be exploited by malicious third parties [111].

Authentication, authorization, and encryption are the most considered areas in the literature. Proper identification of users and systems is a major requirement of any distributed environment, and here capabilities such as identity federation and single sign-on are crucial to comply with distribution. Authentication approaches are numerous and heterogeneous [56,72,93]. Regarding protecting resources from unauthorized users (i.e., authorization), common standards such as OAuth [114], SAML [115], and XACML [116] are adopted. Permissions are stored in policies or tokens and granted to users by means of attributes, easing federated scenarios. Regarding secure transmission, encryption mechanisms by using public keys and algorithms such as RSA, AES, or ARX are described in several works [37,77,84,106]. Furthermore, attribute-based encryption (ABE) is more and more popular to guarantee secure transmission as in [60]. Besides, protocols as SSL or WBAN are commonly adopted to secure transmission between parties [28,84].

Using blockchain for security and privacy is a relevant current trend [82,104,106]. Blockchain is approached as a mechanism to guarantee secure EHR sharing amongst users [65], anonymize data before transmission [74], or manage consent in distributed settings [90]. The limitation of devices to behave as blockchain nodes may be eased by eliminating the 'proof of work' [105].

Finally, security issues such as confidentiality, integrity, availability, and compliance with GDPR or HIPAA are scarcely addressed in IoT-based health approaches. Furthermore, concepts such as 'security by design' or 'security by default' do not guide the design and development of IoT solutions approached. Due to the relevance of health data managed and the potential attacks to patient safety, security should be a crucial requirement for every IoT solution in health.

4.3. Theme 3: human-related issues

Requirements and trends about human issues on health identified in literature are shown in Table 5. A wide variety of end-users (with different needs and expectations) may interact with an IoT-based solution, and both system acceptance and success depend greatly on its alignment with them.

In most of the reviewed papers, users are not considered in the design and development of IoT-based solutions, and their accessibility and usability requirements are mostly disregarded. Exceptionally, some works promote IoT-based services adaptable to user profiles (e.g., patient with impairment [75]) or capabilities [30]. Others put the stress on improving usability by means of information delivery adaptable to different kind of users [67,77,85,95].

Usability and accessibility standards (e.g., [117,118]) provide requirements that should be addressed in any IoT-based solution interacting with users. For instance, [118] states accessibility requirements such as: suitability for the widest range of users, conformity with user expectations, support for individualization, approachability, perceivability, understandability, controllability, usability, or equitable use. In [83], user needs are gathered before design applying a user-centred design (UCD) methodology.

Finally, the specific requirements of the health domain are stated by legislation and policies established by health organizations, administrative bodies, or standardization organizations. Being compliant with regulatory measures guarantees a proper adaptation of technology to the domain. Nevertheless, our literature review shows a low compliance (even low awareness) of standards or policies of the sector. Some papers mention FDA approval and CE certifications as a guarantee of validity and reliability of devices [43]. Regarding protection and confidentiality of health information, HIPAA is the most referred specification [57,70].

5. Conclusion

Despite the potential of IoT in healthcare, this domain is far behind others such as smart cities or industry regarding IoT adoption. The complexity of the domain hinders the successful application of IoT solutions, and current developments are rarely deployed in real scenarios. This work has aimed at understanding the extent to which IoT-based solutions in healthcare are coping with the specific requirements of the domain, identifying current trends and limitations based on a literature review.

Findings show that most approaches apply IoT merely as any other domain (industry, smart cities…), with no regard of the specific requirements of health. Most health IoT solutions deploy isolated platforms consisting in one sensor and a smartphone serving as gateway connected to cloud services. Ad-hoc IoT solutions may serve as proof of concept but should not be considered for real environments. Indeed, scalability, extensibility, integration, and security issues are frequently neglected.

Cloud computing and blockchain are two main technologies used in combination with IoT, but their weaknesses for the health domain are barely referred. Whereas Cloud computing presents bottlenecks regarding to security and privacy, reliability of patient data, opacity of infrastructure, and hard performance monitoring, blockchain may be used for security but it shows high latency and lack of scalability. Hence, these technologies should be adapted to the health domain, where patient data protection, real-time performance, and QoS maintenance are crucial requirements (amongst others).

Future research on this topic is promising since IoT-based solutions will allow to feed artificial intelligence algorithms for prediction or diagnosis, they will make possible to transfer hospital-based services to patient home or community, or they will support innovative healthcare services. Nonetheless, current and future health IoT solutions should pave the way ahead by taking healthcare requirements (e.g., security, interoperability, usability, etc.) into account in order to achieve high impact and success.

Declaration of Competing Interest

The authors declared that they do not have any conflict of interest.

Acknowledgements

This work was supported in part by UE Eurostars programme [project FRAIL], in part by Fundación Mutua Madrileña [project VÍA-RENAL], and in part byConsejería de Conocimiento, Investigación y Universidad, Junta de Andalucía [grant P18-TPJ-3074].

References

[1] F. Firouzi, B. Farahani, M. Weinberger, G. DePace, F.S. Aliee, IoT fundamentals:definitions, architectures, challenges, and promises, in: F. Firouzi, K. Chakrabarty, S. Nassif (Eds.), Intelligent Internet of Things, Springer, Cham, 2020, pp. 3–50.

[2] R. Watson, Top 8 Healthcare Technology Trends to Watch Out for in 2020. https://www.datadriveninvestor.com/2019/11/30/top-8-healthcare-technology-trends-to-watch-out-for-in-2020/ , 2019 (accessed 19 November 2020).

[3] S. Ansari, T. Aslam, J. Poncela, P. Otero, A. Ansari, Internet of Things-based healthcare applications, in: B.S. Chowdhry, F.K. Shaikh, N.A. Mahoto (Eds.), IoT Architectures, Models, and Platforms for Smart City Applications, IGI Global, 2020, pp. 1–28.

[4] K.L.M. Ang, J.K.P. Seng, Application specific Internet of Things (ASIoTs): taxonomy, applications, use case and future directions, IEEE Access 7 (2019) 56577–56590.

[5] S. Garde, P. Knaup, Requirements engineering in health care: the example of chemotherapy planning in paediatric oncology, Requir. Eng. 11 (4) (2006) 265–278.

[6] J. Qi, P. Yang, G. Min, O. Amft, F. Dong, L. Xu, Advanced internet of things for personalised healthcare systems:a survey, Pervasive Mob. Comput. 41 (2017) 132–149.

[7] S.R. Islam, D. Kwak, M.H. Kabir, M. Hossain, K.S. Kwak, The internet of things for health care: a comprehensive survey, IEEE Access 3 (2015) 678–708.

[8] Y.I.N. Yuehong, Y. Zeng, X. Chen, Y. Fan, The internet of things in healthcare: an overview, J Ind. Inf. Integr. 1 (2016) 3–13.

[9] I. de Morais Barroca Filho, G.S. de Aquino Junior, IoT-based healthcare applications: a review, in: O. Gervasi, B. Murgante, S. Misra (Eds.), Int. Conf. Comput. Sci. Appl., Springer, Cham, 2017, pp. 47–62.

[10] H. Ahmadi, G. Arji, L. Shahmoradi, R. Safdari, M. Nilashi, M. Alizadeh, The application of internet of things in healthcare: a systematic literature review and classification, Univers. Access Inf. Soc. 18 (2019) 837–869.

[11] G. Aceto, V. Persico, A. Pescapé, Industry 4.0 and health: internet of things, big data, and cloud computing for healthcare 4.0, J Ind. Inf. Integr. 18 (2020) 100129.

[12] L. Greco, G. Percannella, P. Ritrovato, F. Tortorella, M. Vento, Trends in IoT based solutions for health care: moving AI to the edge, Pattern Recognit. Lett. 135 (2020) 346–353.

[13] R.P. Singh, M. Javaid, A. Haleem, R. Suman, Internet of things (IoT) applications to fight against COVID-19 pandemic, Diab. Metab. Syndrom: Clin. Res. Rev. 14 (4) (2020) 521–524.

[14] S. Swayamsiddha, C. Mohanty, Application of cognitive internet of medical things for COVID-19 pandemic, Diab. Metab. Syndrom: Clin. Res. Rev. 14 (5) (2020) 911–915.

[15] H. Habibzadeh, K. Dinesh, O.R. Shishvan, A. Boggio-Dandry, G. Sharma, T. Soyata, A survey of healthcare internet of things (HIoT): a clinical perspective, IEEE Internet Things J. 7 (1) (2020) 53–71.

[16] G. Gardašević, K. Katzis, D. Bajić, L. Berbakov, Emerging wireless sensor networks and internet of things technologies—foundations of smart healthcare, Sensors 20 (13) (2020) 3619.

[17] C. Butpheng, K.H. Yeh, H. Xiong, Security and privacy in IoT-cloud-based e-health systems—a comprehensive review, Symmetry (Basel) 12 (7) (2020) 1191.

[18] J.L. Shah, H.F. Bhat, A.I. Khan, Integration of cloud and IoT for smart e-healthcare, in: V.E. Balas, S. Pal (Eds.), Healthcare Paradigms in the Internet of Things Ecosystem, Academic Press, 2021, pp. 101–136.

[19] L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, Comput. Netw. 54 (2010) 2787–2805.

[20] C.A. da Costa, C.F. Pasluosta, B. Eskofier, D.B. da Silva, R. da Rosa Righi, Internet of health things: toward intelligent vital signs monitoring in hospital wards, Artif. Intell. Med. 89 (2018) 61–69.

[21] V. Baljak, A. Ljubovic, J. Michel, M. Montgomery, R. Salaway, A scalable realtime analytics pipeline and storage architecture for physiological monitoring big data, Smart Health 9 (2018) 275–286.

[22] M. Asif-Ur-Rahman, F. Afsana, M. Mahmud, M.S. Kaiser, M.R. Ahmed, O. Kaiwartya, A. James-Taylor, Towards a heterogeneous mist, fog, and cloud based framework for the internet of healthcare things, IEEE Internet Things J. 6 (3) (2018) 4049–4062.

[23] A. Onasanya, S. Lakkis, M. Elshakankiri, Implementing IoT/WSN based smart saskatchewan healthcare system, Wirel. Netw. 25 (7) (2019) 1–22.

[24] A. Onasanya, M. Elshakankiri, Secured cancer care and cloud services in IoT/WSN based medical systems, in: Int. Conf. Smart Grid Internet Things, Cham, Springer, 2018, pp. 23–35.

[25] A. Alamri, Ontology middleware for integration of IoT healthcare information systems in EHR systems, Comput. 7 (4) (2018) 51.

[26] J. Rei, C. Brito, A. Sousa, Assessment of an IoT platform for data collection and analysis for medical sensors, in: IEEE 4th Int. Conf. Collab. Internet Comput. (CIC), 2018, pp. 405–411.

[27] S.A. Khowaja, A.G. Prabono, F. Setiawan, B.N. Yahya, S.L. Lee, Contextual activity based healthcare internet of things, services, and people (HIoTSP): an architectural framework for healthcare monitoring using wearable sensors, Comput. Netw. 145 (2018) 190–206.

[28] D. Yacchirema, D. Sarabia-Jácome, C.E. Palau, M. Esteve, System for monitoring and supporting the treatment of sleep apnea using IoT and big data, Pervasive Mob. Comput. 50 (2018) 25–40.

[29] G. Manogaran, R. Varatharajan, D. Lopez, P.M. Kumar, R. Sundarasekar, C. Thota, A new architecture of internet of things and big data ecosystem for secured smart healthcare monitoring and alerting system, Futur. Gener. Comp. Syst. 82 (2018) 375–387.

[30] A. Dridi, S. Sassi, S. Faiz, Towards a semantic medical internet of things, in: IEEE/ACS 14th Int. Conf. Comput. Syst. Appl. (AICCSA), 2017, pp. 1421–1428.

[31] P.M. Kumar, U.D. Gandhi, A novel three-tier internet of things architecture with machine learning algorithm for early detection of heart diseases, Comput. Electr. Eng. 65 (2018) 222–235.

[32] P. Amirian, F. van Loggerenberg, T. Lang, A. Thomas, R. Peeling, A. Basiri, S.N. Goodman, Using big data analytics to extract disease surveillance information from point of care diagnostic machines, Pervasive Mob. Comput. 42 (2017) 470–486.

[33] M.M. Rathore, A. Paul, A. Ahmad, M. Anisetti, G. Jeon, Hadoop-based intelligent care system (hics): analytical approach for big data in iot, ACM Trans. Internet Technol. 18 (1) (2017) 8.

[34] S. He, B. Cheng, H. Wang, Y. Huang, J. Chen, Proactive personalized services through fog-cloud computing in large-scale IoT-based healthcare application, China Commun. 14 (11) (2017) 1–16.

[35] F. Ullah, M.A. Habib, M. Farhan, S. Khalid, M.Y. Durrani, S. Jabbar, Semantic interoperability for big-data in heterogeneous IoT infrastructure for healthcare, Sust. Cities Soc. 34 (2017) 90–96.

[36] J. Hong, P. Morris, J. Seo, Interconnected personal health record ecosystem using IoT cloud platform and HL7 FHIR, in: IEEE Int. Conf. Healthc. Inform. (ICHI), 2017, pp. 362–367.

[37] P.K. Gupta, B.T. Maharaj, R. Malekian, A novel and secure IoT based cloud centric architecture to perform predictive analysis of users activities in sustainable health centres, Multimed. Tools Appl. 76 (18) (2017) 18489–18512.

[38] Á. Garai, I. Péntek, A. Adamkó, Á. Németh, A clinical system integration methodology for bio-sensory technology with cloud architecture, Acta. Cybern. 23 (2) (2017) 513–536.

[39] P. Dineshkumar, V.N. Rajavarman, R.S. Ponmagal, M-caemon: modified cloud access execution and monitoring for big data analytics of health sensor system, Int. J. Appl. Eng. Res. 12 (23) (2017) 13096–13103.

[40] C.A. Velasco, Y. Mohamad, P. Ackermann, Architecture of a web of things ehealth framework for the support of users with chronic diseases, in: 7th Int. Conf. Softw. Develop. Technol. Enhancing Access. Fighting Info-exclusion, 2017, pp. 47–53.

[41] M.M. Rathore, A. Ahmad, A. Paul, J. Wan, D. Zhang, Real-time medical emergency response system: exploiting IoT and big data for public health, J. Med. Syst. 40 (12) (2016) 283.

[42] M.M. Rathore, A. Ahmad, A. Paul, The internet of things based medical emergency management using Hadoop ecosystem, in: IEEE Sensors, 2015, pp. 1–4.

[43] D.G. Páez, M. de Buenaga Rodríguez, E.P. Sánz, M.T. Villalba, R.M. Gil, Big data processing using wearable devices for wellbeing and healthy activities promotion, in: Int. Work-Conf. Amb. Assist. Liv., 2015, pp. 196–205.

[44] Y. Li, Y. Guo, Wiki-health: from quantified self to self-understanding, Futur. Gener. Comp. Syst. 56 (2016) 333–359.

[45] D.F. Santos, A. Perkusich, H.O. Almeida, Standard-based and distributed health information sharing for mHealth IoT systems, in: IEEE 16th Int. Conf. e-Health Netw., Appl. Serv. (Healthcom), 2014, pp. 94–98.

[46] P. Maia, T. Batista, E. Cavalcante, A. Baffa, F.C. Delicato, P.F. Pires, A. Zomaya, A web platform for interconnecting body sensors and improving health care, Proced. Comput. Sci. 40 (2014) 135–142.

[47] S.K. Datta, C. Bonnet, A. Gyrard, R.P.F. Da Costa, K. Boudaoud, Applying internet of things for personalized healthcare in smart homes, in: 24th Wirel, Opt. Commun. Conf. (2015) 164–169.

[48] A. Menychtas, C. Doukas, P. Tsanakas, I. Maglogiannis, A versatile architecture for building IoT quantified-self applications, in: IEEE 30th Int. Symp. Comput. Med. Syst. (CBMS), 2017, pp. 500–505.

[49] D.C. Yacchirema, D. Sarabia-Jácome, C.E. Palau, M. Esteve, A smart system for sleep monitoring by integrating IoT with big data analytics, IEEE Access 6 (2018) 35988–36001.

[50] O. Akrivopoulos, I. Chatzigiannakis, C. Tselios, A. Antoniou, On the deployment of healthcare applications over fog computing infrastructure, in: IEEE 41st Annu. Comput. Softw. Appl. Conf. (COMPSAC), 2017, pp. 288–293.

[51] A. Ruiz-Zafra, K. Benghazi, C. Mavromoustakis, M. Noguera, An IoT-aware architectural model for smart habitats, in: IEEE 16th Int. Conf. Embedded Ubiquit. Comput. (EUC), 2018, pp. 103–110.

[52] S. Din, H. Ghayvat, A. Paul, A. Ahmad, M.M. Rathore, I. Shafi, An architecture to analyze big data in the internet of things, in: 9th Int. Conf. Sensing Technol. (ICST), 2016, pp. 677–682.

[53] D. Sarabia-Jacome, A. Belsa, C.E. Palau, M. Esteve, Exploiting IoT data and smart city services for chronic obstructive pulmonary diseases risk factors monitoring, in: IEEE Int. Conf. Cloud Eng. (IC2E), 2018, pp. 351–356.

[54] S. Çoban, M.O. Gökalp, E. Gökalp, P.E. Eren, A. Koçyiğit, Predictive maintenance in healthcare services with big data technologies, in: IEEE 11th Conf. Serv.-Oriented Comput. Appl. (SOCA), 2018, pp. 93–98.

[55] R. Zgheib, A. De Nicola, M.L. Villani, E. Conchon, R. Bastide, A flexible architecture for cognitive sensing of activities in ambient assisted living, in: IEEE 26th Int. Conf. Enabling Technol.: Infrastruct. Collab. Enterp. (WETICE), 2017, pp. 284–289.

[56] M. Fazio, A. Celesti, F.G. Marquez, A. Glikson, M. Villari, Exploiting the FIWARE cloud platform to develop a remote patient monitoring system, in: IEEE Symp. Comput. Commun., 2015, pp. 264–270.

[57] N. Boutros-Saikali, K. Saikali, R.A. Naoum, An IoMT platform to simplify the development of healthcare monitoring applications, in: 3rd Int. Conf. Electric. Biomed. Eng., Clean Energy Green Comput. (EBECEGC), 2018, pp. 6–11.

[58] S. Sakr, A. Elgammal, Towards a comprehensive data analytics framework for smart healthcare services, Big Data Res. 4 (2016) 44–58.

[59] P. Asghari, A.M. Rahmani, H. Haj Seyyed Javadi, A medical monitoring scheme and health-medical service composition model in cloud-based IoT platform, Trans. Emerg. Telecommun. Technol. 30 (6) (2019) e3637.

[60] A.M. Elmisery, S. Rho, M. Aborizka, A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services, Clust. Comput. 22 (1) (2019) 1611–1638.

[61] N.E. Maghawry, S. Ghoniemy, A proposed internet of everything framework for disease prediction, Int. J. Online Biomed. Eng. 15 (4) (2019) 20–27.

[62] H.L. Pham, T.H. Tran, Y. Nakashima, A secure remote healthcare system for hospital using blockchain smart contract, in: IEEE Globecom Workshops, 2018, pp. 1–6.

[63] T. Kim, J. Lim, An edge cloud–based body data sensing architecture for artificial intelligence computation, Int. J. Distrib. Sens. Netw. 15 (4) (2019) 1550147719839014.

[64] N.C. Taher, I. Mallat, N. Agoulmine, N. El-Mawass, An IoT-cloud based solution for real-time and batch processing of big data: application in healthcare, in: 3rd Int. Conf. Bioeng. Smart Technol. (BioSMART), 2019, pp. 1–8.

[65] D.C. Nguyen, P.N. Pathirana, M. Ding, A. Seneviratne, Blockchain for secure EHRs sharing of mobile cloud based E-health systems, IEEE Access 7 (2019) 66792–66806.

[66] R. Dautov, S. Distefano, R. Buyya, Hierarchical data fusion for smart healthcare, J. Big Data 6 (1) (2019) 19.

[67] A. Celesti, M. Fazio, F. Galán Márquez, A. Glikson, H. Mauwa, A. Bagula, F. Celesti, M. Villari, How to develop IoT cloud e-health systems based on FIWARE: a lesson learnt, J. Sens. Actuator Netw. 8 (1) (2019) 7.

[68] P. Pace, G. Aloi, G. Caliciuri, R. Gravina, C. Savaglio, G. Fortino, G. Ibanez–Sanchez, A. Fides-Valero, J. Bayo-Monton, M. Uberti, M. Corona, INTER-health: an interoperable IoT solution for active and assisted living healthcare services, in: IEEE 5th World Forum Internet Things (WF-IoT), 2019, pp. 81–86.

[69] A. Alexandru, D. Coardos, E. Tudora, IoT-based healthcare remote monitoring platform for elderly with fog and cloud computing, in: 22nd Int, Conf. Control Syst. Comput. Sci. (2019) 154–161.

[70] S.H. Chang, R.D. Chiang, S.J. Wu, W.T. Chang, A context-aware, interactive M-health system for diabetics, IT Prof. 18 (3) (2017) 14–22.

[71] S.P. Korres, A. Menychtas, P. Tsanakas, I. Maglogiannis, A low-cost IoT-based health monitoring platform enriched with social networking facilities, in: IEEE Int. Conf. Pervasive Comput. Commun. Workshops, 2018, pp. 173–178.

[72] J. Rafferty, J. Synnott, C.D. Nugent, A. Ennis, P.A. Catherwood, I. McChesney, I. Cleland, S. McClean, A. Scalable, Research oriented, generic, sensor data platform, IEEE Access 6 (2018) 45473–45484.

[73] A. Helmer, B. Song, W. Ludwig, M. Schulze, M. Eichelberg, A. Hein, U. Tegtbur, et al., A sensor-enhanced health information system to support automatically controlled exercise training of COPD patients, in: 4th Int. Conf. Pervasive Comput. Technol. Healthc., 2010, pp. 1–6.

[74] L.A. Kalogiros, K. Lagouvardos, S. Nikoletseas, N. Papadopoulos, P. Tzamalis, Allergymap: a hybrid mHealth mobile crowdsensing system for allergic diseases epidemiology: a multidisciplinary case study, in: IEEE Int. Conf. Pervasive Comput. Commun. Workshops, 2018, pp. 597–602.

[75] M. Oliver, M. Teruel, J. Molina, D. Romero-Ayuso, P. González, Ambient intelligence environment for home cognitive telerehabilitation, Sensors 18 (11) (2018) 3671.

[76] G.R. Librelotto, C. Ribeiro, S. Vizzotto, E. Bastiani, L.O. Freitas, Architecture of central monitoring for pervasive homecare systems, in: X.L. Lat (Ed.), Am. Comput. Conf., 2014, pp. 1–7.

[77] O. Banos, M.B. Amin, W.A. Khan, T. Ali, M. Afzal, B.H. Kang, S. Lee, Mining minds: an innovative framework for personalized health and wellness support, in: 9th Int. Conf. Pervasive Comput. Technol. Healthc., 2015, pp. 1–8.

[78] L. Syed, S. Jabeen, S. Manimala, A. Alsaeedi, Smart healthcare framework for ambient assisted living using IoMT and big data analytics techniques, Futur. Gener. Comp. Syst. 101 (2019) 136–151.

[79] S.H. Lee, J.H. Song, J.H. Ye, H.J. Lee, B.K. Yi, I.K. Kim, SOA-based integrated pervasive personal health management system using PHDs, in: 4th Int. Conf. Pervasive Comp. Technol. Healthc., 2010, pp. 1–4.

[80] S. Rubí, N. Jesús, L. Gondim, R. Paulo, IoMT platform for pervasive healthcare data aggregation, processing, and sharing based on OneM2M and OpenEHR, Sensors 19 (19) (2019) 4283.

[81] P.P. Ray, D. Dash, D. De, Intelligent internet of things enabled edge system for smart healthcare, Natl. Acad. Sci. Lett. (2020) 1–6.

[82] M.S. Ali, M. Vecchio, G.D. Putra, S.S. Kanhere, F. Antonelli, A decentralized peer-to-peer remote health monitoring system, Sensors 20 (6) (2020) 1656.

[83] P.C. Santana-Mancilla, L.E. Anido-Rifón, J. Contreras-Castillo, R. Buenrostro–Mariscal, Heuristic evaluation of an IoMT system for remote health monitoring in senior care, Int. J. Environ. Res. Public Health 17 (5) (2020) 1586.

[84] J. Wang, K. Han, A. Alexandridis, et al., A blockchain-based eHealthcare system interoperating with WBANs, Futur. Gener. Comp. Syst. 110 (2020) 675–685.

[85] H.B. Hassen, N. Ayari, B. Hamdi, A home hospitalization system based on the internet of things, fog computing and cloud computing, Inform. Med. Unlocked 20 (2020) 100368.

[86] X. Li, Y. Lu, X. Fu, Y. Qi, Building the internet of things platform for smart maternal healthcare services with wearable devices and cloud computing, Futur. Gener. Comp. Syst. 118 (2021) 282–296.

[87] C. Ellaji, G. Sreehitha, B.L. Devi, Efficient health care systems using intelligent things using NB-IoT, in: Mater. Today: Proc., 2020 (in press).

[88] S. Tuli, N. Basumatary, S.S. Gill, et al., Healthfog: an ensemble deep learning based smart healthcare system for automatic diagnosis of heart diseases in integrated IoT and fog computing environments, Futur. Gener. Comp. Syst. 104 (2020) 187–200.

[89] M.A. Serhani, H.T. El-Kassabi, K. Shuaib, A.N. Navaz, B. Benatallah, A. Beheshti, Self-adapting cloud services orchestration for fulfilling intensive sensory data-driven IoT workflows, Futur. Gener. Comp. Syst. 108 (2020) 583–597.

[90] P.E. Velmovitsky, P.A.D.S.E. Souza, H. Vaillancourt, T. Donovska, J. Teague, P.P. Morita, A blockchain-based consent platform for active assisted living: modeling study and conceptual framework, J. Med. Internet Res. 22 (12) (2020) e20832.

[91] D. Fozoonmayeh, H.V. Le, E. Wittfoth, et al., A scalable smartwatch-based medication intake detection system using distributed machine learning, J. Med. Syst. 44 (4) (2020) 1–14.

[92] A. Rhayem, M.B.A. Mhiri, K. Drira, S. Tazi, F. Gargouri, A semantic-enabled and context-aware monitoring system for the internet of medical things, Expert Syst. 38 (2) (2021) e12629.

[93] R. Amin, S.H. Islam, P. Gope, K.K.R. Choo, N. Tapas, Anonymity preserving and lightweight multimedical server authentication protocol for telecare medical information system, IEEE J. Biomed. Health Inform. 23 (4) (2018) 1749–1759.

[94] A. Bhawiyuga, S.A. Kharisma, B.J. Santoso, D.P. Kartikasari, A.P. Kirana, Cloud-based middleware for supporting batch and stream access over smart healthcare wearable device, Bull. Elec. Engin. Inform. 9 (5) (2020) 1990–1997.

[95] K.M. Tsiouris, D. Gatsios, V. Tsakanikas, A.A. Pardalis, et al., Designing interoperable telehealth platforms: bridging IoT devices with cloud infrastructures, Enterp. Inform. Syst. 14 (8) (2020) 1194–1218.

[96] K. Chung, H. Yoo, Edge computing health model using P2P-based deep neural networks, Peer Peer Netw. Appl. 13 (2) (2020) 694–703.

[97] W. Sriborrirux, P. Laortum, Healthcare center IoT edge gateway based on containerized microservices, in: Proc. 4th Int. Conf. Intel. Syst, 2020, pp. 24–29.

[98] J.N.S. Rubí, P.R.D.L. Gondim, Interoperable internet of medical things platform for e-health applications, Int. J. Distrib. Sensor Netw. 16 (1) (2020) 1550147719889591.

[99] K.P. Satamraju, Proof of concept of scalable integration of internet of things and blockchain in healthcare, Sensors 20 (5) (2020) 1389.

[100] S.R. Hassan, I. Ahmad, S. Ahmad, A. Alfaify, M. Shafiq, Remote pain monitoring using fog computing for e-healthcare: an efficient architecture, Sensors 20 (22) (2020) 6574.

[101] Z. Jiao, Y. Xiao, Y. Jin, X. Chen, Tianxia120: a multimodal medical data collection bioinformatic system for proactive health management in internet of medical things, J. Healthc. Eng. (2020).

[102] P. Cedillo, X. Riofrio, D. Prado, M. Orellana, A middleware for managing the heterogeneity of data provining from IoT devices in ambient assisted living environments, IEEE ANDESCON, 2020.

[103] P. Barbosa, A. Figueiredo, S. Souto, E. Gaeta, E. Araujo, T. Teixeira, An open source software architecture and ready-to-use components for health IoT, in: IEEE 33rd Int. Sym. Comp. Med. Syst., 2020, pp. 374–379.

[104] R. Akkaoui, X. Hei, W. Cheng, EdgeMediChain: a hybrid edge blockchain-based framework for health data exchange, IEEE Access 8 (2020) 113467–113486.

[105] A.D. Dwivedi, G. Srivastava, S. Dhar, R. Singh, A decentralized privacy-preserving healthcare blockchain for IoT, Sensors 19 (2) (2019) 326.

[106] A. Yazdinejad, G. Srivastava, R.M. Parizi, A. Dehghantanha, K.K.R. Choo, M. Aledhari, Decentralized authentication of distributed patients in hospital networks using blockchain, IEEE J. Biomed. Health Inform. 24 (8) (2020) 2146–2156.

[107] B. Blobel, Challenges and solutions for designing and managing pHealth ecosystems, Front. Med. 6 (2019) 83.

[108] ISO/IEEE 11073 Health informatics – personal health device communication, 2014-2019.

[109] S. Balakrishna, M. Thirumaran, Semantic interoperability in IoT and big data for health care: a collaborative approach, in: A. Banerjee, C. Chakraborty, A. Kumar, D. Biswas (Eds.), Handbook of Data Science Approaches for Biomedical Engineering, Academic Press, 2020, pp. 185–220.

[110] Y. Nan, W. Li, W. Bao, F.C. Delicato, P.F. Pires, A.Y. Zomaya, Cost-effective processing for delay-sensitive applications in cloud of things systems, in: Proc. IEEE 15th Int. Symp. Netw. Comput. Appl. (NCA), 2016, pp. 162–169.

[111] M.M. Mahmoud, J.J. Rodrigues, S.H. Ahmed, et al., Enabling technologies on cloud of things for smart healthcare, IEEE Access 6 (2018) 31950–31967.

[112] C. Peng, P. Goswami, Meaningful integration of data from heterogeneous health services and home environment based on ontology, Sensors 19 (8) (2019) 1747.

[113] M. Alramadhan, K. Sha, An overview of access control mechanisms for internet of things, in: 26th Int. Conf. Comput. Comm. Netw. (ICCCN), 2017, pp. 1–6.

[114] IETF. RFC 6749 – The OAuth 2.0 Authorization Framework, 2012.

[115] OASIS. Security Assertion Markup Language (SAML) v2.0 Technical Overview, 2008.

[116] OASIS. eXtensible Access Control Markup Language (XACML) v3.0, 2013.

[117] ISO. ISO 9241-210:2019 - Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems, 2019.

[118] ISO. ISO/IEC 29138-1:2018 - Information technology – User interface accessibility – Part 1: User accessibility needs, 2018.

[119] G. Fersi, Study of middleware for internet of healthcare things and their applications, in: Proc. Int. Conf. Smart Homes Health Telematics, Cham, Springer, 2020, pp. 223–231.

[120] E.M. Abou-Nassar, A.M. Iliyasu, P.M. El-Kafrawy, et al., DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems, IEEE Access 8 (2020) 111223–111238.