Measurement: Sensors 22 (2022) 100375

Contents lists available at ScienceDirect

Measurement: Sensors

journal homepage: www.sciencedirect.com/journal/measurement-sensors

Adaptation and application of the IEEE 2413-2019 standard security mechanisms to IoMT systems

Alejandro Talaminos-Barroso *, Javier Reina-Tosina, Laura M. Roa

Biomedical Engineering Group, Dept. of Signal Theory and Communications (Universidad de Sevilla), Higher Technical School of Engineering, C. de los Descubrimientos s/n, 41092, Seville, Spain

ARTICLE INFO

Keywords:
Internet of medical things (IoMT)
Interoperability
Security
Smart sensor device
IEEE 2413-2019
Connected health

ABSTRACT

Healthcare information systems are evolving from traditional centralised architectures towards highly-mobile distributed environments within the connected health context. The IoMT paradigm is at the forefront of this technological revolution underlying the development of communication infrastructures connecting smart medical devices, healthcare information systems and services. The IEEE 2413 standard, a promising general architectural framework for the design and implementation of IoT systems, has recently been announced. This standard proposes a general description for different types of domains, including healthcare, but it does not contain an extension developed for the IoMT systems domain. This paper presents a first approach to adapt the IEEE 2413 standard to the design of IoMT systems from a security perspective, considering the most relevant aspects of the standard for the construction of this type of systems. The application to an IoMT system for monitoring patients with chronic obstructive pulmonary disease is presented as a use case.

1. Introduction

The rapid development of mobile technology, wireless communications, body area networks and embedded systems is helping healthcare systems to become a key vehicle in the new era of connected health [1]. This combination of medical devices and applications interconnected through the network is part of a subset of Internet of Things (IoT) technologies, called the Internet of Medical Things (IoMT). This new paradigm facilitates the continuous monitoring of a person's health status through real-time monitoring systems using wearable medical devices and smart sensors, representing a significant evolution and a step towards personalised medicine [2].

Edge computing [3] is emerging as an alternative to classical data processing in the cloud. This newly distributed information architectural approach moves medical applications to data sources, decreasing latency and providing advantages in portability, quality of service, interaction and characterisation [4]. IoMT-based healthcare platforms are assuming these functionalities to make medical processes more efficient, faster and ubiquitous. Other advantages include patient empowerment in the sense of making them aware of their health status and taking control of it [1], facilitating the intervention of healthcare professionals. The advances that derive thereof will have favourable implications in rural or hard-to-reach communities [5], developing countries or areas affected by major disasters, where healthcare professionals are limited or non-existent.

IoMT-based healthcare monitoring solutions [6] have highlighted the need to design and implement scalable, reliable and robust architectures. In this sense, the heterogeneity of smart sensors involves the integration of different data schemas to achieve interoperability or, better yet, the adoption of communication standards for medical devices such as ISO/IEEE 11073 [7], although its actual adoption is low [8]. Another barrier for the design and implementation of IoMT platforms [1] is to consider healthcare applications with no regard of the specific requirements of this domain [8].

An IoMT platform [9] consists of applications focused on the acquisition, transfer, storage, processing, and visualization of data under online, offline and/or real-time conditions [10]. The distribution of these applications is spread across all architectural levels of the platform, from sensor/actuator data collection in the lower layers to advanced data analysis services based on cloud computing solutions at the higher levels. The use case delimits the functionality and scope of the applications deployed according to the specific requirements and the objectives to be achieved. In this regard, a wide variety of IoMT platforms of different nature have been presented in recent years. These systems are generally approached from different perspectives, such as

* Corresponding author. Higher Technical School of Engineering, C. de los Descubrimientos s/n, 41092, Seville, Spain.
E-mail addresses: atalaminos@us.es (A. Talaminos-Barroso), jreina@us.es (J. Reina-Tosina), lroa@us.es (L.M. Roa).

https://doi.org/10.1016/j.measen.2022.100375
Received 30 July 2021; Accepted 1 May 2022
Available online 16 May 2022

Abbreviations

BYOD	Bring Your Own Device
DMZ	Demilitarised Zone
CPS	Cyber-Physical Systems
IoT	Internet of Things
ISMS	Information Security Management System
IoMT	Internet of Medical Things
MQTT	MQ Telemetry Transport
P2P	Peer-To-Peer
PDIoT	Reference Architecture for IoT Power Distribution
RASC	Reference Architecture for Smart City

the application of artificial intelligence techniques [5], transmission and storage of data in standardised formats [11], user experience and human-machine interfaces [12], communications [13], scalability [14] or medical applications with low latency requirements [15], among others. Generally, most of these platforms are mainly designed as ad-hoc solutions and do not offer interoperability with other systems.

The works related to the description of layered architectures for IoMT platforms are also important [16,17]. Although there are proposals for four-layer architectures [18] or five [19], generally the three-layer approach stands out [20]: things layer, fog layer and cloud layer. The things layer is made up of all monitoring devices, including sensors, actuators, pharmacy controls, etc. The fog level operates between the things layer and cloud layer, including data centres that leverage local processing to provide real-time feedback to users. Finally, the cloud layer consists of advanced computational and storage resources for analysis and decision support systems.

Another key determinant of the success and acceptance of IoMT systems is the security of information and communications. In this regard, IoMT devices are underlying elements of the network infrastructure and are generally vulnerable and exposed to different types of security threats, thus representing a significant risk to patient privacy [21]. Recent surveys [22] reveal that security is the main concern for IoMT adoption, including data protection and the potential risks brought about the Bring Your Own Device (BYOD) habit. In order to address these issues, different security frameworks have been introduced in recent years [23,24], including three main areas [22]: device security, communication security and cloud security. New technologies such as blockchain are also being incorporated into some platforms [25] to preserve privacy and data integrity and, at the same time, facilitate data exchange between healthcare professionals and electronic health records. Authentication between devices has also been addressed with blockchain in some works [5] and the number of related papers in this sense is increasing in the last years [26].

The IEEE has recently announced an architectural standard for IoT (IEEE 2413-2019 or P2413) [27] with the aim of promoting heterogeneous interaction and system/vendor interoperability. This standard provides a guide for unifying IoT systems and minimising fragmentation in industry under three objectives: I) to provide a secure, interoperable framework for IoT systems in multiple application domains; II) a framework for evaluation and comparison of IoT systems; and III) a framework to help accelerate the design, operation and deployment of IoT systems.

Currently, the standard lacks an extension developed for IoMT systems domain [28], although it proposes a general description for all types of application domains, including healthcare. This paper presents a first approach for adapting the IEEE 2413 standard to the design of IoMT systems. Due to the importance of information and communication security for IoMT systems [22,29], as well as the wide scope of the standard, this work focuses on these security aspects.

This paper is structured as follows: Section 2 presents the Materials and Methods and contains two subsections. Subsection 2.1 provides an overview of the IEEE 2413-2019 standard, extensions to different domains and current status in relation to the health domain. Subsection 2.2 introduces the architectural framework of the standard and the most relevant viewpoints with respect to information and communication security. Section 3 presents the results of the work in three subsections. In 3.1, the stakeholders and concerns related to security in the context of IoMT systems are identified. This is followed by a description of the use case under study in 3.2. Then, the adaptation of the standard to the proposed use case is presented in 3.3. Finally, the conclusions of the work are drawn in section 4.

2. Materials and methods

2.1. IEEE 2413-2019

IEEE 2413-2019 (P2413) is a standard that defines an architectural framework for IoT. It contains descriptions applicable to various domains (energy, home, health, transport, etc.), definitions of domain abstractions and identification of intersection points between different domains [30], including a reference model covering basic architectural modules and how they can be integrated into IoT systems of multiple architectural levels. The standard also addresses documentation and mitigation between divergent architectures and includes a methodology centred on data abstraction and the need for trust between entities using appropriate protection, privacy and security mechanisms.

Currently, P2413 also includes the P2413.1 extension as a standard for a Reference Architecture for Smart City (RASC) [31]. The RASC provides an architectural design for the implementation of a smart city in the context of IoT, based on the description of the interactions and interoperability between system domains, including water management, waste, street lighting, smart parking, environmental monitoring, etc. On the other hand, the P2413.2 extension defines a standard for a Reference Architecture for IoT Power Distribution (PDIoT), with a similar approach to the RASC standard, but with a cloud-based orientation and the coexistence of microservices and migration mechanisms from legacy IoT-based systems.

The P2413 standard does not currently define a specific standard for IoMT platform design [28]. In this sense, P2413 briefly outlines a domain focused on health, although it is not developed. According to the standard, the health sector is evolving from a connected health perspective to provide a level of automation, smart health and support networks of autonomous and context-aware intelligent agents. The heterogeneity of connected devices has a significant importance in supporting and assisting patients, such as, for example, persons who self-manage chronic diseases or citizens concerned with improving their lifestyle and behavioural habits. In particular, for this domain, the standard underlines the importance of security, considering confidentiality, integrity and the serious repercussions of possible data breaches and leaks. Finally, the convergence between social networks, smart cities services and IoT platforms are potentially interesting to build digital communities for patients, citizens, community caregivers and health professionals.

2.2. Architectural framework of the IEEE 2413-2019 standard and security-related concerns

The P2413 standard defines an architectural framework in terms of domains, stakeholders and viewpoints, in accordance with the ISO/IEC/IEEE 42010:2011 standard. In this sense, six sections are identified within the architectural framework: i) general information, ii) viewpoints and model kinds, iii) architecture development, iv) rationale for key decisions, v) stakeholders and concerns, and vi) viewpoint catalogue. The last section is the most important and serves as a reference for the adaptation of the standard to IoMT systems. The relationships between each of the parts of the architectural framework are presented in

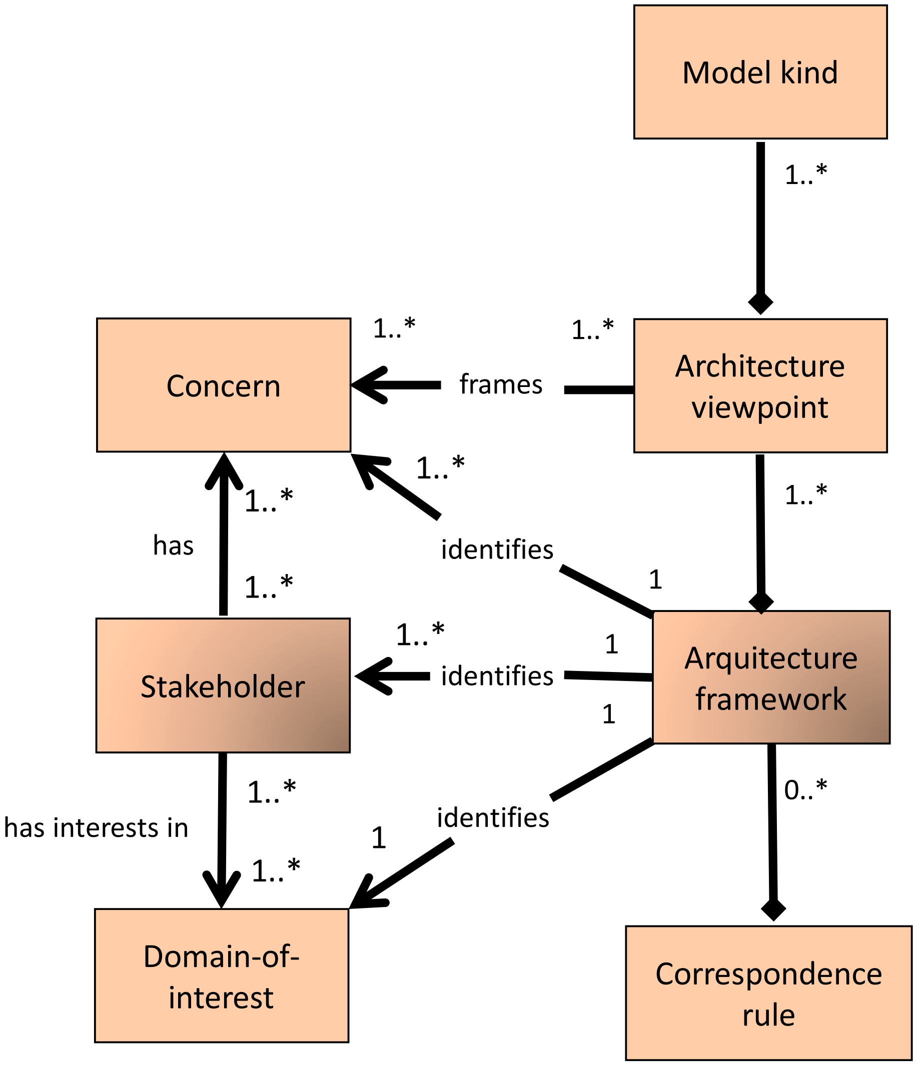

Fig. 1. Conceptual model of an architectural framework of the P2413 standard (based on ISO/IEC/IEEE 42010:2011).

Fig. 1.

As a preliminary step to describe the architectural framework, the standard defines stakeholders and their respective concerns in relation to the system of interest. In particular, stakeholders are individuals or groups of individuals who have common objectives and who identify entities of interest within the system. These stakeholders are modelled through a set of generalised roles defined in the ISO/IEC/IEEE 42010:2011 standard, while concerns are related to stakeholder needs and how the architecture should be adapted to meet them. The list of concerns listed in the standard is based on the Framework for Cyber-Physical Systems [32], developed by the National Institute of Standards and Technology. This standard considers an IoT platform as a set of cyber-physical systems (CPS) that combine networks of sensors and actuators with embedded computing to monitor and control the physical environment.

The identification of stakeholders and concerns guide the identification of the key design points of the IoT system (section 6.6 of the P2413 standard). In this section, different functional and non-functional viewpoints are described in depth. In relation to security, the viewpoints described in the standard are as follows:

- Threat model viewpoint: aims at identifying potential threats or vulnerabilities that could be exploited.
- Security and safety monitoring viewpoint: is the process of monitoring events occurring in an IoT system as analysis for possible incidents, violations or imminent threats.
- Access control viewpoint: determines the activities allowed by legitimate users to access resources in the IoT system.
- Adequate design for required security viewpoint: emphasises the importance of describing the system design from a security view.
- Privacy and trust viewpoint: describes the privacy and trust aspects of IoT architectures.

3. Results

The results of this work are divided into three subsections. Subsection 3.1 identifies the most characteristic stakeholders and concerns in an IoMT environment, considering the P2413 standard. Subsection 3.2 provides a technological description of the use case under study. Finally, subsection 3.3 discusses the application and evaluation of this use case from a security perspective according to the standard.

3.1. Identification of stakeholders and concerns in the IoMT context

The standard establishes, on the one hand, a broad set of stakeholders with logistical and technological profiles and, on the other hand, end-users who shape the functionality of the IoT system and make use of it. In this sense, the number of stakeholders in an IoMT system can be considerable depending on the scope and objectives to be covered [33,34]. The following four stakeholders are considered in this work:

- Users: citizens who use connected biomedical devices to monitor their health periodically or in real time, as part of their maintenance, diagnosis, follow-up or treatment.
- Healthcare professionals: include doctors, nurses, pharmacists, laboratory technicians and others. They are responsible for examining the data collected and establishing high-level operating conditions for biomedical devices.
- Professional and non-professional caregivers: persons who care for a child or a sick, elderly, or disabled person.
- Engineers or technology experts: the standard defines a broad set of profiles related to the technological and architectural aspects of the IoT system, including system administrators, maintainers, production engineers, technical support staff, testers, etc.

On the other hand, the P2413 standard defines an extensive set of concerns to cover a wide range of IoT domains. The most important [27] that may apply to an IoT system from a security perspective are described in Table 1.

The importance of each of these concerns in an IoMT system varies depending on the characteristics of the system and the application context, but generally end-user protection against injury or physical damage is the major concern [35]. Other relevant concerns, which are also highlighted in the P2413 standard within the healthcare domain, are privacy [36] and data breach/leaks [37]. The standard highlights that while all concerns should be considered initially, IoT architects are in charge with delving deeper into those that may have the higher impact on the design and development of their systems. Table 2 presents security-related concerns and possible examples of application in IoMT systems.

Table 1
Security concerns related to the P2413 standard.

Concern	Description
Adaptability	Ability of a CPS to achieve an intended purpose regardless of changing conditions.
Controllability	Ability of a CPS to modify its functionality without impacting the service behaviour or its availability.
Evolvability	Ability of the system to evolve and be functional with new and emerging technologies.
Human factors	Characteristics of an CPS with respect to how they are used by humans.
Identity	Related to the ability of the system to accurately recognise interaction identities.
Maintainability	Capabilities related to the ease and reliability with which a CPS can be kept in operation.
Measurability	Related to the ability to measure the characteristics and performance of a CPS.
Monitorability	Relating to the ease and reliability with which authorised entities can know and maintain knowledge of the status of a CPS.
Physical	Related to the physical environment of a CPS, including perimeter security.
Privacy	Concerns related to the ability to prevent unauthorised access to data in storage or in transit.
Quality	Concerns related to the ease and reliability of assessing whether an CPS meets the expectations of stakeholders.
Regulatory	Related to regulatory requirements and certifications.
Resilience	Related to the ability of a CPS to withstand instability and unexpected system conditions.
Security	Related to the ability to ensure that devices, processes and services are protected internally and/or externally. Includes confidentiality, integrity and availability.
Standardization	Related to the availability and applicability of standards.
Safety	Related to the ability to ensure the absence of catastrophic consequences to the life and health of stakeholders and the physical environment.

Table 2
Security concerns and examples of application in an IoMT system.

Concern	IoMT system application example
Adaptability	Ability of a biomedical sensor to autonomously and remotely update its firmware to correct a security flaw.
Controllability	Ability of a biomedical sensor to adapt in a controlled and safe way to changing environmental situations, user needs or reconfiguration from a remote location.
Evolvability	Ability of the system to introduce a new technological improvement without impacting functionality.
Human factors	Simple and adaptable user interfaces to help simplify the security management process for users with all kinds of capabilities and constraints.
Identity	Strong authentication systems and role-based access control.
Maintainability	Capabilities related to the ease and reliability with which a device can be kept in operation.
Measurability	Concerns related to the ability to measure the characteristics and performance of a biomedical device.
Monitorability	Logging and auditing functionality at all levels of the system for authorised users.
Physical	Mitigation mechanisms for the possible loss or theft of a biomedical device
Privacy	Encryption mechanisms at all levels of the system, including communications and data storage.
Quality	Ability of the system to deliver a quality of service within the minimum required by end-users
Regulatory	Adequacy of the measures necessary to guarantee the right to the protection of personal data.
Resilience	Ability of the system to provide tolerable service to the end-user in the event of system degradation.
Security	Implementation of an Information Security Management System (ISMS) on the basis of protecting all critical information resources in the system.
Standardization	Use of standardised and open communication protocols such as ISO/IEEE 11073 to achieve interoperability between different systems and devices.
Safety	Manuals detailed and adapted to all types of users with regard to the handling of the devices, applications and services.

3.2. Description of the use case

The use case for this work focuses on an IoMT remote monitoring platform for patients suffering from chronic obstructive pulmonary disease [38]. Patients wear a smart vest that monitors their health status and tracks their physical activity under the supervision of healthcare professionals. The system considers the four types of stakeholders already discussed in Section 3.1.

The heterogeneity of scenarios and stakeholders in the proposed platform is in accordance with the many-to-many communication paradigm, where all communicating entities can generate and receive information, under security and privacy conditions. To meet these needs, the standardised MQ Telemetry Transport (MQTT) protocol was integrated into the system to provide communication based on the publisher/subscriber pattern and, at the same time, provide confidentiality, authentication and access control mechanisms.

A simplified diagram of the different scenarios and stakeholders in the platform is shown in Fig. 2. In general, the other stakeholders take a passive action, receiving data from the patient's device and other information based on their need, authorisation and consent from the patient. A more exhaustive description of the platform can be found in previous works by the authors [38].

In order to improve the stability, security and scalability of the system, this work presents the extension of the platform in order to integrate the security aspects included in the P2413 standard. In addition, different software modules are incorporated to cover new functional and non-functional requirements of the end users. These modules are distributed in each of the three architectural levels of the platform, following a classic design for systems of this nature [39]:

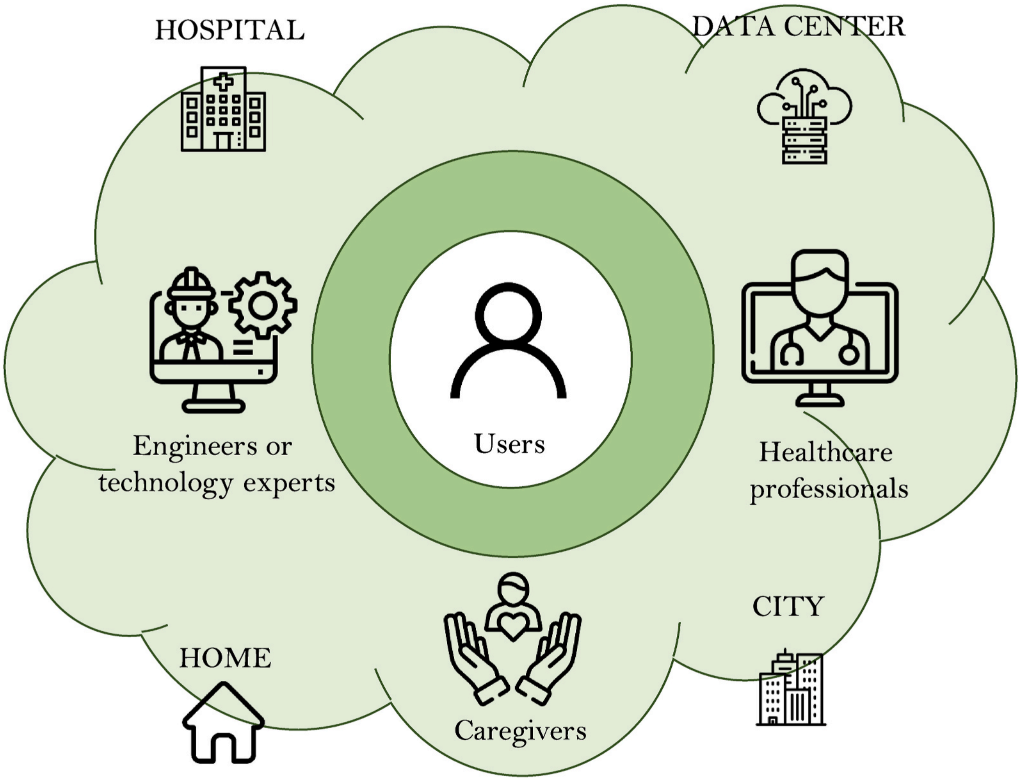

Fig. 2. Diagram of the proposed IoMT platform.

- Device layer: includes the smart vest and embedded software for data collection, pre-processing, basic storage and Bluetooth communications with the edge computing layer.
- Edge computing layer: includes devices whose capabilities vary according to the communication restrictions present in the different scenarios described above, as well as the end-user computing skills and the limitations of the devices. The objective of this layer is optimise the provision of services to the end user without relying on the cloud computing layer. This allows to provide basic offline operation to users without the need to rely on network availability.
- Cloud computing layer: integrates advanced services for storage, search, data mining and knowledge generation.

Fig. 3 presents the architecture of the proposed IoMT platform, evolved with a focus on the capabilities available for each of the different devices framed within the edge computing layer. This includes smartphones, low-end devices, interconnection devices, computers without graphical interfaces and different processing capabilities and, finally, display screens.

The main capabilities present in the devices (communication,

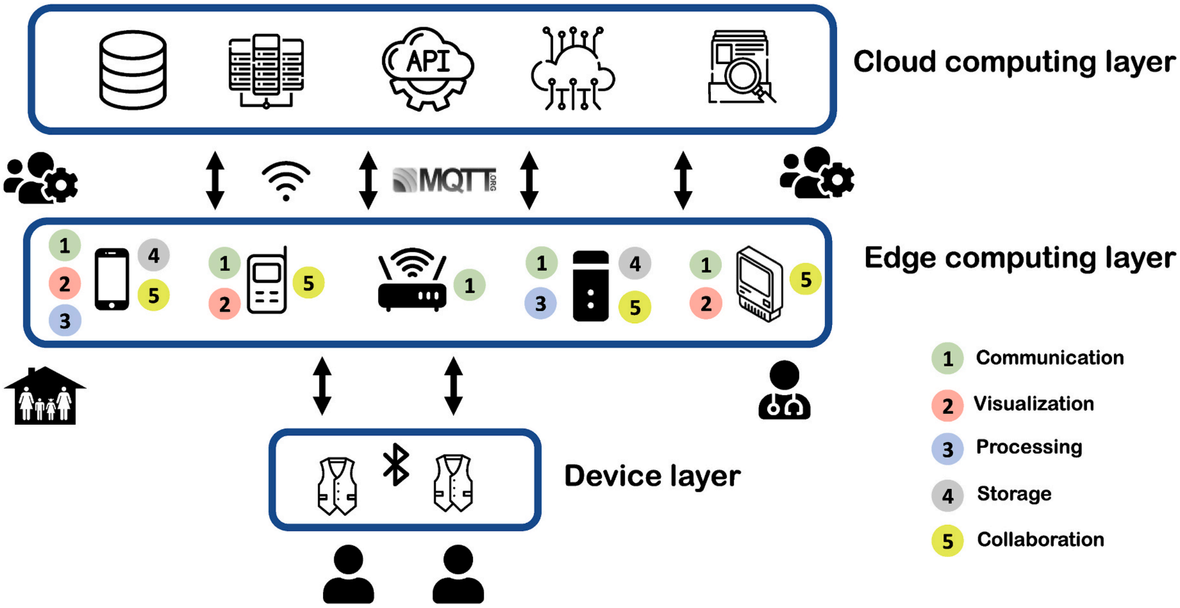

Fig. 3. Layered architecture for the proposed IoMT platform.

visualization, processing and storage) can be shared from a collaborative way. A first approximation to this approach was presented by the authors [40] through the deployment of a peer-to-peer (P2P) network based on Wi-Fi Direct technology, without the need for connection to wireless access points. Similarly, standardised device management and communications in the context of IoMT has also been addressed by the authors and incorporated in the IoMT platform [41], as well as the incorporation of advanced security mechanisms and technical interoperability between different IoT protocols based on the publisher/subscriber pattern [42].

3.3. Application of the security viewpoints of the P2413 standard for the proposed use case

Each viewpoint of the standard contains a number of elements or questions that the IoMT architect must address during system design. In the following subsections these elements are summarised, classified according to the security concerns and applied individually to the use case presented in the previous subsection. In addition, the potential impact associated with each of these issues is also listed based on different constituent entities in most IoMT systems: devices, users, data and security.

3.3.1. Threat model viewpoint

Fig. 4 presents each of the elements of the threat model viewpoint of the P2413 standard. Most of them are focused on identifying potential vulnerabilities that can be exploited by malicious user attacks. Each of these elements is checked in the proposed use case as shown in Table 3, briefly describing the solution adopted in case of compliance or proposed in case of non-compliance. In particular, the use case under study is deployed in a controlled network infrastructure for research purposes, where all end-users are known and trusted. As a consequence, the impact of non-compliance with the elements of this viewpoint is partially mitigated by the difficult access of external agents.

Table 3
Elements, related concerns and solutions adopted or proposed considering threat model viewpoint.

Element	Concern	Compliance	Solution adopted or proposed
1	Controllability	Yes	Documented and tested operational interfaces
2	Safety	Yes	Testing processes to ensure that the smart vest is harmless, non-obtrusive and electrically isolated
3	Privacy	Yes	Personal data of users isolated in an isolated network infrastructure
4	Monitorability	No	Security audit of all system software
5	Physical	Yes	Equipment adequately protected by security perimeters
6	Confidentiality	Yes	Encryption of data storage
7	Integrity	Yes	Principle of least privilege applied to the access of each of the resources available in the system
8	Availability	No	Filtering of suspicious traffic
9	Resilience	No	Periodic security updates
10	Monitorability	Yes	Anonymous identities not allowed
11	Identity	Yes	System access log system

3.3.2. Safety and adequate design for required security viewpoints

The viewpoints of protection and adequacy of security design are unified in this subsection given the similarity between the different elements discussed in both. The elements in this subsection are focused exclusively on the security mechanisms implemented in the system, as presented in Fig. 5. Table 4 shows the application of these elements to the proposed use case.

3.3.3. Access control viewpoint

Access control and security management is addressed in this section of the standard. Fig. 6 presents the different associated elements, focused not only on ensuring the robustness of the access control, but also on providing information and control to the user on the management of his own security considering the operational scope. Table 5 shows the application of the elements of the viewpoint to the proposed use case.

3.3.4. Privacy and trust viewpoint

The last point of the standard that includes security elements is

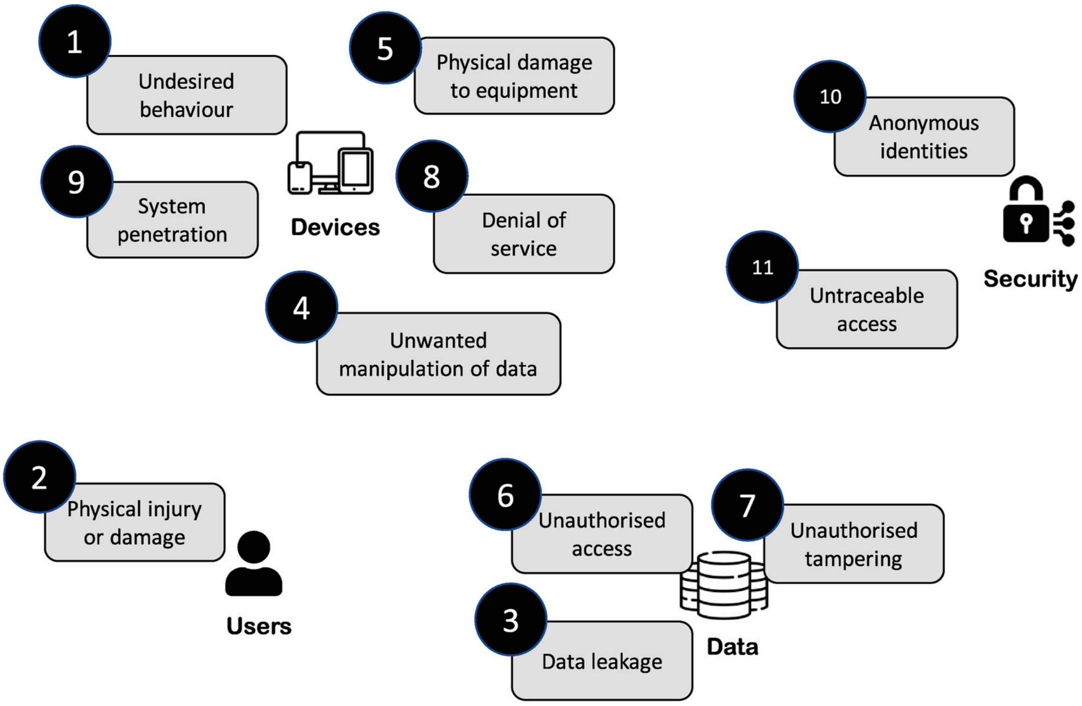

Fig. 4. Elements of each entity considered from the threat model viewpoint.

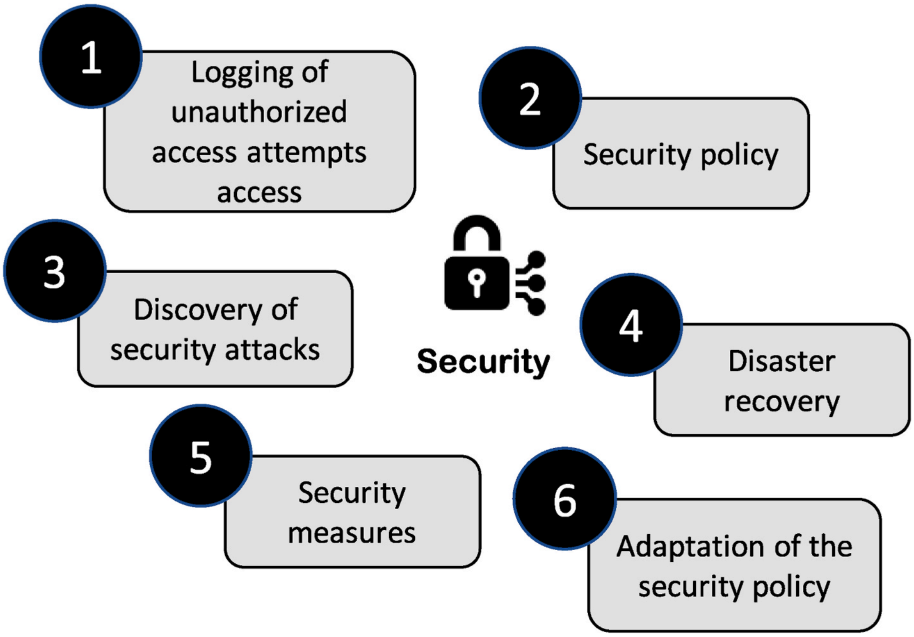
1
Logging of unauthorized access attempts access
2
Security policy
3
Discovery of security attacks
Security
4
Disaster recovery
5
Security measures
6
Adaptation of the security policy

Fig. 5. Elements of each entity considered from the safety and adequate design for required security viewpoints.

Table 4
Elements, related concerns and solutions adopted or proposed considering safety and adequate design for required security viewpoints.

Element	Concern	Compliance	Solution adopted or proposed
1	Monitorability	Yes	Auditing system of all system actions and events
2	Security	No	Security audit of networks and systems
3	Safety	No	Use of a Demilitarised Zone (DMZ)
4	Resilience	Yes	Automated disaster recovery failover based on software containers
5	Measurability	No	Graphical administration interface for security incident monitoring
6	Evolvability	Yes	Automated and properly documented unit tests to check all critical system interfaces and processes

related to privacy and trust. Fig. 7 presents each of them, while Table 6 shows their application to the use case. The concerns column in this table has been omitted given the broad set of concerns for each of the elements in this viewpoint, including privacy, policy, integrity, confidentiality, regulation, discoverability, data relationships and others.

4. Conclusions

The lack of open standards in the context of IoT, and particularly IoMT, is a real and ongoing problem, limiting the mass adoption of such systems. In the field of connected health, the difficulties spread to information and communication security, due the unique characteristics of the healthcare domain and the personal data that is processed.

Table 5
Elements, related concerns and solutions adopted or proposed considering access control viewpoint.

Element	Concern	Compliance	Solution adopted or proposed
1	Adaptability	No	Adapting role-based access control to a context-based approach
2	Maintainability, human factors	Yes	Simple and intuitive graphical user interfaces for security management
3	Security	Yes	Authorisation to resources based on roles and permissions
4	Standardization	Yes	Compliance with data protection national laws and regulations

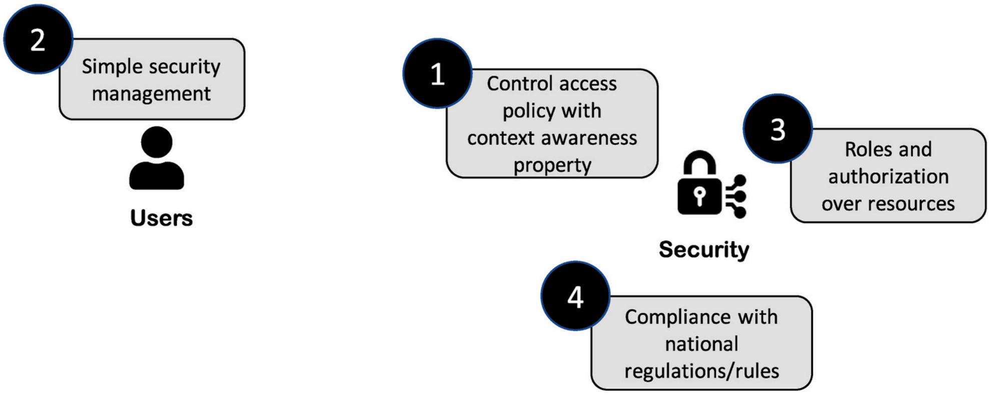
2
Simple security management
Users
1
Control access policy with context awareness property
3
Roles and authorization over resources
Security
4
Compliance with national regulations/rules

Fig. 6. Elements of each entity considered from the access control viewpoint.

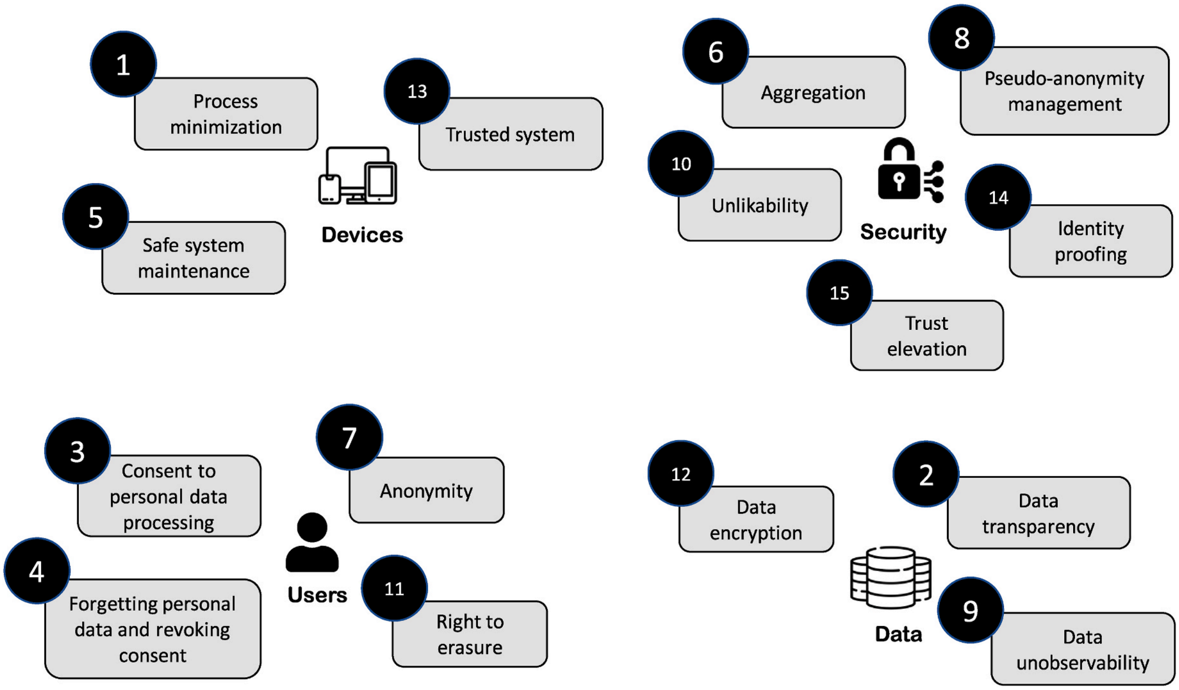

Fig. 7. Elements of each IoMT entity considered from the privacy and trust viewpoint.

Table 6
Elements, related concerns, solutions adopted or proposed considering privacy and trust viewpoint.

Element	Compliance	Solution adopted or proposed
1	Yes	All system processes are restricted to the minimum information and resources necessary for their functional purposes according to the basic principle of minimum exposure.
2	Yes	System access log system
3	Yes	Obligatory declaration of the user's consent to the use of personal data
4	Yes	Easily accessible and user-friendly mechanisms for the right to be forgotten and to revoke consent
5	Yes	Automated checking and testing of system maintenance in a controlled environment
6	No	Use of in-transit data aggregation protocols
7	Yes	Data recognised by unique identifiers that do not reveal information about the target user.
8	Yes	Use of unique identifiers and usernames unrelated to personal information
9	Yes	Use of secure end-to-end communications
10	Yes	Data encryption in communications
11	No	Easily accessible and user-friendly mechanisms for the deletion of their data at all levels of the system
12	Yes	Encryption of data storage
13	No	Surveys to assess user trust in the system
14	Yes	Role-based access control
15	No	Implementation of dynamic and auditable mechanisms for changes in user roles and permissions

The P2413 standard, recently proposed by the IEEE, arises as a result of such challenges. It provides an integrated and extensible architectural framework that is continuously evolving and will unify the effort of creating new extensions to the standard in the context of IoT across different application domains and technologies. The importance of IoMT applications may lead to the harmonisation of such systems with the P2413.1 extension in the context of smart cities.

This work has identified the concerns, viewpoints and elements related to security under the P2413 standard. The standard allows a systematic and efficient approach to the evaluation of security mechanisms for IoMT systems.

Under this perspective, this work has presented the application of P2413 standard from a security perspective in an IoMT system for monitoring chronic patients with chronic obstructive pulmonary. The result revealed that 25 elements out of the 36 raised in the standard were covered satisfactorily. The non-compliance of the elements has been assessed as admissible, considering that the IoMT system presented has been designed, implemented and deployed as a prototype with a certain level of technological maturity (TRL 7), utilizing an isolated network infrastructure, no storage, communication or processing of personal data, and with clearly identified and trusted end-users. At the same time, the steps followed for the adaptation proposed in this work can serve as a guide to address the security aspects of the P2413 standard for IoMT systems already developed or under development.

In summary, the application of the P2413 standard to the IoMT platform for the management of chronic patients with obstructive pulmonary disease has allowed us to identify technical issues at TRL 7 level, regarding the audit and management of the security of the system architecture, shortcomings in the current network topology and complementary security procedures that will be adopted in a TRL 8 version.

Declaration of competing interest

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

Acknowledgements

This work was supported in part by “Fundación Mutua Madrileña” under grant VÍA-RENAL, in part by Fundación Progreso y Salud, Junta de Andalucía, under grant EvaRehaResp (PIN-0394-2017), in part by Consejería de Transformación Económica, Industria, Conocimiento y Universidades, Junta de Andalucía, under grant P18-TPJ-3074, in part by Fundación Mutua Madrileña under grant VIA-RENAL, and in part by Sociedad Española de Diabetes under grant SED-2020.

References

[1] J.N.S. Rubí y, P.R.L. Gondim, IoMT platform for pervasive healthcare data aggregation, processing, and sharing based on OneM2M and OpenEHR, Sensors 19 (19) (oct. 2019) E4283, https://doi.org/10.3390/s19194283.

[2] N.S. Abul-Husn y, E.E. Kenny, Personalized medicine and the power of electronic health records, Cell 177 (1) (mar. 2019) 58–69, https://doi.org/10.1016/j.cell.2019.02.039.

[3] W. Jiang, B. Han, M.A. Habibi, y H.D. Schotten, The road towards 6G: a comprehensive survey, IEEE Open J. Commun. Soc. 2 (2021) 334–366, https://doi.org/10.1109/OJCOMS.2021.3057679.

[4] A. Al-Ansi, A.M. Al-Ansi, A. Muthanna, I.A. Elgendy, y A. Koucheryavy, Survey on intelligence edge computing in 6G: characteristics, challenges, potential use cases, and market drivers, Future Internet 13 (5) (may 2021), https://doi.org/10.3390/fi13050118. Art. n.º 5.

[5] M.A. Khan y, F. Algarni, A healthcare monitoring system for the diagnosis of heart disease in the IoMT cloud environment using MSSO-ANFIS, IEEE Access 8 (2020) 122259–122269, https://doi.org/10.1109/ACCESS.2020.3006424.

[6] G. Villarrubia, J. Bajo, J.F. De Paz, y J.M. Corchado, Monitoring and detection platform to prevent anomalous situations in home care, Sensors 14 (6) (jun. 2014) 9900–9921, https://doi.org/10.3390/s140609900.

[7] Z.Y. Huang, Y. Wang, y L. Wang, ISO/IEEE 11073 treadmill interoperability framework and its test method: design and implementation, JMIR Med. Inform. 8 (12) (dic. 2020), e22000, https://doi.org/10.2196/22000.

[8] J. Calvillo-Arbizu, I. Román-Martínez, y J. Reina-Tosina, Internet of things in health: requirements, issues, and gaps, Comput. Methods Progr. Biomed. 208 (sep. 2021), 106231, https://doi.org/10.1016/j.cmpb.2021.106231.

[9] S. Bharati, P. Podder, M.R.H. Mondal, y P.K. Paul, in: A.E. Hassanien, A. Khamparia, D. Gupta, K. Shankar, y A. Slowik (Eds.), Applications and Challenges of Cloud Integrated IoMT», en *Cognitive Internet of Medical Things for Smart Healthcare: Services and Applications*, Springer International Publishing, Cham, 2021, pp. 67–85, https://doi.org/10.1007/978-3-030-55833-8_4.

[10] L.J.R. Lopez, G.P. Aponte, y A.R. Garcia, Internet of things applied in healthcare based on open hardware with low-energy consumption, Healthc Inform. Res. 25 (3) (jul. 2019) 230–235, https://doi.org/10.4258/hir.2019.25.3.230.

[11] N. Yadav, Y. Jin, y L.J. Stevano, AR-IoMT mental health rehabilitation applications for smart cities, in: en 2019 IEEE 16th International Conference on Smart Cities: Improving Quality of Life Using ICT IoT and AI (HONET-ICT), oct. 2019, pp. 166–170, https://doi.org/10.1109/HONET.2019.8907997.

[12] A. Adarsha, K. Reader, y S. Erban, User experience, IoMT, and healthcare, AIS Trans. Hum.-Comput. Interact. 11 (4) (dic. 2019) 264–273, https://doi.org/10.17705/1thci.00125.

[13] H. Zhang, J. Li, B. Wen, Y. Xun, y J. Liu, Connecting intelligent things in smart hospitals using NB-IoT, IEEE Internet Things J. 5 (3) (jun. 2018) 1550–1560, https://doi.org/10.1109/JIOT.2018.2792423.

[14] R. Cao, Z. Tang, C. Liu, y B. Veeravalli, A scalable multicloud storage architecture for cloud-supported medical Internet of things, IEEE Internet Things J. 7 (3) (mar. 2020) 1641–1654, https://doi.org/10.1109/JIOT.2019.2946296.

[15] I. Tanseer, N. Kanwal, M.N. Asghar, A. Iqbal, F. Tanseer, y M. Fleury, Real-time, content-based communication load reduction in the Internet of multimedia things, Appl. Sci. 10 (3) (2020), https://doi.org/10.3390/app10031152. Art. n.º 3, ene.

[16] J. Silvestre-Blanes, V. Sempere-Payá, y T. Albero-Albero, Smart sensor architectures for multimedia sensing in IoMT, Sensors 20 (5) (2020), https://doi.org/10.3390/s20051400. Art. n.º 5, ene.

[17] K.K. Karmakar, V. Varadharajan, U. Tupakula, S. Nepal, y C. Thapa, Towards a security enhanced virtualised network infrastructure for Internet of medical things (IoMT), in: en 2020 6th IEEE Conference on Network Softwarization (NetSoft), jun. 2020, pp. 257–261, https://doi.org/10.1109/NetSoft48620.2020.9165387.

[18] G. Xu, et al., An IoT-based framework of Webvr visualization for medical big data in connected health, IEEE Access 7 (2019) 173866–173874, https://doi.org/10.1109/ACCESS.2019.2957149.

[19] C. Liu, F. Chen, C. Zhao, T. Wang, C. Zhang, y Z. Zhang, IPv6-Based architecture of community medical Internet of things, IEEE Access 6 (2018) 7897–7910, https://doi.org/10.1109/ACCESS.2018.2801563.

[20] S. Razdan y S. Sharma, Internet of medical things (IoMT): overview, emerging technologies, and case studies, IETE Tech. Rev. (may 2021) 1–14, https://doi.org/10.1080/02564602.2021.1927863, 0, 0.

[21] M. Papaioannou, et al., A survey on security threats and countermeasures in Internet of medical things (IoMT), Trans. Emerg. Telecommun. Technol. (2021) e4049, https://doi.org/10.1002/ett.4049, n/a, n.º n/a.

[22] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, y C. Tsatsoulis, Review of security and privacy for the Internet of medical things (IoMT), in: en 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), may 2019, pp. 457–464, https://doi.org/10.1109/DCOSS.2019.00091.

[23] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, y R. Jain, Recent advances in the internet-of-medical-things (IoMT) systems security, IEEE Internet Things J. (2021), https://doi.org/10.1109/JIOT.2020.3045653.

[24] L. Wang, Y. Ali, S. Nazir, y M. Niazi, ISA evaluation framework for security of Internet of health things system using AHP-TOPSIS methods, IEEE Access 8 (2020) 152316–152332, https://doi.org/10.1109/ACCESS.2020.3017221.

[25] Md A. Uddin, A. Stranieri, I. Gondal, y V. Balasubramanian, Continuous patient monitoring with a patient centric agent: a block Architecture, IEEE Access 6 (2018) 32700–32726, https://doi.org/10.1109/ACCESS.2018.2846779.

[26] R.M. Aileni y, G. Suciu, in: M.A. Khan, M.T. Quasim, F. Algarni, y A. Alharthi (Eds.), «IoMT: A Blockchain Perspective», en *Decentralised Internet of Things: A Blockchain Perspective*, Springer International Publishing, Cham, 2020, pp. 199–215, https://doi.org/10.1007/978-3-030-38677-1_9.

[27] IEEE 2413-2019 - IEEE standard for an architectural framework for the Internet of things (IoT). https://standards.ieee.org/standard/2413-2019.html, 2019. (Accessed 16 July 2021).

[28] A.H. Mohd Aman, W.H. Hassan, S. Sameen, Z.S. Attarbashi, M. Alizadeh, y L. A. Latiff, IoMT amid COVID-19 pandemic: application, architecture, technology, and security, J. Netw. Comput. Appl. 174 (2021), 102886, https://doi.org/10.1016/j.jnca.2020.102886 ene.

[29] D.T. Parra y, C.D. Guerrero, Technological variables for decision-making IoT adoption in small and medium enterprises, J. Inform. Syst. Eng. 5 (4) (2020), em0124, https://doi.org/10.29333/jisem/8484 ago.

[30] T. Lynn, P.T. Endo, A.M.N.C. Ribeiro, G.B.N. Barbosa, y P. Rosati, in: T. Lynn, J. G. Mooney, B. Lee, y P.T. Endo (Eds.), «The Internet of Things: Definitions, Key Concepts, and Reference Architectures», en *The Cloud-to-Thing Continuum: Opportunities and Challenges in Cloud, Fog and Edge Computing*, Springer International Publishing, Cham, 2020, pp. 1–22, https://doi.org/10.1007/978-3-030-41110-7_1.

[31] E. Bernardi, M.Y. Miyake, A.S. dos Santos, M.P. Merichelli, M.J. Pereira, y M. Polkorny, Brazilian scenarios for smart cities deployment from public policies perspectives, in: en 2020 IEEE International Smart Cities Conference (ISC2), sep. 2020, pp. 1–8, https://doi.org/10.1109/ISC251055.2020.9239096.

[32] E.R. Griffor, C. Greer, D.A. Wollman, y M.J. Burns, «Framework for Cyber-Physical Systems:, vol. 1, Overview», jun. 2017. Accedido: jul. 16, 2021. [En línea]. Disponible en: https://www.nist.gov/publications/framework-cyber-physical-systems-volume-1-overview.

[33] F. Alsubaei, A. Abuhussein, V. Shandilya, y S. Shiva, IoMT-SAF: internet of medical things security assessment framework, Internet of Things 8 (2019), 100123, https://doi.org/10.1016/j.iot.2019.100123 dic.

[34] R.M. Swarna Priya, et al., An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture, Comput. Commun. 160 (jul. 2020) 139–149, https://doi.org/10.1016/j.comcom.2020.05.048.

[35] Y.B. Zikria, M.K. Afzal, y S.W. Kim, Internet of multimedia things (IoMT): opportunities, challenges and solutions, Sensors 20 (8) (2020), https://doi.org/10.3390/s20082334. Art. n.º 8, ene.

[36] L. Tawalbeh, F. Muheidat, M. Tawalbeh, y M. Quwaider, IoT privacy and security: challenges and solutions, Appl. Sci. 10 (12) (2020), https://doi.org/10.3390/app10124102. Art. n.º 12, ene.

[37] A. Sobecki, J. Szymański, D. Gil, y H. Mora, Framework for integration decentralized and untrusted multi-vendor IoMT environments, IEEE Access 8 (2020) 108102–108112, https://doi.org/10.1109/ACCESS.2020.3000636.

[38] D. Naranjo Hernández, et al., Smart vest for respiratory rate monitoring of COPD patients based on non-contact capacitive sensing, 2018, https://doi.org/10.3390/s18072144.

[39] M.A. Jabraeil Jamali, B. Bahrami, A. Heidari, P. Allahverdizadeh, y F. Norouzi, in: M.A. Jabraeil Jamali, B. Bahrami, A. Heidari, P. Allahverdizadeh, y F. Norouzi (Eds.), «IoT Architecture», en *Towards the Internet of Things: Architectures, Security, and Applications*, Springer International Publishing, Cham, 2020, pp. 9–31, https://doi.org/10.1007/978-3-030-18468-1_2.

[40] A. Talaminos, J. Reina-Tosina, y L.M. Roa-Romero, Sistema IoMT para la comunicación distribuida y descentralizada de sensores en redes de área personal, 2019. Sevilla.

[41] A. Talaminos, D. Naranjo, G. Barbarov, L.M. Roa, y J. Reina-Tosina, Design and implementation of a standardised framework for the management of a wireless body network in an Mobile Health environment, Healthc. Technol. Lett. 4 (3) (2017) 88–92, https://doi.org/10.1049/htl.2016.0101.

[42] A. Talaminos, J. Reina-Tosina, y L.M. Roa-Romero, Interceptor-Pattern-Based Middleware for IoT Protocol Interoperability», en *IoT and Cloud Computing for Societal Good*, Springer International Publishing, 2022, https://doi.org/10.1007/978-3-030-73885-3.