Model for Implementing a IoMT Architecture with ISO/IEC 27001 Security Controls for Remote Patient Monitoring

Brandon Alegría
Universidad Peruana de Ciencias Aplicadas
Lima, Perú
brandonalegriavivanco1998@gmail.com

Lenis Wong
Universidad Peruana de Ciencias Aplicadas
Lima, Perú
lwongpuni@gmail.com

Diego Bedriñana
Universidad Peruana de Ciencias Aplicadas
Lima, Perú
diego.bedrinana.910@gmail.com

***Abstract*—Due to the recent pandemic, the healthcare sector has been forced to incorporate new technologies into its systems, such as IoT and Fog Computing. However, being new technologies, they are prone to security breaches. From this context, it is identified that medical systems do not have a sufficient level of security, due to the use of new technologies such as IoT and the lack of controls to protect these new technologies. Therefore, a model for implementing an Internet of Medical Things (IoMT) Architecture with ISO/IEC 27001 security controls for remote patient monitoring is proposed. This model has 4 stages: Stage 1 selects an information security standard for the healthcare sector. Stage 2 selects the information security controls of the selected standard. Stage 3 selects and evaluates an IoMT architecture applicable to the healthcare sector. And Stage 4 designs the information security controls for each layer of the IoMT architecture. The IoMT architecture and information security controls are simulated and experimented with physicians (the productivity of the system) and with information security expert (the quality of the implemented controls). The results of the first experiment show that "effectiveness", "productivity", and "satisfaction" regarding the use of the IoMT architecture have an average rating of 4.05 (high level). The results of the second experiment show that "Information Security", "Awareness" and "Security Incident Management" regarding the quality of the security controls implemented have an average rating of 3.65 (high level).**

I. Introduction

The medical industry has developed and evolved in terms of technology in recent years [1]. The Covid-19 pandemic was an important factor for the technological advancement of the medical sector, since complex systems were developed that were accompanied with Internet of Things (*IoT*), for an improvement in medical care, as these new technologies allowed to improve the processes of monitoring, treatment and diagnosis of diseases [2]. However, due to this complexity and new emerging technologies, it is expected that cyber-attacks on this sector will also be on the rise [3].

The main problem afflicting the health sector is the modern technologies acquired and their ineffective security controls. Where its main causes are (i) *IoMT* environments have become more complex, while information security solutions have lagged behind [4]. (ii) The significant increase in cyber-attacks on the healthcare sector has led to the discovery of security breaches and new vulnerabilities in *IoMT* devices [5] and (iii) The human factor that works with clinical data and people in general has little knowledge of information security, making them more prone to be victims of cyber-attacks [6].

According to statistics, in the first quartile of the year 2020, at the beginning of the pandemic, cyberattacks on the health sector were in third place [7] , a big difference is seen in the first quartile of the year 2021, where it is the most attacked sector [8] and which is repeated in the year 2022 [9].

The increase in cyberattacks on hospitals, is a major risk, since it not only puts at risk and danger the critical infrastructure of a country, but also the private information of patients and even their lives.

Therefore, several studies have emerged that provide different positions and techniques on how to address these security problems in medical systems such as risk analysis in *IoMT* systems [10] and the minimum security requirements that *IoMT* should have [11], thus avoiding known malware attacks. However, these only focus on the protection of some systems and devices, leaving aside the human factor that are the ones that manage these technologies.

For this reason, this paper proposes a security model for remote patient monitoring, based on an *IoMT* architecture that covers the need to secure the information obtained from patients' *IoMT* devices, applying ISO 27001 security controls. These controls focus on 14 control areas, such as: Awareness for people using *IoMT* and medical systems, *IoMT* Asset Management, Incident Management, Secure Media Reuse and Destruction, and Physical and Environmental Security. In this way, using the best security practices to maintain the security level of systems, devices and people at an acceptable level and avoid security incidents.

This paper is organized as follows: Section 2 presents related works. Section 3 describes the model. Section 4 presents the experiments. Finally, section 5 presents the results, conclusions, and future works.

II. Related Works

For the analysis of the related works, a review of the literature is conducted, considering the following phases [12]: Planning, development and analysis. In the planning phase, the research categories are defined, which are translated into 3 key questions: (Q1) What security problems do *IoMT* and its associated technologies present? (Q2) What technologies make up *IoMT* and *IoMT* architectures? And finally (Q3) What security measures or proposals currently exist for *IoMT* and *IoMT* architectures?

The following keywords are defined: "IoT", "IoMT", "Health", "Architecture", "Design", "Security" and "Secure". The scientific database engines selected for the search of scientific articles are: ElSevier and Scopus. All articles that are considered for the research are from journals published after 2017. In the development phase, articles related to the categories that answered the questions posed in the previous phase are obtained (Table I).

TABLE I. Table of articles found for the research questions

Category	References
Problems (Q1)	[13][14][15][16][17] [18][19][20] [21][22]
Technologies (Q2)	[23][24][25][26][27][28][29] [30] [31] [32]
Security measures (Q3)	[10][33][11][34][35][36][37][38][39][40]

Regarding the "Problems" category, in [16], [17], [18], [19], the authors focus on disclosing and defining the types of *attacks on the layers of IoMT architectures*. However, they do not specify the types of attacks to which *IoMT* architectures are exposed like the author in [13]. Unlike them, in [22], the author focuses on vulnerabilities, not by layers, but by type of attack, where he talks about *information, host and network attacks*. In [20], the author categorizes *IoMT* attacks according to The Open Web Application Security Project (OWASP) [41]. On the other hand, in [21], the authors disclose the network attacks to which *IoMT* is exposed. Likewise, there is [15], where the author categorizes vulnerabilities and attacks in *hardware, social engineering, legislation, Denial of Service (DoS) and lack of user awareness*. Finally, in [14], the author focuses on the *human factor* as the weakest link in any system, which allows to have a new point of view about the weaknesses or vulnerabilities in the systems.

On the other hand, in the "Technologies" category, in [23], [26], [30] and [28], the authors explain *Fog* and *Edge Computing*, and propose an *IoMT* architecture using these technologies. Unlike [27], where the author proposes an architecture for *IoMT* using *Fog* and *Cloud Computing*. In [24], the author explains the technologies that can work together with *IoMT*, having *Cloud Computing*, *Artificial Intelligence* and *Big Data* as the main ones. In [32], the author focuses on the use of *IoMT sensors*, for the diagnosis of Covid19. On the other hand, in [25], the author explains technologies associated with an *IoMT* architecture based on the P2413.1 RASC standard. Another *IoMT* architecture proposed, is found in [29], where the author uses *Cloud Computing* and *Gateways*, in order to increase the security of the architecture. Lastly, in [31], the author analyzes and compares the security and components of three *IoMT* architectures.

Finally, in the category "Security measures". In [10], the author presents a cybersecurity model, combining the best practices of *NIST*, *ISO* and *OWASP*, with *risk analysis* as the main attraction. Similarly, in [36], the author proposes *13 security and privacy principles* that could mitigate existing *IoMT* attacks. In [33], the author, unlike the other authors, proposes security measures not only for systems in use, but also for systems that are being prepared for use and those that are no longer in use. On the other hand, in [39], the author focuses on hardening the security of *IoMT* communications, using *Fri-Jam*. In [11], the author proposes requirements and security measures that *IoMT* should have such as *IDS*, *Access Control* and *authentication*. Regarding the layers of the *IoMT* architecture, in [34] and [35], the authors propose security measures against attacks in each layer of the *IoMT* architecture, and unlike these, in [37], the author also sees the physical and environmental aspect as vulnerabilities and proposes solutions to these. In the use of *Fog Computing* as a security measure, there is [40], where the author uses this technology and explains what security measures can be added to it, to harden the security of the *IoMT* architecture, however, in [38], the author also proposes technologies such as *Edge Computing*, *Blockchain* and *machine learning* as measures to secure *IoMT*.

III. Proposed Model

This section presents the proposed security model for remote patient monitoring, based on an *IoMT* architecture that covers the need to secure the information obtained by *IoMT* devices from patients, applying security controls. This proposal is divided into 4 phases: (a) Selection of an information security standard that applies to the medical sector, (b) Selection of security controls from the chosen framework, applicable to the proposed model, (c) Selection and evaluation of the selected *IoMT* architecture and, (d) Design of information security controls according to the vulnerabilities found in the layers and technologies associated with the proposed *IoMT* architecture.

A. Security Framework selection

It is concluded after analyzing the information security frameworks that there is not much difference between them. The controls and good practices they handle are similar and both have the same purpose, which is to maintain information security. For this reason, it is determined that the only discriminating factor for choosing one of them is their compatibility with information security frameworks for the health sector.

After performing the analysis and benchmarking of the two information security frameworks (see Table II), it is observed that both met all the criteria; however, ISO 27001 is chosen because it is a direct family of ISO 27799 [42], which is an ISO that provides best practices for maintaining information security at an acceptable level and is specific to the health sector, unlike NIST, which also has a program for the health sector but is not as specific in its controls [43]. For this reason, ISO 27001 offers us adequate compatibility and integration

with the policies and controls that are planned to be used within the model to be carried out, so ISO 27001 is the appropriate Information Security framework to continue with the research.

TABLE II. COMPARATIVE TABLE BETWEEN INFORMATION SECURITY FRAMEWORKS

Category	ISO 27001	NIST
Risk Analysis	Yes	Yes
Safe device preparation and disposal	Yes	Yes
Communications security	Yes	Yes
Access control and authentication	Yes	Yes
Physical and environmental security	Yes	Yes
Functional for the healthcare sector	Yes	Yes
Compatibility with healthcare security frameworks	Yes	Regular

B. Selection of security controls

After choosing the ISO 27001 security framework, an analysis of its 114 controls is carried out, from which 24 controls are chosen, which should be specific to the research and proposed model (see Table III). These controls are sent to a security expert, who is in charge of reviewing and providing his judgment as an expert in ISO 27001.

TABLE III. ISO 27001 CONTROLS SPECIFIC TO THE PROPOSED MODEL

Category		Control	
CA1	Information Security	C01 C02 C03 C04 C05 C06	Mobile Device Policy Asset Ownership Proper use of assets Return of assets Transfer of physical media Use of Secret Authentication Information
CA2	Awareness	C07 C06	Information security awareness, education, and training Use of secret authentication information
CA3	Asset Management	C08 C02 C03 C04 C05 C09	Asset inventory Asset ownership Proper use of assets Return of assets Transfer of physical media Disposal or reuse of equipment
CA4	Access control and authentication	C10 C11	Access control policy Access to networks and network services
CA5	Secure password	C12 C13	Secure login procedures Password management system
CA6	Environmental and physical security	C14 C15 C16 C17 C18	Off-site equipment security Information security continuity planning Information security continuity implementation Verification, review, and assessment of information security continuity Data processing center availability
CA7	Security Incident Management	C19 C20	Controls against malicious software Technical vulnerability management
CA8	Operations Security	C21 C22	Event logging Protection of log information
CA9	Network services management	C23	Network services security
CA10	Procurement and development	C24	Application transaction protection

C. IoMT architecture evaluation

1) Selection of IoMT architecture and technologies: The architectures selected for the analysis are those of the authors [25], [23] and [11], as shown in Table IV.

The first architecture to evaluate is raised in [25], where the author proposes an architecture based on the IEEE 2413-2019 standard, which is an architecture standard for *IoMT*, focused on interoperability of systems [44], which has 4 layers: (i) Device Layer, where sensors such as cameras and thermometers are located, (ii) Communication Network Layer, where communication protocols such as 5G and Bluetooth are located, (iii) Platform Layer where technologies such as Cloud Computing and middleware such as Fog Computing are located and (iv) Application Layer, where devices such as monitoring and telemedicine systems are located.

The second architecture to evaluate is proposed in [23], where the author proposes different architectures, where the most striking and functional for the research, consists of 5 layers: (i) Physical, where the sensors are located, (ii) Edge Layer, where the information from the sensors is received and functions as Gateway, (iii) Fog Layer that is responsible for pre-processing the information sent by Edge Layer, (iv) Cloud Layer that stores and process information sent by Fog and (v) Application Layer where user information is displayed.

The third architecture to evaluate is proposed by [11] and [45], where the authors propose an architecture with 3 layers: (i) Device Layer where the sensors are located, (ii) Fog Layer where the Fog nodes are located and (iii) Cloud Layer where the servers that store and analyze the information are located.

To perform the benchmarking, a comparative analysis is performed (see Table IV). The result of this analysis is that Architecture 1, presented in [25], is based on an IoMT architecture standard (IEEE 2413-2019), and this makes it easy to integrate with other current technologies or components, unlike the other two architectures that are not based on any architectural standard. For this reason, Architecture 1 is chosen as the model architecture for further research.

TABLE IV. IOMT ARCHITECTURES COMPARISON TABLE

Quality	Architecture 1 [25]	Architecture 2 [23]	Architecture 3 [11] and [45]
Fog Computing	Yes	Yes	Yes
Edge Computing	Yes	Yes	No
Scalable	Yes	Yes	Yes
Functional for the healthcare sector	Yes	Yes	Yes
Compatibility with technologies used in the health sector	Yes	Regular	Regular
Under IEEE 2413-2019 standard	Yes	No	No

2) Architecture Tradeoff Analysis Method (ATAM): This method [46] is used to evaluate the IoMT architecture [25] selected in the previous step. The main purpose of performing this analysis is to obtain the risks, sensitivity points and tradeoffs, obtained from the architectural decisions taken. In

this way, it is possible to focus information security controls on the weak points of the selected architecture and significantly improve its security. The phases used for the analysis are the following: (i) Presentation, where the business and architecture objectives are presented, (ii) Research and analysis where architectural approaches are identified, the tree of utility attributes, scenarios, and their risks, sensitivity points and tradeoffs are obtained, (iii) Testing in which the scenarios are prioritized and validates that the architecture complies with quality attributes and (iv) Report where the results obtained are presented.

First phase. The main result is that the proposed architecture would be the one chosen in the previous point, and the business objectives would be five: (i) Security, to maintain the integrity, confidentiality and availability of the information, (ii) Availability, so that the information is accessible whenever required, (iii) Performance, to provide quick responses and decision making, (iv) Interoperability, so that the systems can be easily integrated, and (v) Scalability, so that in the future it can go from remote monitoring to intensive care monitoring.

Second phase. The main result is the architectural approach, i.e., the technologies that the selected architecture has. This architecture has 4 layers and their respective technologies (Table V).

TABLE V. PROPOSED IOMT ARCHITECTURE LAYERS AND TECHNOLOGY

Layer	Technology		Description
Application	T6	Browsers	Allows viewing of medical system information
Platform	T5	Cloud - Medical system	Stores and monitors patient information to be displayed
	T4	Fog	Processes data from the Edge, and decides if the physician should be notified of an emergency
	T3	Edge	Validates data received from sensors
Communication	T2	Bluetooth (Simulated)	Sends captured data to Edge (App)
Device	T1	Sensor IoMT (Simulated)	Captures patient data (App)

The utility tree [46] is also performed (see Table VI). This table shows the columns of (i) Quality attributes, which are obtained according to the research objectives and the sector for which the *IoMT* architecture is proposed, (ii) Tactics, which refers to the tactics that are used to ensure compliance with the quality attribute, (iii) Description, which allows a better understanding of what the system is expected to accomplish, according to the quality attributes, and (iv) Solution, which are the security controls that are used to comply with the quality attributes, which go hand in hand with the tactics to be used.

Third phase. After analyzing whether the proposed architecture satisfies the quality attributes, the main result is that it satisfies both security and interoperability; however, in terms of availability and performance, tactics must be applied to achieve compliance with the quality attributes (see Table VII).

TABLE VI. PROPOSED IOMT ARCHITECTURE UTILITY TREE

Quality Attribute	Tactic	System capacity	Solution
Security	Information integrity	Do not allow patient information or transactions to be modified by third parties, in transmission or storage	Controls related to access management and encryption of information in storage and transmission
	Confidentiality of information	Do not allow patient information to be accessed by unauthorized persons	
Availability	Recover from failures	Send requests to a replica server when it detects that the main server is down	Implementation of a replica server, which should have similar characteristics to the main server, and should take requests if another one goes down
Interoperability	System integration	Integrate with other systems that comply with the same architectural development standard	Implementation of technologies under development frameworks or standards
Performance	Load Balancing	Load balancing in case one of your systems has many requests	Employ a replica server, which are able to receive requests and avoid overloading

TABLE VII. ANALYSIS OF ARCHITECTURAL APPROACH ACCORDING TO PROPOSED ARCHITECTURE

Attribute	Does it satisfy?	How does it satisfy?	How will it be satisfied?
Security	Yes	Fog and Edge Computing, will have their security layer, access validation and authorization, on the other hand, will help the processing and transmitted data not to go directly to the datacenter, but in the intermediate nodes, making the information more private and secure	-
Availability	No	-	A Fog node or backup systems should be implemented for business continuity
Interoperability	Yes	The Fog nodes consume the services provided by the hospital's datacenter, thus enabling the hospital to augment the IoMT Architecture as an additional module	-
Performance	No	-	Fog nodes or extra systems should be implemented so as not to saturate the nodes and achieve acceptable and optimal performance

Fourth phase. Finally, it is concluded that the proposed architecture does meet several quality attributes, so it serves to continue the research (see Fig. 1), where the 4 layers of the architecture with their respective technologies are observed.

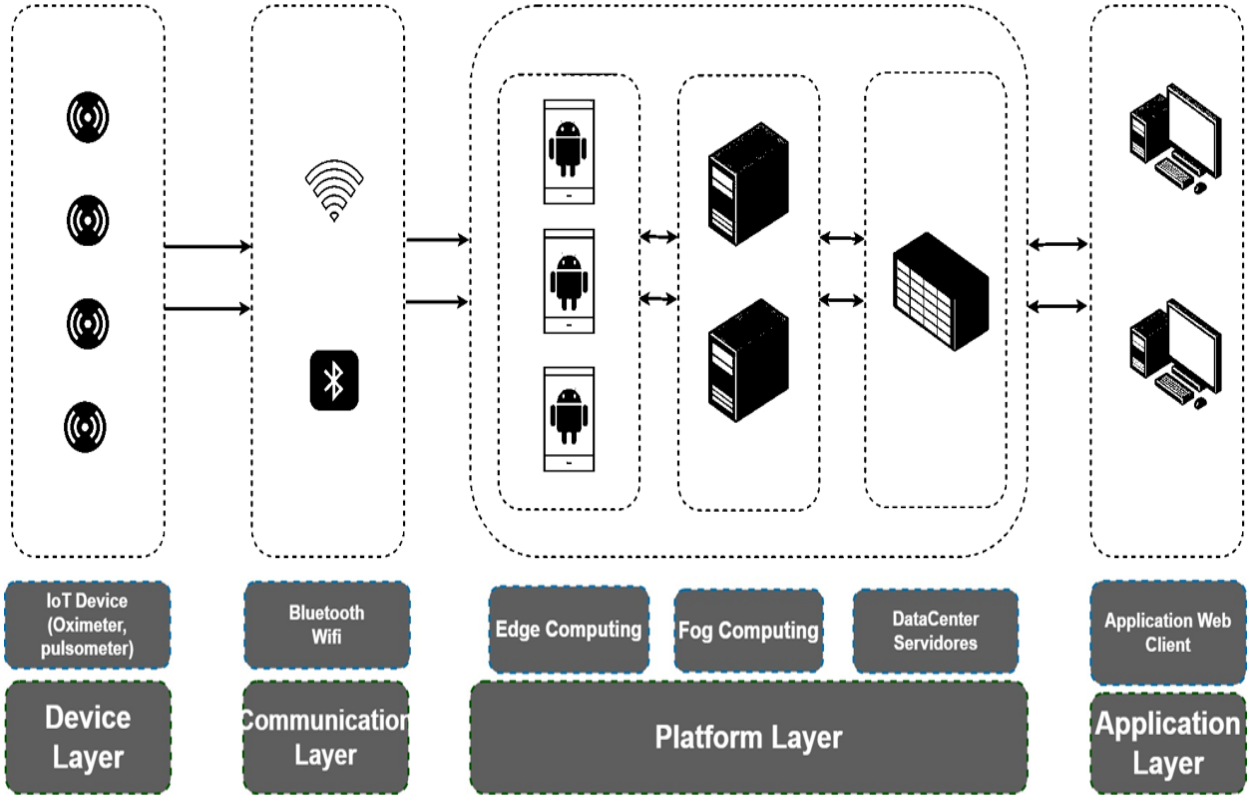

Fig. 1. Proposed IoMT architecture based on Architecture 1

On the other hand, risks, sensitivity points and tradeoffs are also obtained (see Table VIII). The table contains the following columns: (i) Scenario, explains a possible scenario related to a quality attribute, where there is a stimulus or an action by a user that affects a system, which provides a response to the stimulus, (ii) Risk, are the risks associated with the stimulus obtained in the scenario, (iii) Sensitivity points, are architectural decisions that affect a quality attribute and (iv) Tradeoffs, are architectural decisions that affect 2 or more quality attributes.

D. Design of security controls for IoMT architecture

1) Review of common IoMT vulnerabilities and attacks: At this point, it is reviewed the most common vulnerabilities and attacks within IoMT architectures and their associated technologies, which are found in the first category of related works (see Table IX).

2) Categorization of vulnerabilities by IoMT architecture layer: At this point, the vulnerabilities defined in the previous point are categorized and linked to the layers of the proposed *IoMT* architecture. Table X shows a mapping of possible vulnerabilities or attacks in each layer. For example, the Application and Platform (Edge) layers are vulnerable to "Trojan" attacks.

TABLE VIII. SCENARIO, RISKS, SENSITIVITY POINTS AND TRADEOFFS

Scenario	Risk	Architectural decision
Security: A patient or physician logs into the smartphone app to collect and send the data collected from the sensors to the medical systems.	In case the data is not encrypted, and intercepted, confidential information may be accessed	- Sensitivity Point: Unencrypted Data Affects Security - Encrypted data affects performance
Availability: The Fog node or main hospital system is down due to a failure.	If any of the servers go down, it would count as a risk if a contingency or replacement server is not available	Tradeoff: Server downtime directly influences System Availability and Performance
Interoperability: The Fog nodes try to send and consume the services of the hospital's native systems in order to store the information.	Lack of interoperability between Fog nodes and the native system	Sensitivity Point: Possible failure in interoperability of the systems.
Performance: The hospital's Fog nodes and main system receive a large amount of data from IoMT sensors.	If it receives a lot of information and there are no measures, such as load balancing, it is possible that the node goes down	Tradeoff: If the node goes down, it directly affects the Availability and Performance of the system

TABLE IX. COMMON IOMT VULNERABILITIES AND ATTACKS

Vulnerability	Description	Autor
Trojan	Software that allows you to remotely control devices and execute commands on the system	[16]
Lack of Updating	Vulnerability that allows an attacker to gain access to systems by not correcting and updating security bugs	[20]
Physical Attacks	Attack in which the attacker has physical access to the hardware, which allows the direct obtaining of information or source code	[22][15]
Man in the Middle (MITM)	Attack in which communications are intercepted, with the possibility of reading and editing content	[17][22][18] [19]
Eavesdropping	Attack in which private communications channels are tapped	[16][21][19] [15]
Sniffing	Attack in which communications are listened to and intercepted	[19]
Unauthorized /Unauthenticated access	Vulnerability that allows attackers to gain unauthenticated or unauthorized access to information	[16]
Brute Force	Trial-and-error attack, which seeks to gain access to directories or user accounts by trying to guess credentials	[17][19]
Phishing	Social engineering attack that consists of obtaining confidential information from people, deceiving them while pretending to be trustworthy entities	[17][19]
Session Hijacking	Attack in which a user's session token or cookie is hijacked, allowing access to the user's information.	[17]
Reverse Engineering	Attack that consists of converting an executable file to another, where the source code can be read	-
Misconfiguration	Vulnerability that allows access to attackers, from default passwords or mismanagement of permissions in the system	[20]
Distributed Denial of Service (DDoS)	Attack in which many requests are sent to the server, consuming bandwidth, and system resources, leaving them out of service	[16][17][22] [19][15]
SQL Injection	Attack in which malicious queries are sent to the server in order to obtain confidential information that should not be accessible	[17][19]
Port Scanning	Attack in which the ports of the systems are scanned to obtain information on technologies and information	[21]
Cross-Site Scripting (XSS)	Attack in which malicious scripts written in JavaScript are sent to obtain confidential information	[17][19]
Social Engineering	Attacks that consist of deceiving and manipulating users, some of the common attacks are phishing and spoofing	[15][14]
Weak passwords	Vulnerability where the system has default passwords or passwords that are very easy to guess	[20]
Physical / Environmental	Attacks or vulnerabilities related to the environment or nature, such as: floods, fire, natural disasters, and power failure	-

3) Security controls to mitigate vulnerabilities: At this point, the vulnerabilities found in each layer of the IoMT architecture proposed for the model are taken into account, and security controls are applied according to their category (Table III). The ISO 27001 controls to be implemented to mitigate vulnerabilities and attacks for each layer of the IoMT architecture are presented below (Table XI).

TABLE X. COMMON VULNERABILITIES AND ATTACKS FOR EACH PROPOSED IOMT ARCHITECTURE LAYER

Vulnerability	T1	T2	T3	T4	T5	T6
Trojan			✓			✓
Lack of Updating	✓	✓	✓	✓	✓	
Physical Attacks	✓					
MITM		✓	✓			✓
Eavesdrop		✓	✓			✓
Sniffing		✓	✓			✓
Unauthorized access			✓		✓	✓
Brute Force			✓		✓	✓
Phishing			✓			✓
Session Hijacking			✓		✓	✓
Reverse Engineering			✓			
Misconfiguration	✓	✓	✓		✓	
DDoS				✓	✓	
SQL Injection					✓	✓
Port Scanning					✓	
XSS						✓
Social Engineering		✓	✓			✓
Weak passwords		✓	✓		✓	✓
Physical / Environmental				✓	✓	

TABLE XI. ISO 27001 CONTROLS FOR EACH LAYER OF PROPOSED IOMT ARCHITECTURE

Vulnerability	Security category/Control	Mitigation
Device Layer		
Lack of Updating Misconfiguration	CA1: C06	Maintain sensor operating systems and libraries up to date
Physical Attacks	CA2: C07, C06	Awareness campaigns, training and providing manuals to users
Communication Layer		
Lack of Updating Misconfiguration	CA1: C06	Maintain operating systems and libraries up to date
Social Engineering MITM Eavesdropping Sniffing	CA2: C07, C06	Awareness campaigns, training and providing manuals to users
Weak passwords	CA5: C12	Passwords with uppercase letters, numbers, symbols, and minimum number of characters
Platform Layer – Edge Computing		
Lack of Updating Misconfiguration	CA1: C06	Maintain operating systems and libraries up to date
Social Engineering	CA2: C07, C06	Awareness campaigns, training and providing manuals to users
Weak passwords	CA5: C12	Passwords with uppercase letters, numbers, symbols, and minimum number of characters
Unauthorized/Unauthenticated access Brute Force Phishing Session Hijacking Reverse Engineering	CA4: C10, C11	Source code obfuscation, limiting failed login attempts and token and session validation
MITM Eavesdropping Sniffing	CA10: C24	Encrypted communications

Platform Layer – Fog Computing		
Lack of Updating Misconfiguration	CA1: C06	Maintain operating systems and libraries up to date
DDoS	CA7: C20	Firewall Load balancing
Fires, floods, power failures and natural disasters	CA6: C14, C18	Risk Management and Business Continuity Plan
Platform Layer – Datacenter (Medical System)		
Lack of Updating Misconfiguration	CA1: C06	Maintain operating systems and libraries up to date
Social Engineering	CA2: C07, C06	campaigns, training and providing manuals to users
Weak passwords	CA5: C12	Passwords with uppercase letters, numbers, symbols, and minimum number of characters
DDoS SQL Injection Port Scanning Unauthorized/Unauthenticated access Brute Force Session Hijacking	CA7: C20	Firewall Load balancing Parameter sanitization Limit maximum login failure attempts Token and session validation
Fires, floods, power failures and natural disasters	CA6: C14, C18	Risk Management and Business Continuity Plan
Application Layer		
Social Engineering	CA2: C07, C06	Awareness campaigns, training and providing manuals to users
Weak passwords	CA5: C12	Passwords with uppercase letters, numbers, symbols, and minimum number of characters
Unauthorized/Unauthenticated access, Brute Force, Phishing, Session Hijacking, SQL Injection, XSS	CA4: C10, C11	Parameter sanitization Limit failed login attempts. Token and session validation
MITM Eavesdropping Sniffing	CA10: C24	Encrypted communications

IV. Experimentation

To conduct the experimentation, the *IoMT* architecture is developed by implementing the information security controls according to each category and layer, as shown in Table XI. For this purpose, a component diagram is designed, where the main modules of the system can be seen (see Fig. 2).

Based on this, each module has different functions and is developed in different programming languages and frameworks. For example, Device Layer, would have *IoMT* technology, in this case it has no associated modules, however, its responsibility is to simulate the data collection of *IoMT* sensors through an app developed in Kotlin (Table XII).

A. Experiment 1: Interviewing Physicians

For this experiment, 3 physicians related to the health sector are considered, who followed the following steps: (i) login to the system with the assigned user and password, (ii) use of the monitoring system according to the list of assigned patients and (iii) development of a survey to obtain their expert judgment. The survey is 7 closed questions (Table XIII). And it has 5 options: 1 = Very low, 2 = Low, 3 = Normal, 4 = High and 5 = Very high; and is based on ISO 9126 [47] specifically on the quality model of a software product based on its use.

TABLE XII. Main modules of the simulated IoMT architecture

Technology	Module	Responsibility	Language / Framework
T1	None	Simulate the measurement of temperature and saturation	Frontend: Kotlin
T2	Validation Controller	Allows to validate the data obtained by the IoMT sensors, thus informing the patient if the capture has been correct or incorrect. Allows the information to be sent to the Fog Node.	Frontend: Kotlin
T3	Processing Controller	Allows to process the information received by Edge Computing, before sending it to the medical system and alert the doctor of a patient in emergency. Allows sending information to the Datacenter.	Backend: Nodejs
T5	Sign In Controller	Allows to authorize and validate the credentials of the doctor who tries to enter the medical system and block the doctor's account in case he/she exceeds the maximum number of failed attempts.	Backend: C# .NET Core Database: SQL Server
	Monitoring Controller	Allows to manage the information received by IoMT devices from patients, this component is responsible for storing and displaying patient data for a medical diagnosis.	
	Patient Controller	It allows to manage patient information, from their personal record to the medical information record.	
	Interface Controller	It allows the physician to navigate between the different views of the system, being able to visualize requested information.	Frontend: Vue.js

B. Experiment 2: Interviewing computer security experts

For this experiment, 2 experts in information security and security penetration testing are considered, who followed the following steps: (i) review of the ISO 27001 architecture and controls applied in each layer of the architecture, (ii) design of security penetration tests (Table XIV), (iii) review of the results of the penetration tests performed and (iv) development of a survey to obtain their expert judgment.

The survey has 8 closed questions and 1 open question for improvement opportunities (Table XV). The closed questions have 5 options: 1 = Poor, 2 = Bad, 3 = Fair, 4 = Good and 5 = Excellent; and are based on the gap analysis (GAP) of ISO 27001, which is the first phase of implementation (planning) [48].

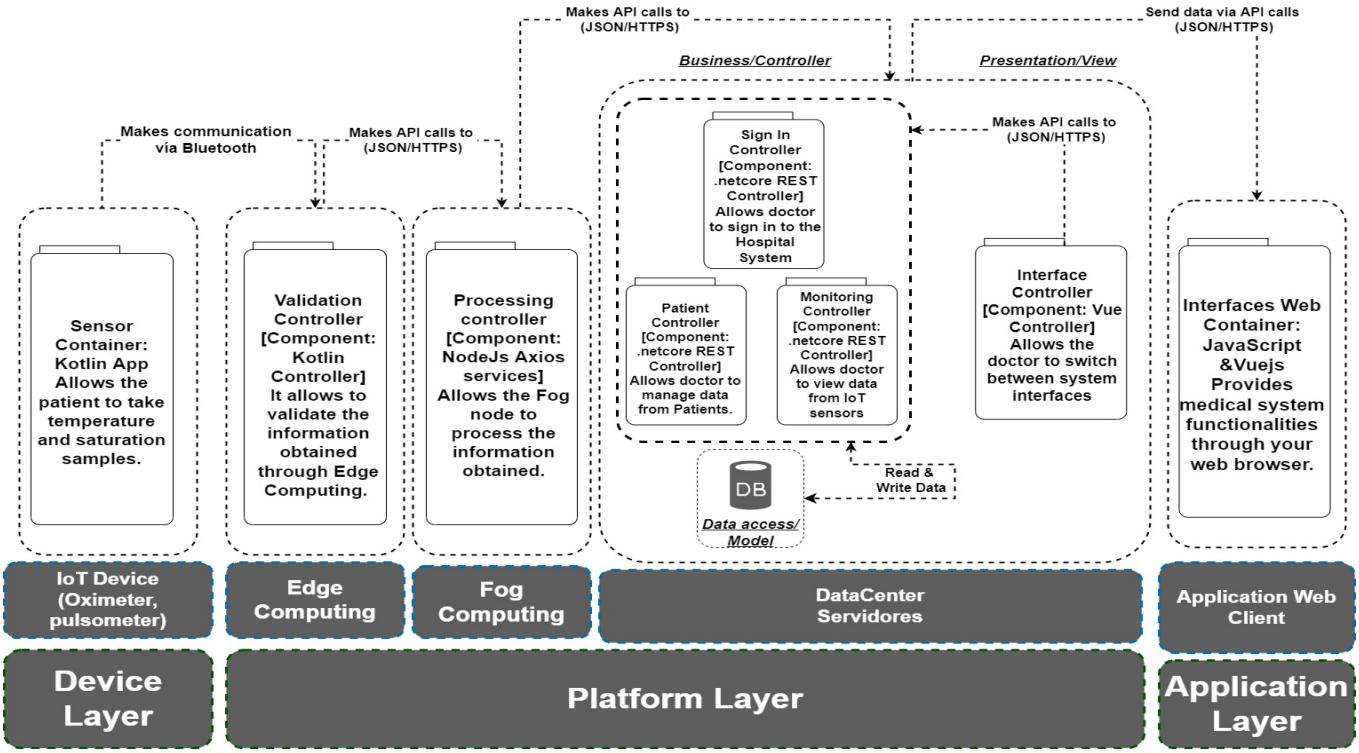

Fig. 2. Main modules of the simulated IoMT architecture

TABLE XIII. QUESTIONS FOR EXPERIMENT 1

Question		Type
Effectiveness		
QM1	What is the level of compliance with the proposal regarding patient monitoring?	Closed
QM2	What is the level of system usability shown?	Closed
Productivity		
QM3	As a physician, how easy do you think it is to use the system shown to monitor patients?	Closed
QM4	Compared to performing remote monitoring manually, what is your level of improvement that a system like the one shown would offer in terms of patient monitoring?	Closed
Satisfaction		
QM5	In contrast to in-person monitoring, what is the level of satisfaction you would have in monitoring a patient remotely?	Closed
QM6	What is the level of satisfaction a physician would have in monitoring a patient remotely using a system like the one shown?	Closed
QM7	What do you think is the level of usefulness of a medical system that allows remote patient monitoring?	Closed

TABLE XIV. PENETRATION TESTING RESULTS

Attack	Technology	State
Dictionary Attack Brute force	T3 T5 T6	Not vulnerable
SQL Injection	T5	Not vulnerable
Session Hijacking	T3 T5 T6	Not vulnerable
Reverse Engineering	T3	Not vulnerable

TABLE XV. QUESTIONS FOR EXPERIMENT 2

Categoría de Seguridad	Question		Type	
CA1	QE1	What do you think is the quality of the implementation of controls in the CA1 category?	C06	Closed
CA2	QE2	What do you think is the quality of the implementation of controls in the CA2 category?	C06 C07	Closed
CA4	QE3	What do you think is the quality of the implementation of controls in the CA4 category?	C10 C11	Closed
CA5	QE4	What do you think is the quality of the implementation of CA5 category controls?	C12	Closed
CA6	QE5	What do you think is the quality of the implementation of CA6 category controls?	C14 C18	Closed
CA7	QE6	What do you think is the quality of the implementation of CA7 category controls?	C20	Closed
CA10	QE7	What do you think is the quality of the implementation of CA10 category controls?	C24	Closed
-	QE8	What controls do you think should be improved to secure IoMT architectures?	-	Closed

V. Results And Discussion

Fig. 3 shows the results obtained by the 3 physicians (M1, M2 and M3) of experiment 1, to evaluate the "effectiveness" of the medical system. The results show that the respondents rate compliance with respect to patient monitoring (QM1) and ease of use of the system (QM2), with an average value of 3.67, respectively. In other words, *effectiveness* is rated between "normal" and "high".

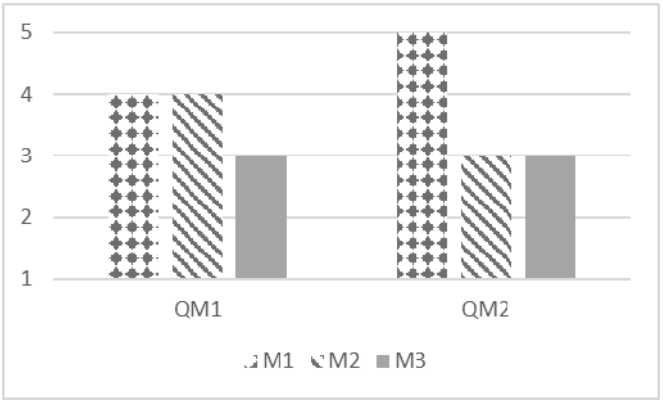

Fig. 3. Results of Experiment 1 - Effectiveness

Fig. 4 shows the results obtained by the 3 physicians (M1, M2 and M3) of experiment 1 to evaluate the "productivity" of the medical system. The results show that the respondents rate the ease of use of the system for remote monitoring (QM3) and a level of improvement in patient monitoring (QM4) with an average value of 4.33, respectively. In other words, *productivity* is rated between "high" and "very high".

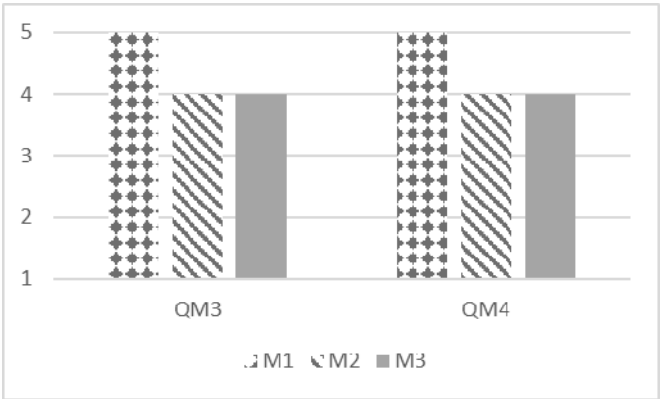

Fig. 4. Results Experiment 1 - Productivity

Fig. 5 shows the results obtained by the 3 physicians (M1, M2 and M3) in experiment 1, based on the physicians' "satisfaction" with the simulation. The results show that the respondents rate the satisfaction offered by monitoring patients remotely (QM5) and the satisfaction of remote monitoring using an *IoMT* system (QM6) with an average value of 4.00, respectively. While the average value rated by respondents regarding the usefulness of a system that enables remote monitoring with *IoMT* (QM7) is 4.33. In other words, *satisfaction* has a rating between "high" and "very high".

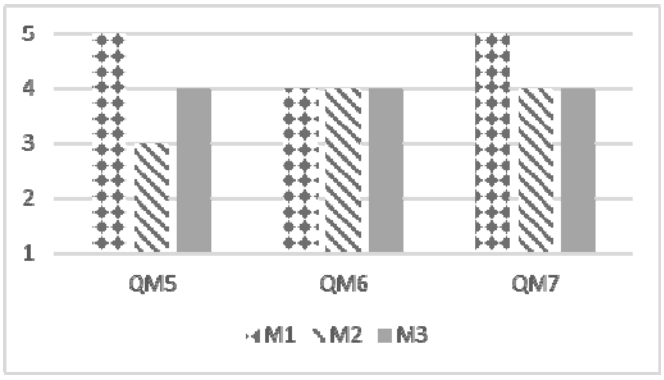

Fig. 5. Results Experiment 1 - Satisfaction

Fig. 6 shows the results obtained from experiment 2, based on the "quality" of the implementation of ISO 27001 controls in the IoMT architecture layers. The results show that the respondents rate the quality of the controls related to questions QE1, QE2 and QE7 with an average value of 4.00, respectively. Likewise, the average value obtained by the interviewees for the quality of the controls corresponding to questions QE3, QE4 and QE5 is 3.50. Finally, respondents rated the quality of implementation for the control related to question QE6 with an average value of 3.00. In other words, the *quality of implementation of information security controls* has a rating between "normal" and "good".

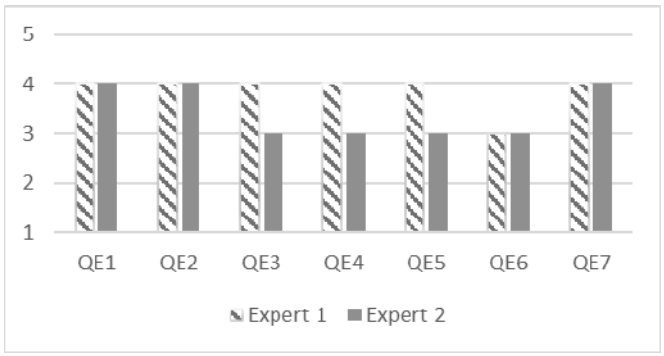

Fig. 6. Results of Experiment 2

Overall, the results of the experiments show that for experiment 1, the physicians rate the "effectiveness", "productivity", and "satisfaction" of the remote monitoring system with an average value of 3.67, 4.33 and 4.11 respectively, i.e., between "normal" and "high". On the other hand, for experiment 2, the security experts rate the quality of the implemented controls with an average value of 3.65, i.e., between "normal" and "good".

VI. Conclusion and Future Work

In this study, it is conducted the proposal, design, analysis, and simulation of an *IoMT* architecture with information security controls based on ISO 27001. For this design, a literature review took place, where common IoT vulnerabilities, possible *IoMT* architectures and mitigation or security measures for *IoMT* are obtained. This enables the design of an IoMT architecture with security controls, where

ISO 27001 is chosen because it provides guidelines for information security.

Two experiments are conducted to obtain expert judgment. Experiment 1 is with physicians, to measure the applicability, functionality, and usability of the system. Experiment 2 is with security experts, to measure the quality of the information security controls.

The results of experiment 1 allow the rating of *effectiveness*, *productivity* and *satisfaction* related to the remote monitoring system, obtaining an average value of 3.67, 4.33 and 4.11, respectively. That is, between "normal" and "high". This indicates the current usefulness of remote monitoring implementations using *IoMT* in the ambulatory health sector.

The result of the experiment 2 is the rating given by security experts related to the quality of implementation of information security controls in the *IoMT* architecture had an average value of 3.42, i.e., between "normal" and "good". This, transferred to the maturity levels of ISO 27001 results in a level between 3 or 4, which means that the implemented controls have an adequate level of security.

As future work, it is recommended to implement the *IoMT* architecture with the proposed security controls in real environments such as: clinics, hospitals, and health centers. In this way to obtain better judgments related to *IoMT* architecture and applied information security controls.

ACKNOWLEDGMENTS

To the Research Department of the Universidad Peruana de Ciencias Aplicadas for the support provided to carry out this research work.

REFERENCES

[1] M. Cabrera, “El internet de las cosas (IoT) y la salud en la era de la COVID-19 | Marketing | Actualidad | ESAN,” Feb. 17, 2021. https://www.esan.edu.pe/conexion/actualidad/2021/02/17/el-internet-de-las-cosas-iot-y-la-salud-en-la-era-de-la-covid-19-1/ (accessed Aug. 28, 2021).

[2] H. Zhu et al., “Smart Healthcare in the Era of Internet-of-Things,” IEEE Consum. Electron. Mag., vol. 8, no. 5, pp. 26–30, Sep. 2019, doi: 10.1109/MCE.2019.2923929.

[3] EUROPOL, “Pandemic profiteering,” 2020.

[4] R. Priyadarshini, M. R. Panda, and B. K. Mishra, “Security in Healthcare Applications Based on Fog and Cloud Computing,” Cyber Secur. Parallel Distrib. Comput., pp. 231–243, Mar. 2019, doi: 10.1002/9781119488330.CH15.

[5] D. McMillen, “Internet of Threats: IoT Botnets Drive Surge in Network Attacks,” Apr. 22, 2021. https://securityintelligence.com/posts/internet-of-threats-iot-botnets-network-attacks/ (accessed Aug. 28, 2021).

[6] N. Agarwal, “How to Ensure Cybersecurity in the Age of IoT,” Mar. 03, 2021. https://appinventiv.com/blog/how-to-ensure-cybersecurity-in-iot/ (accessed Aug. 28, 2021).

[7] P. Passeri, “Q1 2020 Cyber Attacks Statistics – HACKMAGEDDON,” Apr. 14, 2020. https://www.hackmageddon.com/2020/04/14/q1-2020-cyber-attacks-statistics/ (accessed Mar. 26, 2022).

[8] P. Passeri, “Q1 2021 Cyber Attack Statistics – HACKMAGEDDON,” Apr. 13, 2021. https://www.hackmageddon.com/2021/04/13/q1-2021-cyber-attack-statistics/ (accessed Mar. 26, 2022).

[9] P. Passeri, “January 2022 Cyber Attacks Statistics – HACKMAGEDDON,” Feb. 16, 2022. https://www.hackmageddon.com/2022/02/16/january-2022-cyber-attacks-statistics/ (accessed Mar. 26, 2022).

[10] A. Echeverría, C. Cevallos, I. Ortiz-Garces, and R. O. Andrade, “Cybersecurity Model Based on Hardening for Secure Internet of Things Implementation,” Appl. Sci. 2021, Vol. 11, Page 3260, vol. 11, no. 7, p. 3260, Apr. 2021, doi: 10.3390/APP11073260.

[11] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, “IoMT Malware Detection Approaches: Analysis and Research Challenges,” IEEE Access, vol. 7, pp. 182459–182476, 2019, doi: 10.1109/ACCESS.2019.2960412.

[12] L. R. Wong, D. Mauricio, and G. D. Rodriguez, “A systematic literature review about software requirements elicitation,” J. Eng. Sci. Technol., vol. 12, no. 2, pp. 296–317, Feb. 2017.

[13] P. Kumar, G. P. Gupta, and R. Tripathi, “An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks,” Comput. Commun., vol. 166, pp. 110–124, Jan. 2021, doi: 10.1016/J.COMCOM.2020.12.003.

[14] K. Hughes-Lartey, M. Li, F. E. Botchey, and Z. Qin, “Human factor, a critical weak point in the information security of an organization’s Internet of things,” Heliyon, vol. 7, no. 3, p. e06522, Mar. 2021, doi: 10.1016/J.HELIYON.2021.E06522.

[15] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, “An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security,” IEEE Internet Things J., vol. 7, no. 10, pp. 10250–10276, Oct. 2020, doi: 10.1109/JIOT.2020.2997651.

[16] M. Snehi and A. Bhandari, “Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks,” Comput. Sci. Rev., vol. 40, p. 100371, May 2021, doi: 10.1016/J.COSREV.2021.100371.

[17] M. A. Amanullah et al., “Deep learning and big data technologies for IoT security,” Comput. Commun., vol. 151, pp. 495–517, Feb. 2020, doi: 10.1016/J.COMCOM.2020.01.016.

[18] E. Staddon, V. Loscri, and N. Mitton, “Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey,” Appl. Sci. 2021, Vol. 11, Page 7228, vol. 11, no. 16, p. 7228, Aug. 2021, doi: 10.3390/APP11167228.

[19] M. Mahbub, “Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics,” J. Netw. Comput. Appl., vol. 168, p. 102761, Oct. 2020, doi: 10.1016/J.JNCA.2020.102761.

[20] P. Ferrara, A. K. Mandal, A. Cortesi, and F. Spoto, “Static analysis for discovering IoT vulnerabilities,” Int. J. Softw. Tools Technol. Transf. 2020 231, vol. 23, no. 1, pp. 71–88, Nov. 2020, doi: 10.1007/S10009-020-00592-X.

[21] N. B. Samyuel and B. A. Shimray, “Securing IoT device communication against network flow attacks with Recursive Internetworking Architecture (RINA),” ICT Express, vol. 7, no. 1, pp. 110–114, Mar. 2021, doi: 10.1016/J.ICTE.2020.08.001.

[22] S. Ketu and P. K. Mishra, “Internet of Healthcare Things: A contemporary survey,” J. Netw. Comput. Appl., vol. 192, p. 103179, Oct. 2021, doi: 10.1016/J.JNCA.2021.103179.

[23] D. Gupta, S. Bhatt, M. Gupta, and A. S. Tosun, “Future Smart Connected Communities to Fight COVID-19 Outbreak,” Internet of Things, vol. 13, p. 100342, Mar. 2021, doi: 10.1016/J.IOT.2020.100342.

[24] M. Javaid and I. H. Khan, “Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic,” J. Oral Biol. Craniofacial Res., vol. 11, no. 2, pp. 209–214, Apr. 2021, doi: 10.1016/J.JOBCR.2021.01.015.

[25] A. H. Mohd Aman, W. H. Hassan, S. Sameen, Z. S. Attarbashi, M. Alizadeh, and L. A. Latiff, “IoMT amid COVID-19 pandemic: Application, architecture, technology, and security,” J. Netw. Comput. Appl., vol. 174, p. 102886, Jan. 2021, doi: 10.1016/J.JNCA.2020.102886.

[26] C. S. S. Guimarães, M. de Andrade, F. R. de Avila, V. E. de Oliveira Gomes, and V. C. Nardelli, “IoT Architecture for Interoperability and Monitoring of Industrial Nodes,” Procedia Manuf., vol. 52, pp. 313–318, Jan. 2020, doi: 10.1016/J.PROMFG.2020.11.052.

[27] G. Manogaran, R. Varatharajan, D. Lopez, P. M. Kumar, R. Sundarasekar, and C. Thota, “A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system,” Futur. Gener. Comput. Syst., vol. 82, pp. 375–387, May 2018, doi: 10.1016/J.FUTURE.2017.10.045.

[28] B. Omoniwa, R. Hussain, M. A. Javed, S. H. Bouk, and S. A. Malik, "Fog/edge computing-based IoT (FECIoT): Architecture, applications, and research issues," IEEE Internet Things J., vol. 6, no. 3, pp. 4118–4149, Jun. 2019, doi: 10.1109/JIOT.2018.2875544.
[29] I. Bica, B.-C. Chifor, Ştefan-C. Arseni, and I. Matei, "Multi-Layer IoT Security Framework for Ambient Intelligence Environments," Sensors 2019, Vol. 19, Page 4038, vol. 19, no. 18, p. 4038, Sep. 2019, doi: 10.3390/S19184038.
[30] L. Greco, G. Percannella, P. Ritrovato, F. Tortorella, and M. Vento, "Trends in IoT based solutions for health care: Moving AI to the edge," Pattern Recognit. Lett., vol. 135, pp. 346–353, Jul. 2020, doi: 10.1016/J.PATREC.2020.05.016.
[31] H. Liu, J. Li, and D. Gu, "Understanding the security of app-in-the-middle IoT," Comput. Secur., vol. 97, p. 102000, Oct. 2020, doi: 10.1016/J.COSE.2020.102000.
[32] S. K. Elagan, S. F. Abdelwahab, E. A. Zanaty, M. H. Alkinani, H. Alotaibi, and M. E. A. Zanaty, "Remote diagnostic and detection of coronavirus disease (COVID-19) system based on intelligent healthcare and internet of things," Results Phys., vol. 22, p. 103910, Mar. 2021, doi: 10.1016/J.RINP.2021.103910.
[33] X. Yao, F. Farha, R. Li, I. Psychoula, L. Chen, and H. Ning, "Security and privacy issues of physical objects in the IoT: Challenges and opportunities," Digit. Commun. Networks, vol. 7, no. 3, pp. 373–384, Aug. 2021, doi: 10.1016/J.DCAN.2020.09.001.
[34] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis," Sensors 2020, Vol. 20, Page 3625, vol. 20, no. 13, p. 3625, Jun. 2020, doi: 10.3390/S20133625.
[35] I. Butun, P. Osterberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," IEEE Commun. Surv. Tutorials, vol. 22, no. 1, pp. 616–644, Jan. 2020, doi: 10.1109/COMST.2019.2953364.
[36] S. Piasecki, L. Urquhart, and P. D. McAuley, "Defence against the dark artefacts: Smart home cybercrimes and cybersecurity standards," Comput. Law Secur. Rev., vol. 42, p. 105542, Sep. 2021, doi: 10.1016/J.CLSR.2021.105542.
[37] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, "Smart home security: challenges, issues and solutions at different IoT layers," J. Supercomput. 2021, pp. 1–37, May 2021, doi: 10.1007/S11227-021-03825-1.
[38] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," IEEE Access, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.
[39] X. Li, H. N. Dai, Q. Wang, M. Imran, D. Li, and M. A. Imran, "Securing Internet of Medical Things with Friendly-jamming schemes," Comput. Commun., vol. 160, pp. 431–442, Jul. 2020, doi: 10.1016/J.COMCOM.2020.06.026.
[40] K. Sha, T. A. Yang, W. Wei, and S. Davari, "A survey of edge computing-based designs for IoT security," Digit. Commun. Networks, vol. 6, no. 2, pp. 195–202, May 2020, doi: 10.1016/J.DCAN.2019.08.006.
[41] OWASP, "OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation." https://owasp.org/ (accessed Sep. 17, 2022).
[42] ISO, "ISO - ISO 27799:2016 - Health informatics — Information security management in health using ISO/IEC 27002," 2016. https://www.iso.org/standard/62777.html (accessed Oct. 04, 2021).
[43] J. Cawthra et al., "Securing Telehealth Remote Patient Monitoring Ecosystem Volume B: Approach, Architecture, and Security Characteristics," pp. 1800–1830, 2022, doi: 10.6028/NIST.SP.1800-30.
[44] IEEE SA Board of Governors/Corporate Advisory Group (BoG/CAG), "2413-2019 - IEEE Standard for an Architectural Framework for the Internet of Things (IoT)," 2020.
[45] V. S. Naresh, S. S. Pericherla, P. S. R. Murty, and S. Reddi, "Internet of things in healthcare: Architecture, applications, challenges, and solutions," Comput. Syst. Sci. Eng., vol. 35, no. 6, pp. 411–421, Nov. 2020, doi: 10.32604/CSSE.2020.35.411.
[46] R. Kazman, M. Klein, and P. Clements, "ATAM: Method for Architecture Evaluation," 2000.
[47] "ISO 9126 - INFORMATICA." https://web.archive.org/web/20201009071354/https://sites.google.com/site/informaticamcprats/iso-9126 (accessed Jun. 01, 2022).
[48] "Planning for & Implementing ISO 27001 | ISACA Journal." https://www.isaca.org/resources/isaca-journal/past-issues/2011/2011-planning-for-and-implementing-iso-27001 (accessed Jun. 01, 2022).