Migration Letters

Volume: 21, No: S2 (2024), pp. 711-728

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

Iomt Data Server Risks And Vulnerabilities

Carlos Martínez Santander[1], Sebastià Galmès[2], Yolanda de la N Cruz Gavilánez[2]

Abstract

The Internet of Medical Things (IoMT) is the convergence between technology and healthcare, in which data networks are used to support interconnected medical attention. That is an interconnection of medical devices, sensors, diagnostic equipment, information systems, and healthcare platforms through the Internet for the collection and analysis of data in real-time, allowing timely diagnosis and treatment, as well as the simplification of these processes. Despite the enormous advantages of IoMT, it also presents a significant challenge to the security, availability, and privacy of medical data and interoperability between different devices and platforms. If a hacker takes advantage of these vulnerabilities and manages to exploit them, he or she could engage in patient or healthcare institution extortion, medical identity theft, and even modification, alteration, or blocking of IoMT devices in use, endangering the health and lives of patients. It is essential to carry out different studies in this area to ensure the protection and welfare of people who use these means, thus maintaining trust in IoMT technologies in the medical field. The present study makes the following very important contributions to the field of IoMT security research. On the one hand, it evaluates the knowledge of healthcare professionals on the subject. On the other hand, it shows the main vulnerabilities in healthcare management data servers according to the Common Vulnerability Scoring System (CVSS) 3.1.

Keywords *Internet of Medical Things (IoMT), Security, Vulnerabilities, Common Vulnerability Scoring System (CVSS).*

1. Introduction

Internet of Medical Things (IoMT) is the convergence between technology and healthcare, in which data networks are used to support interconnected medical attention [1]–[3]. That is an interconnection of medical devices, sensors, diagnostic equipment, information systems, and healthcare platforms throug[1]h the Internet for real-time data collection and analysis [4], [5]. This allows for improving the quality of health management, including early diagnosis of pathologies, prevention, and personalized treatment [6]. Through the use of IoMT devices, such as portable vital sign monitors, glucose sensors, wireless ECG (electrocardiogram) electrodes, digital pills, physical activity tracking devices, and sleep monitors, real-time valuable healthcare information can be provided to both the patients and the doctors.

However, despite the enormous advantages of IoMT, it also presents a significant challenge to the security, availability, and privacy of medical data as well as the interoperability

[1]Carrera de Medicina, Universidad Católica de Cuenca Cuenca - Ecuador
[2]Dpto. Ciencias Matemáticas e Informática, Universidad de las Islas Baleares
Islas Baleares – España.

between different devices and platforms [7]. In this context, it is essential to be concerned about mitigating all these challenges because, according to the Gartner report, in 2020, there were about 20.4 billion interconnected devices, and it is expected that by 2025 there will be 1.0 trillion, more than 50% being IoMT devices [8], [9]. In [10], the FBI revealed that IoMT solutions are highly vulnerable, complemented by the wireless transmission of data and that for subsequent analysis of these data, it is necessary to store them on remote servers. The vulnerabilities affecting IoMT technology represent a danger to the health and integrity of patients since these systems manage confidential health information, historical data, medication, and other identifiable personal data. If a hacker takes advantage of these vulnerabilities and manages to exploit them, he/she could incur the extortion of the patient or the healthcare institution, medical identity theft, and even modification, alteration, or blocking of IoMT devices in use, endangering the health and life of patients [5], [11]–[15].

The most common attack recorded in IoMT devices is the DOS (Denial of Service), which is the most dangerous for overloading or exhausting the resources in IoMT devices, networks, or server management systems where the data with patient information is stored. Normally the most used ports are 80 (HTTP) and 443 (HTTPS), among others; if the attack is successful, the physical integrity of the patient is at stake because the devices are related to medical care [10]. Other attacks recorded in these environments are MITM (Man-in-the-Middle), impersonation, brute force, and malware [12]. IoMT devices are susceptible to attacks, directly through their wireless connections (Bluetooth, Wi-Fi, NFC, GPS, cellular networks, Zigbee, and LoRa), and also through the Internet, which is also used by hackers to launch any attack on other components of the IoMT system (servers, instruments on the healthcare provider site) [16].

With the increase exponential growth of medical devices connected to the network, patient data become vulnerable to cyber-attacks; it is essential to conduct various studies in this area to ensure the protection and welfare of people who have use of these means, and so guarantee confidence on IoMT technologies in the medical field. This study aims to contribute to the IoMT security research. Moreover, it evaluates the knowledge of healthcare professionals on the subject; on the other hand, it shows the main vulnerabilities in healthcare management data servers according to CVSS 3.1.

1.1 Background

This section presents an analysis of the literature on IoMT security and how it is distributed or at what points we can find vulnerabilities in the whole system; it was necessary to divide the scheme of an IoMT system, as shown in Fig 1. The first security line groups the devices that are subject to short and medium-range attacks, that is, hackers must be at short distances to sabotage these services. This is the IoMT wearable devices line. The second security line is the connection between the smartphone and the Internet (network), where medium and long-range attacks can take place. Finally, the third line is the Internet and the server where IoMT data are stored and managed; the attacks will be long-range, remote attacks (IoMT Servers).

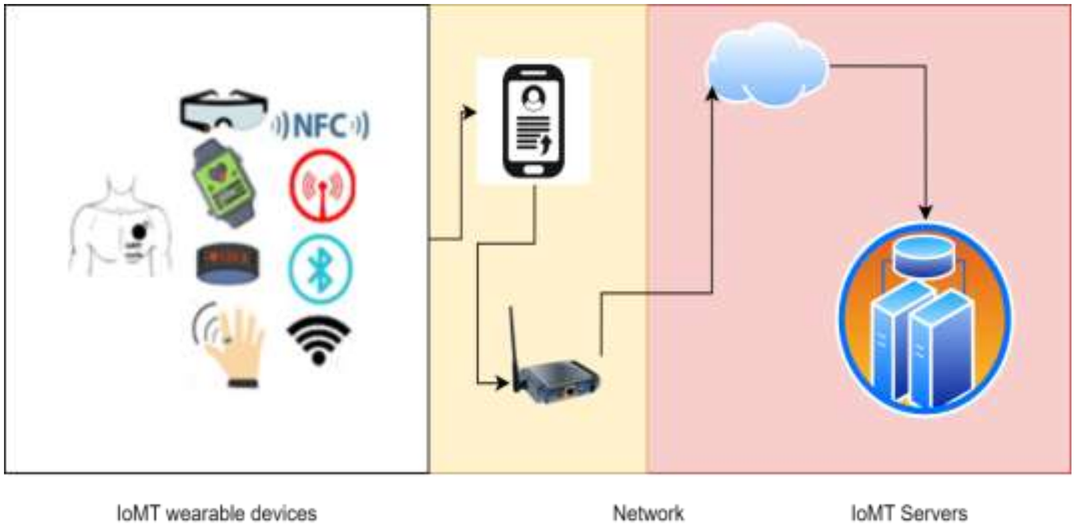

Figure 1. IoMT Network Structure.
Source: Author of the research, (Martinez C,2023)

First, this infrastructure is made up of IoMT wearables devices, superimposed or implanted in the patient's body, these are connected using short-range link technologies to a mobile device to finally reach the IoMT Server through the Internet infrastructure, where the patient's information will be stored or managed, each of these parts is detailed below.

1.1.1 IoMT wearable device

IoMT wearable devices are composed of body sensors that constantly monitor the behavior of organs or vital signs in real-time. These devices provide freedom to patients because they can perform their daily activities normally [17] Examples are brain monitors pacemakers and stents for vascular and neurological diseases, among many others. Once IoMT devices collect user data, they send them to IoMT servers using wireless short and medium-range technologies, such as NFC (Near Field Communication), Bluetooth, and Wi-Fi, among others.

In Table 1, the technologies used and potential vulnerabilities in these first-line devices are detailed. If they are breached, the patient's life is at stake [4], [9], [18].

Table 1. Vulnerabilities of short-range link technologies

Wearable	**Technology**	**Ports**	**Protocol**	**Vulnerabilities**
Heart Rate Monitor (Smartwatch)	Bluetooth, ANT+	N/A	Bluetooth, ANT+	Insecure data exchange
				Spoofing attacks Firmware and software vulnerabilities Denial of service (DoS) attacks Falsification of health data
Glucose Sensor	Bluetooth, NFC		Bluetooth, NFC	Manipulation of glucose data
				Communication interruptions

				Denial of Service (DoS) attacks
Insulin Pump	Bluetooth	N/A	Bluetooth	Spoofing attacks Insulin dose manipulation Denial of Service (DoS) attacks Authentication and authorization failures
IoMT hearing aids	Bluetooth	N/A	Bluetooth	Unauthorized eavesdropping Service interruption attacks Bluetooth pairing vulnerabilities
Swallowable Capsules (Digital Pills)	Bluetooth, NFC	N/A	Bluetooth, NFC	Insecure data exchange Denial of service attacks (DoS) Falsification of medical data Privacy and confidentiality issues
Sleep Monitor	Bluetooth	N/A	Bluetooth	Unauthorized collection and transmission of sleep data Firmware and software vulnerabilities Identity theft

Source: Author of the research, (Martinez C,2023)

1.1.2 Networks

The connection at this first level is the smartphones with home wireless networks, thus representing significant security risks, especially with technologies such as Wi-Fi due to its multiple known vulnerabilities. Table 2 shows the main vulnerabilities present in this section of the system. Moreover, wired Ethernet technology has been included due to its prominence in domestic networks.

Table 2. Vulnerabilities in the transmission of IoMT data

Network	Technologies	Ports	Common Ports	Vulnerabilities
Wi-Fi	Wi-Fi 802.11a/b/g/n/ac/ax	80 (HTTP), 443 (HTTPS), and other ports, depending on the applications and services used	TCP, UDP, HTTP, HTTPS, DNS, and DHCP, among others	Unauthorized access to the Wi-Fi network Wi-Fi traffic interception Spoofing attacks
Bluetooth	Bluetooth Classic (2.1) Bluetooth Low Energy (4.0 and subsequent) Bluetooth 5.0	Based on profiles and services	RFCOMM, L2CAP, SDP	Unauthorized pairing attacks Bluetooth device spoofing Bluetooth traffic interception
Zigbee	Zigbee (IEEE 802.15.4)	N/A	Zigbee	Man-in-the-middle attack

				Zigbee spoofing
NFC	Near Field Communication (NFC)	N/A	NFC	NFC communication interception NFC tag counterfeiting
				Unauthorized use of NFC functions
Mobile network	3G, 4G, 5G	80 y 443 para-HTTP/HTTPS	TCP, UDP, HTTP, HTTPS, among others	Cellular infrastructure vulnerabilities Denial of Service (DoS) attacks Cellular traffic interception
Ethernet	Ethernet	N/A	TCP, UDP	Unauthorized wired network access attacks

Source: Author of the research, (Martinez C,2023)

1.1.3 IoMT Servers

The communication of IoMT devices with data management, storage, or administration servers is a critical aspect due to the nature of the data. This transmission opens the door to possible exploitations of vulnerabilities and security risks; as stated in previous points, attacks directed to IoMT servers can unleash serious consequences such as unauthorized access to sensitive health information, manipulation of patient data, sabotage of devices, or denial of services. Table 3 lists the main vulnerabilities linked to the lack of IoMT security standards the use of insecure protocols and weak encryption algorithms.

Table 3. IoMT data storage level vulnerabilities

IoMT Data Servers	Technologies	Ports	Protocols	Vulnerabilities
Cloud storage	N/A	N/A	HTTP, HTTPS, and others depending on the provider	Unauthorized access to data in the cloud Leakage of sensitive information Denial of service attacks (DoS)
Database	SQL, NoSQL, MySQL, PostgreSQL, Oracle	1433, 1434, 3306, 5432,1521	SQL, NoSQL, UDP, TDS	SQL Injection Database Configuration Vulnerabilities Unauthorized database access
API (Application Programming Interface)	REST, GraphQL, other	80, 443	HTTP, HTTPS	Brute force API attacks Authentication and authorization failures

				Exposure of sensitive data through the API
Network Security	Firewall, VPN	20, 21, 22, 25, 53, 80, 443,143, 68,123,161, 5353, 4500	TCP, UDP	Denial of service attacks (DoS) Spoofing attacks (spoofing) Man-in-the-middle (man-in-the-middle) attacks

Source: Author of the research, (Martinez C,2023)

1.1.4 CVSS Vulnerability Score 3.1

CVSS (Common Vulnerability Scoring System) is a tool that presents a set of standards for assessing the severity of security vulnerabilities in devices or computing environments[19]–[23]. Nevertheless, when applied, although it is a valuable tool, it is not 100% perfect, so experts in the field should apply it with caution to avoid making mistakes. Table 4 shows some characteristics of these standards [24]–[30].

Table 4. CVSS Characteristics

Item	Advantages	Disadvantages	Uses
Standard evaluation	Provides a standardized way of rating vulnerabilities.	Subjectivity can still influence the final score l.	It helps security specialists identify and classify vulnerabilities.
Ease of use	It is relatively simple to understand and use.	It does not always capture all the complexities of vulnerabilities.	Allows different analysts or teams to perform consistent assessments.
Based on metrics	It is based on metrics and factors to assign scores.	It does not always reflect the actual risk for a specific environment.	Allows organizations to prioritize vulnerability mitigation.
Quantitative scale	It uses a numerical scale to express the severity of vulnerabilities.	It does not take into account the operational context of an organization.	It helps determine the severity of a vulnerability.
Effective communication	Allows clearer communication for decision-making.	It does not always take into account personalized impact factors.	Facilitates discussion on the relative importance of vulnerabilities.
Community support	Community of users and experts who contribute to its continuous improvement.	It does not always reflect the relevance of a vulnerability to a specific use case.	Encourages collaboration and sharing of vulnerability information.

Source: Author of the research, (Martinez C,2023)

2. Research Method

This study has two phases. In the first phase, a survey was applied to 85 healthcare professionals, the instrument consisted of 15 questions on knowledge of patient information security. One of the questions gave rise to the second phase of the study, which focused on cloud-based medical data management and storage systems: "Which ones have you used, or do you use?". Respondents could select one of the proposed answers or even specify any others not included in the list. As indicated, in the second phase, starting from the IoMT applications or servers used by healthcare professionals Figure 7; proceeded to collect the main vulnerabilities present in these data servers for research purposes by passive scanning without damaging the data infrastructure or violating data security. Tools such as the Kali Linux operating system, vulnerability scanning applications (Nessus, Cadaver, Davtest, Nikto, Skipfish, Wapiti, Whatweb, Wpscan), and Nmap, among others, were implemented.

The Common Vulnerability Scoring System (CVSS) is a framework for the evaluation and subsequent reporting of vulnerabilities in computer systems, providing a numerical score to reflect the severity of a vulnerability. This tool is widely used in computer security. Scoring is done based on scale and equation provided by the National Vulnerability Database (NVD)

Fig. 2, Table 5 [31]–[33].

CVSS v3 Equations

The CVSS v3.0 equations are defined below.

Base

The Base Score is a function of the Impact and Exploitability sub score equations. Where the Base score is defined as,

If (Impact sub score <= 0) *0 else,*

Scope Unchanged[4] $Roundup(Minimum[(Impact + Exploitability), 10])$

Scope Changed $Roundup(Minimum[1.08 \times (Impact + Exploitability), 10])$

and the Impact sub score (ISC) is defined as,

Scope Unchanged $6.42 \times ISC_{Base}$

Scope Changed $7.52 \times [ISC_{Base} - 0.029] - 3.25 \times [ISC_{Base} - 0.02]^{15}$

Where,

$ISC_{Base} = 1 - [(1 - Impact_{Conf}) \times (1 - Impact_{Integ}) \times (1 - Impact_{Avail})]$

And the Exploitability sub score is,

$8.22 \times AttackVector \times AttackComplexity \times PrivilegeRequired \times UserInteraction$

Temporal

The Temporal score is defined as,

$Roundup(BaseScore \times ExploitCodeMaturity \times RemediationLevel \times ReportConfidence)$

Environmental

The environmental score is defined as,

If (Modified Impact Sub score <= 0) 0 else,

If Modified Scope is Unchanged Round up(Round up (Minimum [(M.Impact + M.Exploitability) ,10]) × Exploit Code Maturity × Remediation Level × Report Confidence)

If Modified Scope is Changed Round up(Round up (Minimum [1.08 × (M.Impact + M.Exploitability) ,10]) × Exploit Code Maturity × Remediation Level × Report Confidence)

And the modified Impact sub score is defined as,

If Modified Scope is Unchanged $6.42 \times [ISC_{Modified}]$

If Modified Scope is Changed $7.52 \times [ISC_{Modified} - 0.029]-3.25\times [ISC_{Modified} - 0.02]$ 15

Where,

$ISC_{Modified} = Minimum\ [[1 - (1 - M.IConf \times CR) \times (1 - M.IInteg \times IR) \times (1 - M.IAvail \times AR)], 0.915]$

The Modified Exploitability sub score is,

$8.22 \times M.AttackVector \times M.AttackComplexity \times M.PrivilegeRequired \times M.UserInteraction$

4 Where “Round up” is defined as the smallest number, specified to one decimal place, that is equal to or higher than its input. For example, Round up (4.02) is 4.1; and Round up (4.00) is 4.0.

Figure 2. The CVSS v3.0 equations
Source: Author of the research, (Martinez C,2023)

Table 5. Qualitative Severity Ratings

CVSS v2.0 Ratings		**CVSS v3.0 Ratings**	
Severity	**Severity Score Range**	**Severity**	**Severity Score Range**
		None*	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

Fuente: https://nvd.nist.gov/vuln-metrics/cvss

3. Results

The next part descriptive analysis of the responses to the most relevant questions asked of the healthcare professionals. Of the respondents, 40 stated that they were physicians by profession, followed by 13 nursing professionals, 10 pharmaceutical chemists, and 9 biochemists, among others, as shown in Fig 3. Most of the professionals were engaged in practice, teaching, or research they belonged to an educational institution in Ecuador.

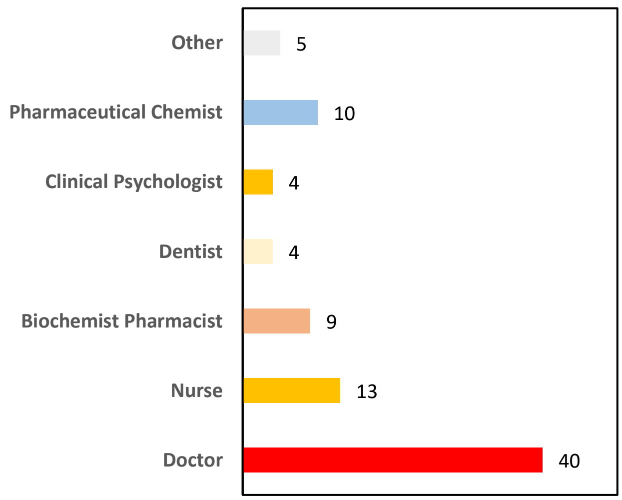

Figure 3. Professionals in the health field.
Source: Author of the research, (Martinez C,2023)

Another relevant question is whether healthcare professionals use electronic devices to store patient data. As shown in Fig 4, 64 professionals answered in the affirmative, while 21 stated that they do not use electronic devices, storing their patients' data in physical form, or paper medical records.

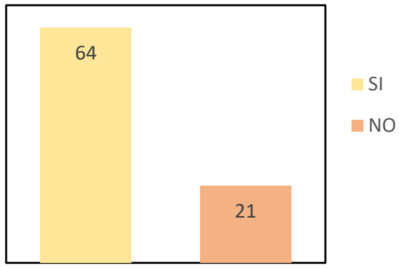

Figure 4. Count of professionals using electronic devices
Source: Author of the research, (Martinez C,2023)

Regarding the advantages of the use of electronic devices during patient consultation, it can be seen in Fig 5, that most of the professionals who previously responded affirmatively to the use of electronic devices say these technologies support and facilitate the recording, storage, diagnosis, and availability of the clinical history, in other words, in all the processes that involve the treatment of sensitive data.

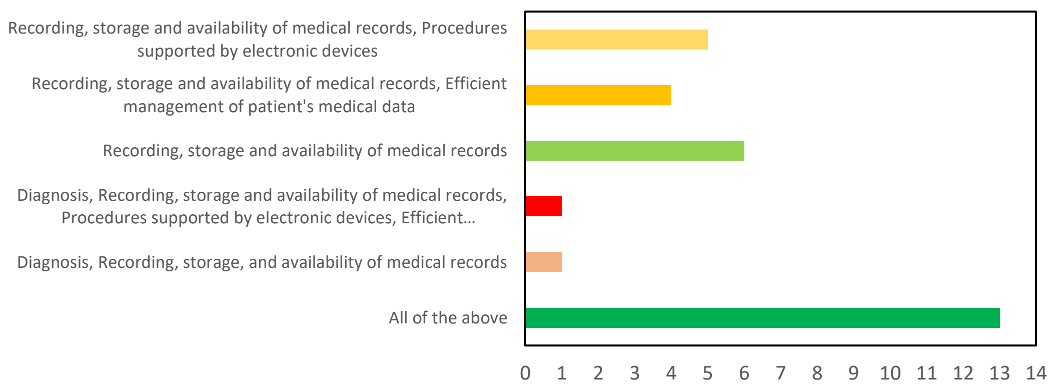

Figure 5. Advantages of using electronic devices for patient consultations
Source: Author of the research, (Martinez C,2023)

Regarding IT security issues related to patient data, all healthcare professionals report a general and basic understanding related to the integrity, privacy, and confidentiality of digital clinical data.

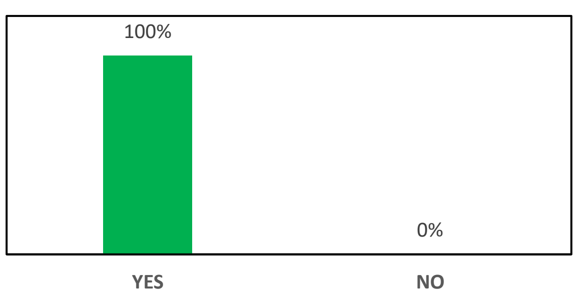

Figure 6. Percentage of health professionals who say they are aware of data security issues.

Source: Author of the research, (Martinez C,2023)

A crucial question that enables us to draw firm conclusions regarding the methodologies adopted by data protection professionals revolves around the safeguarding of patient information, which essentially pertains to information security. Inquiring ¿how do health professionals protect this data? resulted in varied responses. To analyze these responses effectively, a word cloud was utilized. The primary answers highlighted in the word cloud included terms such as encryption, local storage, and external USB devices, among others, as illustrated in Figure 7.

Figure 7. Word cloud on the methods used by professionals for data protection.
Source: Author of the research, (Martinez C,2023)

The professionals list applications used for patient data management systems in Figure 8, this information is important, it was used for the subsequent analysis of vulnerabilities present in the servers that housed the records. For this task free software allowed passive scanning for security errors to quantify according to CVSS 3.0.

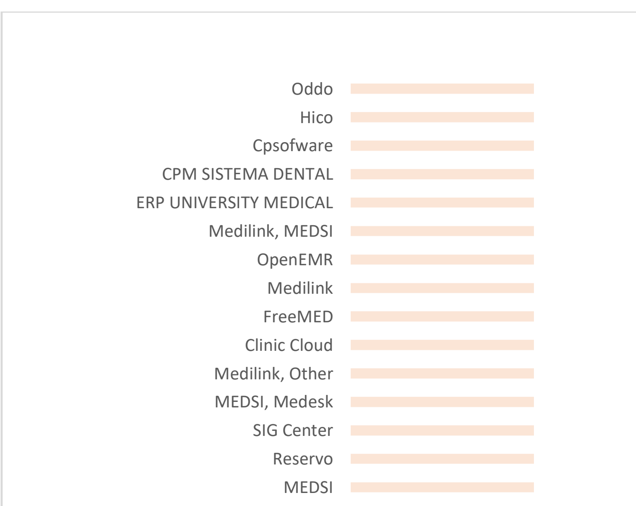

Figure 8. Patient data management systems used by healthcare professionals.

Source: Author of the research, (Martinez C,2023)

Table 6. IoMT Server Ports and Services

Name	IP	Country	Port/Service
SIG Center	34.74.107.247	ECUADOR	22/tcp open ssh 80/tcp open http 443/tcp open https 3306/tcp open mysql
SMARTSHEET	151.101.2.91	SPAIN	80/tcp open http 443/tcp open https 8008/tcp open http
Athenahealth	208.78.141.209	USA	80/tcp filtered http 135/tcp filtered msrpc 139/tcp filtered netbios-ssn 443/tcp filtered https 445/tcp filtered microsoft-ds 8008/tcp open http
Reservo	18.231.17.174	CHILE	80/tcp open http 443/tcp open https
Medilink	52.55.54.43	USA	80/tcp open http 443/tcp open https
Nimbo	199.36.158.100	USA	80/tcp open http 443/tcp open https
Clinic Cloud	3.67.61.128	SPAIN	443/tcp open https
OpenMRS	149.165.155.251	USA	22/tcp open ssh 80/tcp open http 113/tcp closed ident 443/tcp open https 8008/tcp open http 8010/tcp closed xmpp
NextGen Office	206.71.175.203	USA	80/tcp open http 135/tcp filter msrpc 139/tcp filtered netbios-ssn 443/tcp open https 445/tcp filtered microsoft-ds 8008/tcp open http
FreeMED	173.236.229.94	USA	21/tcp open ftp 22/tcp open ssh 25/tcp closed smtp 80/tcp open http 113/tcp closed ident 443/tcp open https

			587/tcp open submission 8008/tcp open http 8010/tcp closed xmpp
OpenEMR	165.227.241.138	USA	22/tcp open ssh 80/tcp open http 135/tcp filtered msrpc 139/tcp filtered net-bios-ssn 443/tcp open https 445/tcp filtered microsoft-ds 8008/tcp open http 8010/tcp closed xmpp
NOSH	192.0.78.12	USA	80/tcp open http 113/tcp closed ident 443/tcp open https 8008/tcp open http 8010/tcp closed xmpp
Solismed	69.16.202.22	USA	21/tcp open ftp 22/tcp open ssh 25/open smtp 53/tcp open domain 80/tcp open http 110/tcp open pop3 143/tcp open imap 443/tcp open https 465/tcp open smtps 587/tcp open submission 993/tcp open imaps 995/tcp open pop3s 8008/tcp open http
smarteCare	51.15.76.131	R UNITED KINGDOM	22/tcp open ssh 80/tcp open http 113/tcp closed ident 443/tcp open https 8008/tcp open http 8010/tcp closed xmpp
Oscar EMR	Not available	Not available	Not available
GNU Health	167.86.107.188	USA	80/tcp open http 135/tcp filtered msrpc 139/tcp filtered netbios-ssn 443/tcp open https 445/tcp filterd microsoft-ds 8008/tcp open http
MEDSI	104.236.173.110	MÉXICO	80/tcp open http 113/tcp closed ident 443/tcp open https 481/tcp open dvs

			8008/tcp open http 8010/tcp closed xmpp
Nubimed	54.76.166.41	DUBLIN	N/A
CPM Sistema Dental	185.213.81.171		20/tcp closed ftp-data 21/tcp open ftp 22/tcp closed ssh 80/tcp open http 113/tcp closed ident 443/tcp open https 3306/tcp open mysql 7443/tcp open oracleas-https 8008/tcp open http 8010/tcp closed xmpp 8443/tcp open https_alt 60443/tcp closed unknown

Source: Author of the research, (Martinez C,2023)

Table 7 IoMT Server Vulnerabilities according to CVSS 3.1

Name	**of Vulnerabilities**	**DoS**	**Code Execution**	**Overflow**	**Memory Corruption**	**SQL Injection**	**XSS**	**Directory Traversal**	**HTTP Response Splitting**	**Bypass something**	**Gain Information**	**Gain Privileges**	**CSRF**	**File Inclusion**	**CVSS v3.0**	**Result**
SIG Center	23	YES	YES	YES	YES	YES	YES	NO	YES	NO	YES	YES	YES	YES	10	CRITICAL
SMARTSHEET	15	YES	YES	NO	YES	NO	YES	YES	YES	NO	YES	YES	YES	NO	8	HIGH
Athena health	18	YES	YES	NO	YES	YES	YES	YES	YES	NO	YES	YES	YES	NO	9	CRITICAL
Reservo	2	YES	NO	YES	YES	NO	NO	NO	NO	NO	NO	NO	YES	NO	2	LOW
Medilink	11	YES	NO	YES	YES	YES	YES	NO	YES	YES	YES	NO	YES	NO	7	HIGH
Nimbo	5	YES	NO	NO	NO	NO	NO	NO	YES	NO	NO	NO	YES	NO	2	LOW
Clinic Cloud	3	YES	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	YES	NO	2	LOW

Open MRS	22	YES	YES	YES	YES	YES	YES	YES	YES	NO	YES	YES	YES	YES	9	CRITICAL
NextGen Office	12	YES	YES	YES	YES	YES	YES	NO	YES	YES	YES	NO	YES	NO	8	HIGH
FreeMED	12	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO	YES	NO	8	HIGH
OpenEMR	14	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES	NO	YES	NO	8	HIGH
NOSH	10	NO	NO	YES	YES	YES	YES	YES	YES	NO	YES	NO	YES	NO	6	MEDIUM
Solismed	25	YES	YES	YES	YES	YES	YES	YES	YES	NO	YES	YES	YES	YES	9	CRITICAL
Smarte Care	18	YES	YES	YES	NO	YES	NO	YES	YES	YES	NO	NO	NO	NO	8	HIGH
Oscar EMR	0	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	0	NONE
GNU Health	13	YES	YES	NO	NO	YES	NO	NO	YES	NO	NO	NO	YES	NO	7	HIGH
MEDSI	17	YES	YES	YES	NO	YES	YES	NO	YES	NO	NO	NO	YES	NO	8	HIGH
Nubimed	0	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	0	NONE
CPM Sistema Dental	25	YES	YES	YES	YES	YES	YES	YES	YES	NO	NO	NO	YES	YES	10	CRITICAL

Source: Author of the research, (Martinez C,2023)

Table 6 shows the open ports and the services running on the IoMT servers. From the analyzed servers, only two have implemented security measures, such as solutions that prevent and scan for vulnerabilities. Conversely, despite the expectation for IoMT servers to maintain a higher standard of security protocols and policies, it's apparent that certain ports and services allow the exploitation of multiple vulnerabilities. This situation poses risks to both patient data and their well-being.

Concerning the vulnerabilities found in IoMT data management servers reported by healthcare professionals, subsequent quantification based on the CVSS score reveals that 42% of vulnerabilities pose a high risk, 26% are critical, 16% demonstrate a low level of risk, and 11% do not pose any threat. These findings hold significance as an increasing number of healthcare professionals rely on information and communication technologies for managing and storing patient data. Inadequate system security not only jeopardizes sensitive information but also places patients' lives at risk.

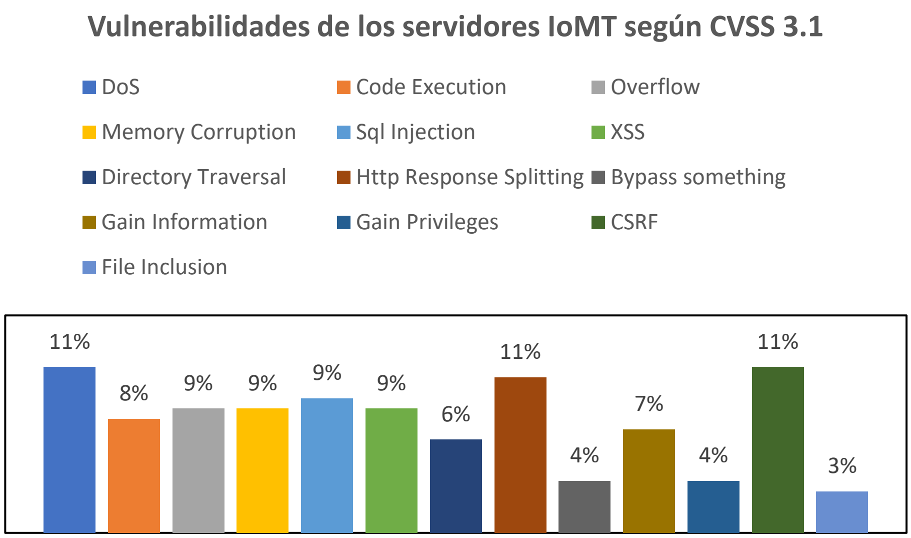

Figure 9 Count of IoMT server vulnerabilities according to CVSS 3.1
Source: Author of the research, (Martinez C,2023)

The identified recurrent vulnerabilities in the analyzed IoMT servers include susceptibility to DoS attacks, unauthorized data retrieval, and CSRF, among other potential threats. Once the multiple vulnerabilities that hackers could exploit have been identified, the next step is to mitigate them with good IT security practices.

4. Conclusions

This study presents the security threats that IoMT servers currently face. The obtained results show the various vulnerabilities present in this equipment and the serious threats they represent to privacy, confidentiality, and availability of patients' medical information. This can lead to the publication of critical data, data theft, and even the death of the patient due to the risk of the availability of these services associated with treating a pathology.

IoMT devices, from biosensors to data servers, must be treated differentially compared to other applications; for example, the implementation of strong end-to-end encryption, complemented with strong authentication methods, constant security updates, separation of IoMT networks from others, constant monitoring, among others.

Education is a critical aspect of the evolution of IoMT technology. It is vitally important for patients and healthcare professionals to learn and be aware of IoMT security. The present study shows a lack of knowledge of security issues applied to patient data; therefore, the end user continues to be the weakest segment in the information security chain.

Another important aspect to consider is the collaboration that should exist between healthcare professionals, patients, and cybersecurity experts to address the problem of insecurity in IoMT systems. Moreover, this collaboration can lead to effective measures to strengthen the privacy, availability, and reliability of these environments.

One of the main vulnerabilities found in these servers is DoS, and it is necessary to apply security patches or implement hardware or software solutions to prevent cybercriminals from exploiting it and, in turn, putting patients' lives at risk. Some solutions may include firewalls such as network traffic filters, load balancers, connection limits, adequate bandwidth, SYN flood protection, and DoS mitigation services.

Bibliographic References

[1] A. A. Mawgoud, A. I. Karadawy, and B. S. Tawfik, "A Secure Authentication Technique in Internet of Medical Things through Machine Learning," 2019, [Online]. Available: http://arxiv.org/abs/1912.12143

[2] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment," Proceedings - 2017 IEEE 42nd Conference on Local Computer Networks Workshops, LCN Workshops 2017, no. 6, pp. 112–120, 2017, doi: 10.1109/LCN.Workshops.2017.72.

[3] M. Papaioannou et al., "A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT)," Transactions on Emerging Telecommunications Technologies, no. December 2019, pp. 1–15, 2020, doi: 10.1002/ett.4049.

[4] S. Pirbhulal, W. Wu, and G. Li, "A biometric security model for wearable healthcare," in IEEE International Conference on Data Mining Workshops, ICDMW, IEEE, 2019, pp. 136–143. doi: 10.1109/ICDMW.2018.00026.

[5] A. K. Chattopadhyay, A. Nag, D. Ghosh, and K. Chanda, "A Secure Framework for IoT-Based Healthcare System," 2019, pp. 383–393. doi: 10.1007/978-981-13-1544-2_31.

[6] M. F. Khan et al., "An iomt-enabled smart healthcare model to monitor elderly people using machine learning technique," Comput Intell Neurosci, vol. 2021, 2021, doi: 10.1155/2021/2487759.

[7] H. A. M. Puat and N. A. A. Rahman, "IoMT: A Review of Pacemaker Vulnerabilities and Security Strategy," J Phys Conf Ser, vol. 1712, no. 1, 2020, doi: 10.1088/1742-6596/1712/1/012009.

[8] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, and C. Tsatsoulis, "Review of security and privacy for the internet of medical things (IoMT): Resolving the protection concerns for the novel circular economy bioinformatics," Proceedings - 15th Annual International Conference on Distributed Computing in Sensor Systems, DCOSS 2019, pp. 457–464, 2019, doi: 10.1109/DCOSS.2019.00091.

[9] F. Alsubaei, A. Abuhussein, V. Shandilya, and S. Shiva, "IoMT-SAF: Internet of Medical Things Security Assessment Framework," Internet of Things, vol. 8, p. 100123, 2019, doi: 10.1016/j.iot.2019.100123.

[10] F. Alsubaei, A. Abuhussein, and S. Shiva, "Ontology-Based Security Recommendation for the Internet of Medical Things," IEEE Access, vol. 7, pp. 48948–48960, 2019, doi: 10.1109/ACCESS.2019.2910087.

[11] M. A. Habib et al., "Privacy-based medical data protection against internal security threats in heterogeneous Internet of Medical Things," Int J Distrib Sens Netw, vol. 15, no. 9, 2019, doi: 10.1177/1550147719875653.

[12] 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.

[13] D. Nkomo and R. Brown, "Hybrid Cybersecurity Framework for the Internet of Medical Things (IOMT)," Proceedings of 12th International Conference on Global Security, Safety and Sustainability, ICGS3 2019, p. 19, 2019, doi: 10.1109/ICGS3.2019.8688030.

[14] D. Rizk, R. Rizk, and S. Hsu, "Applied layered-security model to IoMT," 2019 IEEE International Conference on Intelligence and Security Informatics, ISI 2019, p. 227, 2019, doi: 10.1109/ISI.2019.8823430.

[15] P. P. Ray, D. Dash, and N. Kumar, "Sensors for internet of medical things: State-of-the-art, security and privacy issues, challenges and future directions," Comput Commun, vol. 160, pp. 111–131, 2020, doi: 10.1016/j.comcom.2020.05.029.

[16] C. J. Martínez and S. Galmés, "Analysis of the primary attacks on IoMT Internet of Medical Things communications protocols," IEEE, 2022.

[17] A. K. Tyagi, K. Agarwal, D. Goyal, and N. Sreenath, "A Review on Security and Privacy Issues in Internet of Things," pp. 489–502, 2020, doi: 10.1007/978-981-15-0222-4_46.

[18] S. R. Khan, M. Sikandar, A. Almogren, I. Ud Din, A. Guerrieri, and G. Fortino, "IoMT-based computational approach for detecting brain tumor," Future Generation Computer Systems, vol. 109, pp. 360–367, 2020, doi: 10.1016/j.future.2020.03.054.

[19] N. T. Le and D. B. Hoang, "" Security threat probability computation using Markov Chain and Common Vulnerability Scoring System," 2018.

[20] M. B. Alexander S. Gillis, "¿Qué es CVSS_ _ Definición de TechTarget," 2023.

[21] D. Fall and Y. Kadobayashi, "The Common Vulnerability Scoring System vs. Rock Star Vulnerabilities: Why the Discrepancy?," in ICISSP 2019 - Proceedings of the 5th International Conference on Information Systems Security and Privacy, SciTePress, 2019, pp. 405–411. doi: 10.5220/0007387704050411.

[22] M. Bharadwaj R.K., J. Yeojin, and G. D. S. Borja, "Implementation of the Common Vulnerability Scoring System to Assess the Cyber Vulnerability in Construction Projects," Periodica Polytechnica Budapest University of Technology and Economics, 2020, pp. 117–124. doi: 10.3311/ccc2020-030.

[23] G. Spanos, A. Sioziou, and L. Angelis, "WIVSS: A new methodology for scoring information systems vulnerabilities," in ACM International Conference Proceeding Series, 2013, pp. 83–90. doi: 10.1145/2491845.2491871.

[24] M. Walkowski, J. Oko, and S. Sujecki, "Article vulnerability management models using a common vulnerability scoring system," Applied Sciences (Switzerland), vol. 11, no. 18, Sep. 2021, doi: 10.3390/app11188735.

[25] P. Mell, K. Scarfone, and S. Romanosky, "The common vulnerability scoring system (CVSS) and its applicability to federal agency systems," Gaithersburg, MD, 2007. doi: 10.6028/NIST.IR.7435.

[26] X. Ou and A. Singhal, "The common vulnerability scoring system (cvss)," in SpringerBriefs in Computer Science, vol. 0, no. 9781461418597, Springer, 2011, pp. 9–12. doi: 10.1007/978-1-4614-1860-3_3.

[27] A. Feutrill, D. Ranathunga, Y. Yarom, and M. Roughan, "The Effect of Common Vulnerability Scoring System Metrics on Vulnerability Exploit Delay," in Proceedings - 2018 6th International Symposium on Computing and Networking, CANDAR 2018, Institute of Electrical and Electronics Engineers Inc., Dec. 2018, pp. 1–10. doi: 10.1109/CANDAR.2018.00009.

[28] K. Gencer and F. Başçiftçi, "The fuzzy common vulnerability scoring system (F-CVSS) based on a least squares approach with fuzzy logistic regression," Egyptian Informatics Journal, vol. 22, no. 2, pp. 145–153, Jul. 2021, doi: 10.1016/j.eij.2020.07.001.

[29] J. Ruohonen, "A look at the time delays in CVSS vulnerability scoring," Applied Computing and Informatics, vol. 15, no. 2, pp. 129–135, Jul. 2019, doi: 10.1016/j.aci.2017.12.002.

[30] H. Holm and K. K. Afridi, “An expert-based investigation of the Common Vulnerability Scoring System,” Comput Secur, vol. 53, pp. 18–30, Jun. 2015, doi: 10.1016/j.cose.2015.04.012.

[31] US-CERT Security Operations Center, “NATIONAL VULNERABILITY DATABASE .” Accessed: Jul. 27, 2023. [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss

[32] M. R. Nowak, M. Walkowski, and S. Sujecki, “Support for the Vulnerability Management Process Using Conversion CVSS Base Score 2.0 to 3.x,” Sensors, vol. 23, no. 4, Feb. 2023, doi: 10.3390/s23041802.

[33] H. H. Kim and J. Yoo, “Analysis of Security Vulnerabilities for IoT Devices,” Journal of Information Processing Systems, vol. 18, no. 4, pp. 489–499, Aug. 2022, doi: 10.3745/JIPS.03.0178.

[34] MITRE Corporation, “Vulnerabilities By Types/Categories.” Accessed: Jul. 27, 2023. [Online]. Available: https://www.cvedetails.com/vulnerabilities-by-types.php