




# A review of “A comprehensive review of the state of the art on security and privacy issues in Healthcare”

Antonio López Martínez , Manuel Gil Pérez , and Antonio Ruiz-Martínez   
Faculty of Computer Science, University of Murcia, 30100 Murcia, Spain  
Email: antonio.lopez41@um.es, mgilperez@um.es, arm@um.es

**Abstract**—The healthcare industry plays a crucial role in society, and with the increasing use of technology in this field it has become a prime target for malicious activities. Cyber attacks on healthcare systems can cause serious damage to patient safety and privacy, making cybersecurity a critical concern for healthcare organizations. Recent advancements in technologies, computing systems, and wireless communications provide numerous benefits to healthcare but have also introduced new complexities and vulnerabilities. Our article provided a comprehensive review of cybersecurity in healthcare, highlighting the main stakeholders and architecture, security issues and threats, security mechanisms and research lines, as well as future research challenges in this area.

**Index Terms**—Survey, Healthcare, Security, Privacy

**Tipo de contribución:** *Investigación ya publicada*

## I. INTRODUCTION

The healthcare environment is experiencing an evolution with regard to new technologies and advances incorporated into this field, mainly with the adoption of Internet of Things (IoT), Big data, and Blockchain technologies. These technologies allows healthcare to improve all processes by achieving new purposes not addressed so far. Different types of sensors and technologies are incorporated in this environment, such as implantable and wearable medical devices (IWMDs) and body area networks (BANs), among others, improving the functionality and capacity of supervising patient health and expanding the environment’s complexity.

Security and privacy issues are major concerns, with cyber-attacks targeting hospitals and medical devices. IoT is the most adopted technology for medical devices, but its use introduces deficiencies such as integration issues, risk of failure, and security/privacy issues. Patient safety is also a concern, leading to legal frameworks categorizing medical devices and operations with certain risk levels. Protecting the healthcare environment is a top priority target.

The authors contributed with a comprehensive review of security and privacy issues in healthcare [1], including the architecture, stakeholders, technologies, and components involved. We identified threats and attacks and proposed security mechanisms, inspecting the available datasets. Our work aimed to incorporate security, privacy, and safety requirements in future implementations in this scenario, with a threat taxonomy aligned with a reference framework to provide scalability and compatibility with other related projects.

## II. MAIN FINDINGS FROM LITERATURE

The main surveys conducted on the healthcare sector were analysed, providing a holistic view of the previous literature. However, certain limitations were observed, and differences with our proposal were noted. Firstly, the overall vision of the healthcare ecosystem, including all stakeholders and technologies, has not been addressed in previous works. Thus, we presented a comprehensive scenario composed by three locations: (i) patient body, including IWMDs; (ii) Internet of Medical Things (IoMT) edge networks, with interfaces used for collecting the patient data; and (iii) central healthcare infrastructure, composed by hospitals and central services.

Secondly, there is a lack of using threat modelling in a targeted manner, with frameworks or knowledge bases in terms of threats and attacks. In our work, we incorporated threat modelling through MITRE ATT&CK to provide a reference framework and compatibility for comparison with related works and possible automation in threat modelling. Thirdly, existing works have not adequately addressed the search, enumeration, and categorisation of existing datasets in the healthcare environment. To address the issue, we inspected the main search engines specialised in datasets.

In general lines, our work provided a necessary knowledge base for further research in the medical environment, particularly in terms of security and privacy.

## III. MITRE ATT&CK ALIGNMENT AND ATTACK ENUMERATION

The decision to align the classification of threats in healthcare with a globally accessible knowledge base like MITRE ATT&CK was taken into account because these types of tools have become increasingly important in recent years for threat modelling. This alignment offers several advantages, including the compatibility of this work with other related projects and the provision of a reference framework to compare the threat classification.

While there are other alternatives, such as Cyber Kill Chain and Diamond Model, MITRE ATT&CK is the most widely adopted by the industry and community due to its comprehensive coverage of attack and defense sides and its inclusion of examples and references with data on threat groups. The knowledge base is composed of twelve categories that map to the steps executed in a cyber-attack, and it includes three different matrices for diverse scenarios.

For healthcare, we selected the Enterprise and ICS matrices because most threats found in healthcare infrastructure are

Table I  
ATTACKS ON HEALTHCARE WITH CVSS TO MEDICAL DEVICES (MITRE) CLASSIFICATION

Attack	Target	MITRE		CVSS for Healthcare	
		Category	Technique	Vector	Score
Malware	IWMD/Healthcare	Resource Development	De/Ob/StCa	AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L	5.4
Outdated OSs	Healthcare	Resource Development	ObCa	AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8
Dropbear SSH Server	Healthcare	Resource Development	CoIn	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	8.1

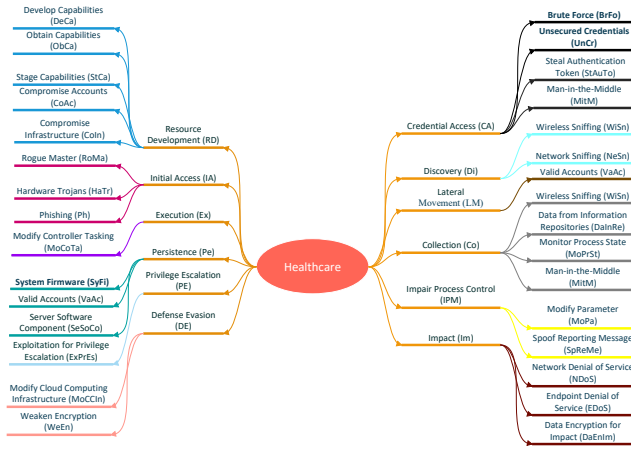


Figure 1. Threat taxonomy with MITRE ATT&CK alignment.

more related to the Enterprise matrix, and some medical devices are vulnerable to attacks similar to those found in industry-specific devices and operations. The complete threat taxonomy aligned with MITRE ATT&CK is shown in Figure 1, divided into twelve categories, nine of which are shared between Enterprise and ICS matrices, two are Enterprise-specific, and one is ICS-specific. Here, only the MITRE categories were mapped with the specific vulnerabilities and attacks identified in healthcare.

At this point, we discussed the framework used to evaluate the impact of vulnerabilities found in healthcare. The Common Vulnerability Scoring System (CVSS) v3 is the most widely used framework for vulnerability scoring, but it is not designed specifically for healthcare. Other examined alternatives include the Risk Scoring System for Medical Devices (RSS-MD) and the work of Carreon *et al.* [2], which added two new metrics to CVSS to incorporate health and privacy concerns. On the other hand, the Federal Risk and Authorization Management Program (FedRAMP) contracted MITRE to adapt the CVSSv3 to medical devices, resulting in the “Rubric for applying CVSS to medical devices”, which is the selected framework for this work.

We created two complete tables with all attacks discovered in healthcare, sorted by their category, and presented the CVSS score for each attack using the Rubric proposed by MITRE. The main difference between the MITRE Rubric and CVSSv3 is the reformulation of questions and options to evaluate the metrics, incorporating processes and data managed in healthcare. In Table I, the three first attacks are presented with their MITRE Category and Technique, the CVSS vector obtained, and the final score generated. The CVSS vector of each attack is a novel contribution performed by us answering the rubric created by MITRE.

We explained all attacks and their implication in the health-

care environment. In this paper, we explained the examples of attacks available in Table I. We detected *Malware*, *Outdated Operating Systems (OSs)*, *Dropbear SSH Server*, and *Social Engineering* as healthcare threats allocated in the *Resource Development (RD)* category. *Malware* encompasses all code that is installed in healthcare assets with malicious intentions. Newaz *et al.* [3] presented different Malware, such as “Conflicker”, a malware that allowed attackers to execute arbitrary code on vulnerable systems (X-ray machine, mammography and a gamma camera), and “Kwampirs” malware, which provides attacker to trigger equipment malfunction or delay in accessing information. *Outdated OSs* is also a very common threat in healthcare devices allowing attackers to exploit bugs fixed in newer versions. This attack is depicted in [3], where Newaz *et al.* affirmed that many devices are out of date in the medical environment. *Dropbear SSH Server*, analysed in [4], is a small Linux distribution that allows medical devices to have a SSH connection, and the incorrect protection of this server can suppose an entering point in the healthcare infrastructure.

#### IV. CONCLUSIONS

This work presented a comprehensive view of cybersecurity in healthcare, including an analysis of the architecture and main stakeholders, security, privacy, and safety requirements, and primary threats identified in the literature. These threats were formalized using MITRE ATT&CK to provide interoperability and a reference framework for comparison with other works. Additionally, we listed the main research lines and public datasets available for use in security mechanisms in healthcare. The review highlighted the challenges faced in this area and emphasized the need for continued research in topics such as access control, trust management, and telehealthcare.

#### ACKNOWLEDGMENTS

This work has been partially funded by the strategic project CDL-TALENTUM from the Spanish National Institute of Cybersecurity (INCIBE) by the Recovery, Transformation and Resilience Plan, Next Generation EU.

#### REFERENCES

- [1] A. López Martínez, M. Gil Pérez, and A. Ruiz-Martínez, “A Comprehensive Review of the State-of-the-Art on Security and Privacy Issues in Healthcare,” *ACM Comput. Surv.*, vol. 55(12), p. 249, 2023.
- [2] N. A. Carreón, C. Sonderer, A. Rao, and R. Lysecky, “A medical vulnerability scoring system incorporating health and data sensitivity metrics,” *Internat. J. Comput. Inform. Engrg.*, vol. 15, no. 8, pp. 458–466, 2021.
- [3] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, “A survey on security and privacy issues in modern healthcare systems: Attacks and defenses,” *ACM Trans. Comput. Healthc.*, vol. 2, no. 3, pp. 1–44, 2021.
- [4] A. Razaque *et al.*, “Survey: Cybersecurity vulnerabilities, attacks and solutions in the medical domain,” *IEEE Access*, vol. 7, pp. 168 774–168 797, 2019.