# Threat Modeling in Healthcare: An Analysis of Trends, Gaps, and Emerging Challenges

**Juliana Mello Severo, Juliana Silva Herbert, Muriel Figueredo Franco**

[1]Federal University of Health Sciences of Porto Alegre (UFCSPA)
Sarmento Leite, 245 – 90050-170 – Porto Alegre – RS – Brazil
*[julianase, julianash, muriel.franco]@ufcspa.edu.br*

***Abstract.*** *This study analyzes trends and gaps in the application of threat modeling approaches to healthcare systems. We examined recent works to identify how frameworks, such as STRIDE, PASTA, and LINDDUN, have been adopted and adapted across domains. The results show that their use in healthcare remains limited and largely generic, overlooking patient safety, clinical workflows, and vulnerabilities related to the Internet of Medical Things (IoMT). The findings underscore the necessity for context-aware frameworks that integrate technical, organizational, and human factors to enhance cybersecurity and risk assessment in healthcare.*

## 1. Introduction

Healthcare information systems are essential components for storing, managing, and exchanging sensitive medical data that support clinical workflows and institutional operations within healthcare organizations. Electronic Health Records (EHRs), telemedicine platforms, and Internet of Medical Things (IoMT) devices operate in interconnected networks that require both interoperability and resilience [Al-Fuqaha et al. 2023]. However, this connectivity significantly increases the attack surface, exposing healthcare infrastructures to complex cybersecurity threats that may cause technical, economic, legal, and societal impacts [Franco et al. 2023]. Incidents such as ransomware, database tampering, and large-scale data breaches have become increasingly frequent, resulting in the leakage of personally identifiable health information, service interruptions, and a loss of trust between patients and healthcare providers [Franco et al. 2025].

Established threat modeling frameworks (*e.g.*, STRIDE, DREAD, and LINDDUN) provide structured approaches to identify potential attack vectors [von der Assen et al. 2022]. These models were initially designed for general-purpose software systems and may not fully capture the specific characteristics of healthcare environments. Clinical systems operate under distinct constraints, including legacy hardware, safety-critical operations, and strict privacy regulations (*e.g.*, GDPR, LGPD, and HIPAA). Consequently, the healthcare domain presents risk scenarios in which security incidents can result in ethical, social, and clinical consequences that extend beyond technical or financial impacts [Cartwright 2023].

The increasing integration of Artificial Intelligence (AI) into both healthcare applications [Apell and Eriksson 2023] and the cybersecurity field [Mohammed 2023] introduces additional layers of complexity, which are not adequately addressed by traditional threat modeling methodologies. AI-based attackers can exploit vulnerabilities with minimal domain expertise, using automated inference and pattern recognition on leaked

data to perform targeted attacks [Li et al. 2025]. This reduces the knowledge barrier required for sophisticated intrusions, enabling model inversion attacks that threaten not only confidentiality but also the reliability of AI-driven diagnostic systems. Within this context, data leakage has become a critical threat vector: once exposed, patient data can be reused to train malicious models, risk the authentication methods, or contaminate clinical datasets.

Only a limited number of studies have attempted to map threat modeling practices in the healthcare sector. Although various frameworks are available, few have been specifically tailored to the operational and regulatory complexities of healthcare systems. The literature still lacks a comprehensive understanding of how conventional threat models, for example, *(i)* capture the specific vulnerabilities of the healthcare domain and *(ii)* account for risks such as AI-driven data leakage, adversarial manipulation, or dependencies among interoperable healthcare systems. Therefore, we advocate that existing threat models fail to capture the clinical, ethical, and operational dependencies in healthcare.

In this work, we conduct an analysis to identify efforts to apply threat models in healthcare and understand current trends in threat modeling. The goal is to highlight limitations and uncover research opportunities that could lead to domain improvements in cybersecurity practices. The focus on threat modeling in healthcare is especially relevant because security failures in this sector can directly compromise patient safety, disrupt clinical operations, and undermine public confidence in digital health infrastructures.

The remainder of this work is organized as follows. Section 2 presents briefly related work in threat modeling. Section 3 describes the methodology applied, while Section 4 presents threat modeling in healthcare evaluation and provides a discussion. Section 5 concludes the paper and gives directions for future research.

## 2. Related Work

Healthcare systems constitute safety-critical infrastructures in which failures extend beyond technical problems and may disrupt clinical decision-making and care continuity. They rely on time-sensitive processes such as emergency triage, medication management, and life-support monitoring, where even brief latency or unavailability can alter clinical outcomes [Ali et al. 2025]. These environments are constrained by regulatory requirements while supporting multidisciplinary workflows performed under intense cognitive and temporal pressure.

Early studies on threat modeling in healthcare adapted established security frameworks originally designed for general-purpose systems environments. These works demonstrated that structured threat-identification methods can help to organize and document potential risks within healthcare architectures. However, research such as [Vakhter et al. 2022], [Mehrtak et al. 2021], and [Yeng et al. 2020] highlights significant limitations. Traditional models often fail to capture healthcare-specific threats and contextual factors, leaving critical vulnerabilities unaddressed.

Although temporal criticality is often cited as a defining characteristic of healthcare, it represents only one dimension of a multi-layered challenge. In clinical domains, cyber incidents can impact not only with data integrity and confidentiality, but also with diagnostic reliability, and treatment continuity, thereby directly compromising patient

safety, as discussed in [Oster and Braaten 2025] and [Vakhter et al. 2022]. These failures tend to propagate across interconnected processes, amplifying human error and increasing the potential of irreversible harm. Nevertheless, recent threat modeling approaches still underrepresent factors such as clinical urgency, care interdependence, and patient-centered impact as core components of risk analysis.

Studies increasingly combine threat modeling with risk assessment standards and frameworks. [International Organization for Standardization (ISO-14971) 2019] and related regulations provide guidance on clinical harm and acceptable risk levels, aspects absent in models like STRIDE. The continued reliance on non-adapted models highlights a persistent methodological gap: healthcare necessitates risk assessment approaches that integrate clinical, ethical, and regulatory dimensions.

## 3. Methodology

This study employed a Systematic Literature Review (SLR) methodology to examine how threat modeling techniques are applied across different domains and to identify gaps, trends, and methodological challenges in healthcare. The review followed the PRISMA guidelines to ensure transparency, reproducibility, and consistency throughout the process [Sarkis-Onofre et al. 2021].

The methodology comprised four main stages: (a) formulation of research questions, (b) search and identification of relevant studies, (c) application of inclusion and exclusion criteria, and (d) data extraction, classification, and synthesis. The review was then guided by two research questions: (*i*) Which threat modeling frameworks and methodologies have been proposed or applied across domains? and (*ii*) What challenges and research opportunities are reported in healthcare-oriented threat modeling studies?

Initial searches were conducted across IEEE Xplore and SBC Open Lib (SOL). Then, Google Scholar was used as a search engine to aggregate results from various libraries and databases, such as IEEE Xplore, SOL, ACM Digital Library, and PubMed. The searches were made by combining terms related to threat modeling, cybersecurity risk analysis, and healthcare, resulting in the final query *("threat modeling" OR "cybersecurity risk analysis" OR "risk assessment") AND ("framework" OR "methodology") AND ("healthcare" OR "industry")*. To capture recent developments, the review was limited to papers published between 2020 and 2025. This period is also significant due to the advances in IoMT, mHealth, and AI in recent years, as well as the increase in data leakages in the healthcare sector during and after the COVID-19 pandemic. Duplicate results were removed, and titles and abstracts were screened for relevance. The inclusion criterion required that the study explicitly apply at least one threat modeling approach within the healthcare domain.

The studies were included only if they proposed, evaluated, or applied a threat modeling framework that focused on structured security risk identification or mitigation, and provided methodological details sufficient for replication or comparison. As summarized in Figure 1, after applying all criteria, 26,700 studies were initially retrieved, 32 remained after filtering, and 24 were ultimately selected for in-depth analysis. For each study, different information was identified, such as the threat modeling approach being used (*e.g.*, STRIDE, PASTA, LINDDUN, and attack trees), the application domain, the type of contribution, the identified threats and mitigations, and the reported challenges

and research directions. From the 24 full-text papers, 8 did not meet the inclusion criteria, thus resulting in 16 studies being included.

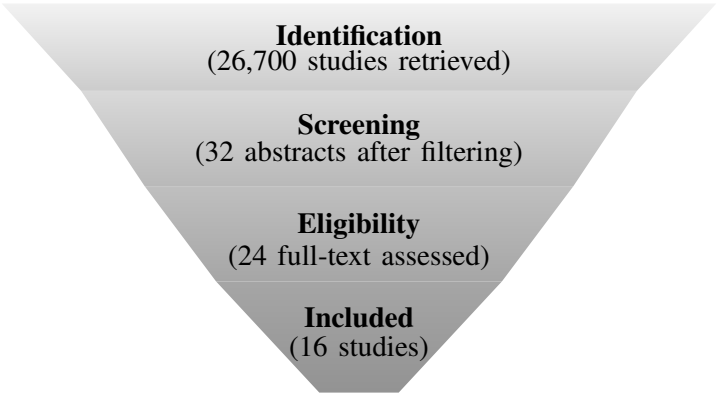


**Figure 1. Representation of the SLR methodology based on PRISMA.**

## 4. Results and Discussion

Table 1 summarizes studies examples from the analysis conducted by comparing different works. The analysis of these selected studies demonstrates that, although threat modeling has evolved and matured in recent years across various fields, its application in healthcare remains limited, fragmented, and relies mostly on general-purpose approaches. Across the reviewed literature, the STRIDE model persists as the predominant methodology, frequently used either in isolation or in hybrid configurations with PASTA or Attack Trees. This recurrence highlights STRIDE's conceptual flexibility but also reveals its limited semantic depth in addressing domain-specific risks within healthcare ecosystems.

**Table 1. Examples of threat modeling studies identified in healthcare**

| Work | Method | Domain | Main Findings |
|---|---|---|---|
| [Hossain and Hasan 2023] | STRIDE | Health Information Systems (HISs) | Highlight security practices in HISs |
| [Sobahi and Bamabad 2024] | STRIDE and DREAD | Oximeter Devices | Compares implementation complexity for different frameworks. |
| [Mauri and Damiani 2022] | STRIDE-AI | AI/ML Healthcare | Adapts STRIDE for AI/ML threats. |
| [Mehrtak et al. 2021] | STRIDE-based taxonomy | Cloud Computing | Extends STRIDE categories to cloud healthcare infrastructures. |
| [Nadifi et al. 2025] | STRIDE-based | IoTM | Emphasizes use risk assessments to analyze IoTM sensors |
| [Silvestri et al. 2023] | STRIDE and DREAD | IoTM | Uses NLP to extract threats in Healthcare Information Infrastructure (HCII) |
| [Vallabhaneni et al. 2024] | STRIDE | mHealth and IoTM | Applies STRIDE to wearable BAN devices, addressing interoperability risks. |
| [Vakhter et al. 2022] | STRIDE-based | Miniaturized Wireless Biomedical Devices (MWBD) | Propose a new threat model for MWBD. |
| [Yeng et al. 2020] | STRIDE, PASTA, and Attack Trees | Cloud Healthcare | Compare different frameworks. |

Most of the analyzed works adapt generic models to specific contexts, such as IoMT, mHealth applications, and cloud-based healthcare infrastructures. For instance, both [Vallabhaneni et al. 2024] and [Silvestri et al. 2023] utilize STRIDE to identify interoperability and data transmission vulnerabilities in IoT-driven healthcare networks.

Similarly, [Mauri and Damiani 2022] proposes STRIDE-AI, an extended version that addresses AI-specific risks in healthcare, such as model poisoning and adversarial inference. Recently, [Adesokan-Imran et al. 2025] developed a predictive threat-detection model in healthcare to identify risks earlier than framework-based assessments and to create proactive measures to safeguard. While these adaptations represent progress, they remain incremental improvements rather than conceptual advances, as they do not redefine the threat landscape based on healthcare's distinctive operational, ethical, and regulatory contexts.

A consistent observation across the reviewed corpus is that healthcare is often treated as a mere application domain rather than a unique cyber-physical environment requiring dedicated modeling paradigms. The sector's inherent dependencies (*e.g.*, real-time data availability, legacy device interoperability, and compliance with strict privacy regulations) introduce complexities that existing frameworks do not systematically capture. Consequently, none of the examined studies present an integrated taxonomy that aligns clinical safety, ethical accountability, and cybersecurity under a unified threat modeling approach. This lack of domain-oriented frameworks represents a significant research gap. Traditional models like STRIDE effectively identify common software vulnerabilities (*e.g.*, spoofing, tampering, information disclosure); yet, they fail to account for the cascading effects of cyber incidents in healthcare systems, where, for example, a single compromised telemetry device or misconfigured API may propagate errors across diagnostic, therapeutic, and administrative processes. In such safety-critical environments, the consequences of a cyber event are not merely technical but potentially clinical and life-threatening.

Furthermore, AI-driven threats remain underrepresented in current threat modeling literature. While [Mauri and Damiani 2021] takes an initial step toward integrating AI into STRIDE, comprehensive frameworks capable of modeling risk (*e.g.*, data poisoning, model inversion, and adversarial perturbations in clinical machine learning pipelines) are still lacking. The convergence of AI, IoMT, and cloud infrastructures amplifies the system's attack surface, demanding threat models that can reflect these interdependencies with analytical rigor.

Overall, our findings reveal that the state-of-the-art in healthcare threat modeling is in an emerging phase, dominated by adaptations of preexisting frameworks rather than domain-specific innovations. Future research should prioritize the development of healthcare-centric threat modeling methodologies that explicitly link technical vulnerabilities to clinical, ethical, and regulatory dimensions. Such frameworks should also promote a shared risk taxonomy between cybersecurity professionals and clinical stakeholders, fostering a common language for assessing and mitigating threats in digital health systems.

## 5. Conclusion

This study reviewed threat modeling approaches in the healthcare domain and found that, although frameworks such as STRIDE, PASTA, and LINDDUN are well established, their use in healthcare remains limited. This gap is critical given the digitalization of clinical data and the growing interconnection of medical systems and devices. Most works address generic security or privacy aspects, overlooking healthcare-specific challenges such as patient safety, regulatory compliance (*e.g.*, LGPD, HIPAA, and GDPR), and vulner-

abilities of medical IoT. Without healthcare-specific threat models, security analysis remains incomplete, and clinicians lack actionable tools to identify and mitigate threats in real-world workflows.

As future work, we propose the development of a context-aware threat modeling framework tailored to healthcare ecosystems, thereby integrating technical, organizational, and human factors. Such a framework could help bridge existing protection gaps, support more precise risk assessments, and ultimately strengthen the overall cybersecurity posture of modern healthcare infrastructures.

## References

Adesokan-Imran, T. O., Popoola, A. D., Ejiofor, V. O., Salako, A. O., and Onyenaucheya, O. S. (2025). Predictive cybersecurity risk modeling in healthcare by leveraging ai and machine learning for proactive threat detection. *Journal of Engineering Research and Reports*, 27(4):144–165.

Al-Fuqaha, A. et al. (2023). Secure access control for healthcare information systems: A body area network perspective. *IEEE Access*, 11:45621–45637.

Ali, T. E., Ali, F. I., Eyvazov, F., and Zoltán, A. D. (2025). Integrating ai models for enhanced real-time cybersecurity in healthcare: A multimodal approach to threat detection and response. *Procedia Computer Science*, 259:108–119.

Apell, P. and Eriksson, H. (2023). Artificial intelligence (ai) healthcare technology innovations: the current state and challenges from a life science industry perspective. *Technology Analysis & Strategic Management*, 35(2):179–193.

Cartwright, A. J. (2023). The Elephant in the Room: Cybersecurity in Healthcare. *Journal of Clinical Monitoring and Computing*, 37(5):1123–1132.

Franco, M. F., Granville, L. Z., and Stiller, B. (2023). CyberTEA: a Technical and Economic Approach for Cybersecurity Planning and Investment. In *36th IEEE/IFIP Network Operations and Management Symposium (NOMS 2023)*, pages 1–6, Miami, USA.

Franco, M. F., Soares, L. R., and Nobre, J. C. (2025). Saúde Sob Ataque: Da Avaliação de Riscos ao Desenvolvimento de Estratégias de Investimentos em Cibersegurança na Área da Saúde. *XXV Simpósio Brasileiro de Computação Aplicada à Saúde (SBCAS 2025)*, 36:1–44.

Hossain, M. I. and Hasan, R. (2023). Improving security practices in health information systems with stride threat modeling. In *2023 IEEE 9th World Forum on Internet of Things (WF-IoT)*, pages 1–6.

International Organization for Standardization (ISO-14971) (2019). Iso 14971:2019: Medical devices - application of risk management to medical devices. Genève, Switzerland.

Li, X., Zhang, H., et al. (2025). Adversarially-aware architecture design for robust medical ai systems. *arXiv preprint arXiv:2510.23622*.

Mauri, L. and Damiani, E. (2021). Stride-ai: An approach to identifying vulnerabilities of machine learning assets. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 147–154.

Mauri, L. and Damiani, E. (2022). Modeling threats to ai-ml systems using stride. *Sensors*, 22(17):6662.

Mehrtak, M., Alieyan, M. S., Ngwum, N., et al. (2021). Security challenges and solutions using healthcare cloud computing. *Journal of Medicine and Life*, 14(4):448–453.

Mohammed, A. (2023). The paradox of ai in cybersecurity: Protector and potential exploiter. *Baltic Journal of Engineering and Technology*, 2(1):70–76.

Nadifi, Z. et al. (2025). Stride-based threat modeling and risk assessment framework for iot-enabled smart healthcare systems. *International Journal of Online & Biomedical Engineering*, 21(9).

Oster, C. A. and Braaten, J. S. (2025). *High reliability organizations: A healthcare handbook for patient safety & quality*. Sigma Theta Tau.

Sarkis-Onofre, R., Catalá-López, F., Aromataris, E., and Lockwood, C. (2021). How to properly use the PRISMA Statement. *Systematic reviews*, 10(1):117.

Silvestri, S., Islam, S., Amelin, D., Weiler, G., Papastergiou, S., and Ciampi, M. (2023). Cyber threat assessment and management for securing healthcare ecosystems using natural language processing. *International Journal of Information Security*, 23(1):31–50.

Sobahi, N. and Bamabad, A. (2024). Cyber-attacks risk analysis of a connected pulse oximeter device: A threat modeling using stride and dread models. *International Journal for Scientific Research*, 3(5):280–315.

Vakhter, V., Soysal, B., Schaumont, P., and Guler, U. (2022). Threat modeling and risk analysis for miniaturized wireless biomedical devices. *IEEE Internet of Things Journal*, 9(15):13338–13352.

Vallabhaneni et al. (2024). Threat modeling for enhanced security in the healthcare industry with a focus on mobile health and iot. *Engineering and Technology Journal*, 9(10):5329–5331.

von der Assen, J., Franco, M. F., Killer, C., Scheid, E. J., and Stiller, B. (2022). CoReTM: An Approach Enabling Cross-Functional Collaborative Threat Modeling. In *IEEE International Conference on Cyber Security and Resilience (CSR 2022)*, pages 1–8, Rhodes, Greece.

Yeng, P. K., Wolthusen, S. D., and Yang, B. (2020). Comparative analysis of threat modeling methods for cloud computing towards healthcare security practice. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 11(11):772–784.