PeerJ Computer Science

Safeguarding the healthcare sector from ransomware attacks: insights from a literature review

Amna Shahzadi[1], Kashif Ishaq[1], Abdul Basit Dogar[1], Javed Ali Khan[2], Alexios Mylonas[2], Naeem A. Nawaz[1], Affan Yasin[3] and Fawad Ali Khan[1]

[1] School of Systems and Technology, University of Management & Technology, Lahore, Lahore, Pakistan
[2] Cybersecurity and Computing Systems Research Group, Department of Computer Science, University of Hertfordshire, Hatfield, United Kingdom
[3] School of AI and Advanced Computing, Xi'an Jiaotong University, Suzhou, China

ABSTRACT

Cybersecurity integrates a broad spectrum of concerns, addressing numerous cyber threats and malicious factors that pose significant risks to the system's integrity and functionality. Among these threats, ransomware presents a significant challenge. Often executed through phishing emails, ransomware attacks result in compromised data encrypting, with attackers demanding considerable ransoms for decryption. While these attacks target various sectors, including business, academia, and banking, the healthcare industry is particularly vulnerable due to its possession of sensitive data, the disclosure of which could lead to severe repercussions. This article provides a thorough literature review (LR) of ransomware attacks in the healthcare setup, encompassing studies from 2016 to 2024 and including an analysis of 60 articles. It addresses several critical research questions related to the topic. It also investigates the variants of ransomware targeting the healthcare sector, their propagation methods, and data encryption techniques. This article also examines the impacts of ransomware attacks on healthcare organizations, concentrating on financial losses, patient care disruptions, and data breach issues. Moreover, it examines various strategies and best practices that healthcare organizations have adopted to prevent, detect, and respond to ransomware attacks. This study analyzes ransomware attacks' legal and regulatory implications, focusing on patient data protection and compliance with the Health Insurance Portability and Accountability Act (HIPAA) and other relevant regulations. It also evaluates the effectiveness of existing cybersecurity frameworks and guidelines, like the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Health Information Trust Alliance Common Security Framework (HITRUST CSF), in aiding healthcare organizations to guard against ransomware attacks. Lastly, this article develops a taxonomy to explain the novelty and contributions of this research within the context of ransomware attacks in the healthcare sector.

Subjects Human-Computer Interaction, Computer Education, Computer Networks and Communications, Security and Privacy, Social Computing

Keywords Cyber threat, Cyber security framework, Data encryption, Malicious entities, Phishing attack, Ransomware attack, Regulatory compliance

Submitted 3 February 2025
Accepted 3 July 2025
Published 3 October 2025

Corresponding authors
Javed Ali Khan, j.a.khan@herts.ac.uk
Alexios Mylonas, a.mylonas@herts.ac.uk

Academic editor
Elad Michael Schiller

Additional Information and Declarations can be found on page 33

DOI **10.7717/peerj-cs.3073**

How to cite this article Shahzadi A, Ishaq K, Dogar AB, Khan JA, Mylonas A, Nawaz NA, Yasin A, Khan FA. 2025. Safeguarding the healthcare sector from ransomware attacks: insights from a literature review. **PeerJ Comput. Sci. 11:e3073 DOI 10.7717/peerj-cs.3073**

INTRODUCTION

In the modern era, integrating advanced technology and digital transformation has significantly increased data vulnerability to cyber threats and malicious actors (*Burke et al., 2024*; *Kok et al., 2019a*; *Razaulla et al., 2023*). The expansion of digital infrastructure in healthcare has been accompanied by a sharp rise in cybersecurity risks, particularly ransomware attacks, which have become notably prevalent and damaging (*Razaulla et al., 2023*; *Tully et al., 2020*; *Vithanwattana et al., 2021*). Ransomware spreads through malicious programs that force users to pay ransoms in exchange for access to encrypted data (*Cen et al., 2024*; *Kok et al., 2019b*; *Song, Kim & Lee, 2016*; *Zhang-Kennedy et al., 2018*; *Lawall & Beenken, 2024*; *Nagar, 2024*; *Murray, Falkeling & Gao, 2024*). These attacks are typically financially motivated, leveraging sophisticated encryption algorithms to lock critical information and demand payment for its release (*Kok et al., 2019a*; *Thamer & Alubady, 2021*; *Al-Najjar, Mahmoud & Al Najjar, 2024*; *Lee, Oh & Yim, 2017*; *Patel & Tailor, 2020*). It usually encrypts confidential data using strong encryption algorithms and demands a ransom for its decryption (*Butt et al., 2019*; *Saeed et al., 2020*).

The healthcare sector has emerged as a prime target for such attacks. Hospitals and clinics maintain large volumes of sensitive data, particularly electronic health records (EHRs), which are essential to patient care and medical operations (*Minnaar & Herbig, 2021*). Ransomware incidents in healthcare settings have disrupted medical services, endangered patient outcomes, and compromised the confidentiality of patient information (*Minnaar & Herbig, 2021*; *Zlatolas, Welzer & Lhotska, 2024*; *Zhan et al., 2024*; *Dameff et al., 2023*). Although ransomware has existed for some time, its evolution has been striking, with reported attacks increasing by 300% since 2015, and the frequency continues to grow. This surge poses significant threats to sectors like healthcare, emphasizing the need for continuous research and innovation in cybersecurity. The rising complexity of cyberattacks highlights the urgent need for adaptive, proactive strategies to safeguard against these growing risks (*Farringer, 2016*).

Hence, hospitals, which rely heavily on digital services like EHRs to store patient data, face immense challenges in safeguarding the privacy, security, and confidentiality of this sensitive information (*Nowrozy et al., 2024*; *Javaid et al., 2023*). The primary vulnerability in healthcare cybersecurity lies in human factors, as staff are often the entry point for ransomware attacks, creating substantial risks (*Spence et al., 2018*). Effective resource allocation within hospitals requires decision-makers to assess the likelihood and potential impact of cyber threats. This is crucial for prioritizing the immediate security measures and responses needed to combat such threats. A significant contributor to the rise of ransomware attacks is the presence of outdated or proprietary software, which compromises critical infrastructure and exposes healthcare organizations to further risks (*Gazzan & Sheldon, 2023*; *Chaudhary et al., 2022*; *Alshaikh, Ramadan & Hefny, 2020*; *Nawaz et al., 2023*; *Amjad et al., 2025*). By evaluating the probability and impact of various cyber threats, healthcare organizations can better allocate resources and enhance their cybersecurity posture (*Mahler, Elovici & Shahar, 2020*). The healthcare sector has already

experienced severe consequences from ransomware attacks, including unauthorized access and exfiltration of sensitive patient records.

This review targets cybersecurity researchers, healthcare IT professionals, hospital administrators, and policymakers by offering practical, evidence-based insights into ransomware threats in healthcare. The taxonomy of attack types, evaluation of commonly used datasets, and analysis of regulatory frameworks such as Health Insurance Portability and Accountability Act (HIPAA) provide actionable guidance for improving detection, prevention, and response strategies. The findings aim to support risk assessment, enhance compliance efforts, and inform the development of more robust cybersecurity protocols within healthcare institutions by bridging technical and regulatory perspectives. While previous reviews have primarily focused on the technical aspects of ransomware or general cybersecurity practices in healthcare, this study distinguishes itself by offering a comprehensive taxonomy of ransomware threats, analyzing their legal and regulatory implications (*e.g.*, HIPAA compliance), and evaluating commonly used datasets. Unlike earlier work, it bridges technical, clinical, and policy perspectives to provide a holistic view of ransomware's impact on the healthcare sector.

This study examines the various types of ransomware attacks, detailing their strategies for targeting healthcare infrastructure. It aims to highlight the strategy and tactics inherent in such attacks. Through a detailed examination, this research offers a comprehensive analysis that explores the distinct characteristics of ransomware attacks and their mechanisms for compromising sensitive healthcare information. This study introduces novel contributions to the platform of ransomware attacks in healthcare organizations:

(1) This review offers a comprehensive overview of established datasets commonly used to evaluate ransomware attacks.

(2) A comprehensive overview conducts a detailed analysis of various types of ransomware attacks within healthcare systems, focusing on their propagation mechanisms and data encryption methods aimed at extracting sensitive information or blackmailing victims. This analysis incorporates the impacts of ransomware attacks on healthcare, including financial losses, disruptions to patient care, and data breach issues.

(3) The various strategies and best practices implemented within the healthcare sector to effectively and efficiently prevent, detect, and respond to ransomware attacks are rigorously examined.

(4) A detailed analysis of the legal and regulatory implications of ransomware attacks on healthcare, particularly regarding patient data confidentiality and compliance with regulations such as HIPAA, is discussed comprehensively.

(5) This study also examines existing cybersecurity measures within frameworks and guidelines, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and Health Information Trust Alliance Common Security Framework (HITRUST CSF), highlighting challenges in adhering to these strategies to enhance and improve cybersecurity defense strategies against malicious entities.

(6) Illustrates a comprehensive taxonomy of ransomware attacks in the healthcare sector.

The structure of the article is organized as follows: 'Background' presents a review of relevant literature, discussing different types of ransomware attacks targeting the electronic health sector, preventive strategies, and the role of machine learning (ML) and deep learning (DL) in enhancing the automated detection, analysis, and response to such threats. 'Methodology' outlines the research methodology, which involves data extraction through a search strategy, rigorous quality assessment, and specific criteria for including and excluding articles. In 'Research Objectives', we formulated research inquiries regarding the types of ransomware attacks, detection, prevention, and response measures for these attacks, as well as the involvement of various regulatory bodies and compliance authorities. 'Research Questions' portrayed a taxonomy that addresses ransomware attack typologies, detection methods, prevention strategies, and response measures while discussing relevant regulatory frameworks and compliance authorities. Finally, 'Conclusion' concludes the article by presenting key insights and implications drawn from the study.

BACKGROUND

Cybersecurity remains a pressing issue across various sectors, with the healthcare industry emerging as one of the most vulnerable due to its reliance on sensitive patient data and interconnected digital systems. Among the growing threats to healthcare cybersecurity, ransomware has gained prominence as a particularly disruptive and dangerous form of attack. Ransomware is a type of malware that encrypts critical data and demands a ransom payment in exchange for data recovery or to prevent the release of private information. The healthcare sector is a prime target for such attacks due to its need for uninterrupted access to patient data and services, often making institutions more likely to pay the ransom to restore operations quickly.

To better understand this threat, a structured literature review (LR) was conducted, aimed at exploring the different variants of ransomware attacks that specifically target healthcare institutions. This methodological approach enables the identification and analysis of prior research on ransomware in healthcare, offering synthesized insights for researchers and practitioners. The review supports the integration of relevant findings into specific cybersecurity inquiries, helping shape improved protection strategies for healthcare systems.

General cybersecurity threats

Several researchers have examined cybersecurity challenges from different technological perspectives. For instance, *Abdullahi et al. (2022)* conducted a literature review on the application of artificial intelligence (AI) in detecting cybersecurity attacks within the Internet of Things (IoT) domain. Their work highlighted the growing prevalence of threats such as ransomware across various sectors, including healthcare. Moreover, they demonstrated the effectiveness of ML and DL techniques—such as support vector machines (SVM), random forests (RF), and neural networks (NN)—in identifying cyber threats. However, their review did not directly address the characteristics and impact of ransomware attacks in the healthcare domain, instead offering a broader sectoral focus.

Similarly, AI plays a pivotal role in developing natural language processing (NLP). *Shinde et al. (2024)* further contributed to the literature by discussing AI's growing role in healthcare cybersecurity, particularly through applications like natural language processing (NLP) and computer vision. They identified critical vulnerabilities in AI pipelines and recommended blockchain-based solutions to secure data integrity and system trustworthiness. Although their work addresses general cybersecurity threats and adversarial risks, it does not directly consider ransomware's unique implications in healthcare environments. Despite these valuable contributions, a noticeable gap remains in the literature and no single review comprehensively examines ransomware attacks in the healthcare sector by combining aspects such as attack types, prevention methods, AI techniques, and regulatory considerations. Most studies address only parts of the issue, often overlooking sector-specific needs, regulatory compliance, or the application of advanced technologies like ML and DL.

Healthcare-specific ransomware challenges

From a healthcare-specific perspective, *Mahmood et al. (2023)* examined the Internet of Medical Things (IoMT), which connects medical devices and systems, significantly enhancing healthcare delivery but also increasing exposure to cyber threats like ransomware. Their review stressed the importance of maintaining the confidentiality, integrity, and availability (CIA) of patient data while advocating for stronger security architectures and stakeholder engagement. Nonetheless, a significant limitation of their study was the absence of guidance on the use of AI-based technologies, such as ML and DL, for detecting or preventing ransomware attacks.

The world is growing exponentially in health departments. In a related study, AS, *Aijaz, Nazir & Mohammad (2023)* addressed the impact of technological advancements in healthcare IT, including the use of electronic health records and connected medical devices. These innovations have improved healthcare outcomes but also introduced new attack surfaces for cybercriminals. The authors evaluated Threat Modeling and Analysis (TMA) tools like STRIDE, attack trees, and attack graphs, which help in identifying potential vulnerabilities. While offering a valuable framework for assessing risk, the study did not integrate AI-based detection techniques, nor did it exclusively focus on ransomware in healthcare.

AI techniques, limitations, and research gaps (*Shinde et al., 2024*)

AI techniques, including ML and DL, have shown considerable potential in detecting and mitigating cybersecurity threats. Algorithms such as support vector machines (SVM), RF, and neural networks (NN) are particularly effective in identifying suspicious patterns and anomalies. These tools can be powerful in predicting, detecting, and potentially stopping ransomware attacks before they cause significant damage. Hence, our article comprehensively addresses the detection, prevention, and impact of ransomware attacks in the healthcare sector. It also explores various classes of ransomware attacks and the role of regulatory bodies in mitigating these threats, thoroughly examining strategies necessary to impede ransomware attacks. As illustrated in Table 1, the sections include references, titles,

Table 1 Review of ransomware attacks in healthcare.

Ref	Ransomware attacks	Health care sector	Prevention techniques	ML & DL techniques	Regulatory compliance	SLR	Date range	Database
Abdullahi et al. (2022)	Yes	No	Yes	Yes	No	Yes	2016–2021	MDPI
Shinde et al. (2024)	Yes	Yes	Yes	No	Yes	Yes	2009–2022	IEEE
Mahmood et al. (2023)	Yes	Yes	Yes	No	Yes (NIST)	Yes	2012–2023	Springer
Aijaz, Nazir & Mohammad (2023)	No	Yes	Yes	Yes	No	Yes	2016–2023	Wiley online library
This article	Yes	Yes	Yes	Yes	Yes	Yes	2016–2024	WoS

ransomware attacks, the healthcare sector, prevention techniques, ML and DL techniques, regulatory compliance, LR, data range, and databases.

The aforementioned discussion brings to light the significant amount of research on ransomware attacks in the healthcare sector. These research efforts aim to introduce various methodologies and strategies for encrypting the hospital's sensitive data, testing different tools and techniques, and determining the preventive measures necessary in the state-of-the-art technologies' algorithms responsible for the propagation of these attacks. This review we conducted brings together and summarizes the existing research comprehensively. In Table 1, the author visually compares the current study with other relevant research in the landscape of ransomware attacks, using keywords (Yes) to indicate what is included and (No) to indicate what is not included. In this context, this study uses a structured approach to mapping out the landscape of various categories of ransomware attacks to gather, categorize, and thoroughly discuss the existing knowledge related to techniques, approaches, and other essentials to identifying authors.

METHODOLOGY

To maintain the primary focus of this study, which is to review the research conducted in the area of ransomware attacks in health institutions, we have gathered insights and advice from existing methods described in various studies (*Abdullahi et al., 2022*; *Shinde et al., 2024*; *Mahmood et al., 2023*; *Aijaz, Nazir & Mohammad, 2023*). By drawing on this knowledge, we have formulated clear research objectives and devised appropriate research questions and search strategies. This approach allows us to effectively search for and identify relevant articles in the domain of ransomware attacks.

Type of review conducted

This study adopts a systematic literature review (SLR) methodology to ensure a rigorous, replicable, and transparent approach. The review protocol was developed in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to enhance the quality and reproducibility of the process.

Sources and databases

A combination of academic databases such as ACM Digital Library, IEEE Xplore, SpringerLink, Elsevier (ScienceDirect), and MDPI were used due to their comprehensive

coverage of healthcare cybersecurity and machine learning. These sources provided peer-reviewed research, technical articles, and interdisciplinary studies on topics like AI in healthcare, cybersecurity frameworks, and data protection in medical systems. Additional platforms like PubMed and Google Scholar were also consulted for a broader range of relevant studies.

Search strategy

The search string was developed using Boolean operators and relevant keywords, as detailed in the Research Strategy section. The search was conducted for publications dated between 2016 and 2024.

Screening and selection process

After removing duplicates, titles and abstracts of 1,700 initial studies were screened against predefined inclusion and exclusion criteria. Articles passing the abstract-level screening underwent full-text review to ensure they met all requirements.

Ethical considerations

To ensure transparency and integrity in the review process, all study selection steps were conducted independently by two authors and followed the PRISMA framework. Any conflicts or disagreements were resolved through discussion. No conflicts of interest were identified by the authors during the study.

Quality assessment

To ensure the reliability and validity of included studies, we applied a quality evaluation checklist, evaluating studies based on:

- Relevance to the research questions
- Clarity of methodology
- Contribution to ransomware detection/prevention
- Adherence to regulatory standards (*e.g.*, HIPAA, General Data Protection Regulation (GDPR))

Data extraction

A structured data extraction form was developed to collect the following attributes:

- Study title, authors, year, and source
- Ransomware type or category addressed
- Techniques used (*e.g.*, ML, DL)
- Sector and region of application
- Key findings and contributions
- Compliance frameworks considered (NIST, HIPAA, *etc.*)

Data synthesis

The extracted data were thematically analyzed using a narrative synthesis approach, identifying recurring patterns, research gaps, and future trends. Where possible, visual summaries (*e.g.*, tables and figures) were used to enhance clarity and comparison.

Limitations of the review

While every effort was made to ensure a comprehensive review, potential limitations include:

- Exclusion of non-English publications
- Potential publication bias favoring positive findings
- Rapidly evolving threat landscape, meaning some findings may become outdated.

RESEARCH OBJECTIVES

The research objectives for the LR on ransomware attacks are depicted in Fig. 1. The review process begins with clearly defined research questions and objectives focused on the nature, impact, and mitigation of ransomware attacks in healthcare. A structured search strategy using specific search strings was applied across major academic databases. Inclusion and exclusion criteria were used to ensure the selection of relevant, high-quality studies. The selected articles were critically analyzed, and the findings are systematically reported to inform practical cybersecurity improvements in the healthcare sector. aiming to achieve the following:

- Identify and analyze prevalent ransomware attack techniques used within the healthcare sector to encrypt confidential and sensitive data.
- To investigate and compare effective strategies to prevent and detect ransomware attacks.
- Explore various regulatory bodies and cybersecurity frameworks designed to implement checks and balances within the healthcare sector to mitigate ransomware attacks.

As illustrated in Fig. 2 (*Frumento, 2019*; *Page et al., 2021*), the research objectives encompass the research questions, strategy, selection process, analysis, and reporting.

RESEARCH QUESTIONS

The formulated questions will deal with the motivational factors behind ransomware attacks, each designed to explore distinct aspects of this malicious entity. The current LR has illuminated the various classes of ransomware attacks employed across sectors employing various ML and deep learning techniques. This review has predominantly focused on the taxonomy of ransomware attacks and their detection and prevention mechanisms alongside regulatory bodies tasked with mitigating ransomware-induced damage. The research questions are presented in Table 2, along with their underlying motivations.

Figure 1 **Research objective of ransomware attacks.** Full-size DOI: 10.7717/peerj-cs.3073/fig-1

RESEARCH STRATEGY

Search string

For ransomware attacks in the healthcare sector, the search string would be:

("Ransomware attacks") AND ("detection" OR "analysis") AND ("prevention strategies" OR "detection methods" OR "response techniques" OR "mitigation approaches" OR "defense mechanisms") AND ("cybersecurity frameworks" OR "guidelines" OR "best practices" OR "security measures") AND ("trends" OR "tactics" OR "evolving techniques" OR "emerging threats") AND ("challenges" OR "limitations" OR "impediments" OR "obstacles").

Study selection

The study selection is a critical step in the literature review process. It involves reviewing the titles and abstracts of the articles obtained through the search strategy to identify relevant studies that meet the inclusion and exclusion criteria. This step aims to reduce the number of articles to a manageable level while retaining those most likely to provide helpful information. Figure 2 portrays the steps involved in the study selection of the articles and how articles are included and excluded from the selected criteria.

Inclusion criteria

- Research publications that focus on ransomware attacks in the healthcare sector.
- Studies utilizing ML and DL techniques to address ransomware threats.

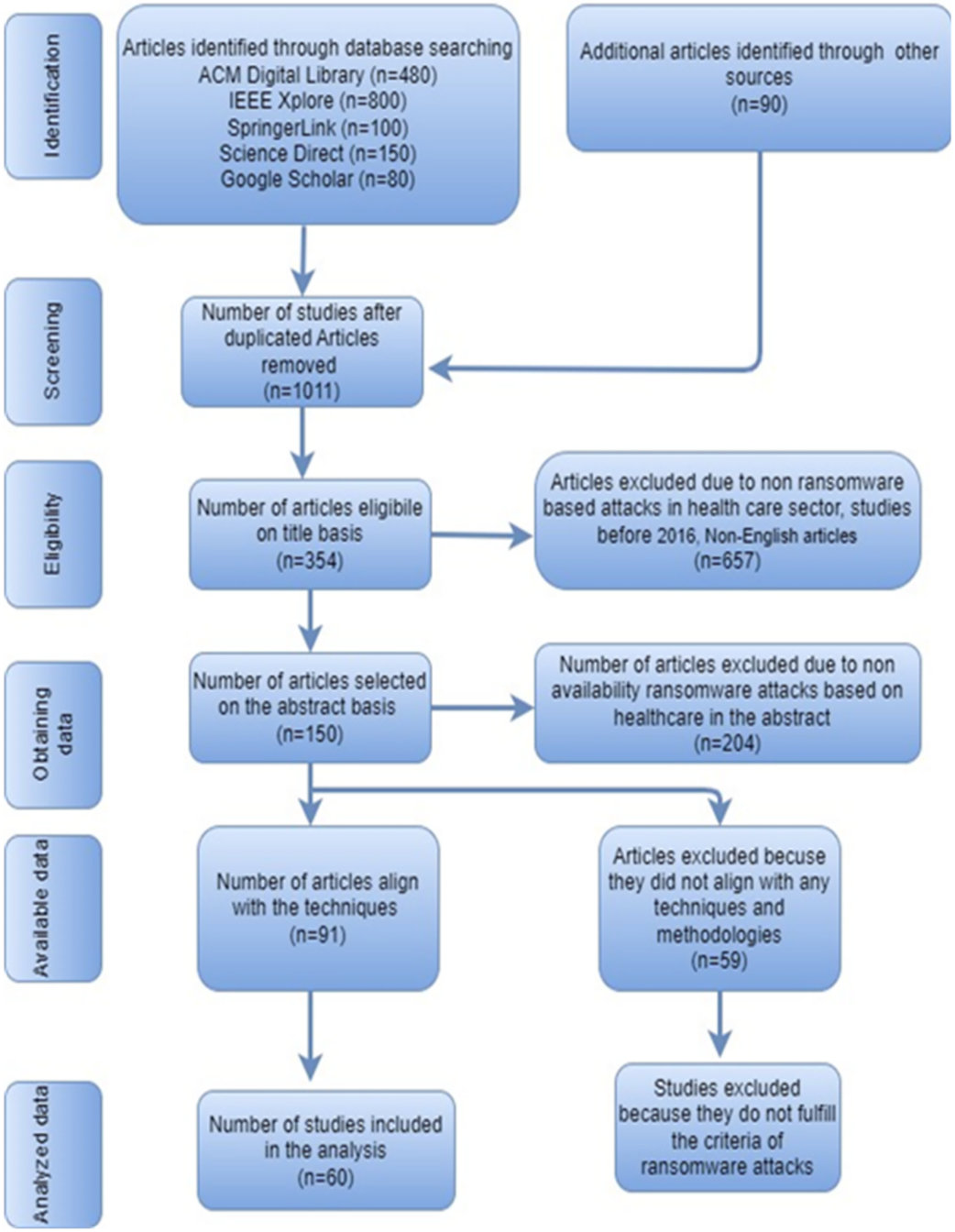

Figure 2 **Prisma diagram (*Frumento, 2019*; *Page et al., 2021*).**
Full-size DOI: 10.7717/peerj-cs.3073/fig-2

- Studies that propose or evaluate methods for discovering, ranking, and assessing security threats in healthcare systems.
- Studies that incorporate or align with HIPAA, GDPR, or NIST standards to ensure compliance and data protection.
- Publications from 2016 to 2024.

Table 2 Research questions and their motivations.

Sr. No	Research questions	Motivation
RQ 1	What methods are recommended to verify the reliability of literature on ransomware attacks and to assess its quality?	Ensure the reliability and validity of research findings to enhance the credibility and applicability of the SLR.
RQ 2	What are the common types of ransomware targeting the healthcare sector, and how do they propagate and encrypt data?	To understand the types, propagation procedures, and encryption techniques for ransomware in the healthcare sector that assist in effective cybersecurity defense.
RQ 3	What are the impacts of ransomware attacks on healthcare organizations in terms of financial losses, patient care disruption, and data breaches?	Understanding the impacts of ransomware attacks on financial losses, patient care disruption, and data breaches is important for prioritizing cybersecurity investments and strategies in healthcare organizations.
RQ 4	What strategies and best practices have healthcare organizations implemented to prevent, detect, and respond to ransomware attacks?	Identify effective strategies and best practices for preventing, detecting, and responding to ransomware attacks in the healthcare sector to safeguard patient data.
RQ 5	What are the legal and regulatory implications of ransomware attacks on healthcare organizations, particularly concerning patient data protection and compliance with HIPAA and other regulations?	Realizing the legal and regulatory implications of ransomware attacks in the healthcare environment to ensure compliance with various regulations while effectively protecting patient data
RQ 6	How effective are existing cybersecurity frameworks and guidelines, such as the NIST Cybersecurity Framework and HITRUST CSF, in helping healthcare organizations defend against ransomware attacks?	Evaluating the effectiveness of existing cybersecurity frameworks and guidelines helps determine their suitability for protecting the health sector against ransomware attacks and identifies areas for improvement.

Exclusion criteria

- Articles not published in English are excluded.
- Publications that do not focus on the healthcare sector are excluded.
- Studies focusing solely on intrusion detection, anomaly detection, or other prevention techniques without specifically addressing ransomware are excluded.
- Publications outside the 2016-to-2024-time frame are excluded.

In this study, 1,700 initial studies were retrieved for author identification from various authentic sources. As mentioned above, the selection process involved shortlisting the articles based on predefined inclusion and exclusion criteria.

***Duplicated articles*:** At the initial stage, articles that are duplicated and collected from multiple databases are carefully eliminated and discarded. Many irrelevant articles were present at this phase. After this step, only 1,011 articles remained for further assessment.

***Title-based search*:** In the second stage, articles sorted out by their titles are carefully eliminated. There were a lot of irrelevant articles at this point. After this step, only 354 articles remained to securitize them for further stages.

***Abstract-based search*:** The second step is to exclude the article based on the abstracts of the articles selected in the initial stage. The articles are organized for analysis and research methodology. After this point, there were just 150 articles left.

***Technique text-based analysis*:** At this stage, the quality of the articles is assessed. The study's analysis was based on any technique implemented in the article. Of the 150 articles, 91 articles were selected to assess further.

Table 3 Extracted articles from various publishers.

Data extract	Search string	Duplicated	Title	Abstract	Technique & methodologies	Full text
ACM	480	250	45	19	10	7
IEEE	800	478	68	16	12	11
Springer	100	89	76	25	18	14
Elsevier	150	74	67	32	14	10
MDPI	80	64	50	27	20	6
Others	90	56	48	31	17	12

***Full text-based analysis*:** At this stage, the empirical quality of the articles chosen in the earlier stage is assessed. A comprehensive text analysis of the study has been done. From 91 articles, a total of 60 articles were selected to assess the selected articles further for analysis.

Study selection results

A total of 60 articles were identified and analyzed for the answers to the RQs described above. Table 3 shows the source-wise study distribution from various article selection platforms for further consideration.

RQ1: what methods are recommended to verify the reliability of literature on ransomware attacks and to assess its quality?

Quality assessment

The following are the criteria used to assess the quality of the selected primary studies. This quality assessment was conducted by two authors as explained above.

(a) The study focuses on the Integration and Analysis of the data, the possible answers were Yes (1), and No (0).

Integration and analysis: This criterion evaluates whether the study integrates data or findings into a meaningful discussion relevant to the ransomware landscape in the healthcare sector. A score of Yes (1) is assigned if the article:

- Synthesizes various attack types or techniques (*e.g.*, phishing, brute-force attack),
- Links vulnerabilities or incidents to specific impacts in healthcare settings (*e.g.*, patient data breach, service disruption),
- Provides comparative or trend-based analysis across cases,
- Discusses mitigation strategies or correlates technical findings with real-world implications.

A score of No (0) is given if the article only reports isolated incidents or descriptive information without connecting it to broader patterns, challenges, or implications

(b) Assessment: 2021–2024 = (3), 2018–2020 = (2), 2016–2017 = (1), and before 2016 = (0).

(c) The articles are cited more than 200 = (4), 150–200 = (3), 100–149 = (2), 99–50 = (1), 49–1 = (0.5).

Table 4 Score pattern of publication channels.

Sr.	Journal	Conference	Score
1	Q1	Core A	3
2	Q2	Core B	2
3	Q3	Core C	1
4	Q4	—	0.5

(d) The study is published in a well-reputed venue that is adjudged through the CORE ranking (A, B, and C) of conferences, and for journals, letters along with scientific reports it is categorized on Scientific Journal Ranking (SJR) into Q1, Q2, Q3 and Q4 as shown in Table 4.

A comprehensive overview of ransomware attacks, detailing references, publication year, methodology, and source (like book, journal, conference or pre-prints), methodology section defines the research approach of the article (quantitative, qualitative, or mixed methods) and the specific procedures used to conduct the study along with a quality assessment. The literature review underscores the importance of cybersecurity self-evaluation in healthcare, with sources published between 2016 and 2024 in books (B), journals (J), conferences (C), or ArXiv (A). These works encompass various technical methods, denoted by (a), the year of publication is marked by (b), the number of citations each article has received, indicated by (c), and the rank of each article is denoted by (d). The final column represents the total quality assessment score, with a range where 10 is the highest and 2.5 is the lowest, indicating a moderate level of reliability and impact within the field as detailed in Table 5.

RQ2: what are the common types of ransomwares targeting the healthcare sector, and how do they propagate and encrypt data?

Ransomware attacks in the healthcare sector often exploit software vulnerabilities, social engineering, and brute-force attacks to penetrate systems and get access of the systems. These attacks use advanced encryption to lock data, demanding cryptocurrency payments for decryption. Variants such as SamSam, Locky, and WannaCry have caused significant disruptions, emphasizing the importance of regular software updates, employee training, and secure backups to mitigate threats. Effective cybersecurity measures are crucial for protecting sensitive healthcare data and maintaining patient care.

Types of ransomware attacks in health sector

These ransomware variants often utilize a combination of social engineering tactics (*Frumento, 2019*), software vulnerabilities, and brute-force attacks to infiltrate networks within the healthcare sector. Once inside, they employ sophisticated encryption techniques to render data inaccessible, demanding ransom payments in cryptocurrency for decryption keys. Cryptocurrency is an untraceable payment method that malicious parties use to receive ransom from the victims to hide their identity (*Reshmi, 2021*). Ransomware typically spreads through email attachments or malicious downloads, encrypting victims'

Table 5 Summary of extracted articles and quality assessment.

Ref	Year	Methodology	Book/Journal/Conference/Arxiv	Quality assessment				
				a	b	c	d	Total
Burke et al. (2024)	2024	Qualitative	J	1	3	0	3	7
Cen et al. (2024)	2024	Mixed	J	1	3	0.5	3	7.5
Al-Najjar, Mahmoud & Al Najjar (2024)	2024	Mixed	J	1	3	0.5	0	4.5
Zlatolas, Welzer & Lhotska (2024)	2024	Mixed	J	1	3	0.5	3	7.5
Zhan et al. (2024)	2024	Mixed	J	1	3	0.5	3	7.5
Nowrozy et al. (2024)	2024	Mixed	J	1	3	0.5	3	7.5
Aijaz, Nazir & Mohammad (2023)	2024	Mixed	J	1	3	0.5	3	7.5
Reshmi (2021)	2024	Mixed	J	1	3	0.5	0	4.5
Jobair et al. (2022)	2024	Mixed	J	1	3	0	0.5	4.5
Thakur (2024)	2024	Mixed	J	1	3	0	0	4
Guvçi & Şenol (2023)	2024	Qualitative	J	1	3	0.5	3	7.5
Al-Qarni (2023)	2024	Qualitative	J	1	3	0	0	4
Neprash et al. (2022)	2024	Mixed	J	1	3	0.5	3	7.5
Razaulla et al. (2023)	2023	Mixed	J	1	3	1	3	8
Dameff et al. (2023)	2023	Mixed	J	1	3	0.5	3	7.5
Javaid et al. (2023)	2023	Qualitative	J	1	3	1	2	7
Gazzan & Sheldon (2023)	2023	Qualitative	J	1	3	0.5	2	6.5
Shinde et al. (2024)	2023	Mixed	J	1	3	0.5	3	7.5
Mahmood et al. (2023)	2023	Qualitative	J	1	3	0.5	2	6.5
Sunil & Mathew (2024)	2023	Quantitative	B	1	3	0.5	0	4.5
Triplett (2024)	2023	Qualitative	J	1	3	0.5	0	4.5
Newaz et al. (2019)	2023	Mixed	J	1	3	0.5	1	5.5
Swasey (2020)	2023	Qualitative	J	1	3	0.5	3	7.5
van Boven et al. (2024)	2023	Qualitative	J	1	3	0.5	0	4.5
Baker & Shortland (2023)	2023	Mixed	J	1	3	0.5	0	4.5
Kolade et al. (2023)	2023	Mixed	J	1	3	0.5	2	6.5
Chaudhary et al. (2022)	2022	Mixed	J	1	3	0.5	1	5.5
Abdullahi et al. (2022)	2022	Mixed	J	1	3	4	2	10
Alenizi & Alrashdi (2023)	2022	Mixed	J	1	3	0.5	3	7.5
Branch et al. (2019)	2022	Quantitative	B	1	3	1	3	8
Ramadan et al. (2021)	2022	Mixed	J	1	3	0.5	0	4.5
Mukhopadhyay & Jain (2024)	2022	Qualitative	J	1	3	0.5	0	4.5
Vithanwattana et al. (2021)	2021	Mixed	C	1	3	0.5	2	6.5
Thamer & Alubady (2021)	2021	Qualitative	C	1	3	0.5	0	4.5
Minnaar & Herbig (2021)	2021	Mixed	J	1	3	0.5	0	4.5
Li & Madisetti (2024)	2021	Qualitative	J	1	3	2	3	8
Logue & Shniderman (2021)	2021	Mixed	J	1	3	1	2	7
Robinson, Corcoran & Waldo (2022)	2021	Qualitative	J	1	3	0.5	1	5.5
Reddy et al. (2023)	2021	Mixed	J	1	3	0.5	0	4.5
Tully et al. (2020)	2020	Qualitative	J	1	2	1	3	7

Table 5 (continued)

Ref	Year	Methodology	Book/Journal/Conference/Arxiv	Quality assessment				
				a	b	c	d	Total
Patel & Tailor (2020)	2020	Mixed	J	1	2	0.5	2	5.5
Saeed et al. (2020)	2020	Qualitative	C	1	2	0.5	1	4.5
Alshaikh, Ramadan & Hefny (2020)	2020	Qualitative	J	1	2	0.5	1	4.5
Mahler, Elovici & Shahar (2020)	2020	Mixed	A	1	2	0.5	0	3.5
Slayton (2018)	2020	Mixed	J	1	2	0.5	0	3.5
Kok et al. (2019a)	2019	Quantitative	J	1	2	3	1	7
Kok et al. (2019b)	2019	Quantitative	J	1	2	2	2	7
Butt et al. (2019)	2019	Mixed	C	1	2	0.5	0	3.5
Yeng, Yang & Snekkenes (2019)	2019	Mixed	J	1	2	0.5	2	5.5
Chernyshev, Zeadally & Baig (2019)	2019	Mixed	C	1	2	2	0	5
Blessing, Drean & Radway (2022)	2019	Mixed	C	1	2	0.5	0	3.5
Sittig & Singh (2016)	2019	Mixed	J	1	2	0.5	2	5.5
Farringer (2019)	2019	Mixed	J	1	2	2	3	8
Kandasamy et al. (2022)	2019	Mixed	J	1	2	0.5	3	6.5
Lee, Oh & Yim (2017)	2018	Qualitative	J	1	2	0.5	2	5.5
Spence et al. (2018)	2018	Mixed	J	1	2	1	1	5
Page et al. (2021)	2018	Mixed	J	1	2	0.5	1	4.5
Song, Kim & Lee (2016)	2016	Quantitative	J	1	1	3	1	6
Farringer (2016)	2016	Mixed	J	1	1	0.5	0	2.5
Nawaz et al. (2023)	2016	Qualitative	J	1	1	2	2	6

data and locking their computers. The two main types are Crypto Ransomware, which encrypts specific file types, and Locker Ransomware, which locks access to the entire system. For instance, CryptoLocker (*Kok et al., 2019b*) and Cryptowall (*Thamer & Alubady, 2021*). To mitigate the impact of ransomware attacks, healthcare organizations must implement robust cybersecurity measures, including continuous updates to anti-ransomware solutions (similar to software updates), regular system patching, comprehensive employee training on phishing awareness, and secure, regularly tested backup systems (*Reshmi, 2021*). Furthermore, ransomware attacks represent significant threats in the healthcare sector, employing diverse strategies to infiltrate and encrypt sensitive hospital information. The scareware (*Kok et al., 2019b*) Ransomware tricks victims by pretending to be authorities as well as threatening to reveal their secrets, making them pay out of fear of getting in trouble or being embarrassed. Also, variants of ransomware attacks demand user interaction, while others do not. For instance, SamSam specifically targets the healthcare department by exploiting vulnerabilities in Remote Desktop Protocol (RDP), File Transfer Protocol (FTP), and Java servers. Additionally, Locky ransomware is activated through user interaction, often distributed *via* phishing emails that contain malicious payloads (*Minnaar & Herbig, 2021*). On the other hand, WannaCry spreads swiftly without requiring user interaction, leading to instant and widespread disruptions.

Notably, WannaCry gained attention in 2017 for exploiting vulnerabilities within Windows systems and utilizing worm-like capabilities to propagate across interconnected networks rapidly (*Butt et al., 2019*; *Mahler, Elovici & Shahar, 2020*; *Jobair et al., 2022*; *Thakur, 2024*; *Guvçi & Şenol, 2023*). This ransomware propagates by exploiting unpatched software, highlighting the crucial role of timely updates and security patches in defending against these cyber threats. However, ransomware variants like Ryuk and SamSam (*Al-Qarni, 2023*) Gain entry into healthcare networks through phishing emails or by exploiting weak authentication credentials and unprotected remote access points. Once inside the network traffic, attackers precisely target crucial and sensitive data, such as patient records and administrative files, for encryption. The encryption methods used by ransomware employ advanced algorithms, making the data inaccessible without the precise decryption key, which the attackers demand in exchange for ransom payments. These incidents highlight the urgent need for robust cybersecurity protocols. Essential measures include comprehensive employee training to identify phishing tactics, proactive monitoring of network activities, and the implementation of secure backup solutions.

Overall, several high-impact ransomware strains have uniquely targeted the healthcare sector, each with distinct technical mechanisms and consequences. SamSam is notorious for exploiting weak Remote Desktop Protocol (RDP) credentials through brute-force attacks, allowing attackers to gain access to hospital networks and manually deploy custom-built payloads that bypass traditional antivirus tools. Once inside, SamSam encrypts entire systems using RSA and AES algorithms, crippling core operations. WannaCry, on the other hand, spread globally in 2017 by exploiting the EternalBlue vulnerability in the SMB protocol. Its worm-like behavior enabled it to propagate rapidly across unpatched systems without user interaction, encrypting files with AES and demanding ransom in Bitcoin, infamously disrupting the UK's NHS. Ryuk uses a multi-stage attack, often delivered through Emotet or TrickBot malware, which enables credential theft and lateral movement across the network before encrypting high-value systems. Ryuk disables backups and shadow copies, making data recovery extremely difficult. Locky typically spreads *via* phishing emails containing macro-enabled Office attachments. Once opened, it connects to command-and-control servers to execute encryption using AES and appends distinctive extensions like. locky. Lastly, Netwalker gained traction during the COVID-19 pandemic by targeting overwhelmed healthcare institutions. Operated as a ransomware-as-a-service (RaaS), it uses phishing and exploits to infiltrate systems, then conducts double extortion by encrypting and exfiltrating data, threatening public leaks if ransoms are not paid. These strains illustrate the evolving sophistication of ransomware threats and their devastating impact on healthcare delivery and patient safety.

These strategies are essential for mitigating the severe impacts of ransomware attacks on electronic health operations and ensuring the protection of patient care and the confidentiality of their data. Table 6 summarizes key ransomware types affecting healthcare organizations, highlighting their impact, methods of propagation, encryption techniques, and ransom demands. Attacks like Crypto ransomware, WannaCry, and Ryuk have caused major disruptions by encrypting critical systems and demanding

Table 6 Variants of ransomware attacks in the healthcare sector.

Ref	Ransomware type	Impact on healthcare organizations	Propagation method	Encryption technique	Ransom demand
Kok et al. (2019b), *Thamer & Alubady (2021)*, *Butt et al. (2019)*, *Farringer (2016)*, *Sunil & Mathew (2024)*, *Li & Madisetti (2024)*	Crypto ransomware	Forced shutdown of electronic health records (EHR) systems	Spreads through phishing emails or malicious links	Often uses symmetric encryption, primarily AES (Advanced Encryption Standard).	45 bitcoins = $19,000
Butt et al. (2019), *Mahler, Elovici & Shahar (2020)*, *Reshmi (2021)*, *Sunil & Mathew (2024)*, *Triplett (2024)*, *Alenizi & Alrashdi (2023)*, *Li & Madisetti (2024)*, *Yeng, Yang & Snekkenes (2019)*	WannaCry	Causing widespread system outages and disrupting patient care in healthcare organizations.	Exploiting SMB (Server Message Block) Vulnerabilities	Combines AES for file encryption and RSA for key encryption.	Bitcoin
Kok et al. (2019b), *Minnaar & Herbig (2021)*, *Newaz et al. (2019)*, *Li & Madisetti (2024)*	Locky ransomware	It disrupts healthcare organizations by encrypting critical patient data and medical record	Typically spreads *via* phishing emails with a Word document attachment containing malicious macros	Uses RSA-2048 and AES-128 encryption algorithms.	Bitcoin
Sunil & Mathew (2024), *Triplett (2024)*, *Newaz et al. (2019)*, *Li & Madisetti (2024)*	NetWalker	Encrypting data and disrupting healthcare operations, compromising patient records and confidentiality	Phishing Emails, exploiting vulnerabilities	Uses AES encryption with a customized implementation	Cryptocurrency
Newaz et al. (2019)	Ryuk	Leading to extensive data encryption, operational disruptions, and financial losses.	Phishing Emails, exploiting RDP	Employs AES-256 for data encryption and RSA-2048 for key encryption	Bitcoin
Kok et al. (2019b)	Scareware	Causes fear and operational disruption without real data encryption.	Fake warnings or phishing emails.	No real encryption used; relies on social engineering tactics.	Cryptocurrency

cryptocurrency payments. Most propagate *via* phishing or by exploiting system vulnerabilities, using strong encryption methods like Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA). Scareware, while not using actual encryption, relies on fear tactics to extort victims. The data emphasizes the need for robust cybersecurity measures in healthcare settings.

RQ3: what are the impacts of ransomware attacks on healthcare organizations in terms of financial losses, patient care disruption, and data breaches?

Ransomware attacks cause significant financial losses, disturb patient care, and lead to data breaches in healthcare organizations. These attacks can also responsible to force hospitals to pay ransoms, face operational costs, and invest in cybersecurity upgrades. Patient care is delayed due to system inaccessibility, while data breaches expose sensitive patient

information, damaging reputation and resulting in legal and regulatory penalties. Hence, comprehensive strategies are essential to mitigate these impacts.

Impacts of ransomware attack in the health sector

Ransomware attacks have an unfavorable impact on the sensitivity of hospital data, leading to financial losses, interruptions in patient care, and data breaches. Below is an analysis of how ransomware attackers contribute to these economic losses, disruptions in patient care, and other adverse events in healthcare organizations. Moreover, ransomware attacks have complicated impacts on healthcare organizations, including severe financial losses, disruptions in patient care, and compromised data security. From a financial perspective, these attacks impose direct costs, including ransom payments that often leave no traceable record, that can escalate depending on the ransomware variant and the volume of data encrypted (*Kok et al., 2019b*; *Zlatolas, Welzer & Lhotska, 2024*; *Reshmi, 2021*). Additionally, healthcare providers face considerable expenses in alleviating operational disruptions, conducting forensic investigations, and implementing cybersecurity enhancements to prevent future incidents. Patient care disruption is a major concern (*Frumento, 2019*; *Neprash et al., 2022*; *Sunil & Mathew, 2024*; *Triplett, 2024*; *Newaz et al., 2019*; *Swasey, 2020*) appointments, and compromised medical records. Moreover, such disruptions can threaten patient safety and compromise the quality of care provided. Data breaches resulting from ransomware attacks usually expose sensitive patient information to unauthorized access, potentially violating healthcare privacy regulations and triggering legal consequences. The long-term penalties include damaged reputation (*Thamer & Alubady, 2021*; *Minnaar & Herbig, 2021*) loss of patient trust and data (*Sunil & Mathew, 2024*; *van Boven et al., 2024*), and regulatory fines and insurance-related costs (*Minnaar & Herbig, 2021*), further intensifying the financial (*Thamer & Alubady, 2021*; *Frumento, 2019*; *Neprash et al., 2022*; *Baker & Shortland, 2023*), and operational burden on healthcare organizations (*Frumento, 2019*). Also, it is essential to implement effective insurance against ransomware attacks that require a public-private partnership, with governments navigating through co-insurance, regulation, and investment (*Baker & Shortland, 2023*). However, mitigating these impacts necessitates comprehensive cybersecurity strategies, robust incident response protocols, and continuous staff training to reinforce defenses and safeguard patient welfare and organizational resilience against evolving cyber threats. As explained in Table 7, the impacts and types of losses associated with ransomware attacks in the healthcare sector are detailed.

RQ4: what strategies and best practices have healthcare organizations implemented to prevent, detect, and respond to ransomware attacks?

With the growing threat of ransomware attacks targeting healthcare organizations through various sophisticated methods, including advanced encryption algorithms, the need for effective mitigation strategies has become critical. These attacks often prevent data owners from immediately recovering their information or decrypting it at once. As outlined below, numerous preventive measures are essential to effectively combat these ransomware attacks.

Table 7 Impacts of ransomware attack in the healthcare sector.

Ref	Impact	Description	Types of losses
Thamer & Alubady (2021), *Minnaar & Herbig (2021)*, *Zlatolas, Welzer & Lhotska (2024)*, *Thakur (2024)*, *Branch et al. (2019)*, *Li & Madisetti (2024)*, *Slayton (2018)*, *Yeng, Yang & Snekkenes (2019)*	Financial losses	Costs incurred due to ransom payments, operational disruptions, fines, and insurance premiums.	Ransom payments, operational disruption costs, financial penalties (*e.g.*, regulatory fines), insurance costs
Kok et al. (2019b), *Zlatolas, Welzer & Lhotska (2024)*, *Jobair et al. (2022)*, *Slayton (2018)*, *Yeng, Yang & Snekkenes (2019)*	Operational disruptions	Disruptions in patient care, operational inefficiencies, and downtime in accessing critical systems and electronic health records (EHRs).	Ransom payments, operational disruption costs, financial penalties (*e.g.*, regulatory fines), insurance costs (premiums, claims, deductibles)
Zlatolas, Welzer & Lhotska (2024), *Jobair et al. (2022)*, *Thakur (2024)*, *Guvçi & Şenol (2023)*, *Branch et al. (2019)*, *Slayton (2018)*, *Yeng, Yang & Snekkenes (2019)*, *Chernyshev, Zeadally & Baig (2019)*	Patient care impact	Delays in treatments and procedures, risks to patient safety, and impact on overall quality of care.	Treatment delays, patient safety concerns, quality of care impact
Thamer & Alubady (2021), *Minnaar & Herbig (2021)*	Reputational damage	Diminished trust among patients and stakeholders, negative publicity, and potential loss of customer base.	Loss of trust, damage to reputation, customer loss
Minnaar & Herbig (2021)	Legal and regulatory impact	Legal expenses, fines for non-compliance with data protection laws, and costs associated with compliance remediation.	Legal fees, regulatory fines, compliance remediation costs
Minnaar & Herbig (2021), *Swasey (2020)*	Insurance related costs	Costs related to cyber insurance premiums, claims, deductibles, and policy adjustments.	Cyber insurance premiums, claims and deductibles, policy adjustments

Prevention measures in the health sector

Emerging cyber threats are increasing drastically and ransomware attacks are most favorite for the attackers to launch due to instant results with encrypting devices and demanding ransom. However, it is quite impossible to retrieve everything swiftly, without executing the plans of disaster recovery and backup strategy and it is a matter of fact that the foundation for implementing prevention strategies lies in the business continuity plan (*Spence et al., 2018*; *Tully et al., 2020*; *Vithanwattana et al., 2021*) and data backup procedures (*Vithanwattana et al., 2021*; *Thamer & Alubady, 2021*; *Spence et al., 2018*). The healthcare industry has undoubtedly integrated Information and Communication Technology (ICT) to significantly enhance the valuable and sensitive infrastructure of hospital platforms. This digitalization, beginning with the computerization of hospital environments has made the healthcare sector a prime target for cybercriminals seeking to compromise sensitive patient information due to the unawareness of employees (*Spence et al., 2018*; *Frumento, 2019*) and bring various devices into the organization. Therefore, it is crucial to implement effective risk mitigation strategies within the healthcare landscape (*Frumento, 2019*). Currently, hospitals are increasingly adopting digital technologies, including digital devices, which makes them vulnerable to digital assaults. Indeed, medical devices, increasingly connected to networks and the Internet, face cybersecurity threats like ransomware, which can disable devices, disrupt their operations and compromise patient data (*Kolade et al., 2023*).

The healthcare sector also combats ransomware by implementing some conventional methods like network segmentation with firewalls (*Tully et al., 2020*; *Butt et al., 2019*), conducting rigorous risk assessments for medical devices, *Mahler, Elovici & Shahar (2020)* and integrating various technologies (*Triplett, 2024*). Hospitals also prioritize software and system updates with automated patch management to mitigate ransomware risks effectively. Therefore, it is crucial to implement optimal strategies to mitigate financial costs, unforeseen business losses, and reputation damage resulting from these severe attacks. Similarly, key risk mitigation techniques include developing business continuity plans, maintaining data backups, and educating employees about ransomware threats (*Vithanwattana et al., 2021*; *Thamer & Alubady, 2021*; *Spence et al., 2018*).

Apart from conventional methods, some of the novel methods are also there to impede the way of ransomware attacks like as threat identification, ontology-based likelihood, severity decomposition, and risk integration (TLDR) methodology to assess these risks by identifying vulnerabilities and using expert input to estimate likelihood and severity (*Mahler, Elovici & Shahar, 2020*). In addition to methodologies, emerging techniques are playing a crucial role in enhancing the cybersecurity of the healthcare sector. Various techniques like Blockchain (*Vithanwattana et al., 2021*; *Al-Qarni, 2023*; *Alenizi & Alrashdi, 2023*), Software Defined Networking (SDN) and ML are instrumental in combating cyber threats (*Jobair et al., 2022*). These technologies reinforce systems, detect anomalies, and make a strong barrier against potential threats, thereby preventing the compromise of data and services (*Thamer & Alubady, 2021*).

Table 8 outlines various strategies and best practices that healthcare organizations can implement to prevent, detect, and respond to ransomware attacks, along with their descriptions, implementation methods, effectiveness, challenges, and examples.

Detection strategies in the health sector

Detecting ransomware presents a challenging challenge, prompting healthcare organizations to employ various methods like deploying intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor and mitigate malicious activities attentively. IDS and IPS are critical in detecting and preventing ransomware attacks by monitoring and analyzing network traffic for suspicious activities (*Branch et al., 2019*). IDS identifies potential threats by comparing network patterns against known vulnerabilities and signatures, providing early warnings. IPS actively blocks malicious traffic and entities, preventing ransomware from entering the network premises (*Ramadan et al., 2021*; *Mukhopadhyay & Jain, 2024*). They also enforce end-user security measures like restricting website access and deploying network segmentation to mitigate ransomware attacks efficiently. Moreover, end-to-end security balances these systems by ensuring comprehensive protection through strong authentication techniques and performing continuous monitoring of all devices (*Tully et al., 2020*; *Ramadan et al., 2021*; *Mukhopadhyay & Jain, 2024*). Likewise, penetration testing works as a strong pillar among the detection strategies (*Mukhopadhyay & Jain, 2024*). Collectively, these measures establish a solid defense strategy against ransomware attacks. In addition to traditional approaches, ML techniques have emerged as powerful tools for the early detection of

Table 8 Prevention measures of ransomware attack in the healthcare sector.

Ref	Prevention strategy	Implementation	Challenges	Examples in healthcare organizations
Tully et al. (2020), *Vithanwattana et al. (2021)*, *Spence et al. (2018)*, *Thakur (2024)*, *Al-Qarni (2023)*	Proper business continuity and disaster plans	Assessing risks, developing strategies, and training staff	Resource constraints, technological issues, and the evolving threat landscape	Hospitals performing continuous testing and updates to ensure readiness and adaptation to new threats
Vithanwattana et al. (2021), *Thamer & Alubady (2021)*, *Spence et al. (2018)*, *Al-Qarni (2023)*	Adequate data backups	Risk assessment and planning, adopting backup rules and plans	Challenges that need to be addressed through careful planning, resource allocation, and continuous improvement.	Hospitals implemented backup plans to restore their sensitivity at the time of any unfavorable event
Spence et al. (2018), *Thakur (2024)*, *Al-Qarni (2023)*, *van Boven et al. (2024)*, *Yeng, Yang & Snekkenes (2019)*, *Blessing, Drean & Radway (2022)*	Employee education on ransomware	Critical need to enhance employee education and awareness programs to mitigate these risks	Consistently to ensure that all employees can identify and respond properly to potential cybersecurity threats	Hospitals conducting monthly cybersecurity awareness training
van Boven et al. (2024), *Yeng, Yang & Snekkenes (2019)*	Implementing bring your own device (BYOD)	Implement robust mobile device management (MDM) solutions to secure devices used in the healthcare environment.	Ensuring data security, maintaining regulatory compliance, managing diverse devices, providing adequate IT support, and safeguarding patient privacy.	Implementing BYOD in hospitals involves deploying robust mobile device management (MDM) solutions,
Tully et al. (2020), *Butt et al. (2019)*	Network segmentation	Implementing firewalls to separate sensitive data and critical systems to limit the spread of ransomware	Complex implementation requires ongoing maintenance	Hospitals segment administrative and clinical networks.
Mahler, Elovici & Shahar (2020), *Thakur (2024)*	Identify risks and assess risk methodology	Identify vulnerable components, estimate likelihood, and severity level with expert input	Requires significant resources and expertise and updates for emerging threats	Hospitals assess risks for networked devices, manufacturers integrate security into the design
Vithanwattana et al. (2021), *Jobair et al. (2022)*, *Sunil & Mathew (2024)*, *Newaz et al. (2019)*, *Baker & Shortland (2023)*	Usage of emerging technologies like blockchain, software defined networking (SDN), and ML	Ensure performance and address privacy concerns, do network segmentation	Integrating complexities ensure data accuracy and protect the privacy of patient's data	Hospitals manage patient records effectively, supply chain integrity, and fraud detection in the billing system
Thamer & Alubady (2021)	Ensuring all software and systems are up-to-date and not pirated with the latest security patches.	Automated patch management systems and don't use pirated software	Requires constant monitoring and management	Hospitals segment administrative and clinical networks.

ransomware, particularly in critical environments like smart healthcare systems (SHS). One such method is the Pre-Encryption Detection Algorithm (PEDA), which applies ML to detect crypto-ransomware in its early stages by analyzing API call patterns. With a low false positive rate of 1.56%, PEDA has demonstrated superior performance compared to

Table 9 Detection strategies of ransomware attack in healthcare sector.

Ref.	Detection strategy	Implementation	Challenges	Examples in healthcare organizations
Neprash et al. (2022), *Logue & Shniderman (2021)*, *Sittig & Singh (2016)*	Use of intrusion detection/ prevention systems (IDS/IPS)	Deploying IDS/IPS and SIEM solution across the network	High cost, requires skilled personnel to manage	Large healthcare systems using SIEM for real-time threat monitoring.
Tully et al. (2020), *Neprash et al. (2022)*, *Logue & Shniderman (2021)*	Continuous monitoring and response to threats on endpoints.	Implementing EDR solutions on all workstations and servers.	Resource-intensive needs constant updates	Hospitals use EDR to monitor and respond to endpoint threats.
Javaid et al. (2023), *Neprash et al. (2022)*, *Li & Madisetti (2024)*	Penetration testing	Engaging third-party security firms for tests.	Costly, requires external expertise	Health systems performing penetration tests.
Kok et al. (2019b), *Al-Qarni (2023)*	Pre-encryption detection algorithm (PEDA)	ML algorithms analyze API data	High false positive rates and complex data patterns	Detecting ransomware before it encrypts patient records.
Chernyshev, Zeadally & Baig (2019)	Smart healthcare system (SHS)	ML techniques (ANN, decision tree, random forest, k-NN) to detect malicious activities in SHS	Difficult to train the ML model on diverse data, maintaining high accuracy, and handling new and evolving security threats	Detection of unauthorized access and prevention of tampering with medical devices

other detection algorithms (*Kok et al., 2019b*; *Li & Madisetti, 2024*). Similarly, HealthGuard is an ML-based security framework designed to detect malicious activities in SHS, utilizing techniques like artificial neural network (ANN), decision tree (DT), random forest (RF), k-Nearest Neighbor (kNN), and decision tree. Trained on data from eight devices, HealthGuard achieves 91% accuracy and a 90% F1-score in threat detection, addressing security concerns in IoT-integrated medical devices (*Newaz et al., 2019*). Table 9 outlines the detection strategies for ransomware attacks in the healthcare sector.

Responsive attitude in the health sector

Responsive behavior involves having detailed disaster recovery plans in place to enable a quick and efficient recovery if an attack occurs (*Spence et al., 2018*; *Reshmi, 2021*). Additionally, responding to incidents effectively by implementing measures such as regularly updating incident response plans with training and maintaining automated backups stored offsite to ensure data integrity and rapid recovery is crucial (*Al-Najjar, Mahmoud & Al Najjar, 2024*; *Reshmi, 2021*). Many hospitals and clinics prioritize these practices to enhance their resilience against cyber threats. Protecting the organization's reputation is crucial to minimize the impact and costs associated with an attack. These combined strategies help healthcare facilities prevent ransomware attacks and respond effectively to minimize damage and ensure continuity. Moreover, ransomware attacks are rising, and cyber insurance provides crucial coverage for related costs, helping businesses recover quickly. It also offers preventive and mitigative services to reduce the likelihood and impact of attacks. By supporting organizations before and after breaches, cyber insurance covers it to some extent, but sometimes it is also a costly solution

Table 10 Responsive measures of ransomware attack in the healthcare sector.

Ref	Responsive strategy	Implementation	Challenges	Examples in healthcare organizations
Spence et al. (2018), *Li & Madisetti (2024)*	Disaster recovery plans	Comprehensive data backup protocols, ensuring off-network storage, and conducting regular backup tests	Challenges include convincing healthcare staff to adhere strictly to these protocols, particularly avoiding personal email and maintaining up-to-date user education.	Hospitals enforce user education and security policies.
Al-Najjar, Mahmoud & Al Najjar (2024), *Sittig & Singh (2016)*	Incident response plan	Developing and regularly updating an incident response plan and conducting drills.	Requires regular updates and training	Hospitals have a detailed incident response plan and conduct regular drill.
Al-Najjar, Mahmoud & Al Najjar (2024), *Li & Madisetti (2024)*	Data backups and recovery	Implementing automated backup systems with offsite storage.	Ensuring backup integrity and a quick restoration process	Clinics and hospitals with daily automated backups stored offsite.
van Boven et al. (2024), *Robinson, Corcoran & Waldo (2022)*, *Sittig & Singh (2016)*	Cyber insurance	Cyber insurance and conduct a full assessment of IT capabilities	High costs, varying levels of coverage, and potential exclusions like loss of revenue from downtime	Healthcare organizations obtaining cyber insurance to protect against the financial impacts of cyberattacks

(*Kolade et al., 2023*; *Branch et al., 2019*; *Logue & Shniderman, 2021*). Table 10 demonstrates the responsive measures to ransomware attacks in the healthcare sector.

RQ5: what are the legal and regulatory implications of ransomware attacks on healthcare organizations, particularly concerning patient data protection and compliance with HIPAA and other regulations?

The healthcare sector significantly faces many challenges to protect and safeguard sensitive patient information, especially in the face of rising ransomware attacks. These attacks disrupt healthcare delivery and increase legal and regulatory concerns, especially about patient data protection. It is critical to ensure robust cybersecurity measures, timely breach reporting, and the secure use of EHRs. Additionally, frameworks like the Computer Fraud and Abuse Act (CFAA) and CISA highlight ongoing challenges in enforcement and collaboration across the healthcare industry.

Legal and regulatory implications of ransomware attacks

The healthcare sector is a diverse field and it has to be tackled from almost every perspective which is why it needs some sort of regulatory body to take care of it, maintain the records of patients in a better way and ensure cybersecurity (*Robinson, Corcoran & Waldo, 2022*). It allocates resources effectively and efficiently, all while ensuring comprehensive employee training and timely breach reporting. The HITECH Act compounds these challenges by requiring the adoption and meaningful use of EHRs, implementing advanced security measures, and integrating compliance with HIPAA (*Tully et al., 2020*; *Vithanwattana et al., 2021*; *Minnaar & Herbig, 2021*; *Farringer, 2016*; *Mahler, Elovici & Shahar, 2020*; *Frumento, 2019*; *Reddy et al., 2023*). The CFAA, which criminalizes unauthorized access to computers and networks, faces jurisdictional concerns

and the emerging nature of cyberattacks (*Page et al., 2021*), making enforcement difficult. CISA's voluntary information-sharing framework struggles with limited participation and the need for significant infrastructure development to facilitate effective communication (*Slayton, 2018*). Moreover, the Affordable Care Act (ACA) is responsible for quality reporting requirements that add another layer of complexity, necessitating continuous adjustments to compliance strategies among evolving cyber threats. Likewise, CMS plays a pivotal role in regulating and setting standards for healthcare delivery, payment, and quality improvement initiatives across the United States (*Tully et al., 2020*).

Similarly, the General Data Protection Regulation (GDPR) addresses the protection of personal data related to an individual's physical or mental health, including healthcare services that reveal information about their health status (*Zlatolas, Welzer & Lhotska, 2024*). In the hospital sector, healthcare professionals are often the weakest link in the security chain, significantly contributing to data breaches (*Yeng, Yang & Snekkenes, 2019*; *Chernyshev, Zeadally & Baig, 2019*). Several other factors intensify these challenges, necessitating the modernization of existing laws, a shift in industry priorities towards IT security, the demand for better products from vendors, and the utilization of available resources to enhance security protections. Similarly, financial institutions strive to comply with anti-money laundering (AML) regulations, but cryptocurrencies largely circumvent these rules, enabling anonymous transfers. Regulators could enforce AML regulations for cryptocurrency transactions, particularly through virtual currency exchanges (VCEs) that convert cryptocurrency to fiat currency. This would involve VCEs verifying customer identities and monitoring large transfers. Global AML initiatives, such as the Financial Action Task Force (FATF), could contribute to reducing ransomware-related transactions to some extent (*Blessing, Drean & Radway, 2022*).

Healthcare providers face significant compliance challenges due to the complexity of regulations, rapid technological changes, resource limitations, and evolving cyber threats. Addressing these challenges requires continuous updates to laws, a multifaceted approach to compliance, and leveraging existing resources and guidance to enhance security measures (*Farringer, 2016*). Table 11 describes ransomware attacks' legal and regulatory implications within the healthcare sector.

RQ6: how effective are existing cybersecurity frameworks and guidelines, such as the NIST cybersecurity framework and HITRUST CSF, in helping healthcare organizations defend against ransomware attacks?

The NIST Cybersecurity Framework (CSF) and HITRUST CSF are widely recognized as essential tools for healthcare organizations to defend against ransomware attacks. These frameworks offer structured approaches to managing cybersecurity risks, including measures for safeguarding EHRs and ensuring regulatory compliance. By emphasizing the importance of collaboration between IT professionals and healthcare end-users, these guidelines enable robust security measures to be implemented. Despite their effectiveness, evolving cyber threats highlight the need for continuous updates within these frameworks to maintain strong defenses against ransomware attacks.

Table 11 Legal and regulatory implications of ransomware attack in the health sector.

Ref.	Regulatory body	Implications	Regulatory requirements	Compliance challenges
Tully et al. (2020), *Vithanwattana et al. (2021)*, *Minnaar & Herbig (2021)*, *Zlatolas, Welzer & Lhotska (2024)*, *Farringer (2016)*, *Mahler, Elovici & Shahar (2020)*, *Kolade et al. (2023)*, *Yeng, Yang & Snekkenes (2019)*, *Kandasamy et al. (2022)*	Health insurance portability and accountability act (HIPAA)	HIPAA sets the standard to protect sensitive patient data and deals with protected health information (PHI)	Privacy rule, security rule, breach notification rule	Complexity of regulations, continuous updates, data breaches, training and awareness
Farringer (2016), *Kolade et al. (2023)*, *Page et al. (2021)*	Health information technology for economic and clinical health (HITECH) act	HITECH was enacted to promote the adoption of health information technology. And strengthened the enforcement of HIPAA by increasing penalties for non-compliance	Meaningful use, breach notification	Interoperability standards, meaningful use requirements, increased penalties for HIPAA violations
Farringer (2016), *Page et al. (2021)*	Computer fraud and abuse act (CFAA)	CFAA is a federal law that criminalizes unauthorized access to computers and networks.	Unauthorized access, penalties	Jurisdictional issues, anonymity of attackers
Farringer (2016), *Reddy et al. (2023)*	Cybersecurity information sharing act (CISA)	CISA promotes the sharing of cybersecurity threat information between the government and the private sector.	Information sharing between the government and private sector, Protection from Liability to share information by the act	Voluntary participation, infrastructure development, and effective coordination between different entities is a hectic task
Farringer (2016)	Affordable care act (ACA)	ACA includes programs that require healthcare providers to implement quality reporting and "meaningful use" regulations for EHRs.	Meaningful use of EHR, and quality reporting requirements to improve patient care and health outcomes.	Must be coordinated with HIPAA and HITECH requirements, the evolving nature of cyber threats requires continuous adjustments, Resource Allocation: Balancing the need to invest in HER (electronic health records) adoption and security enhancements.
Tully et al. (2020)	CMS centers for medicare and medicaid services (CMS).	Maintain effective antivirus software, emphasizes cybersecurity measures to protect patient data and ensure operational continuity in hospitals	Hospitals must develop, implement, and maintain antivirus software capable of preventing unauthorized cyberattacks	Updating outdated systems to support effective antivirus solutions and ensuring ongoing maintenance
Mukhopadhyay & Jain (2024)	Anti-money laundering (AML)	Cryptocurrency exchanges and businesses must follow AML regulations	Reporting and paying taxes on cryptocurrency transactions	Keep accurate and timely reporting and ensure compliance across various jurisdictions
Blessing, Drean & Radway (2022), *Farringer (2019)*	GDPR	Ensures the protection and privacy of personal data for individuals	Implement data protection measures, conduct security audits, ensure lawful processing of personal data	Balancing security with healthcare provision, training staff on GDPR compliance

Table 12 Cybersecurity frameworks and guidelines for a ransomware attack in the healthcare sector.

Ref.	Framework/ Guideline	Description	Key components	Effectiveness against ransomware	Challenges	Healthcare implementation example
Kolade et al. (2023), *Kandasamy et al. (2022)*, *Nawaz et al. (2023)*	NIST	Strategies for enhancing ransomware resilience in healthcare settings through a socio-technical approach	Systematic installation, configuration, Continuous monitoring of the system, Rapid response and recovery	Strengthen defenses against ransomware with system security, educate users, detect threats early, and mitigate impacts	Maintaining comprehensive protection in the healthcare sector, ensuring ongoing staff training,	Healthcare organizations can apply these strategies to safeguard (EHRs) against ransomware, aligned with NIST guidelines
Neprash et al. (2022), *Alenizi & Alrashdi (2023)*	NIST cybersecurity framework (CSF)	Voluntary framework with guidance for improving cybersecurity.	Identify, protect, detect, respond, recover	Managing ransomware risks through its structured approach encompassing identification, protection, detection, response, and recovery strategies	Requires continuous updates and resources	Large hospital networks use it for risk assessments and incident response
Spence et al. (2018)	HIPAA security rule	US regulation for protecting electronic personal health information (ePHI).	Administrative, physical, technical safeguards	Securing patient data through comprehensive encryption methods, both at rest and during transactions	If ransomware only encrypts files and does not steal information, the attack may not be considered a HIPAA breach.	HIPAA ensures compliance while enhancing security and ensuring comprehensive data encryption at all times
Blessing, Drean & Radway (2022)	HSPAMI	Designed to analyze and improve the security practices of healthcare staff	Assessing, monitoring, security practices, implementing, reward systems	Prevention, detection, response, and recovery against ransomware attack	Resource allocation, staff engagement, balancing core duties, regulatory complexity	The hospital implements HSPAMI by conducting regular security training sessions and observational audits to assess staff to follow security protocols
Chernyshev, Zeadally & Baig (2019)	HealthGuard	An ML-based security framework for smart healthcare systems	ML techniques, ANN, DT, RT, k-NN	Highly effective in detecting and mitigating ransomware due to its ML techniques	Training on diverse data sets, ensuring low false positive rates	Continuous monitoring of patient vitals and automatic alert generation for potential critical conditions

Cybersecurity frameworks and guidelines in the health sector

Effective response and collaboration between health IT professionals and end-users are crucial to implementing robust security measures and securing EHR systems. It involves proper installation, user-focused strategies, and continuous monitoring according to NIST guidelines (*Reddy et al., 2023*; *Sittig & Singh, 2016*; *Farringer, 2019*). The CSF and other authoritative guidelines support these efforts. While NIST provides a broad range of standards and guidelines, the NIST CSF is a specific tool designed to help organizations manage and mitigate cybersecurity risks. Existing frameworks such as the NIST CSF and HITRUST CSF are instrumental in helping healthcare organizations strengthen their defenses against ransomware attacks.

The HIPAA Security Rule is like a foundational US regulation that mandates administrative, physical, and technical safeguards to protect patients' electronic personal health information (ePHI). It emphasizes comprehensive encryption methods to secure patient data at rest and during transactions. However, ransomware attacks that solely encrypt files without exfiltrating data may not always trigger HIPAA breach notifications (*Spence et al., 2018*). The NIST CSF offers a voluntary yet structured approach through its

five core functions of Identify, Protect, Detect, Respond, and Recover that help to manage ransomware risks effectively (*Mukhopadhyay & Jain, 2024*; *Kandasamy et al., 2022*). Similarly, the Healthcare Security Practice Analysis, Modeling, and Incentivization (HSPAMI) framework is employed to analyze and enhance the security practices of healthcare staff. It integrates observational measures with incentivization strategies that ensure regulatory compliance to enhance overall security within healthcare organizations (*Yeng, Yang & Snekkenes, 2019*).

Beyond conventional strategies and frameworks, the Smart Healthcare System (SHS), demonstrated by HealthGuard, presents an innovative approach for continuously monitoring patient's vital signs and automatically detecting and preventing critical diseases through ML techniques. HealthGuard utilizes four distinct ML-based detection methods—ANN, decision tree, random forest, and k-nearest neighbor to identify and mitigate malicious activities within an SHS, thereby enhancing security and improving patient care (*Newaz et al., 2019*).

However, challenges such as the need for continuous updates and significant resource allocation remain dominant. Despite these challenges, many large hospital networks utilize the NIST CSF to conduct risk assessments and implement incident response strategies. This demonstrates its practical application and effectiveness in strengthening healthcare cybersecurity defenses against evolving ransomware threats. Table 12 presents the cybersecurity frameworks and guidelines for addressing ransomware attacks in the healthcare sector.

TAXONOMY OF RANSOMWARE ATTACKS IN THE HEALTHCARE SECTOR

We portrayed ransomware attacks in the healthcare sector through a comprehensive taxonomy in which we explain that ransomware attacks in the healthcare sector are increasingly prevalent, involving various types like cryptocurrency-based attacks, Ryuk, Netwalker, and WannaCry. These attacks can hinder the smooth path of communication systems, cause significant financial losses, and halt critical operations, directly affecting patient care setup and damaging the reputation of the healthcare sector. Healthcare organizations must implement robust detection, prevention, and response strategies and techniques to address these threats. Detection methods include continuous network monitoring, IDS, IPS, and behavioral analysis to identify anomalies and irregularities. Prevention methods involve rigorous cybersecurity protocols, employee training sessions, and regular system updates to mitigate vulnerabilities. In the event of an attack, a swift and coordinated response plays a pivotal role, involving incident response teams, data backup systems, recovery plans, and effective communication with relevant authorities. Regulatory bodies such as HIPAA, the Computer Fraud and Abuse Act (CFAA), the Cybersecurity Information Sharing Act (CISA), and the Affordable Care Act (ACA) guide healthcare organizations to maintain rigorous cybersecurity measures. Frameworks like the HIPAA Security Rule and the NIST Cybersecurity Framework (CSF) provide guidelines to help healthcare institutions safeguard against ransomware attacks and avoid major casualties. As illustrated in Fig. 3 presents a comprehensive taxonomy of ransomware attacks in the

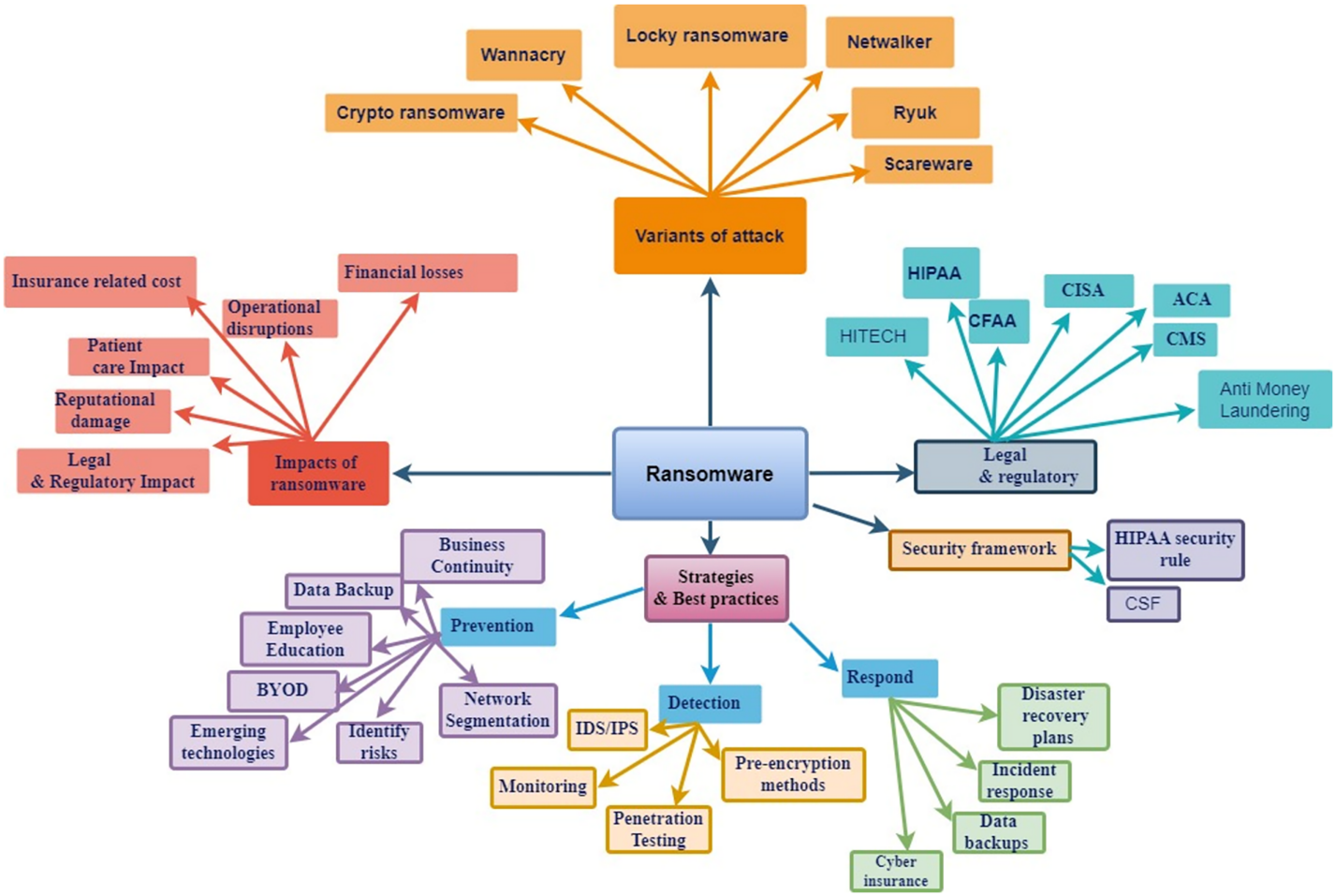

Figure 3 **Taxonomy of ransomware attacks in the healthcare sector.** Full-size DOI: 10.7717/peerj-cs.3073/fig-3

healthcare sector, outlining five interconnected domains: attack variants, impacts, legal and regulatory compliance, strategies and best practices, and security frameworks. It categorizes major ransomware types such as Wannacry, Ryuk, and Locky under crypto ransomware, illustrating the range of threats faced by healthcare institutions. The impacts of ransomware are shown to extend beyond financial losses, including operational disruptions, patient care delays, reputational damage, legal consequences, and increased insurance costs. On the regulatory side, frameworks like HIPAA, HITECH, CFAA, and CISA emphasize the importance of data protection and compliance, while the HIPAA Security Rule and the Cybersecurity Framework (CSF) guide security implementations. Strategies to combat ransomware are divided into prevention (*e.g.*, data backup, employee education, network segmentation), detection (*e.g.*, IDS/IPS, monitoring, penetration testing), and response (*e.g.*, incident response plans, disaster recovery, cyber insurance). Overall, the taxonomy illustrates how these elements collectively define the threat landscape and response framework for ransomware in healthcare.

DISCUSSION

This literature review provides a comprehensive exploration of ransomware attacks in the healthcare sector, reflecting on the strategies, impacts, and frameworks involved in both their propagation and mitigation. Six critical research questions (RQs) guided this inquiry, each addressing essential dimensions of ransomware threats and responses within healthcare environments.

RQ1: verifying the quality of literature

The application of a structured quality assessment framework ensured the credibility of selected studies. Most articles met high standards in terms of methodological clarity, relevance, and scientific contribution, with many appearing in top-tier journals and conferences between 2016 and 2024. The emphasis on peer-reviewed sources and citation analysis strengthened the trustworthiness of the data extracted. This systematic approach supports the reliability of the synthesized findings and ensures that the strategies and observations drawn are grounded in rigorous research.

RQ2: types and propagation of ransomware

The review identified prevalent ransomware variants—such as WannaCry, SamSam, Locky, and Ryuk—known for exploiting vulnerabilities in healthcare infrastructure. These attacks typically propagate *via* phishing, remote desktop protocol (RDP) exploits, and software vulnerabilities. Notably, the speed and autonomy with which some variants like WannaCry spread highlight the urgent need for real-time detection and automated responses. Techniques like encryption of critical data and demand for cryptocurrency-based ransom place immense pressure on healthcare operations. These findings underscore the importance of regular system updates, phishing awareness training, and the deployment of intrusion detection systems.

RQ3: impact on healthcare systems

Ransomware attacks have significant financial, operational, and reputational consequences. Financially, healthcare institutions are burdened by ransom payments, system restoration costs, legal penalties, and long-term investments in cybersecurity upgrades. Operational disruptions directly impact patient care, delaying treatments, cancelling appointments, and jeopardizing patient outcomes. Additionally, data breaches result in the unauthorized exposure of sensitive health information, leading to loss of public trust and potential legal ramifications. The multifaceted impact emphasizes the necessity of integrating robust, pre-emptive cybersecurity protocols within healthcare organizations.

RQ4: strategies for prevention, detection, and response

This study highlights a range of conventional and advanced strategies employed by healthcare providers. Traditional approaches like business continuity planning, data backups, firewalls, and employee training remain foundational. However, the adoption of cutting-edge solutions—including blockchain technology, AI-driven detection models like

HealthGuard and PEDA, and network segmentation—demonstrates the industry's evolution toward a more proactive security posture. Pre-encryption detection, machine learning algorithms, and end-to-end monitoring systems emerged as critical components of effective defence mechanisms. Notably, frameworks like threat likelihood decomposition and risk integration (TLDR) exemplify integrated risk assessment models that aid in tailoring defences to specific vulnerabilities.

RQ5: legal and regulatory implications

Compliance with legal and regulatory frameworks is integral to the healthcare sector's cyber-resilience. The review reveals that acts such as HIPAA, GDPR, and HITECH form the backbone of data protection laws, mandating healthcare organizations to uphold stringent security standards and report breaches promptly. However, challenges remain in enforcing laws like the CFAA and promoting voluntary collaboration under CISA due to jurisdictional and infrastructural limitations. The complexity and dynamic nature of these legal requirements demand continuous education and adaptation by healthcare administrators, especially as new threats and technologies emerge.

RQ6: effectiveness of cybersecurity frameworks

Frameworks like the NIST Cybersecurity Framework and HITRUST CSF were generally found effective in providing structured guidance on cybersecurity practices. These frameworks support a layered security approach, encompassing identification, protection, detection, response, and recovery. Nevertheless, challenges persist in their implementation, particularly among smaller institutions with limited resources. Emerging threats also necessitate regular updates to these frameworks to ensure their continued relevance. Encouragingly, some hospitals have successfully adapted these frameworks into routine operations, illustrating their practical value when adequately supported.

Synthesis and implications

The synthesis of findings suggests a crucial need for a multifaceted and continuously evolving cybersecurity posture in the healthcare sector. Technological solutions—particularly those involving AI and machine learning—show promise but must be backed by sound legal frameworks, organizational policies, and user education. Institutions must strike a balance between adopting cutting-edge innovations and ensuring regulatory compliance to manage risks effectively. Future research should focus on empirical validations and performance benchmarking of AI-driven detection models within a live healthcare environment.

Comparative design approach to ransomware strain analysis

To enhance the analytical depth of this study, a comparative design approach was integrated into the synthesis process to evaluate the behavioral, technical, and operational distinctions between prominent ransomware strains targeting healthcare. This involved systematically extracting and aligning data points across multiple dimensions, such as initial attack vectors, propagation techniques, encryption methods, impact severity, and ransom tactics. For instance, the comparison between WannaCry and SamSam revealed

stark differences in delivery: while WannaCry propagated automatically through the EternalBlue SMB vulnerability, SamSam required manual deployment following brute-force RDP access. Similarly, Ryuk's multi-stage architecture involving credential theft and lateral movement was assessed alongside Locky's reliance on macro-enabled email attachments and command-and-control (C2) communication. Netwalker was further distinguished by its double extortion strategy, combining encryption with data exfiltration under the RaaS model. By capturing these differences through a comparative lens, the review enabled a structured evaluation of how varying technical features influence the scale of disruption and defense requirements in healthcare contexts. This comparison is visually supported in Table 6 and enriches the overall methodological rigor by linking literature synthesis to evidence-based threat profiling.

Limitations and future work

Literature-centric scope

This study primarily adopts a systematic literature review (SLR) methodology and does not include any empirical experimentation or real-world deployment of the techniques discussed. While the SLR provides valuable theoretical insights and consolidates existing research, it lacks validation through practical implementation or case-based testing in real healthcare settings, which may limit its applicability.

Rapid evolution of threat landscape

Ransomware tactics evolve rapidly, with attackers constantly developing new methods of intrusion and data encryption. Given the dynamic nature of these threats, some of the strategies and countermeasures identified in the reviewed literature may quickly become outdated. The current review may not fully reflect the most recent attack variants or defense tactics that emerged after the literature search window.

Absence of performance benchmarking

Although the article explores various ML and DL approaches for ransomware detection and prevention, it does not provide a comparative evaluation of these techniques. Without benchmarking across standardized datasets, it remains unclear which algorithms perform best in healthcare contexts concerning accuracy, efficiency, or adaptability.

Language and data source bias

The review only considers English-language publications and excludes gray literature, such as industry reports or non-peer-reviewed technical documentation. As a result, practical and context-specific knowledge—especially from non-English-speaking regions or small-scale healthcare institutions—may have been overlooked.

Generalization across diverse healthcare settings

The findings and recommendations presented in this review apply broadly to the healthcare sector without distinguishing between different types of organizations. Smaller clinics, regional hospitals, or under-resourced health facilities may have unique vulnerabilities or limitations that are not adequately captured in this generalized synthesis.

Future work

Empirical validation of detection and response methods

Future studies should focus on implementing and validating AI-based detection and response strategies in live healthcare environments. Testing these methods under realistic operational conditions will provide insights into their practical effectiveness, usability, and robustness against real-time ransomware threats.

Unified framework for ransomware mitigation

There is a clear need to develop an integrated and adaptive ransomware mitigation framework that combines real-time monitoring, anomaly detection, incident response, and legal compliance. Such a framework would offer a holistic solution tailored specifically for the healthcare domain and align with both organizational workflows and regulatory requirements.

Comparative analysis of AI techniques

Future research should conduct rigorous comparative studies of AI and ML algorithms using standardized healthcare-specific datasets. Evaluating metrics such as detection rate, false positives, latency, and scalability will help determine the most suitable techniques for different healthcare applications and institutional sizes.

Ethical, legal, and privacy considerations

While technical approaches are essential, future work must also address ethical and privacy issues. This includes concerns about data ownership, algorithmic bias, transparency in decision-making, and ensuring compliance with privacy regulations like HIPAA and GDPR when using AI-driven tools.

Simulation and scenario-based risk assessments

Developing simulation tools and risk modelling platforms could allow healthcare institutions to test their cybersecurity readiness. Simulations can help evaluate how ransomware propagates through digital infrastructure and assess the effectiveness of response strategies under different threat scenarios.

Standardization and policy development

There is a pressing need for collaborative initiatives between researchers, policymakers, and healthcare providers to develop standardized cybersecurity policies and incident response protocols. This would help establish uniform guidelines for ransomware prevention and support coordinated responses across national and international healthcare systems.

CONCLUSION

Ransomware remains a growing and complex threat to the healthcare sector, exploiting technical vulnerabilities, human error, and outdated infrastructure to compromise sensitive data, disrupt essential services, and demand substantial ransoms. Despite the existence of regulatory frameworks such as HIPAA, NIST, and HITRUST CSF, many

healthcare organizations continue to face significant challenges in fully implementing and maintaining effective cybersecurity practices. This review has provided a structured synthesis of existing literature, including a taxonomy of ransomware attack types, propagation methods, impacts, and mitigation strategies, while also examining legal and regulatory implications. The taxonomy serves as a valuable framework for understanding the various facets of ransomware attacks, categorizing them based on their methods and effects. Additionally, the review highlights the emerging role of advanced technologies like machine learning, deep learning, and blockchain in enhancing detection, prevention, and response mechanisms. However, several critical questions remain unanswered, including how machine learning models can be effectively trained on diverse, privacy-sensitive healthcare datasets; how blockchain solutions can be adapted for low-resource hospital settings; and how AI-based detection systems can be optimized for real-time clinical environments with minimal false positives. Furthermore, questions around policy standardization across decentralized healthcare networks persist. Overall, the findings emphasize the need for a comprehensive, multidisciplinary approach to healthcare cybersecurity, one that combines technological innovation with regulatory compliance and organizational readiness to effectively counter the evolving ransomware threat.

ADDITIONAL INFORMATION AND DECLARATIONS

Funding

The authors received no funding for this work.

Competing Interests

The authors declare that they have no competing interests.

Author Contributions

- Amna Shahzadi conceived and designed the experiments, performed the experiments, performed the computation work, prepared figures and/or tables, authored or reviewed drafts of the article, and approved the final draft.
- Kashif Ishaq conceived and designed the experiments, performed the experiments, analyzed the data, performed the computation work, prepared figures and/or tables, authored or reviewed drafts of the article, and approved the final draft.
- Abdul Basit Dogar conceived and designed the experiments, prepared figures and/or tables, authored or reviewed drafts of the article, and approved the final draft.
- Javed Ali Khan conceived and designed the experiments, authored or reviewed drafts of the article, and approved the final draft.
- Alexios Mylonas performed the experiments, authored or reviewed drafts of the article, and approved the final draft.
- Naeem A. Nawaz performed the experiments, performed the computation work, prepared figures and/or tables, authored or reviewed drafts of the article, and approved the final draft.

- Affan Yasin analyzed the data, authored or reviewed drafts of the article, and approved the final draft.
- Fawad Ali Khan analyzed the data, performed the computation work, prepared figures and/or tables, and approved the final draft.

Data Availability

The following information was supplied regarding data availability:

This is a literature review.

REFERENCES

Abdullahi M, Baashar Y, Alhussian H, Alwadain A, Aziz N, Capretz LF, Abdulkadir SJ. 2022. Detecting cybersecurity attacks in internet of things using artificial intelligence methods: a systematic literature review. *Electronics* **11(2)**:198 DOI 10.3390/electronics11020198.

Aijaz M, Nazir M, Mohammad MNA. 2023. Threat modeling and assessment methods in the healthcare-IT system: a critical review and systematic evaluation. *SN Computer Science* **4**:714 DOI 10.1007/s42979-023-02221-1.

Alenizi J, Alrashdi I. 2023. SFMR-SH: secure framework for mitigating ransomware attacks in smart healthcare using blockchain technology. *Sustainable Machine Intelligence Journal* **2(4)**:1–19 DOI 10.61185/SMIJ.2023.22104.

Al-Najjar Y, Mahmoud R, Al Najjar Y. 2024. Cybersecurity in healthcare industry. *Available at www.globalscientificjournal.com*.

Al-Qarni EA. 2023. Cybersecurity in healthcare: a review of recent attacks and mitigation strategies. *International Journal of Advanced Computer Science and Applications* **14(5)**:135–140 DOI 10.14569/IJACSA.2023.0140513.

Alshaikh H, Ramadan N, Hefny HA. 2020. Ransomware prevention and mitigation techniques general terms. *International Journal of Computer Applications* **117(40)**:31–39 DOI 10.5120/ijca2020919899.

Amjad K, Ishaq K, Nawaz NA, Fadhilah Rosdi ABD, Khan FA. 2025. Unlocking cybersecurity: a game-changing framework for training and awareness—a systematic review. *Human Behavior and Emerging Technologies* **2025(1)**:91 DOI 10.1155/hbe2/9982666.

Baker T, Shortland A. 2023. The government behind insurance governance: lessons for ransomware. *Regulation & Governance* **17(4)**:1000–1020 DOI 10.1111/rego.12505.

Blessing J, Drean J, Radway S. 2022. Survey and analysis of U.S. policies to address ransomware. *MIT Science Policy Review* **3**:38–46 DOI 10.38105/spr.iyuyqypkzm.

Branch LE, Eller SW, Bias TK, McCawley MA, Myers DJ, Gerber BJ, Bassler JR. 2019. Trends in malware attacks against United States healthcare organizations. *Available at www.jglobalbiosecurity.com*.

Burke W, Stranieri A, Oseni T, Gondal I. 2024. The need for cybersecurity self-evaluation in healthcare. *BMC Medical Informatics and Decision Making* **24(1)**:11676 DOI 10.1186/s12911-024-02551-x.

Butt UJ, Jahankhani H, Abbod M, Jamal A, Lors A, Kumar A. 2019. Ransomware threat and its impact on SCADA. In: *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*. Piscataway: IEEE.

Cen M, Jiang F, Qin X, Jiang Q, Doss R. 2024. Ransomware early detection: a survey. *Computer Networks* **239(2)**:110138 DOI 10.1016/j.comnet.2023.110138.

Chaudhary S, Kakkar R, Jadav NK, Nair A, Gupta R, Tanwar S, Agrawal S, Alshehri MD, Sharma R, Sharma G, Davidson IE. 2022. A taxonomy on smart healthcare technologies: security framework, case study, and future directions. *Journal of Sensors* **2022(1)**:1863838 DOI 10.1155/2022/1863838.

Chernyshev M, Zeadally S, Baig Z. 2019. Healthcare data breaches: implications for digital forensic readiness. *Journal of Medical Systems* **43(1)**:50 DOI 10.1007/s10916-018-1123-2.

Dameff C, Tully J, Chan TC, Castillo EM, Savage S, Maysent P, Hemmen TM, Clay BJ, Longhurst CA. 2023. Ransomware attack associated with disruptions at adjacent emergency departments in the US. *JAMA Network Open* **6(5)**:e2312270 DOI 10.1001/jamanetworkopen.2023.12270.

Farringer DR. 2016. Send us the bitcoin or patients will die: addressing the risks of ransomware attacks on hospitals. *Seattle University Law Review* **40(3)**:937–984.

Farringer DR. 2019. Maybe if we turn it off and then turn it back on again? Exploring health care reform as a means to curb cyber attacks. *Journal of Law, Medicine and Ethics* **47(4_suppl)**:91–102 DOI 10.1177/1073110519898046.

Frumento E. 2019. Cybersecurity and the evolutions of healthcare: challenges and threats behind its evolution. In: *EAI/Springer Innovations in Communication and Computing*. Cham: Springer Science and Business Media Deutschland GmbH, 35–69.

Gazzan M, Sheldon FT. 2023. Opportunities for early detection and prediction of ransomware attacks against industrial control systems. *Future Internet* **15(4)**:144 DOI 10.3390/fi15040144.

Guvçi F, Şenol A. 2023. An improved protection approach for protecting from ransomware attacks. *Journal of Data Applications* **0(1)**:69–82 DOI 10.26650/joda.1312412.

Javaid M, Haleem A, Singh RP, Suman R. 2023. Towards insighting cybersecurity for healthcare domains: a comprehensive review of recent practices and trends. *Cyber Security and Applications* **1(3)**:100016 DOI 10.1016/j.csa.2023.100016.

Jobair M, Faruk H, Shahriar H, Masum M, Alom K. 2022. *Malware and ransomware classification, detection and prevention using artificial intelligence (AI) techniques*. Gistrup: River Publishers.

Kandasamy K, Srinivas S, Achuthan K, Rangan VP. 2022. Digital healthcare—cyberattacks in Asian organizations: an analysis of vulnerabilities, risks, NIST perspectives, and recommendations. *IEEE Access* **10**:12345–12364 DOI 10.1109/ACCESS.2022.3145372.

Kok SH, Abdullah A, Jhanjhi NZ, Supramaniam M. 2019a. Ransomware, threat and detection techniques: a review. *International Journal of Computer Science and Network Security* **19(2)**:136–146.

Kok SH, Abdullah A, Jhanjhi NZ, Supramaniam M. 2019b. Prevention of crypto-ransomware using a pre-encryption detection algorithm. *Computers* **8(4)**:79 DOI 10.3390/computers8040079.

Kolade A, Onunka T, Daraojimba C, Louis Eyo-Udo N, Onunka O, Omotosho A, Okafor C. 2023. 2023 mitigating cybersecurity risks in the U.S. Healthcare sector research gate.

Lawall A, Beenken P. 2024. A threat-led approach to mitigating ransomware attacks: insights from a comprehensive analysis of the ransomware ecosystem. In: *ACM International Conference Proceeding Series, Association for Computing Machinery*. New York: ACM, 210–216 DOI 10.1145/3655693.3661321.

Lee K, Oh I, Yim K. 2017. Ransomware-prevention technique using key backup. In: *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*. Cham: Springer Verlag, 105–114.

Li X, Madisetti VK. 2024. ERAD: enhanced ransomware attack defense system for healthcare organizations. *Journal of Software Engineering and Applications* **17(5)**:270–296 DOI 10.4236/jsea.2024.175016.

Logue KD, Shniderman AB. 2021. The case for banning (and mandating) ransomware insurance. *Available at https://repository.law.umich.edu/articles/2481/*.

Mahler T, Elovici Y, Shahar Y. 2020. A new methodology for information security risk assessment for medical devices and its evaluation. ArXiv DOI 10.48550/arXiv.2002.06938.

Mahmood M, Khan MI, Hussain H, Khan I, Rahman S, Shabir M, Niazi B. 2023. Improving security architecture of internet of medical things: a systematic literature review. *IEEE Access* **11**:107725–107753 DOI 10.1109/ACCESS.2023.3281655.

Minnaar A, Herbig FJW. 2021. Cyberattacks and the cybercrime threat of ransomware to hospitals and healthcare services during the COVID-19 pandemic. *Acta Criminologica* **34(3)**:154–185 DOI 10.10520/ejc-crim_v34_n3_a10.

Mukhopadhyay A, Jain S. 2024. A framework for cyber-risk insurance against ransomware: a mixed-method approach. *International Journal of Information Management* **74(4)**:102724 DOI 10.1016/j.ijinfomgt.2023.102724.

Murray G, Falkeling M, Gao S. 2024. *Trends and challenges in research into the human aspects of ransomware: a systematic mapping study*. Leeds: Emerald Publishing.

Nagar G. 2024. The evolution of ransomware: tactics, techniques, and mitigation strategies. *International Journal of Scientific Research and Management (IJSRM)* **12(6)**:1282–1298 DOI 10.18535/ijsrm/v12i06.ec09.

Nawaz NA, Ishaq K, Farooq U, Khalil A, Rasheed S, Abid A, Rosdi F. 2023. A comprehensive review of security threats and solutions for the online social networks industry. *PeerJ Computer Science* **9(12)**:e1143 DOI 10.7717/peerj-cs.1143.

Neprash HT, McGlave CC, Cross DA, Virnig BA, Puskarich MA, Huling JD, Rozenshtein AZ, Nikpay SS. 2022. Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016–2021. *JAMA Health Forum* **3(12)**:E224873 DOI 10.1001/jamahealthforum.2022.4873.

Newaz AI, Sikder AK, Rahman MA, Uluagac AS. 2019. HealthGuard: a machine learning-based security framework for smart healthcare systems. ArXiv DOI 10.48550/arXiv.1909.10565.

Nowrozy R, Ahmed K, Kayes ASM, Wang H, McIntosh TR. 2024. Privacy preservation of electronic health records in the modern era: a systematic survey. *ACM Computing Surveys* **56(8)**:1–37 DOI 10.1145/3653297.

Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, Shamseer L, Tetzlaff JM, Akl EA, Brennan SE, Chou R. 2021. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ* **372**:n71 DOI 10.1136/bmj.n71.

Patel A, Tailor J. 2020. A malicious activity monitoring mechanism to detect and prevent ransomware. *Computer Fraud & Security* **2020(1)**:14–19 DOI 10.1016/S1361-3723(20)30009-9.

Ramadan RA, Aboshosha BW, Alshudukhi JS, Alzahrani AJ, El-Sayed A, Dessouky MM. 2021. Cybersecurity and countermeasures at the time of pandemic. *Journal of Advanced Transportation* **2021**:1–19 DOI 10.1155/2021/6627264.

Razaulla S, Fachkha C, Markarian C, Gawanmeh A, Mansoor W, Fung BC, Assi C. 2023. The age of ransomware: a survey on the evolution, taxonomy, and research directions. *IEEE Access* **11**:40698–40723 DOI 10.1109/ACCESS.2023.3268535.

Reddy J, Elsayed N, ElSayed Z, Ozer M. 2023. A review on data breaches in healthcare security systems. *International Journal of Computer Applications* **184(45)**:1–7 DOI 10.5120/ijca2023922333.

Reshmi TR. 2021. Information security breaches due to ransomware attacks—a systematic literature review. *International Journal of Information Management Data Insights* **1(2)**:100013 DOI 10.1016/j.jjimei.2021.100013.

Robinson A, Corcoran C, Waldo J. 2022. New risks in ransomware: supply chain attacks and cryptocurrency citation terms of use share your story. *Available at https://www.belfercenter.org/publication/new-risks-ransomware-supply-chain-attacks-and-cryptocurrency*.

Saeed S, Jhanjhi NZ, Naqvi M, Humayun M, Ahmed S. 2020. Ransomware: a framework for security challenges in internet of things. In: *2020 2nd International Conference on Computer and Information Sciences, ICCIS 2020*. Piscataway: Institute of Electrical and Electronics Engineers Inc. DOI 10.1109/ICCIS49240.2020.9257660.

Shinde R, Patil S, Kotecha K, Potdar V, Selvachandran G, Abraham A. 2024. Securing AI-based healthcare systems using blockchain technology: a state-of-the-art systematic literature review and future research directions. *Transactions on Emerging Telecommunications Technologies* **35(1)**:535 DOI 10.1002/ett.4884.

Sittig DF, Singh H. 2016. A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. *Applied Clinical Informatics* **7(2)**:624–632 DOI 10.4338/ACI-2016-04-SOA-0064.

Slayton TB. 2018. Ransomware: the virus attacking the healthcare industry. *Journal of Legal Medicine* **38(2)**:287–311 DOI 10.1080/01947648.2018.1473186.

Song S, Kim B, Lee S. 2016. The effective ransomware prevention technique using process monitoring on android platform. *Mobile Information Systems* **2016(1)**:1–9 DOI 10.1155/2016/2946735.

Spence N, Bhardwaj N, Paul DP III, Coustasse A. 2018. Ransomware in healthcare facilities: a harbinger of the future? *Available at https://mds.marshall.edu/mgmt_faculty/231/*.

Sunil V, Mathew SP. 2024. A systematic review on cybersecurity threats and challenges in hospitals. *Acta Medica International* **11(1)**:1–6 DOI 10.4103/amit.amit_7_24.

Swasey K. 2020. Insufficient healthcare cybersecurity invites ransomware attacks and sale of PHI on the dark web. *Available at https://www.usu.edu/cai/files/studentpaper-swasey.pdf*.

Thakur M. 2024. Cyber security threats and counter measures in digital age. *Journal of Applied Science and Education (JASE)* **4(42)**:1–20 DOI 10.54060/a2zjournals.jase.42.

Thamer N, Alubady R. 2021. A survey of ransomware attacks for healthcare systems: risks, challenges, solutions and opportunity of research. In: *1st Babylon International Conference on Information Technology and Science 2021, BICITS 2021*. Piscataway: IEEE, 210–216 DOI 10.1109/BICITS51482.2021.9509877.

Triplett WJ. 2024. Cybersecurity vulnerabilities in healthcare: a threat to patient security. *Cybersecurity and Innovative Technology Journal* **2(1)**:15–25.

Tully J, Selzer J, Phillips JP, O'Connor P, Dameff C. 2020. Healthcare challenges in the era of cybersecurity. *Health Security* **18(3)**:228–231 DOI 10.1089/hs.2019.0123.

van Boven LS, Kusters RW, Tin D, van Osch FH, De Cauwer H, Ketelings L, Rao M, Dameff C, Barten DG. 2024. Hacking acute care: a qualitative study on the health care impacts of ransomware attacks against hospitals. *Annals of Emergency Medicine* **83(1)**:46–56 DOI 10.1016/j.annemergmed.2023.04.025.

Vithanwattana N, Karthick G, Mapp G, George C. 2021. Exploring a new security framework for future healthcare systems. In: *2021 IEEE Globecom Workshops (GC Wkshps)*. Piscataway: IEEE.

Yeng K, Yang B, Snekkenes EA. 2019. A framework for healthcare security practice analysis, modeling and incentivization framework for healthcare security practice analysis, modeling and incentivization. *Available at https://www.researchgate.net/publication/337952535*.

Zhan Y, Ahmad SF, Irshad M, Al-Razgan M, Awwad EM, Ali YA, Ayassrah AYBA. 2024. Investigating the role of Cybersecurity's perceived threats in the adoption of health information systems. *Heliyon* **10(1)**:e22947 DOI 10.1016/j.heliyon.2023.e22947.

Zhang-Kennedy L, Rocheleau J, Mohamed R, Baig K, Chiasson S, Assal H. 2018. The aftermath of a crypto-ransomware attack at a large academic institution. *Available at https://www.usenix.org/conference/usenixsecurity18/presentation/zhang-kennedy*.

Zlatolas LN, Welzer T, Lhotska L. 2024. Data breaches in healthcare: security mechanisms for attack mitigation. *Cluster Computing* **27(7)**:8639–8654 DOI 10.1007/s10586-024-04507-2.