Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI)
Vol. 10, No. 1, March 2024, pp. 73-98
ISSN: 2338-3070, DOI: 10.26555/jiteki.v10i1.28192

Uncovering Security Vulnerabilities in Electronic Medical Record Systems: A Comprehensive Review of Threats and Recommendations for Enhancement

Dian Wijayanti, Erik Iman Heri Ujianto, Rianto Rianto
Master of Information Technology, Universitas Teknologi Yogyakarta, Yogyakarta, Indonesia

ARTICLE INFO

Article history:

Received January 11, 2024
Revised February 09, 2024
Published February 28, 2024

Keywords:

Electronic Medical Record Systems;
Security Vulnerabilities;
Threats;
Recommendations for Enhancement;
Cybersecurity

ABSTRACT

Cybersecurity is a critical concern for healthcare organizations in the digital era, as patient data privacy faces significant risks from numerous vulnerabilities. Given the escalating cyberattacks in healthcare, understanding EMR system vulnerabilities has become imperative. This study aimed to find the main weaknesses in Electronic Health Record (EHR) systems and suggest proven methods to improve security and keep patient information private. Utilizing a cross-sectional analysis, we assessed the effectiveness of current security protocols against identified threats. We systematically reviewed 25 recent, high-quality articles (from 2020 to 2023) on EMR vulnerabilities, selected based on their relevance and the efficacy of their proposed solutions. Our analysis revealed that system architecture flaws and credential misuse represented the most significant threats, with hacking incidents most frequently targeting these weaknesses. The analysis identified six key threat categories to EMR security: compromised access, system architecture flaws, data sharing challenges, hacking, credential misuse, and non-compliance with regulations. This framework introduced a multi-layered defense strategy, unique in incorporating both technical and behavioral security measures. The study provided a novel framework combining technological and management safeguards, offering a fresh perspective on modern EMR vulnerabilities. The detailed threat categorization gave healthcare organizations a strategic basis for improved security planning and resource allocation. The actionable insights from this study could greatly enhance EMR security protocols in healthcare settings, potentially reducing data breaches and improving patient trust. Further research was warranted to test the effectiveness of the proposed framework across various healthcare environments.

Corresponding Author:

Dian Wijayanti, Master of Information Technology, Kampus I Universitas Teknologi Yogyakarta, Jl. Siliwangi (Ringroad Utara), Jombor, Sleman, Daerah Istimewa Yogyakarta, 55285, Indonesia
Email: dianwijayanti077@gmail.com

1. INTRODUCTION

Electronic medical records (EMRs) have become very common in healthcare organizations. This has greatly improved the digitization and sharing of health data. Perez (2022) highlighted the necessity for advanced threat detection methods, forming the foundation of our research proposing a comprehensive security framework. Our study proposes an extensive security framework that integrates these detection methods with real-time analytics specifically tailored for EMR systems [1]. Sivan and Zukarnain (2021) studied security and privacy issues in e-health systems. They pointed out major concerns about patient data confidentiality despite the advantages of cloud computing [2]. Wasserman and Wasserman (2022) highlighted serious cybersecurity vulnerabilities in healthcare organizations that put patient data at risk. Their review revealed concerns about the security of medical devices, telemedicine, and records that attackers can exploit [3]. Despite the extensive

literature on EMR security, there remains a critical gap in holistic and integrated frameworks that address the full spectrum of technical, administrative, and policy-related vulnerabilities. This study seeks to address this gap. It provides a thorough analysis of EMR vulnerabilities. It also proposes a practical security framework customized for the specific needs of healthcare organizations [2], [3]. Consequently, this research aims to deliver an extensive and detailed examination of vulnerabilities and dangers associated with the security of patient data within Electronic Medical Records (EMR), aiming to fill the existing gap in academic research.

Thus, our study will specifically explore technical, administrative, and policy-related vulnerabilities in access control, authentication, encryption, auditing, and network security within EMR systems, proposing a comprehensive security framework to address these multifaceted challenges. Potential solutions involve technical controls like identity and access management (ensuring only authorized users can access certain data), cryptography (securing information through encryption), monitoring (continuous surveillance of system activities), and segmentation (dividing the network into separate parts to contain breaches).

This involves evaluating technical controls, including identity and access management, cryptography, monitoring, and segmentation. We propose an integrated framework combining threat modelling, risk assessment, and adaptive safeguards. The proposed framework will be detailed, outlining how threat modelling, risk assessment, and adaptive safeguards can be effectively implemented in healthcare settings. To guide this investigation, we pose the following research questions: What specific vulnerabilities jeopardize patient data security in EMRs, and what technical solutions could significantly enhance their protection? The literature review will critically analyze these questions to provide answers. To ensure a comprehensive understanding of the current state of EMR security, our literature review is exhaustive and critical, scrutinizing prevailing theories and methodologies to identify areas of concern and explore potential solutions. This thorough examination enables a nuanced contribution to the field by identifying potential shortcomings in current strategies and proposing comprehensive solutions. Acquiring a comprehensive understanding can facilitate the development of effective, organization-specific security strategies.

The goal is to identify concerns and solutions to enhance the security of EMR patient data, contributing to robust protection measures. The analyzed solutions include access control, encryption, auditing, and networking, aimed at enhancing data protection. Overall, this offers a comprehensive analysis of vulnerabilities that could potentially compromise the confidentiality of EMR patient data in a systematic manner to develop optimal encryption and authentication solutions for better safeguarding confidential patient Electronic medical records (EMRs) have enabled efficient patient data access to healthcare. However, as providers adopt cloud platforms, EMR security and privacy have become major concerns due to breaches and vulnerabilities. This review examines cryptographic and non-cryptographic approaches proposed to mitigate EMR threats. It evaluates encryption, access controls, and blockchain techniques for analyzing EMR vulnerabilities. It emphasizes the importance of robust security implementation by highlighting risks, including insider threats, insecure APIs, misconfigurations, and data leaks. Further research is recommended to address these concerns.

Studies like Sivan and Zukarnain (2021) have recommended further research on encryption and authentication to safeguard confidential patient data, given security issues in e-health systems [2]. Building on the recommendations by Sivan and Zukarnain (2021), our study contributes to the field by investigating advanced encryption and authentication techniques and introducing a novel, adaptive framework that integrates these techniques with organizational policies to fortify EMR security. As healthcare digitizes, cyberattacks on hospitals and clinics have risen correspondingly. Safeguarding patient data in EMRs and clinical applications remains a pressing issue. Various vulnerabilities have been highlighted, including weak authentication, outdated systems, insufficient endpoint control, and unpatched devices [3]. These flaws make hospitals frequent targets for attackers exploiting medical systems and records. Upon closer examination, it is necessary to thoroughly explore the extent of data security issues and identify the most effective strategies for mitigation.

Next, this paragraph examines the vulnerabilities highlighted in hospitals and clinics from recent cyberattacks and security reviews directly connected to the research exploring EMR vulnerabilities. Alabi (2021) reviewed that adopting cloud computing for health records raises concerns about security, privacy, and trust, given the sensitivity of medical data [4]. PHP frameworks for EMR systems have identified potential security risks, including weak authentication, SQL injection, cross-site scripting, and request forgery. Laravel-based framework is a secure EMR development solution that provides necessary security features to prevent vulnerabilities [5]. Nijor *et al*. (2022) found that information overload in EHRs increases medical errors and threatens patient safety [6]. When integrating patient data into EMRs, developers must secure patient data in electronic medical record systems. Kawu *et al*. (2023) reviewed integrating patient-generated health data into EHRs and highlighted the need for data governance, quality, privacy, and patient trust policies [7]. Davy and Borycki (2021) reviewed that copy-paste in EMRs can lead to overlooked medical issues and patient safety risks [8]. In addressing the vulnerabilities of EMR systems, our literature review systematically synthesizes

findings from key studies such as Wasserman and Wasserman (2022) on cybersecurity vulnerabilities and Kawu *et al*. (2023) on data governance, thereby situating our research within the broader academic discourse [3], [7]. Our study aims to contribute to the existing knowledge by proposing a comprehensive security framework that addresses technical vulnerabilities and incorporates data governance and regulatory compliance aspects. This framework offers a complete solution to the security challenges faced by EMR systems.

Therefore, this study analyzes EMR patient data confidentiality and security vulnerabilities. The key contributions are identifying EMR-specific threats and proposing an integrated security framework tailored to mitigate the identified risks involving access control, encryption, auditing, and network security. The aim is to comprehensively evaluate EMR-specific threats and solutions to safeguard sensitive patient data.

Moving on, this paragraph evaluates the security issues in cloud-based EMR systems. The referenced journals discuss issues related to protecting the privacy of patient data in electronic medical records (EMRs). They cover cloud computing, PHP frameworks, information overload, and copy-paste mistakes. However, this research takes a more in-depth approach by thoroughly analyzing inherent EMR system security vulnerabilities and their impact on patient data. While prior publications provided general overviews, this study deeply analyzes inherent EMR vulnerabilities affecting patient data confidentiality. Moreover, considering all identified EMR data vulnerabilities and risks, a comprehensive framework is proposed.

This research identifies the six main threat categories jeopardizing patient data security in EMR systems. The proposed framework provides technical recommendations involving access control, encryption, auditing, and network security controls to safeguard EMRs. This research also summarizes various frameworks and models previously proposed to address EMR vulnerabilities.

Researchers have extensively examined EMR system security risks. Therefore, we have compiled an overview of recent research findings from 2020-2023 on various EMR security aspects to provide the most up-to-date understanding. The timeframe of 2020-2023 was chosen due to the rapid advancements in EMR technologies and emerging security challenges during this period. However, most studies have focused on a particular aspect or threat type. This comprehensive review of EMR security vulnerabilities offers crucial insights to safeguard sensitive patient data, a pivotal step towards building robust and secure EMR systems. By achieving these objectives, this study aspires to contribute substantially to the field by improving EMR patient data security and offering a systematic analysis of vulnerabilities, thus informing the development of effective, organization-specific security strategies.

Our research aims to significantly enhance the security of EMR systems against cyber threats, thereby contributing to safeguarding sensitive healthcare data globally. This will be achieved through two primary contributions. First, we will conduct a detailed examination of EMR vulnerabilities based on an extensive review of current literature. This will provide a taxonomy categorizing the various vulnerabilities. Second, we will propose an innovative security framework that connects these vulnerabilities to tailored, actionable security controls and policies. The framework is designed to be flexible, adapting to new threats while addressing the particular needs of healthcare organizations. By meticulously analyzing vulnerabilities and implementing a bespoke security plan, our research intends to greatly improve resilience against threats to the confidentiality of patient data in EMR systems.

2. METHODS

The systematic research method for reviewing literature on security weaknesses in patient data within electronic medical records starts by defining the scope of the review, specifically focusing on security weaknesses in patient data contained in electronic medical records. The process involves several stages, including determining research questions to address these weaknesses, identifying keywords, and conducting a search for related literature. Additionally, researchers establish inclusion and exclusion criteria to determine the literature to be reviewed and establish guidelines for assessing its quality. The inclusion criteria specify the use of recent studies published within the last five years, ensuring that the review incorporates the most current information available. On the other hand, sources that are not peer-reviewed or not in English are excluded. These measures were taken to ensure that the review maintains high quality and relevance.

Please refer to Fig. 1 for a comprehensive visual representation of the systematic review process outlined in the text. Fig. 1 presents a flowchart that describes the systematic stages involved in conducting this literature review. Additionally, a comprehensive explanation will be provided to enhance transparency regarding the reasons for excluding specific studies based on the inclusion and exclusion criteria. The purpose of Fig. 1 is to clearly illustrate the systematic review process, mapping out each step from record identification to final inclusion.

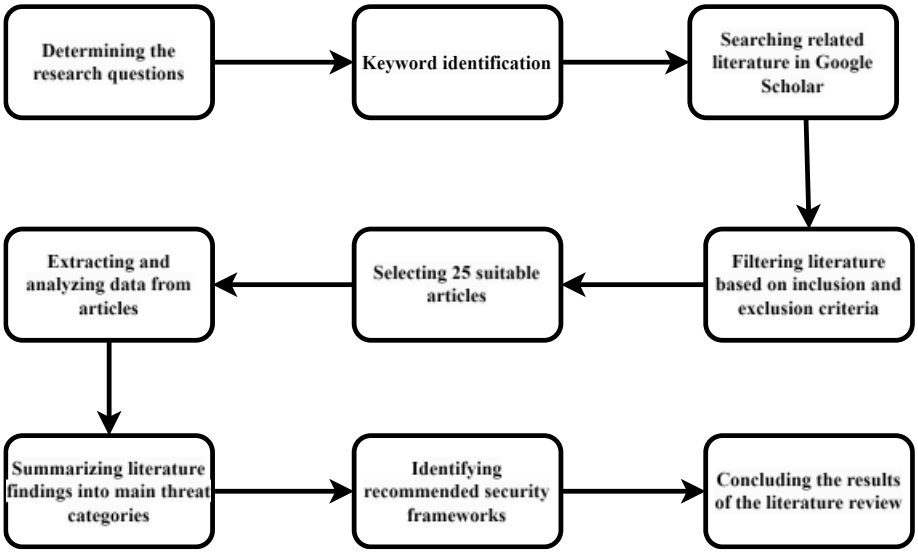


Fig. 1. Research Flowchart

Please ensure that Fig. 1 is included in the appropriate section to provide visual support to the described systematic stages in conducting this literature review. This flowchart provides an overview of the flow of information through the different review phases, starting from identification of records through database searches, screening, assessment for eligibility, and final inclusion in the review. Data extraction and analysis were conducted using a standardized form to ensure consistency across all literature sources, with particular attention to study design, outcomes measured, and statistical validity. Next, the researchers extracted and analyzed data from each selected piece of literature using the quality assessment guidelines to answer the research questions they had previously established. Two independent reviewers meticulously conducted a quality assessment using a predefined checklist that included factors such as methodological transparency, bias risk, and the robustness of results. The study's results will be presented systematically with a summary relating to the scope of the review of security weaknesses in patient data in electronic medical records [9]. Additionally, a discussion on the limitations of the selected studies, including potential biases and methodological weaknesses, will be included to provide context for the findings and recommendations of this review.

2.1. Determining Research Questions (RQ)

The research questions were formulated to investigate this specific topic area. Table 1 presents the specific questions that this study aims to address. The purpose of this is to gain a deeper understanding of the vulnerabilities in electronic medical records and enhance the protection of patient privacy. This overview briefly highlights the common security issues encountered in electronic medical records.

Table 1. Research Questions

ID	Research Questions
RQ1	What categories of vulnerabilities and threats have been identified in the literature regarding the security of patient data in electronic medical records?
RQ2	What security frameworks or models have been suggested by previous studies to address vulnerabilities in safeguarding patient data stored in electronic health records?

2.2. Keyword Identification and Literature Search

This study aims to examine the security weaknesses that put patient data in electronic medical records at risk. Therefore, the literature review process involved several steps:

1. A literature search was conducted in November 2023 to capture the most recent publications at the time of the search for this study. The literature search was conducted using Harzing's Publish or Perish software, a tool known for its effectiveness in academic literature retrieval and selecting the Google Scholar database. Harzing's Publish or Perish was chosen for its ability to facilitate citation analysis and Google Scholar for its extensive collection of scholarly literature; however, the limitations of this approach include potential publication bias and limited access to some databases. Future research may consider using additional databases, such as PubMed and IEEE Xplore, to ensure a comprehensive literature search. The literature

search was guided using a set of relevant keywords and terms determined based on the research objectives. Acknowledging the inherent limitations of keyword-based searches, including the potential omission of relevant studies due to variations in terminology used by different authors, is important. Therefore, supplementary search strategies such as reviewing reference lists of included articles could be employed. These keywords were combined using Boolean operators to refine and focus the search results. The literature search employed Boolean operators to refine the results, using queries such as '("electronic medical records" AND "patient data" AND (vulnerability OR threat))' to precisely target relevant studies.

2. Relevant keywords and phrases were chosen to guide the literature selection in line with the research aims. In this review, "electronic medical record" (EMR) and "electronic health record" (EHR) are used interchangeably, mirroring the literature's usage. The keywords used were: "EMR/EHR," "patient data," "security," "privacy," "confidentiality," "vulnerability," and "threat". Using keywords ensures that only sources directly related to security issues impacting patient information stored in electronic medical record systems are identified and further evaluated for inclusion in the insights.
3. The selection was limited to articles published between 2020 and 2023, sourced from academic journals rated Sinta 3 or above or reputable international journals, as these are considered quality publications that have gone through rigorous peer review. This 5-year time frame was chosen to include the most up-to-date knowledge on security practices and vulnerabilities. By including only sources published within a certain period in selected publications, the time frame and journal criteria ensured a focus on high-quality primary studies with reasonable scientific influence. Although focusing on Google Scholar ensured a robust search, including databases such as PubMed or IEEE would likely offer more comprehensive results.

2.3. Determining Quality Assessment Criteria

The screening process was guided by inclusion and exclusion criteria to select papers relevant for the review. Clear eligibility rules focused the analysis on high-quality reports matching the study aims. Table 2 and Table 3 list the parameters used to determine whether full-text papers would be included or omitted from the final observations. Inclusion criteria include papers that closely examine predetermined aspects of the investigation. In contrast, exclusion criteria eliminate sources that are deemed irrelevant or contain low-quality information. The quality assessment criteria checklist evaluates parameters, including clarity of research objectives and questions, the rigour of research methodology, the validity of findings supported by evidence, sufficient details provided for replication, and depth of discussion and analysis of results. Inclusion criteria include papers that closely examine predetermined aspects of the investigation.

Table 2. Inclusion Criteria

ID	Inclusion Criteria
IC1	Research articles obtained from Google Scholar.
IC2	Research articles published in the 2020-2023 time frame.
IC3	Research is a Journal Article or Book.
IC4	Research articles published in English.
IC5	Research articles explore issues related to vulnerabilities, risks, threats, or breach events involving patient information systems in electronic medical/health records platforms.
IC6	Research articles with sound and rigorous research methodology.
IC7	Research articles published in reputable journals with high impact factors in their field.

Table 3. Exclusion Criteria

ID	Exclusion Criteria
EC1	The research article did not focus its analysis on electronic health/medical systems directly.
EC2	The research article does not examine the security of individual patient data stored electronically.

The systematic application of the inclusion and exclusion criteria in the selection process upholds the principles of objectivity and comprehensiveness. This approach also mitigates the risk of inclusion bias. Establishing transparent decision-making guidelines in the inclusion/exclusion criteria prevents bias in the paper selection. Additionally, inclusion and exclusion criteria help contain the screening workload and focus efforts on high-value literary works. The systematic application of the inclusion and exclusion criteria in the selection process upholds the principles of objectivity and comprehensiveness. This approach also mitigates the risk of inclusion bias. Establishing transparent decision-making guidelines in the inclusion/exclusion criteria prevents bias in the paper selection. Additionally, inclusion and exclusion criteria help contain the screening workload and focus efforts on high-value literary works. In the event of a discrepancy between the

two researchers about including a paper, the issue was settled by engaging in a dialogue until a mutual agreement was achieved. After final screening, the quality of the 25 selected articles was assessed independently by two researchers using a predefined criteria checklist adapted from Taylor-Powell and Renner (2003). Each article was rated as 'High Quality,' 'Acceptable Quality,' or 'Reject' based on the checklist criteria. Whenever there was a difference in opinion between the two investigators on the research quality assessment, they conversed to reconcile their views and arrive at a joint agreement. After quality assessment, 25 articles were deemed to meet the threshold for inclusion. We ensured that only articles meeting the quality standards were included in the final review. This quality appraisal process ensures the validity and reliability of the literature reviewed in this study.

The systematic literature review process followed can be outlined in the following pseudocode algorithm:

Begin
1. Define research questions
2. Identify keywords
3. Search literature databases using keywords
4. Get search results
5. Filter results by:
   - Publication year (2020-2023)
   - Journal (reputable, high impact)
   - Language (English)
6. Apply inclusion criteria:
   - Related to EMR security
   - Rigorous methodology
   - Matches research aims
7. Apply exclusion criteria:
   - Not directly about EMR systems
   - Does not examine patient data security
8. Assess the quality of remaining studies:
   - Clear objectives
   - Valid methodology
   - Sufficient details
   - Adequate discussion
9. Select final studies
10. Extract relevant data
11. Synthesize data narratively by themes
12. Summarize results

End

The pseudocode provides a structured representation of the literature review process, illustrating each step, from developing research questions to synthesizing findings.

2.4. Language Bias

This study only included literature published in English, which may introduce language bias and exclude potentially relevant studies in other languages. However, resource constraints and access to translated material necessitate limiting the scope to English language publications. While findings may be skewed by a lack of literature in other languages, restricting to English remains a common research practice. Future reviews could consider including studies in other languages with the aid of translation services to mitigate this limitation. This potential language bias should be acknowledged as a limitation, although including only English articles is standard in similar systematic reviews. Future studies should consider the feasibility of including articles in multiple languages to provide a more global perspective. The exclusion of non-English literature may preclude insights from important studies published in other languages. Overall, the English-only criteria create a gap in knowledge from relevant non-English literature.

2.5. Potential Bias

This literature review may be subject to publication bias, as studies with positive results are generally easier to publish than those with negative findings. Despite searching for grey literature and unpublished studies to minimize publication bias, efforts were made to search for grey literature and unpublished studies. However, publication bias cannot be fully eliminated. Acknowledging this limitation, the review aimed to provide a balanced perspective by including papers with various outcomes, although the results likely

overrepresent positive findings. The narrow scope focused on published studies may overlook contradicting evidence or alternative perspectives available in unpublished sources. Overall, readers should be aware that while meeting the quality criteria, the literature reviewed may be skewed toward published studies reporting positive security outcomes. Additional constraints encompass the limited number of participants and the dependence on self-reported data in the analyzed primary studies.

2.6. Data Extraction

Two researchers independently extracted data from 25 selected articles using a standardized form. The compiled data included author names, publication year, study location, design methods, number of participants, EMR systems investigated, identified security vulnerabilities, and key conclusions on EMR protection. Only relevant data for the research questions was included. A third-party reviewer could resolve any disagreements between the researchers. The extracted data were categorized into common themes and topics. This allowed evidence synthesis from different studies on EMR security. Involving two independent researchers in data extraction ensures the reliability and objectivity of the analyzed information.

2.7. Narrative Synthesis

The extracted data were synthesized narratively to consolidate evidence from different studies into common themes and topics. This involved categorizing the data based on vulnerabilities, threats, security frameworks, and other key findings. Two researchers conducted. The narrative synthesis independently and compared it to ensure reliability. The narrative synthesis was a thematic analysis to categorize and consolidate key themes, relationships, and conclusions from the extracted data. The researchers reached a consensus on the data's key themes, relationships, and conclusions through discussion. The narrative approach allowed contextualized analysis of textual data from diverse studies to generate insights that address the research questions regarding EMR security vulnerabilities and solutions. Each step in the review process was carefully considered to ensure the reliability and objectivity of the conclusions drawn.

2.8. Material

The initial Google Scholar search found 122 articles. After the initial screening, which applied inclusion criteria IC1 to IC4, 87 articles remained. The second screening with IC5 left 35 articles. Finally, applying exclusion criteria EC1 and EC2 made 25 articles eligible for the review. Most articles were excluded during the title and abstract screening because they needed to meet the inclusion criteria, especially on relevance to EMR security issues.

The process for screening and selecting literature for inclusion in this systematic review is depicted in Fig. 2 using a PRISMA flow diagram. This diagram provides an overview of the flow of information through the different review phases, starting from identifying records through database searches, screening, assessment for eligibility, and final inclusion in the review. The specific numbers at each stage are presented to map the literature screening process transparently and reproducibly.

The process for screening and selecting literature for inclusion in this systematic review is depicted in Fig. 2 using a PRISMA flow diagram. This diagram provides an overview of the flow of information through the different review phases, starting from identifying records through database searches, screening, assessment for eligibility, and final inclusion in the review. The specific numbers at each stage are displayed to map the literature screening process transparently and reproducibly.

Upon an in-depth examination of 25 chosen articles, pertinent information was meticulously gathered by hand, encompassing the authors, year of publication, geographical setting and research methodology, the sample scale, scrutinized EMR/EHR systems, detected security flaws, and significant outcomes. Through narrative synthesis, we consolidated findings from quality publications on EMR vulnerabilities. Table 4 provides the characteristics of the studies in our review to overview the evidence basis informing the analysis and conclusions.

Important information was extracted from the 25 selected articles, including authors, publication year, study methodology, number of subjects, systems investigated, identified security weaknesses, and main results. These data were analyzed using narrative synthesis to consolidate evidence on EMR vulnerabilities. To understand trends over time, the 25 eligible sources were categorized by year of publication, as shown in Fig. 2. This classification helps identify the recent evolution of research focus on EMR security risks. Grouping articles by publication year provides insights into the progression of EMR security research. The annual publication volume indicates a growing research interest in recent years, particularly in 2020. This is likely due to increasing EMR adoption globally and rising data breach concerns.

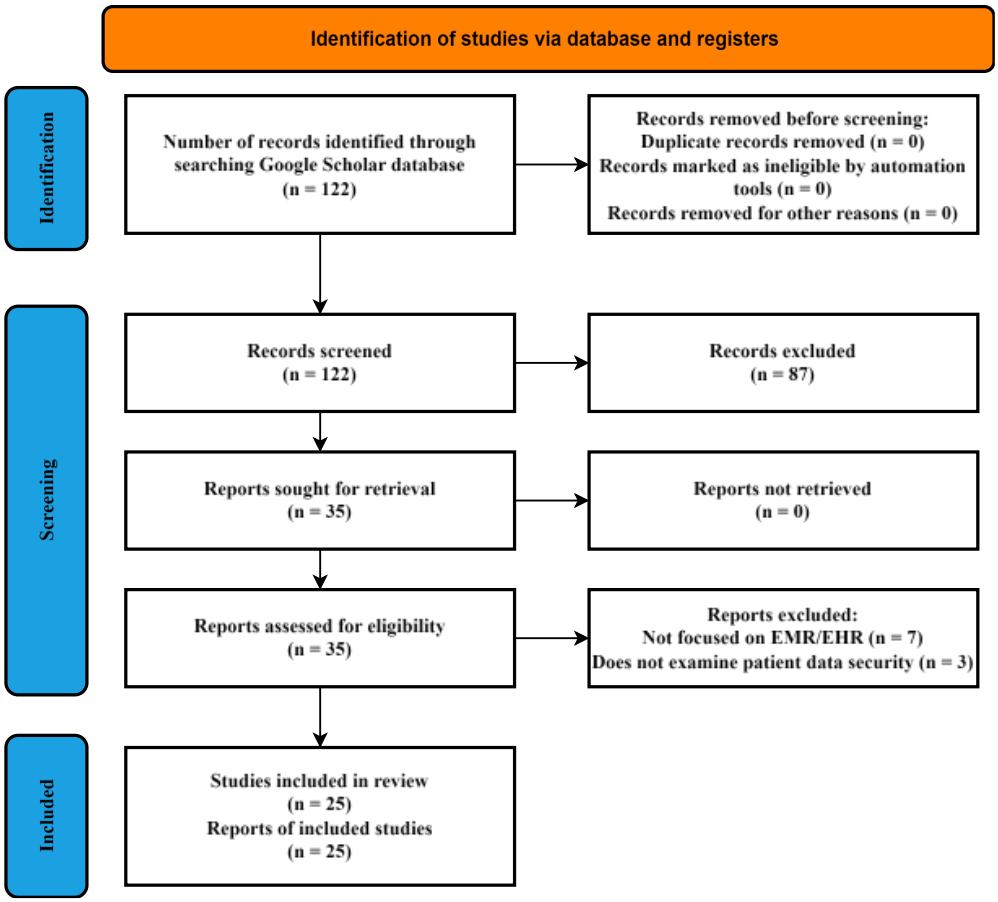


Fig. 2. PRISMA 2020 Flow Diagram

Further analysis of the literature trends over time reveals a shift in research focus. Earlier articles from 2020-2021 featured broader discussions of EMR privacy issues. Meanwhile, publications from 2022-2023 provided a more granular technical analysis of specific vulnerabilities and proposals for advanced security solutions like blockchain. This indicates that the discourse has progressed from conceptual privacy concerns toward more hands-on investigation of tangible threats and exploits. Research interest has also intensified, with more studies exploring exploits, attack vectors, and countermeasures. The evolution of technical cybersecurity topics shows the field maturing rapidly, potentially driven by rising data breach incidents. Understanding these trends is valuable to track research progress and identify leading edges for further inquiry. This review may have inherent biases and limitations from the original studies. Many studies relied on self-reported data, potentially introducing subjectivity. The inclusion criteria limited to English may have created potential language and cultural bias. Publication bias may have favored articles with positive security outcomes. These biases should be taken into account when interpreting the findings of the review. Additionally, the limited number of literatures reviewed might not encompass the complete range of evidence on EMR security issues.

Fig. 3 shows the categorization of articles based on the year of publication. The focus of studies has also evolved, with earlier articles discussing broader aspects of EMR privacy, while later publications have provided technical analysis of vulnerabilities and proposed advanced security solutions such as blockchain. Further analysis of the literature trends over time indicates a shift in research focus. Earlier articles from 2020-2021 primarily addressed broader discussions on EMR privacy issues.

Conversely, publications from 2022-2023 delved into more detailed technical analysis of specific vulnerabilities and proposed advanced security solutions, such as blockchain. This indicates that the discourse has progressed from conceptual privacy concerns toward more hands-on investigation of tangible threats and exploits. Research interest has also intensified, with more studies exploring exploits, attack vectors, and countermeasures. The evolution of technical cybersecurity topics shows the field maturing rapidly, potentially driven by rising data breach incidents. Understanding these trends is valuable to track research progress and identify leading edges for further inquiry.

Table 4. Details of Selected Literature

No.	Title	Authors
1.	Harmonization Over the Regulations of Electronic Medical Records and its Potential to be Abused	Maskun, Rian Nugraha, Hasbi Assidiq, Muhammad Tayyib
2.	Decentralizing Electronic Medical Records on the Blockchain Using Smart Contracts	B.V. Baiju, S. Saranya, D. Sriram, M. Rifath Ahmed
3.	Provably Secure Data Sharing Approach for Personal Health Records in Cloud Storage Using Session Password, Data Access Key, and Circular Interpolation	Naveen John, Shatheesh Sam
4.	Privacy Protection Scheme of Medical Electronic Health Records Based on Blockchain and Asymmetric Encryption	Liang Huang, Zhengyu Zan, Hua Lai, Hyung-Hyo Lee
5.	Security in Electronic Health Records System: Blockchain-Based Framework to Protect Data Integrity	Md Jobair Faruk, Hossain Shahriar, Bilash Saha, Abdul Barek
6.	CEPS: A Cross-Blockchain based Electronic Health Records Privacy-Preserving Scheme	Sheng cao, Jing Wang, Xiaojiang Du, Xiaosong Zhang, Xiaolin Qin
7.	BSF-EHR: Blockchain Security Framework for Electronic Health Records of Patients	Ibrahim Abunadi, Ramasamy Lakshmana Kumar
8.	Current Developments in Electronic Health Records	Nils Pfeuffer, Peter Penndorf, Wolfgang Hoffmann, Neeltje van den Berg
9.	Data Sharing and Electronic Medical Record Privacy Protection of Out-Patient-Department Using Blockchain	Pradorn Sureephong, Pradya Komanee, Chanatip Trongpanyachot
10.	A Framework to Secure Electronic Health Records using Privacy-Enabled Hyperledger Fabric	Md. Rashid Reza, Sunil Kumar Singh
11.	A Blockchain-based Privacy-preserving and Access-control Framework for Electronic Health Records Management	Amit Kumar Jakhar, Mrityunjay Singh, Rohit Sharma, Aman Sharma
12.	Blockchain Enabled Decentralized Application for Securing Electronic Medical Records with Smart Contracts	Rithesh Pakkala, Shamantha Rai B, Akhila Thejaswi, Prakhyath Rai
13.	Irish People's Views on Electronic Health Records and Data Security	SJ Flaherty, O Barry, C Duggan, B Foley, R Flynn
14.	How To Ensure the Confidentiality of Electronic Medical Records on The Cloud: A Technical Perspective	Zongda Wu, Shaolong Xuan, Jian Xie, Chongze Lin, Cheng Lang Lu
15.	A Survey on Healthcare Standards and Security Requirements for Electronic Health Records	B S Sahana Raj, Sridhar Venugopalachar
16.	Privacy Preservation and Access Control for Sharing Electronic Health Records Using Blockchain Technology	Insaf Boumezbeur, Karim Zarour
17.	Effects of Continuous Security Monitoring on Security Controls of Electronic Health Records in Public Hospitals, Tanzania	Ernest Godson, Deus Dominic Ngaruko, George Oreku
18.	Security and Privacy of Electronic Health Records Sharing using Hyperledger Fabric	Vishnuvardhan Komuravelly, M. Ramchander
19.	Secure Storage and Retrieval of Electronic Health Records	Abinav Shibu, Anisha T Anikumar, Ashwin Radhakrishnan, Sminu Izudheen
20.	Misuse of Electronic Medical Records in Blockchain Technology Intelligence Security System	Mirel Wattimena, Dwi Retnowati, Teddy Mantoro
21.	MedRSS: A Blockchain-based Scheme for Secure Storage and Sharing of Medical Records	Zhijie Sun, Dezhi Han, Dun Li, Tien Hsiung Weng, Kuan Ching Li
22.	Electronic Health Records & Data Management using Hyperledger fabric in Blockchain	Rohit Kota, Harsh Wadhawe, Vishaal prasaad, Rohini Sarode
23.	Medical Records and Confidentiality: Evolving Liability Issues Inherent in the Electronic Health Record, HIPAA, and Cybersecurity	James E. Szalados
24.	Enhancing Transaction Security for Handling Accountability in Electronic Health Records	Chian Techapanupreed, Werasak Kurutach
25.	Security and Privacy Consideration for The Deployment of Electronic Health Records: A Qualitative Study Covering Greece and Oman	Ourania Koutzampasopoulou Xanthidou, Dimitrios Xanthidis

This review may contain some biases and limitations inherent in the original studies. Many relied on self-reported data, which can introduce subjectivity. The English-only inclusion criteria created potential language and cultural bias. Publication bias may have favored articles with positive security outcomes. These biases should be considered when interpreting the review findings. Furthermore, the small sample of literature reviewed may not capture the full extent of evidence on EMR security issues.

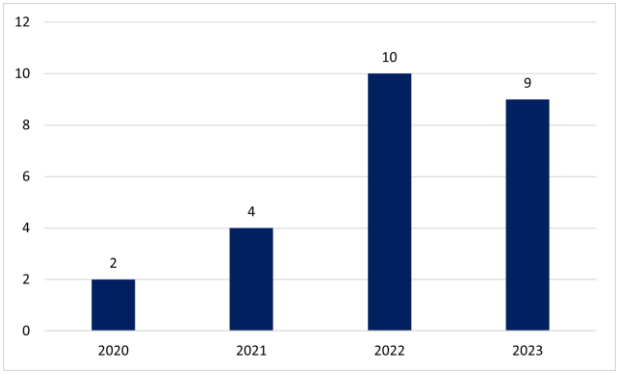


Fig. 3. Classification of Articles based on Year of Publication

3. RESULTS AND DISCUSSION

This section comprehensively analyzes the key vulnerabilities and threats to patient data security in EMR systems. The screening process selected 25 relevant papers addressing vulnerabilities in EMRs and suggestions for strengthening patient data protection. The literature comes from various high-quality peer-reviewed sources published between 2020 and 2023. The screening process revealed several common areas of concern that emerged across publications. Six main threat categories have been identified and discussed in detail below. It is important to note that while these recommendations provide a solid foundation for improving EMR security, practical implementation may vary based on organizational resources and specific healthcare contexts. The review summarizes recommendations from the selected studies to identify optimal approaches for securing patient data within electronic health records.

3.1. RQ1. What categories of vulnerabilities and threats have been identified in the literature regarding the security of patient data in electronic medical records?

The categorization of vulnerabilities and threats, as highlighted in Table 5, offers an organized perspective of the current security challenges in EMR systems. Access control deficiencies and threats to patient privacy emerge as the most frequently cited concerns, referenced in 24 out of the 25 studies reviewed. This finding echoes the insights from Pfeuffer *et al*. (2020), who also emphasized the impact of access control and patient privacy in EMR security [10]. The present study goes beyond the scope of Pfeuffer *et al*. by critically examining a broader range of recent literature, encompassing 25 publications from 2020 to 2023, thus providing an updated and comprehensive analysis of EMR vulnerabilities and threats.

Table 5 categorizes the vulnerabilities and threats identified from the literature into six main areas. The most significant category, 'Lack of access controls and patient privacy', dominates the landscape of security concerns, mentioned in nearly all selected sources. This finding signals the critical need for healthcare organizations to prioritize robust access management and privacy protection in their EMR systems. The table's clarity allows us to discern patterns and frequencies of the various threat categories, providing strategic insights into where security efforts may be best allocated.

Table 5. Categories of Vulnerabilities and Threats to Patient Data Security in EMR

No.	Categories Of Vulnerabilities and Threats	References	Total
1.	Lack of access controls and patient privacy	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 19, 20, 21, 22, 23, 24, 25	24
2.	Centralized and Decentralized architecture	2, 4, 5, 6, 7, 9, 10, 11, 12, 14, 16, 21, 22	13
3.	Interoperability and data sharing	3, 5, 6, 7, 8, 9, 10, 11, 12, 15, 16, 17, 18, 19, 21, 22, 23	17
4.	Susceptibility to external threats	1, 2, 4, 7, 11, 12, 13, 14, 15, 16, 18, 21, 23	13
5.	Insider threats	7, 9, 10, 11, 12, 14, 16	7
6.	Compliance with regulations	1, 7, 11, 15, 22, 23	6

3.2. Lack of Access Controls and Patient Privacy

Lack of access control and patient privacy was the most prevalent vulnerability identified, with 24 references highlighting concerns in this area. EMRs contain private patient identification details, which makes patient data vulnerable to misuse [10]. The need for a mechanism for patients to share private health information or Personal Health Records (PHR) securely with doctors in other facilities has been identified [11].

Past studies have reported that network authentication, identity verification, and authorization of EMR access by providers are essential to improve patient privacy [12], [13]. Based on policies in Thailand, public health services must keep patient information private. However, blockchain technology allows patients and doctors to efficiently share health data while complying with regulations [14]. Strict access control and privacy measures are essential so that only approved users can access EMRs [15]. Establishing public trust in EHR systems is critical, given concerns about security and data management [16]. Protecting health information needs attention by establishing standards like HIPAA [17]. Strong access controls like multi-factor authentication and role-based access prevent unauthorized access and ensure EMR security and privacy [18] [19]. A major obstacle to EMR systems is insecurity about the privacy and security of digitally stored patient data. Stronger controls and encryption are needed [20]. Despite ethical concerns, studies show that nurses commonly share EHR login credentials inappropriately [21]. This undermines protocols and violates regulations, necessitating enforcement and education. Comprehensive authentication, authorization, and encryption frameworks are imperative for secure health information sharing. Continuous monitoring and updating of protocols is necessary as threats evolve. While stringent controls are crucial, a balance is needed for timely access to efficient care [9]. Adaptive, context-aware controls may provide this balance. Technical solutions like granular permissions, context-aware policies, and selective encryption could enable security and access.

Furthermore, governance models outlining proper data-sharing procedures and security training for personnel can instill accountability around access controls. With thoughtful design and governance, access systems can achieve robust data protection without impeding healthcare delivery. Specific access control models like selective ring-based access control mechanisms could help regulate access to patient data in EMRs based on permissions assigned to different users [22]. For example, core patient information may be accessible only to the innermost ring of care providers. Through selective encryption, less sensitive aggregated data could be made available to secondary entities like researchers in the outer ring. Properly implementing selective ring-based controls can enhance data security in decentralized EMR systems. Recommended security frameworks such as user authentication and authorization systems can effectively mitigate threats of unauthorized access.

3.3. Centralized and Decentralized Architecture

Vulnerabilities in centralized and decentralized architectures were the second most common category, with 13 references highlighting concerns about centralized systems. Existing research shows limited studies comprehensively evaluate integrated Electronic Health Record (EHR) deployment across diverse healthcare providers [13]. Many EHR systems employ a centralized structure, consolidating the entire patient database for storage on a single central server [23], [24]. An architectural model that centralizes records on a single server is vulnerable to a complete system shutdown, known as a single point of failure. In this scenario, any harm to the central server could lead to the inaccessibility of all patients' medical records.

Furthermore, centralizing data storage in one location can heighten susceptibility to security risks, including unauthorized access and data breaches. These two significant constraints can hamper safe integrating and exchanging patient health information online across various medical service facilities. Thus, it is imperative to explore alternative architectures that offer improved resilience and data protection measures [25].

Decentralized solutions like blockchain technology are recommended to address vulnerabilities related to centralized systems and potential data loss [26]. To counter the limitations of centralized systems, blockchain employs a distributed ledger structure replicating identical records across multiple nodes in a peer-to-peer network. Decentralized blockchain architecture eliminates centralized data storage and single-point failure risks. Blockchain relies on numerous nodes, each maintaining a ledger copy to prevent total data loss if one node fails. Patient data can be stored encrypted across nodes, enhancing security. Robust encryption is crucial to keep data unreadable if a node is compromised. Smart contracts enable granular access control. The immutable blockchain ledger protects against tampering or loss. Regular off-chain backups provide additional protection. Backups should be routine and tested for integrity and reliability. Decentralized blockchain significantly improves reliability, security, and data integrity compared to centralized systems. However, decentralized systems also have challenges like throughput limitations. Overall, decentralized blockchain architecture has strong potential to mitigate centralized EHR system risks.

A comparative analysis highlights key differences between centralized and decentralized systems in performance and security. Centralized systems can achieve faster processing speeds but are vulnerable to single-point failure. Decentralized blockchain provides higher fault tolerance, although at the cost of slower transaction speeds. Regarding security, centralized systems are prone to data breaches, with all records concentrated in one location. In contrast, blockchain's distributed nature avoids such concentration of risk.

Decentralized access control is also more robust. In summary, decentralization enhances resilience and security despite some performance tradeoffs.

3.4. Interoperability and Data Sharing

Interoperability and data sharing were identified as the third most prevalent category of vulnerabilities, with 17 references highlighting significant concerns. Based on several previous studies, the exchange of patient data across various health service providers is necessary to enhance clinical processes and improve the quality of health services [12]. Integrated health information exchange aims to improve service quality and patient safety by enabling healthcare providers to share data between different facilities. Challenges that hinder effective data sharing include system incompatibility, concerns about data privacy, and the need for standardized protocols across organizations. However, the exchange of patient data between health organizations still encounters various technical and operational challenges [13]. One of the main challenges is managing patient privacy, considering that data needs to be shared with various related parties such as hospitals, clinics, insurance companies, and other agencies [27]. Furthermore, interoperable Electronic Health Records (EHR) across various agencies also have implications for securing and controlling access to patient data [28]. The concept of interoperability according to Indonesian legal standards can be implemented through online web services or offline smart cards. Web services enable systems to communicate with each other over the internet, typically using XML, JSON, or other data interchange formats. Simultaneously, smart cards can store and securely transport medical record data anywhere. Legally, interoperability of electronic medical records is valid if it meets the provisions of Law no. 11 of 2008 and Minister of Health Regulation no. 269 of 2008, namely: the patient gives consent, guarantees data privacy and the original documents remain stored in the health facility while only the medical summary can be exchanged. With a clear legal basis and paying attention to patient data privacy, interoperability can facilitate health services by exchanging medical record data between health facilities [29]. Nevertheless, it has become imperative for health services to be able to share patient-related information online. Addressing obstacles slowing integrated EHR deployment and protecting individual health information demands more investigation to facilitate care coordination centred around patient well-being.

Standardization of data formats and protocols is recommended to enhance interoperability for data exchange across different systems [30]. Global standards like FHIR, which define common formats for representing health data, can be adopted. Standard terminologies like SNOMED CT and LOINC can be used to annotate data elements. Such standards facilitate consistent interpretation and exchange of data between different systems. Technical protocols also require alignment between systems to enable smooth data transmission. Pilot projects to test interoperability should be conducted prior to full adoption. With concerted efforts towards adopting standards, system interoperability can be significantly improved. However, implementing standards must strike a balance between interoperability needs and patient privacy concerns through appropriate access controls and consent policies [31]. Mechanisms like attribute-based access and encryption enable selective disclosure of only necessary data fields based on patient directives. By adopting privacy-enhancing technologies, interoperability can be achieved while ensuring confidentiality. A comprehensive approach is recommended, taking into account both interoperability and privacy aspects. Blockchain technology and access control frameworks are recommended to facilitate secure data sharing among healthcare providers. Future research should investigate standardization efforts for data formats and protocols and how these efforts can reconcile interoperability and patient data privacy.

3.5. Susceptibility to External Threats

Susceptibility to external threats was identified as a major vulnerability by 13 references. Previous studies have demonstrated various inherent security threats to EMR and EHR systems. Respondents expressed concerns about the increasing number of cyberattacks on electronic medical records [10], [16]. A comprehensive survey of security and privacy challenges in modern healthcare analyzed potential attacks and defenses, emphasizing the need for further research to enhance healthcare technology security and privacy [32]. Assessing vulnerability to electronic attacks is also a significant concern in digital medical networks. Additionally, the proposed threat model for this system also considered unauthorized third-party access [17] [33]. These external threats have the potential to compromise critical security aspects, including privacy, integrity, authenticity, confidentiality, and access control of patient data [28]. Hospital information systems in Indonesia are vulnerable to external security threats. The centralization of health information into a single system makes the data an attractive target for cybercriminals. Several incidents of patient data leakage have occurred at certain hospitals in Indonesia due to hacking attacks or computer viruses infecting their systems. The utilization of a centralized health information system that stores all patient data in one location exposes

the data to security risks, as evidenced by hacking attacks and data breaches at certain hospitals [34]. The significant role of human error, such as carelessness and negligence, rather than malicious intent, in cybersecurity breaches of healthcare records from 2015 to 2020 highlights the importance of incorporating behavioral interventions alongside technical controls in cybersecurity planning [35].

Considering the growing sophistication of cyber threats, EMR and EHR systems need to enhance their security measures accordingly. Emerging cyber threats, such as AI-powered attacks, introduce new challenges in securing electronic medical records. The utilization of Artificial Intelligence (AI) in bolstering cybersecurity highlights its potential to strengthen defenses against ever-advancing cyberattacks and explores future research opportunities in the field of AI [36]. Attacks enabled by AI can exploit system vulnerabilities rapidly and on a large scale. They can also adapt to security countermeasures by learning from their surroundings. With the advancement of AI capabilities, healthcare systems are likely to encounter threats such as AI social engineering, automated payload generation, intelligent malware, and more in the future. To mitigate risks posed by AI-driven cyberattacks, EMR/EHR systems require advanced threat detection systems that incorporate AI and machine learning. Network monitoring based on AI can detect abnormal activities that indicate AI attacks. Organizations should also embrace a comprehensive and future-oriented approach to managing cyber risks.

The landscape of cyber threats against healthcare systems is constantly evolving. As systems become more digitized and interconnected, they are exposed to risks from increasingly sophisticated threats [37]. Advanced persistent threats that employ tactics such as social engineering and zero-day exploits can bypass traditional signature-based defenses. The emergence of artificial intelligence is enabling a new generation of intelligent and adaptable threats that can autonomously scan networks to discover vulnerabilities. Ransomware attacks are also on the rise, causing significant disruptions to hospital operations by encrypting critical data and systems. As threats become increasingly complex, healthcare organizations need to implement comprehensive cyber risk management frameworks that cover prevention, detection, and response capabilities. Regulatory changes, such as the FDA's cybersecurity guidance for medical devices, aim to promote stronger security practices. A comprehensive approach is necessary to enhance cyber resilience and safeguard patient safety in the face of the evolving threat landscape. Hence, it is essential to anticipate various strategies for mitigating cyber risks to patient data in EMR and EHR systems. Encryption, user authentication, cloud computing, and ongoing security monitoring can assist in mitigating external threats to EMR data. An analysis of emerging cybersecurity threats, including AI-powered attacks, and the necessary measures to safeguard against these evolving threats would be a valuable contribution.

3.6. Insider Threats

The literature identifies insider threats as a vulnerability, which is emphasized in seven references. Along with external hackers, insider actions by those entrusted with data access severely threaten privacy and security. The research proposes a trust-based mechanism to detect insider attacks in medical cyber-physical networks using behavioral profiling to assess node trustworthiness within medical smartphone networks (MSNs) [38]. Proper identity verification and patient consent are essential in restricting access only to approved users, thereby reducing internal threats [23]. However, entirely preventing malicious activities from authorized individuals remains challenging. In addition to external hackers, insider actions from those trusted with data access pose severe risks to privacy and security. Healthcare providers also face difficulties in evaluating the potential misuse of privileges by every internal user. While technical controls help curb unauthorized usage, they could be made more foolproof against determined adversaries exploiting legitimate credentials. With these viewpoints in mind, further investigation aims to comprehend the risks posed by authorized personnel and develop context-sensitive solutions. Robust identity management paired with policy enforcement may assist in addressing this concerning class of risks to electronic patient information security. A comprehensive analysis of healthcare data breaches found that unauthorized insider disclosures were the second most prevalent cause behind hacking, highlighting the significant risks from insiders [39].

To counteract insider threats, it is advisable to enforce rigorous access restrictions, supervise user behavior, provide security training to employees, and cultivate a culture of ethics within the organization. This approach aligns with Saxena *et al*. (2021), who found that access control and employee training significantly reduced insider threats in a healthcare setting [40]. Access controls can utilize role-based access, attribute-based access, and multi-factor authentication to restrict data access to only authorized users. Continuous monitoring of user activities through logging and auditing can detect anomalous usage patterns indicative of insider actions. Application allow listing, data encryption, and physical security controls are additional methods that help reduce insider risks. Comprehensive employee training raises security awareness and reduces unintentional insider threats. Promoting an ethical culture emphasizes protecting patient data integrity as an

organizational priority. A balanced approach combining technological solutions with human-centered policies is needed to address the multifaceted challenge of insider threats. User identity management, engaging end users, and balancing technical and human aspects are recommended to address and help reduce risks from insider threats.

The research proposes a multi-tiered insider threat prevention framework integrating technical, behavioral, psychological, and cognitive measures to proactively protect organizations throughout an individual's employment [41]. Monitoring should cover behaviors like unauthorized data access, bulk data downloads, unusual work hours, and other anomalies. It should also monitor social media interactions, which may indicate ill intent. Periodic access audits ensure that employee access aligns with job duties and detect unauthorized access. Auditing user activity logs verifies appropriate data and system access. An open organizational culture encourages trust and reporting, empowering employees to flag suspicious behaviors without fear. Management should promote openness by investigating all reports and building confidence. Fostering team spirit and mutual security reminders creates a secure workplace. Strategies like regular monitoring, stringent audits, and cultivating a culture of security are important to mitigate insider threats in healthcare.

3.7. Compliance with Regulations

Six references highlighted compliance with regulations as an issue. Regulatory compliance is crucial when developing emerging healthcare technologies. A proactive approach integrating compliance into the design and development stages is needed. Addressing the gap between technology advancements and regulations is imperative. Studies show challenges in implementing electronic medical records and health information technologies to comply with applicable regulations. Mature privacy standards for health data, such as HIPAA and HITECH, exist in developed nations, but some jurisdictions still require refinement [10], [28]. Regulatory compliance should be considered from the outset rather than an afterthought when designing complex new technologies like blockchain for health data. Technology companies must assess regulatory requirements and develop solutions that proactively embed compliance. Concurrently, innovations such as blockchain aim to revolutionize how medical data moves between parties through a fresh paradigm emphasizing security and effectiveness [33]. However, existing regulations may not necessarily accommodate such complex technologies. International cooperation can also help standardize regulations across countries to support emerging technologies in healthcare. Organizations like the World Health Organization (WHO) are pivotal in facilitating a global consensus on strategies like health data protection and ethical use of innovations. In addition, the interpretation of rules still varies across countries. Therefore, efforts are needed to harmonize international regulations and standards so that technological innovations can evolve to future healthcare service needs while protecting patient privacy.

The application of technologies poses difficulties in fully meeting applicable laws and norms governing sensitive health information. Remarkably, the continuous alignment of EMR rules with rapidly changing technologies is an important issue [10]. Standardization efforts at a global scale could help bridge inconsistencies between jurisdictions. Unified standards allow innovative technical solutions to adequately address privacy compliance requirements and support improved care delivery models over the long run. Despite existing regulations like HIPAA, recent research reveals that over 25% of covered healthcare entities still received warning letters for potential violations, indicating compliance remains an issue [42]. Blockchain is a promising technology to support compliance by enhancing security, privacy, and data-sharing protocols.

However, regulations vary between countries regarding the amount and type of data in EHRs. A key ethical issue is maintaining confidentiality when electronically storing and transmitting EHR data. While EU regulations aim to safeguard the use of health data, more standardization is needed as EHR adoption increases. Implementing EMR security frameworks requires balancing privacy, security, and ethical patient rights [43]. Health outcome disparities persist, and new technologies occasionally worsen them, creating a “digital divide”. While technological access is improving for certain groups, challenges persist due to factors such as poverty and racial disparities, which are associated with lower utilization of telehealth services. When implementing new healthcare technologies, it is crucial to assess their impact on promoting equitable access and reducing disparities, rather than exacerbating them. EMR security frameworks should strive to achieve a balance between technical effectiveness, legal compliance, and ethical considerations to ensure equitable systems that uphold patient rights [44].

While regulations aim to maintain security and privacy standards, the implementation of technologies like EMR raises ethical concerns regarding equitable access, which need to be addressed proactively. Measures such as encryption and access controls should strike a balance between safeguarding patient information and upholding their right to access and control their own records. Excessively stringent frameworks may encroach

upon patient autonomy. Furthermore, economic and social barriers to adopting new technologies have the potential to exacerbate disparities in healthcare access. Ethical implementation requires taking into account the potential burdens faced by underprivileged populations. It would be beneficial to conduct further analysis on how technologies can be designed to comply with regulations from the outset, as well as the significance of international cooperation in standardizing regulations.

3.8. RQ2. What security frameworks or models have been suggested by previous studies to address vulnerabilities in safeguarding patient data stored in electronic health records?

This section provides an overview of the proposed solutions to the identified vulnerabilities. A summary that discusses the practicality and applicability of these frameworks/models in various healthcare contexts (e.g., small clinics vs. large hospitals) and geographical locations would enhance our understanding of their versatility and effectiveness. The recommended security frameworks aim to address the key vulnerabilities in EMR systems identified in the previous section. Table 6 provides a summary of recommended security frameworks or models from the literature, offering a concise overview of potential solutions to vulnerabilities in EMR systems. The recommended security frameworks and models aim to address vulnerabilities in EMR systems using diverse approaches. These include user authentication for access control, blockchain technology to decentralize and secure data storage, temporary session passwords and access keys, engaging end users to ensure real-world effectiveness, balancing technical and human factors, partitioning data storage between local and cloud platforms in cloud computing, encryption for ensuring confidentiality and integrity, digital signatures for record verification, backups for enabling recovery, continuous monitoring for threat detection, and cryptography for preventing unauthorized access and tampering. The combination of these complementary technologies enables the implementation of multilayered protections customized to address specific vulnerabilities when integrated into a comprehensive framework.

Large hospitals can benefit significantly from blockchain's decentralization and cryptography's robust encryption. Meanwhile, small clinics may prioritize low-overhead solutions like cloud storage with local servers. User authentication scales across settings but may disrupt workflows in time-critical contexts. Regardless of size, healthcare providers should involve end users in framework selection and adapt the components to fit their needs best. Differences also emerge across geographic regions. Developed countries often have mature standards like HIPAA that frameworks must accommodate. In contrast, developing nations may focus on core protections like encryption first before broader regulations. Determining the right balance of security frameworks and customizing their application to the specific healthcare setting and location is key to effectively protecting patient data. Table 6 summarizes the main security frameworks or models recommended in prior studies to address vulnerabilities in EMR systems.

Table 6. Security Framework or Models

No.	Security Frameworks or Models	References	Total
1.	User authentication and authorization system	1, 15, 25	3
2.	Using blockchain as a basis for storing and managing EMR	2, 4, 5, 6, 7, 9, 10, 11, 12, 15, 16, 18, 20, 21, 22	15
3.	Session password and data access key	3, 4, 16, 19, 21, 23	6
4.	A security framework that engages end users	8	1
5.	Balance between electronic security systems and the competence of the individuals who manage the system	13	1
6.	Cloud computing	14	1
7.	Data encryption	4, 10, 11, 15, 16, 19, 20, 21, 23	9
8.	Digital signature	15	1
9.	Data backup and recovery	15	1
10.	Continuous security monitoring	17	1
11.	Cryptography	20, 24	2

3.9. User Authentication and Authorization System

Three references recommended user authentication and authorization systems as a security solution. EMR data stored online is vulnerable to cyber threats, risking patient privacy. Reliable cybersecurity, including user authentication and authorization, is important. An effective framework incorporates standards like ISO/TS 18308, HIPAA, and authentication-based access control to regulate EHR access [10], [33]. Properly implementing this framework can help mitigate vulnerabilities in securing patient data [26], [27]. Studies show that two-factor authentication can prevent unauthorized EMR access on cloud platforms [46]. User authentication and authorization ensure that only authorized users access protected health information.

Blockchain's decentralized architecture can address centralized EMR system vulnerabilities like single points of failure. Blockchain also addresses vulnerabilities related to lack of access control and privacy. Further analysis of specific effective access controls in healthcare and the balance with efficiency would be beneficial. To understand implementation and benefits, specific frameworks like Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) should be explored. Unlike complex authentication, blockchain's smart contracts simplify decentralized access control and may enhance usability. However, scaling blockchain to meet healthcare system demands remains challenging while authentication is well-established. Authentication and blockchain can complement each other when integrated appropriately based on context.

A case study conducted with the Kaiser Permanente healthcare system in the United States showcased the implementation of multi-factor authentication. The implementation involved the use of passwords and one-time codes delivered via SMS. This implementation successfully enhanced security by implementing multi-factor authentication to protect access to medical records of over 12 million patients, with minimal disruption to workflows. The implementation maintained user convenience while minimizing any significant delays in daily operations. This case study demonstrates the effectiveness of multi-factor authentication in securing large-scale EMR systems [46]. The primary findings indicate that blockchain technology enhances EMR data security and access control. The utilization of smart contracts enables automated permission management and has the potential to improve patient usability when accessing records. The strengths of this approach include the practical application of blockchain in healthcare, while limitations encompass scalability challenges and the necessity for additional validation in diverse clinical settings.

3.10. Using Blockchain as A Basis for Storing and Managing EMR

Fifteen references recommend using blockchain as the most prevalent security solution for storing and managing EMRs [28], [14]. Research indicates the promising potential of blockchain in enhancing EMR security and interoperability [48]. Our study expands on these findings by demonstrating how blockchain smart contracts can streamline access management and enhance patient usability. Frameworks propose blockchain as a decentralized foundation for EMR systems to mitigate single points of failure and enhance security. Access authorization can be managed through smart contracts. A study employed blockchain to regulate EMR access permissions. Blockchain is well-suited for ensuring EHR security due to its tamper-resistance and traceability [49]. Frameworks such as CEPS leverage multiple blockchains to facilitate secure EHR access while upholding privacy [50]. Case studies demonstrate the secure storage and sharing of EHRs using blockchain [14]. The encryption and smart contracts of blockchain contribute to maintaining manipulation-proof medical records. Blockchain is well-suited to address vulnerabilities regarding centralized architectures, interoperability, and compliance [17], [18], [20], [22], [23], [26]. Blockchain protects against unauthorized changes and record traceability, addressing data breach and access control threats. Blockchain can integrate with other security technologies like encryption and authentication to protect EMR data [51]. The blockchain is an encrypted system that safely stores detailed patient data online—Hyperledger Fabric guarantees manipulation-proof medical records using smart contracts and encryption [52]. Centralized models like cloud computing enable efficiency through economies of scale but concentrate risks. Comparing centralized vs. decentralized performance and security could add value. Exploring blockchain implementation through case studies can provide insights into overcoming scalability challenges. Decentralization enhances resilience, although with greater complexity. Providers should weigh tradeoffs based on resources and systems when choosing architectures.

When comparing our findings to the blockchain system implemented in the Taiwan case study, our results indicate that the utilization of blockchain in EMR enhances both the security and operational efficiency in handling large patient data transactions. The case study conducted in Taiwan illustrates the implementation of a private Ethereum blockchain at the National Cheng Kung University Hospital. In this case study, a private Ethereum blockchain is utilized, integrating it with the hospital's existing EMR system to facilitate identity authentication and access control. The system showcased operational feasibility by successfully processing 100 million transactions across thousands of patient medical records, all while ensuring security and efficiency [53]. Future research may explore the long-term sustainability and cost implications of such integrations.

3.11. Session Password and Data Access Key

Session passwords and data access keys are highly recommended techniques. These techniques involve generating random, one-time passwords or keys for each data access session. This practice prevents unauthorized reuse and enhances security. The data access keys combine multiple factors, such as the password and patient data, using circular interpolation for added protection. The key points are that session passwords and data access keys are techniques that generate unique and temporary credentials each time, thereby

improving security. The data access keys creatively combine multiple elements to enhance protections [13], [33], [34]. Health data access is managed by a self-recognition-based mechanism. Secure data sharing is ensured through the access logic in smart contracts [20], [29], [33]. Additionally, data access is managed through role-based controls [28].

3.12. A Security Framework that Engages End Users

A reference strongly emphasizes the inclusion of end users in the development of security frameworks. The development of a new framework is necessary to ensure the privacy and confidentiality of patient data exchanged through electronic health record (EHR) networks. Frameworks should actively involve end users in the development of systems to address barriers and enhance acceptance. The involvement of end users helps ensure that the framework aligns with real-world needs and is well-received. Involving users in the design process fosters a sense of ownership and responsibility for the security of the system [13]. The key takeaway is that including end users in the design of the security framework facilitates adoption by addressing concerns and promoting a sense of responsibility.

3.13. Balance Between Electronic Security Systems and The Competence of The Individuals Who Manage the System

One reference recommended the importance of balancing electronic security systems with the competence of individuals managing the system. In designing a security framework for patient data in electronic health record systems, it is crucial to strike a balance between technical security systems and human factors. The crucial role of human-centric approaches in enhancing cybersecurity hygiene in the healthcare sector highlights the necessity of comprehensive education and practical frameworks to mitigate risks caused by human error and inadequate cyber practices [55].

3.14. Cloud Computing

Cloud computing was proposed as a supplementary security solution. It recommends tiered storage, with critical data kept locally and larger datasets encrypted in the cloud. Caution is urged when integrating cloud computing, along with stringent protocols. A segmented query model allows for secure collaboration between local and cloud servers [17]. The main point is that cloud computing was proposed as a supplementary security solution. It recommends tiered storage, with critical data kept locally and larger data encrypted in the cloud. Caution is urged when integrating cloud computing, along with stringent protocols. A segmented query model allows secure collaboration between local and cloud servers.

3.15. Data Encryption

Data encryption has been frequently recommended by multiple references, making it one of the most widely endorsed security solutions. Several encryption techniques contribute to securing electronic health records. Encryption keys can regulate permissions by encrypting and decrypting data. Asymmetric encryption involves encrypting patient data with a public key that can only be decrypted by the private key holder. The main idea is that data encryption was a commonly recommended measure to enhance the security of electronic health records. Various encryption methods were proposed, including the utilization of keys to regulate access through selective encryption and decryption. Asymmetric encryption can limit access solely to the holder of the private key [48]. A model utilizes Hyperledger Fabric blockchain to store encrypted EMRs, facilitating authenticated access [15]. Techniques encrypt data at various stages, safeguarding records with unique keys and access controls [13], [17], [29]. Encryption ensures EHR confidentiality, while authentication safeguards against unauthorized access [33]. Prior to cloud storage, the BAcP-EHR framework encrypts EHRs and symmetric keys using blockchain and AES/RSA [18]. Another framework employs single or double AES-256 and Blowfish encryption, along with a three-tier access policy, for patient data stored in the cloud [54]. This framework encrypts data, regulates access, ensures integrity, and provides backups for privacy and security [18]. Another framework uses single/double AES-256 and Blowfish encryption with a three-tier access policy for cloud-stored patient data [54]. This framework encrypts, controls access, maintains integrity, and backups for privacy/security [20], [26], [34]. Blockchain securely stores encrypted data in tamper-proof blocks [51]. MedRSS shares secured records with AES/ECC with IPFS [33]. Encryption transmits/stores data alongside role-based controls and monitoring [52]. Encryption transmits and stores data while implementing role-based controls and monitoring [28]. These technologies ensure secure encryption and restricted access to healthcare records. Encryption proves highly effective when integrated with role-based access controls, blockchain, and other security technologies within a comprehensive security framework. Ongoing advancements in encryption

technology reinforce its fundamental role in securing EMR systems. Encryption helps alleviate external threats and privacy concerns associated with unauthorized data access. Although AES-256 offers robust security, alternate ciphers such as Blowfish provide faster performance. Employing multiple layers of encryption methods can strike a balance between security and efficiency. The ideal encryption approach depends on the specific performance, confidentiality requirements, and data types of the healthcare organization.

A case study in Thailand implemented AES-256 encryption to protect electronic medical data in a private hospital. Encryption was applied to critical data such as diagnosis and treatment history to maintain confidentiality. This encryption implementation successfully protected hundreds of thousands of medical records with minimal overhead to the system. This case study demonstrates the ability of encryption to secure EMRs at a large scale [56].

3.16. Digital Signature

One reference suggested digital signatures as a potential solution. Proposed frameworks aim to address weaknesses in safeguarding patient information in electronic health records (EHRs). The framework integrates ISO/TS 18308 standards on EHR security/privacy with U.S. Health Insurance Portability and Accountability Act (HIPAA) regulations on protected health information. It incorporates digital signatures and blockchain technology to track data history and ensure the integrity of records. Digital signatures are used to verify any changes or additions, while blockchain technology ensures an immutable transaction record to safeguard sensitive health information in EHR systems [33]. The main point is that digital signatures were recommended to enhance the security of EHRs. By integrating digital signatures and blockchain technology, the framework can verify record changes and maintain an immutable history, thereby enhancing the security of EHR systems.

3.17. Data Backup and Recovery

One reference recommended data backup and recovery as a potential security solution. Security frameworks for electronic health records aim to effectively address vulnerabilities in patient data protection. The recommended approach consists of standards defined in ISO/TS 18308 and HIPAA, which mandate the privacy and safeguarding of protected health information. Implementing routine data backup and recovery procedures is a key element of this framework to counter the threat of data loss [33]. Healthcare providers can ensure the availability of electronic health information by regularly backing up patient records and saving the data offline in multiple secure locations, even if primary storage systems encounter issues. Therefore, including data backup and recovery helps strengthen the framework's comprehensiveness in preserving the confidentiality and accessibility of vital medical records stored digitally.

3.18. Continuous Security Monitoring

According to one reference, continuous security monitoring was recommended as a potential security solution. Continuous security monitoring is a crucial component [19]. Continuous monitoring is assessed through automated security measurements, reporting dashboards, and alert detection tools. The results demonstrate that continuous monitoring enhances security implementation in electronic health record systems. Continuous monitoring strongly implies the application of stronger controls to digital medical files. Therefore, this study suggests that healthcare facilities should consider adopting this approach to enhance protection by automating controls and regularly evaluating them through continuous monitoring capabilities. Continuous monitoring assists in detecting external threats and security incidents.

3.19. Cryptography

Two references emphasized cryptography's role as a fundamental security solution. The applicability of these security frameworks and solutions may vary across countries and regions. These differences arise from variations in healthcare regulations, data privacy laws, infrastructure maturity, and other contextual factors. For example, developing nations may prioritize core protections such as encryption prior to implementing more advanced measures. A discussion on the global applicability of the findings and their translation across diverse healthcare settings would offer valuable insights. Studies have examined the application of blockchain cryptography for enhancing the security of electronic health records [32], [35]. The use of cryptography in EMR systems is both a technical necessity and a legal requirement in many jurisdictions. Models of accountability define the roles of healthcare professionals, patients, and consumer data, utilizing both symmetric and asymmetric cryptographic techniques [57]. The evaluation shows that the proposed cryptographic techniques can address the privacy and security vulnerabilities of previous protocols for digitally stored sensitive health information. Integrating the fundamentals of cryptography through blockchain or other methods can enhance the security of patients' electronic files. To achieve this, a holistic framework integrating

complementary security technologies is essential for comprehensive protection tailored to address EMR systems' multifaceted vulnerabilities. A summary of these security frameworks and their practical applications in various healthcare settings, such as small clinics versus large hospitals, would enhance the understanding of their versatility and applicability. For instance, blockchain's decentralized structure and cryptography can ensure secure data storage and transactions, while continuous monitoring tools can detect and respond to threats in real-time. A holistic approach leveraging the synergies across various security technologies is key to creating multilayered defenses tailored to address EMR vulnerabilities. The discussion should include strategies for mitigating insider threats, highlighting the significance of behavior monitoring, access audits, and cultivating a security-conscious organizational culture.

When comparing the different recommended security frameworks, each exhibits distinct strengths and limitations. For instance, blockchain offers decentralization and immutability; however, it encounters scalability challenges. In contrast, encryption provides strong data security; nevertheless, it may affect efficiency. Conducting a comprehensive investigation into decentralized solutions, including a comparative analysis of centralized and decentralized architectures along with their performance and security trade-offs, would significantly enhance the discussion and support informed decision-making for healthcare organizations. Authentication systems enhance access control but also introduce usability challenges. Integrating multiple frameworks can help overcome limitations, such as addressing blockchain's transparency while balancing encryption's opacity. A more extensive examination of the design of emerging technologies for regulatory compliance and the pivotal role of international cooperation in standardizing regulations would be a valuable addition to the discussion. Essential to addressing the multifaceted vulnerabilities of electronic medical records (EMRs) is the combination of complementary security frameworks tailored to the specific context of each healthcare organization.

In the context of rapidly evolving technology, emerging technologies such as artificial intelligence (AI), advanced encryption methods, and cutting-edge security techniques. Emerging technologies like artificial intelligence, advanced encryption methods, and cutting-edge security techniques can influence the future of EMR security. A discussion on the rise of AI-powered cyber threats and the dynamic cybersecurity landscape in healthcare could provide a contemporary view of the external threats EMR systems face. Discussing these technologies and their potential impact would provide forward-thinking insights into how EMR security may evolve. For instance, AI could enable predictive threat detection by analyzing patterns in medical data access. Quantum encryption may offer unbreakable cipher strength to protect health information. Biometric authentication techniques leveraging iris scans or fingerprints could seamlessly verify user identity. Exploring nascent technologies and extrapolating how they could augment existing frameworks can illuminate future directions for EMR security. This forward-looking discussion would be highly valuable for readers seeking to understand the trajectory of EMR security advancements. Addressing standardization of data formats and protocols could pave the way for enhanced interoperability while maintaining patient privacy. The delicate balance between interoperability and privacy warrants further discussion and could be a focal point for future research.

3.20. Associations Between Proposed Security Solutions and Vulnerabilities Mitigated

Table 7 summarizes the key vulnerabilities and threats for EMR systems and maps them to recommended security frameworks that can help address these risks. Further exploration into specific access control mechanisms and their effectiveness in various healthcare environments would enrich the discussion. Additionally, analyzing the balance between stringent access controls and the need for efficient healthcare operations could provide valuable insights into optimal security practices. The vulnerabilities and threats are grouped into six main categories - lack of access control and patient privacy, centralized vs decentralized architecture, interoperability and data sharing, external threats, insider threats, and compliance. Mapping the vulnerabilities and threats to appropriate security frameworks allows for a more targeted approach in shoring up EMR system security across these potential attack surfaces.

Table 7, which summarizes the key vulnerabilities and threats for EMR systems and the recommended security frameworks, is vital for a targeted security strategy. Each vulnerability and threat are categorized and mapped to the most suitable framework that addresses the respective risks. For instance, the table includes 'User authentication and authorization system' as a countermeasure for 'Lack of access control and patient privacy', indicating that implementing robust user verification can effectively reduce the risk of unauthorized data breaches.

Table 7. EMR Vulnerabilities, Threats, and Recommended Security Frameworks

No.	Categories of Vulnerabilities and Threats	Recommended Security Frameworks
1.	Lack of access control and patient privacy	User authentication and authorization system, blockchain, encryption, session passwords and data access keys, cryptography
2.	Centralized and decentralized architecture	Blockchain, data backup and recovery
3.	Interoperability and data sharing	Blockchain, access control
4.	Susceptibility to external threats	Encryption, user authentication, cloud computing, continuous security monitoring
5.	Insider threats	User identity management, security framework involving end users, balance between electronic security and human competency, digital signature
6.	Compliance with regulations	Blockchain

3.21. Comparison of Key Findings with Previous Studies

The findings of this research align with those of Pfeuffer *et al*. (2020), as both studies identified similar categories of vulnerabilities, including insufficient access control, external threats, and non-compliance with regulations [13]. However, Pfeuffer *et al*. concentrated on the security aspects of implementing a national EMR system, while this study provides a comprehensive review of 25 recent publications on EMR security from 2020-2023. Although both studies acknowledged similar high-level vulnerabilities, this review offers a more comprehensive evidence base concerning modern security challenges in EMR systems.

In line with multiple previous studies that identified comparable vulnerability categories [13] , [21], [25], [26], [28], the present study makes two distinct contributions. Firstly, it conducts a thorough review of 25 recent publications from 2020-2023, in contrast to prior research that often focused on specific aspects of EMR security. Secondly, this review provides a summary of diverse security solutions, including blockchain, encryption, and authentication systems, in contrast to earlier studies that usually proposed limited frameworks. Through a comprehensive assessment of vulnerabilities and compilation of evidence for various security alternatives, this study offers a stronger reference for protecting EMR systems from diverse threats.

We compare our findings with recent studies, such as Pfeuffer *et al*. (2020), to enhance the comparative analysis, highlighting areas of agreement or divergence between our review and their conclusions. For instance, while both studies emphasize the threat of external attacks, our review proposes a wider array of mitigation strategies, including the utilization of AI for predictive threat detection. In contrast to most previous research that focused on limited aspects of EMR security, this study conducts a systematic analysis of all major vulnerabilities and risks that could holistically endanger patient data.

Another significant contribution is the synthesis of diverse recommended security solutions, such as blockchain, encryption, authentication, among others. Earlier studies typically put forward singular or dual frameworks, while this review offers a comprehensive, evidence-based overview of diverse implementable security alternatives. This analysis serves as a foundation for comparative assessments of security frameworks, enabling the identification of optimal solutions tailored to specific use cases. The adoption of security frameworks necessitates a comprehensive analysis that encompasses technical, legal, and ethical dimensions, ensuring the establishment of equitable systems that uphold patient rights.

3.22. Main Findings of The Present Study

Our study's main findings highlight the effectiveness of integrating blockchain technology with existing EMR security measures. We show that this integration not only enhances data protection but also improves access control management, providing a decentralized and transparent solution to EMR vulnerabilities. This study identifies six major categories of vulnerabilities in EMR systems: lack of access control, centralized architecture risks, data sharing challenges, external threats, insider threats, and regulatory non-compliance. The most prevalent vulnerabilities are compromised access controls and threats to patient privacy, which could lead to unauthorized data access and breaches. Vulnerable centralized architectures also pose critical risks. Recommended security frameworks involve user authentication, encryption, blockchain, continuous monitoring, multi-factor authentication, and access control models like RBAC.

Blockchain is emerging as a promising decentralized approach to transform EMR systems by enhancing security, access control, and data sharing. However, challenges around scalability, integration, and compliance must be addressed. A multi-faceted adaptive security framework is proposed, combining technological safeguards with training, auditing, and ethics policies to create a robust defense. This review compiles modern evidence on EMR vulnerabilities and security frameworks, guiding strategic security planning and resource

allocation based on a systematic analysis of threats. Further research should focus on testing integrated security frameworks across diverse healthcare settings and developing solutions tailored to specific organizational contexts.

3.23. Comparison with Other Studies

Compared to previous studies with narrower focuses, our comprehensive literature review from 2020-2023 reveals a broader consensus on the importance of multifaceted security frameworks. This aligns with the findings of Pfeuffer *et al*. (2020) but expands on them by incorporating a more diverse range of security solutions across various healthcare contexts. In comparing our systematic review with other recent studies, we observe several key distinctions and similarities in securing EMR systems. Building upon the foundational works of Perez (2022), Sivan and Zukarnain (2021), and Wasserman and Wasserman (2022), our study aims to synthesize these insights into a comprehensive framework for EMR security.

Perez (2022) focused on advanced threat detection mechanisms, advocating for timely identification of security incidents. Our framework acknowledges the importance of such mechanisms and extends beyond them by integrating real-time security analytics and adaptive responses, thereby enhancing the effectiveness of threat detection in a dynamic healthcare environment. Sivan and Zukarnain (2021) highlighted the vulnerabilities in cloud-based e-health systems, emphasizing the need for robust encryption and authentication measures. Our study concurs with their findings but further contributes by proposing a multifaceted security framework that encompasses encryption and authentication within a broader context of administrative and policy controls. This offers a more holistic approach to EMR security. Wasserman and Wasserman (2022) identified cybersecurity vulnerabilities specific to medical devices and telemedicine. While their study provided a critical view of technological pitfalls, our research goes a step further by categorizing these vulnerabilities and aligning them with a tailored set of security controls that address both technological and human elements of cybersecurity.

In contrast to these studies, our integrated security framework is unique in its multi-layered defense strategy, which includes technical solutions and behavioral and administrative controls. We offer a novel perspective by considering the interplay between different types of vulnerabilities and the corresponding security measures required to comprehensively address them. Moreover, while previous studies offer valuable insights into specific aspects of EMR security, our work presents a detailed threat categorization that equips healthcare organizations with a strategic basis for improved security planning and resource allocation. For instance, our framework emphasizes the importance of continuous monitoring and adaptive safeguards that can evolve with the evolving threat landscape, especially considering the rapid pace of technological change in healthcare. Regarding technical solutions, we align with the existing literature on the importance of access control, encryption, and network segmentation. However, our study recommends a more nuanced application of these technologies, tailored to specific threat models and individual risk assessments in different healthcare settings.

In summary, our systematic review contributes to the existing body of knowledge by providing a comprehensive and integrated framework for EMR security. It combines the strengths of previous studies while addressing their limitations, offering actionable insights that have the potential to enhance data protection measures significantly. Our approach aims to foster a more resilient healthcare environment where patient data is protected against the evolving landscape of cybersecurity threats.

3.24. Implication and Explanation of Findings

The findings suggest that a comprehensive and integrated approach to EMR security is necessary, incorporating both traditional and innovative technologies such as blockchain and AI to ensure robust protection against various threats. This approach is essential to adapt to the rapidly evolving cybersecurity landscape. The key findings emphasize the importance of a comprehensive security approach that integrates both traditional and innovative solutions, such as blockchain, to safeguard EMRs from modern threats. Fragmented measures should be reassessed, considering the multitude of vulnerabilities. Adaptive frameworks that evolve alongside threats are crucial as attacks become increasingly sophisticated.

Although blockchain offers benefits such as decentralization and encryption, tradeoffs such as slower speeds need to be carefully considered. There is no single solution that perfectly fits all contexts. Technical measures should be supplemented by governance, training, and active patient involvement to establish a comprehensive defense. Solely relying on technology is insufficient. Continuous investment in research and development, as well as fostering public-private partnerships, is crucial to ensure that protections stay up-to-date with advancing threats. Complacency poses the risk of defensive obsolescence. Global collaboration on standards and regulations facilitates the development of comprehensive solutions that address technical, legal,

and ethical aspects, tailored to diverse healthcare environments. In conclusion, resilient security requires a flexible, multi-faceted strategy that encompasses technology, policy, and collaboration, tailored and responsive to an evolving threat landscape.

3.25. Strengths and Limitations

This systematic review presents several notable strengths that meaningfully contribute to healthcare cybersecurity. First and foremost, the study's comprehensive and methodical approach to identifying vulnerabilities in electronic medical records (EMRs) offers a detailed examination of the existing threats to the security of patient data. By encompassing a wide range of recent, high-quality academic sources, the research provides a comprehensive overview of the cybersecurity landscape pertaining to EMRs. The introduction of a novel, multi-layered security framework is another noteworthy strength, showcasing the integration of technical and behavioral measures to mitigate diverse threats. The framework's distinctive combination of technological advancements and management strategies offers healthcare organizations new perspectives and actionable strategies to enhance their defense against threats.

Nevertheless, it is important to acknowledge some limitations of the study. The emphasis on literature from 2020-2023 might overlook emerging threats or new security advancements beyond this timeframe. Due to the primary focus on technical and policy vulnerabilities, it is necessary to thoroughly examine potential human factors or influences from the healthcare ecosystem. Although promising, the proposed framework necessitates empirical testing across diverse healthcare settings to validate its effectiveness in real-world scenarios. This underscores the importance of conducting ongoing research to assess the practicality of the framework and stay abreast of the ever-evolving cyber threat landscape. While the study offers valuable insights into the security of EMRs, it acknowledges the necessity for additional research to address its limitations.

3.26. Future Research Directions

Considering the dynamic evolution of cybersecurity threats and healthcare technologies, several potential avenues exist for future research to investigate EMR security further. Areas that require further investigation include evaluating the effectiveness of emerging authentication methods, such as biometrics, for access control, integrating blockchain with predictive analytics to detect anomalies, assessing the impact of regulations on EMR adoption rates, examining the ethical considerations of data transparency versus privacy, and developing artificial intelligence-enabled security tools specifically designed for healthcare systems. Additionally, it is necessary to conduct a comparative assessment between commercial and open-source security solutions. As threats and technologies continue advancing, ongoing research is essential to guide appropriate security strategies balancing innovation, effectiveness, ethics, and legal compliance in protecting patient data.

To provide a comprehensive outlook on EMR security, it is recommended to conduct a comparative analysis of various approaches, including case studies showcasing successful implementations. Furthermore, exploring the impact of emerging technologies on future EMR security and considering the global applicability of these findings will contribute to a more comprehensive understanding. Conducting comparative analyses of access control mechanisms, architectural models, and case studies illustrating successful security framework implementations can provide valuable practical insights. Furthermore, incorporating a global perspective when examining these security solutions, taking into account diverse regulations and healthcare infrastructures, would enhance the applicability of the research findings.

4. CONCLUSION

The primary objectives of this study are to identify six core vulnerabilities in EMR systems and propose multifaceted security frameworks as potential solutions. The significance of this research lies in its tailored and integrated approach to safeguarding health data. The analysis identified inadequate access controls, privacy concerns, risks associated with centralized architecture, challenges in interoperability, insider and external threats, and regulatory non-compliance as the key vulnerabilities.

We propose a multifaceted approach, including the integration of blockchain technology, while acknowledging adoption challenges such as scalability and regulatory acceptance. Established frameworks such as NIST and HITRUST offer robust protection. Future research could delve into the application of machine learning for anomaly detection and decentralized identity verification as potential means to enhance privacy. Further investigation is warranted to assess the impact of regulations and explore the potential of emerging technologies such as AI, machine learning, and blockchain. Focused inquiry is necessary to develop comprehensive frameworks that address all aspects of EMR vulnerabilities, ranging from detection to mitigation. Advancing the field requires testing proposed solutions, identifying emerging threats, enhancing

authentication and encryption methods, automating scanning processes, raising awareness, and addressing scalability challenges associated with blockchain technology. This review presents an evidence-based analysis of EMR vulnerabilities and security frameworks, culminating in a proposed integrated model that leverages blockchain, encryption, and AI-driven threat detection. Nevertheless, limitations of this study include reliance on secondary data and the absence of framework validation. Future research should entail conducting field studies and experiments to evaluate the effectiveness of proposed solutions in real-world scenarios. Effective collaboration among healthcare professionals, IT experts, patients, regulators, and other stakeholders is paramount.

To summarize, this review examined the challenges and solutions in EMR security. Further research and testing of protective measures in diverse settings are necessary. Additionally, interdisciplinary efforts that incorporate considerations of ethics and law are crucial.

REFERENCES

[1] A. Garcia-Perez, J. G. Cegarra-Navarro, M. P. Sallos, E. Martinez-Caro, and A. Chinnaswamy, "Resilience in healthcare systems: Cyber security and digital transformation," *Technovation*, vol. 121, p. 102583, 2023, https://doi.org/10.1016/j.technovation.2022.102583.

[2] R. Sivan and Z. A. Zukarnain, "Security and privacy in cloud-based e-health system," *Symmetry,* vol. 13, no. 5, p. 742, 2021, https://doi.org/10.3390/sym13050742.

[3] L. Wasserman and Y. Wasserman, "Hospital cybersecurity risks and gaps: Review (for the non-cyber professional)," *Front. Digit. Heal.*, vol. 4, 2022, https://doi.org/10.3389/fdgth.2022.862221.

[4] O. Alabi, "A review on Information Security of Cloud Based Electronic Health Record," *SSRN Electron. J.*, 2021, https://doi.org/10.2139/ssrn.3834180.

[5] J. Adamu, R. Hamzah, and M. M. Rosli, "Security issues and framework of electronic medical record: A review," *Bull. Electr. Eng. Informatics*, vol. 9, no. 2, pp. 565–572, 2020, https://doi.org/10.11591/eei.v9i2.2064.

[6] S. Nijor, G. Rallis, N. Lad, and E. Gokcen, "Patient Safety Issues from Information Overload in Electronic Medical Records," *J. Patient Saf.*, vol. 18, no. 6, pp. E999–E1003, 2022, https://doi.org/10.1097/PTS.0000000000001002.

[7] A. A. Kawu, L. Hederman, J. Doyle, and D. O'Sullivan, "Patient generated health data and electronic health record integration, governance and socio-technical issues: A narrative review," *Informatics Med. Unlocked*, vol. 37, p. 101153, 2023, https://doi.org/10.1016/j.imu.2022.101153.

[8] A. Davy and E. M. Borycki, "Copy and paste in the electronic medical record: A scoping review," *Knowl. Manag. E-Learning*, vol. 13, no. 4, pp. 522–535, 2021, https://doi.org/10.34105/j.kmel.2021.13.028.

[9] S. Mehta, K. Grant, and A. Ackery, "Future of blockchain in healthcare: Potential to improve the accessibility, security and interoperability of electronic health records," *BMJ Health and Care Informatics*, vol. 27, no. 3, 2020. https://doi.org/10.1136/bmjhci-2020-100217.

[10] R. Nugraha, H. Assidiq, M. Tayyib, and A. Syafira, "Harmonization Over the Regulations of Electronic Medical Records and its Potential to be Abused," *Medico-Legal Updat.*, vol. 21, no. 1, pp. 1760–1765, 2021, https://doi.org/10.37506/mlu.v21i1.2592.

[11] N. John and S. Sam, "Provably Secure Data Sharing Approach for Personal Health Records in Cloud Storage Using Session Password, Data Access Key, and Circular Interpolation," in *Research Anthology on Securing Medical Systems and Records, IGI Global*, pp. 878–902, 2022, https://doi.org/10.4018/978-1-6684-6311-6.ch042.

[12] M. J. H. Faruk, H. Shahriar, B. Saha, A. Barek, and B. S. Md Jobair Hossain Faruk, Hossain Sahriar, "Security in Electronic Health Records System: Blockchain-Based Framework to Protect Data Integrity," in *Advances in Information Security, Springer International Publishing*, pp. 125–137, 2023, https://doi.org/10.1007/978-3-031-25506-9_7.

[13] N. Pfeuffer, P. Penndorf, W. Hoffmann, and N. van den Berg, "Current Developments in Electronic Health Records," in *Systems Medicine: Integrative, Qualitative and Computational Approaches*, vol. 1-3, pp. 557–566, 2020, https://doi.org/10.1016/B978-0-12-801238-3.11662-9.

[14] P. Sureephong, P. Komanee, and C. Trongpanyachot, "Data Sharing and Electronic Medical Record Privacy Protection of Out-Patient-Department Using Blockchain," in 2022 25th International Symposium on Wireless Personal Multimedia Communications (WPMC), pp. 303–307, 2022, https://doi.org/10.1109/WPMC55625.2022.10014978.

[15] I. S. In, I. S. In, M. R. Reza, and S. K. Singh, "A Framework to Secure Electronic Health Records using Privacy-Enabled Hyperledger Fabric," in *2023 IEEE IAS Global Conference on Emerging Technologies (GlobConET)*, pp. 1–7, 2023, https://doi.org/10.1109/GlobConET56651.2023.10150086.

[16] R. Pakkala, "Blockchain Enabled Decentralized Application for Securing Electronic Medical Records with Smart Contracts," *Research Square Platform LLC*, 2023, https://doi.org/10.21203/rs.3.rs-2807625/v1.

[17] Z. Wu, S. Xuan, J. Xie, C. Lin, and C. Lu, "How to ensure the confidentiality of electronic medical records on the cloud: A technical perspective," *Comput. Biol. Med.*, vol. 147, p. 105726, 2022, https://doi.org/10.1016/j.compbiomed.2022.105726.

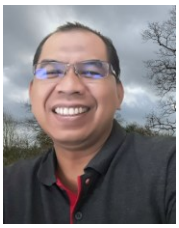
[18] I. Boumezbeur and K. Zarour, "Privacy Preservation and Access Control for Sharing Electronic Health Records Using Blockchain Technology," *Acta Inform. Pragensia*, vol. 11, no. 1, pp. 105–122, 2022, https://doi.org/10.18267/j.aip.176.
[19] E. Godson, D. D. Ngaruko, and G. Oreku, "Effects of Continuous Security Monitoring on Security Controls of Electronic Health Records in Public Hospitals, Tanzania," *East African J. Bus. Econ.*, vol. 6, no. 1, pp. 364–374, 2023, https://doi.org/10.37284/eajbe.6.1.1433.
[20] B. L. Jimma and D. B. Enyew, "Barriers to the acceptance of electronic medical records from the perspective of physicians and nurses:A scoping review," *Informatics Med. Unlocked*, vol. 31, p. 100991, 2022, https://doi.org/10.1016/j.imu.2022.100991.
[21] N. Hj Ismail, Z. Jahali, and Y. Zolkefli, "Nurses' Understanding of Ethical Dimension of Using Electronic Health Records (EHRs)," *Int. J. Care Sch.*, vol. 6, no. 2, pp. 59–68, 2023, https://doi.org/10.31436/ijcs.v6i2.284.
[22] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11717–11731, 2021, https://doi.org/10.1109/JIOT.2021.3058946.
[23] A. Kumar Jakhar, M. Singh, R. Sharma, and A. Sharma, "A Blockchain-based Privacy-preserving and Access-control Framework for Electronic Health Records Management," *Framework for Electronic Health Records Management*, pp. 0–26, 2022, https://doi.org/10.21203/rs.3.rs-2048551/v1.
[24] O. Gutiérrez, G. Romero, L. Pérez, A. Salazar, P. Wightman, and M. Charris, "Healthyblock: Blockchain-based it architecture for electronic medical records resilient to connectivity failures," *Int. J. Environ. Res. Public Health*, vol. 17, no. 19, pp. 1–38, 2020, https://doi.org/10.3390/ijerph17197132.
[25] H. T. Neprash *et al.*, "Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021," *JAMA Heal. Forum*, vol. 3, no. 12, p. E224873, 2022, https://doi.org/10.1001/jamahealthforum.2022.4873.
[26] O. Dib and K. Toumi, "Decentralized identity systems: Architecture, challenges, solutions and future directions," *Ann. Emerg. Technol. Comput.*, vol. 4, no. 5, pp. 19–40, 2020, https://doi.org/10.33166/AETiC.2020.05.002.
[27] M. R. Vishnuvardhan Komuravelly, V. Komuravelly, and M. Ramchander, "SECURITY AND PRIVACY OF ELECTRONIC HEALTH RECORDS SHARING USING HYPERLEDGER FABRIC," *Int. Res. J. Mod. Eng. Technol. Sci.*, no. 08, pp. 2410–2413, 2022, https://doi.org/10.56726/IRJMETS29499.
[28] J. E. Szalados, "Medical Records and Confidentiality: Evolving Liability Issues Inherent in the Electronic Health Record, HIPAA, and Cybersecurity," in *The Medical-Legal Aspects of Acute Care Medicine*, pp. 315–342, 2021, https://doi.org/10.1007/978-3-030-68570-6_13.
[29] E. S. Wardhana, A. Hernawan, and L. E. Nugroho, "Legal Aspects of Interoperability of Electronic Medical Records in Dentistry," *Saudi J. Humanities Soc Sci*, vol. 6256, pp. 348–353, 2021, https://saudijournals.com/media/articles/SJHSS_69_348-353.pdf.
[30] R. D. Kush *et al.*, "FAIR data sharing: The roles of common data elements and harmonization," *J. Biomed. Inform.*, vol. 107, p. 103421, 2020, https://doi.org/10.1016/j.jbi.2020.103421.
[31] P. Thantharate and A. Thantharate, "ZeroTrustBlock: Enhancing Security, Privacy, and Interoperability of Sensitive Data through ZeroTrust Permissioned Blockchain," *Big Data Cogn. Comput.*, vol. 7, no. 4, 2023, https://doi.org/10.3390/bdcc7040165.
[32] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A Survey on Security and Privacy Issues in Modern Healthcare Systems," *ACM Trans. Comput. Healthc.*, vol. 2, no. 3, 2021, https://doi.org/10.1145/3453176.
[33] B. S. S. Raj and S. Venugopalachar, "Multi-data Multi-user End to End Encryption for Electronic Health Records Data Security in Cloud," *Wirel. Pers. Commun.*, vol. 125, no. 3, pp. 2413–2441, 2022, https://doi.org/10.1007/s11277-022-09666-2.
[34] M. U. H. Siddiqui and F. Majeed, "A Comprehensive Review of Current Developments and Future Outlook Pertaining to Electronic Medical Records in the Context of Saudi Arabia, Aimed at Enhancing the Healthcare System," *MDPI AG*, 2023, https://www.preprints.org/manuscript/202310.0866/v2.
[35] L. H. Yeo, J. Banfield, "Human factors in electronic health records cybersecurity breach: an exploratory analysis," *Perspectives in Health Information Management*, vol. 19, 2020, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9123525/.
[36] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing artificial intelligence capabilities to improve cybersecurity," *IEEE Access*, vol. 8, pp. 23817–23837, 2020, https://doi.org/10.1109/ACCESS.2020.2968045.
[37] A. McGowan, S. Sittig, and T. Andel, "Medical internet of things: A survey of the current threat and vulnerability landscape," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 2020-Janua, pp. 3850–3858, 2021, https://doi.org/10.24251/HICSS.2021.466.
[38] W. Meng, W. Li, Y. Wang, and M. H. Au, "Detecting insider attacks in medical cyber–physical networks based on behavioral profiling," *Futur. Gener. Comput. Syst.*, vol. 108, pp. 1258–1266, 2020, https://doi.org/10.1016/j.future.2018.06.007.
[39] A. H. Seh *et al.*, "Healthcare data breaches: Insights and implications," *Healthc.*, vol. 8, no. 2, 2020, https://doi.org/10.3390/healthcare8020133.
[40] N. Saxena, E. Hayes, E. Bertino, P. Ojo, K. K. R. Choo, and P. Burnap, "Impact and key challenges of insider threats on organizations and critical businesses," *Electron.*, vol. 9, no. 9, pp. 1–29, 2020, https://doi.org/10.3390/electronics9091460.

[41] R. A. Alsowai and T. Al-Shehari, "A multi-tiered framework for insider threat prevention," *Electron.*, vol. 10, no. 9, 2021, https://doi.org/10.3390/electronics10091005.
[42] W. Moore and S. Frye, "Review of HIPAA, part 2: Limitations, rights, violations, and role for the imaging technologist," *J. Nucl. Med. Technol.*, vol. 48, no. 1, pp. 17–23, 2020, https://doi.org/10.2967/jnmt.119.227827.
[43] M. Chawki, "Security and Privacy in the Era of Electronic Health Records (EHRs)," RAIS J. Soc. Sci., vol. 5, no. 1, pp. 1–12, 2021, https://www.ceeol.com/search/article-detail?id=981495.
[44] S. A. Saeed and R. M. R. Masters, "Disparities in Health Care and the Digital Divide," *Curr. Psychiatry Rep.*, vol. 23, no. 9, pp. 1–6, 2021, https://doi.org/10.1007/s11920-021-01274-4.
[45] O. Koutzampasopoulou Xanthidou, D. Xanthidis, C. Manolas, and H.-I. Wang, "Security and privacy consideration for the deployment of electronic health records: a qualitative study covering Greece and Oman," *Inf. Secur. J. A Glob. Perspect.*, vol. 32, no. 4, pp. 266–282, 2023, https://doi.org/10.1080/19393555.2021.2003914.
[46] C. B. Marcus, ; Prince, and O. Asagba, "A Secure Cloud-Based Patient Electronic Medical Records System Using Two-Factor Authentication," *Int. J. Innov. Sci. Res. Technol.*, vol. 5, no. 10, 2020, https://ijisrt.com/assets/upload/files/IJISRT20OCT245.pdf.pdf.
[47] B.V. Baiju *et al*, "Decentralizing Electronic Medical Records on the Blockchain Using Smart Contracts," *J. Pharm. Negat. Results*, vol. 13, no. SO3, 2022, https://doi.org/10.47750/pnr.2022.13.S03.050.
[48] L. Huang, Z. Zhan, H. Lai, and H. H. Lee, "Privacy Protection Scheme of Medical Electronic Health Records Based on Blockchain and Asymmetric Encryption," *J. Test. Eval.*, vol. 51, no. 1, pp. 1–14, 2023, https://doi.org/10.1520/JTE20210442.
[49] S. Cao, J. Wang, X. Du, X. Zhang, X. Qin, and X. Q. Sheng Cao, Jing Wang, Xiaojiang Du, Xiaosong Zhang, "CEPS: A Cross-Blockchain based Electronic Health Records Privacy-Preserving Scheme," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, 2020, https://doi.org/10.1109/ICC40277.2020.9149326.
[50] I. Abunadi and R. Kumar, "BSF-EHR: Blockchain Security Framework for Electronic Health Records of Patients," *Sensors*, vol. 21, no. 8, p. 2865, 2021, https://doi.org/10.3390/s21082865.
[51] Wattimena *et al*., M. Wattimena, D. Retnowati, and T. Mantoro, "Misuse of Electronic Medical Records in Blockchain Technology Intelligence Security System," in *2022 IEEE 8th International Conference on Computing, Engineering and Design (ICCED)*, pp. 1–5, 2022, https://doi.org/10.1109/ICCED56140.2022.10010497.
[52] Z. Sun, D. Han, D. Li, T. H. Weng, K. C. Li, and X. Mei, "MedRSS: A blockchain-based scheme for secure storage and sharing of medical records," *Comput. Ind. Eng.*, vol. 183, p. 109521, 2023, https://doi.org/10.1016/j.cie.2023.109521.
[53] E. Chukwu and L. Garg, "A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations," *IEEE Access*, vol. 8, pp. 21196–21214, 2020, https://doi.org/10.1109/ACCESS.2020.2969881.
[54] A. Shibu, A. Anirudh, A. T. Anilkumar, A. Radhakrishnan, and S. Izudheen, "Secure Storage and Retrieval of Electronic Health Records," in *Proceedings of International Conference on Computing, Communication, Security and Intelligent Systems, IC3SIS 2022*, pp. 1–5, 2022, https://doi.org/10.1109/IC3SIS54991.2022.9885484.
[55] K. Kioskli, T. Fotis, S. Nifakos, and H. Mouratidis, "The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0," *Appl. Sci.*, vol. 13, no. 6, 2023, https://doi.org/10.3390/app13063410.
[56] O. Nkem Daniel, "A Security Framework for Electronic Medical Record," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 6, no. 3, pp. 01–11, 2020, https://doi.org/10.32628/CSEIT20634.
[57] C. Techapanupreed and W. Kurutach, "Enhancing Transaction Security for Handling Accountability in," vol. 2020, 2020, https://doi.org/10.1155/2020/8899409.

BIOGRAPHY OF AUTHORS

Dian Wijayanti. The author is a postgraduate student pursuing a master's degree in information technology at Universitas Teknologi Yogyakarta and has worked as an information technology staff at the Sleman Regional General Hospital for the past year. Email: dianwijayanti077@gmail.com, Orcid ID: https://orcid.org/0009-0004-2895-4292.

Erik Iman Heri Ujianto, received his master's in computer sciences and Doctor from Computer Sciences at Gadjah Mada University, Yogyakarta. He was currently working as an Associate Professor at Universitas Teknologi Yogyakarta also. He is a researcher in college; his topic of research is information security. Email: erik.iman@uty.ac.id, Orcid ID: https://orcid.org/0000-0002-3089-5066.



Rianto, was awarded the Erasmus+ scholarship in 2018 and completed the Information Technology Doctoral at Gunadarma University in Jakarta, Indonesia, in 2021. He got a master's in information technology from Gadjah Mada University in 2008. In addition to serving as a lecturer in the Data Science Department, Rianto writes books and contributes to national and international publications—his research interests are Natural Language Processing, Artificial Intelligence, and Machine Learning. Email: rianto@staff.uty.ac.id. Orcid ID: https://orcid.org/0000-0002-5058-4580.