Securing Healthcare Data: A Systematic Review of Compliance, Privacy, and Cybersecurity Strategies

Rohit Singh Raja

rajarohitsingh@gmail.com

Abstract

Introduction: Health Information Systems (HISs) are essential for the management of healthcare data, covering electronic health records (EHRs), clinical decision-making, and administrative functions. Healthcare organizations encounter substantial cyber risks, including ransomware and data breaches, aimed at Patient Health Information (PHI). HIPAA laws require encryption, risk management, and employee training for protecting PHI. Underfunded systems expose developing countries to additional hazards. Cloud computing provides secure solutions that improve data protection through encryption, access controls, and compliance certification. Cybersecurity is essential for modern health care.

Objective: To perform a systematic evaluation of research and their conclusions regarding Compliance, Privacy, and Cybersecurity Strategies related to healthcare data.

Method: This review identified studies which worked on healthcare data security. Key databases, including Scopus and PubMed, were queried with terms such as "medical data" and "privacy," resulting in 36 high-quality papers following thorough screening. The inclusion criteria emphasized the importance of secure data handling. Data extraction adhered to systematic methods, guaranteeing uniformity in analytical methodologies and results.

Result: The study showed that various healthcare technologies enhance security, privacy, and efficiency. IoT is focused on real-time monitoring and data availability, while blockchain, which has been the focus of nine studies, excels at safe, decentralized data management. Five studies found mobile health apps adaptable and user-friendly, while four found cloud computing scalable data management. The primary findings underscore data security, scalability, patient-centric access, and cost-effective solutions, showing several strategies to address healthcare issues.

Conclusion: The study concluded that integrating many technologies to address security, privacy, scalability, and efficiency is necessary to improve healthcare systems.

Keywords: Electronic Health Records, HIPAA, Cybersecurity, Healthcare Data Management

Introduction

As healthcare increasingly relies on digital transformation, protecting patient health information (PHI) becomes a critical priority. Cyberattacks and privacy breaches not only threaten data integrity but also compromise patient trust and care outcomes. They enable decision making and increased patient reported outcomes by the organization through storage, retrieval, analyzing, and exchange of information. A wide range of electronic health records (EHR), clinical decision making, exchange of health information, and administration are included in the HISs, they can be used in various administrations like clinics, hospitals, public health agencies, and at home. It plays an important part in the privacy and security of the data [1, 2].

The healthcare organizations are the main target for cyberattacks, where the most claimed data by cybercriminals is patient health information (PHI). Medical history, treatment planning, diagnosis, and records of bills are included in the PHI which has the most value in the market. The increased risk of cyber-attacks like ransomware, breaching of data, and phishing is significant for the security, privacy, and information available. In response to these cyberattacks, strict guidelines are being adopted by the Health Insurance Portability and Accountability Act (HIPAA) to protect PHI [3]. Based on HIPAA regulations, healthcare providers should adopt physical, technical, and administrative privacy for securing patient data. HIPAA offers some responsibilities to healthcare providers such as encryption of sensitive data, management of risk assessments, management of access to PHI, and employee training on cybersecurity. Healthcare providers face challenges due to constraints in resources, cyber threats, and outdated technologies despite the framework provided by HIPAA. The security environment is made more complex by the digital transformation of data of healthcare, which includes the extensive use of telemedicine and EHRs [2, 3].

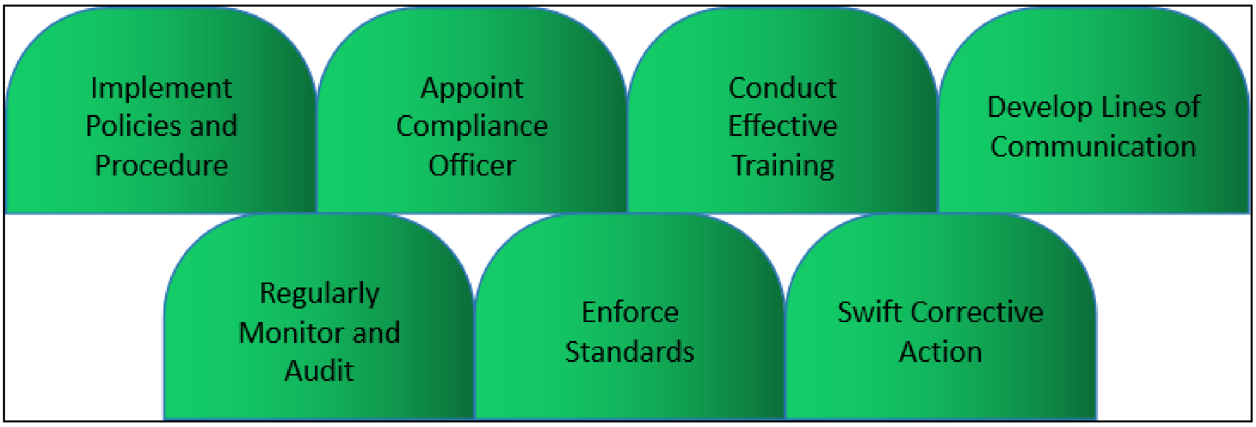
Implement Policies and Procedure
Appoint Compliance Officer
Conduct Effective Training
Develop Lines of Communication
Regularly Monitor and Audit
Enforce Standards
Swift Corrective Action

Figure 1: Factors involved in HIPAA compliance

There is an increase in cyberattacks in the healthcare system, as they can decrease the trust of patients, endanger human life, and disturb the health systems, hence cybersecurity is important in healthcare organizations. Such security requires new policies, technological changes, and behavioral changes. It is imperative that both service providers and service recipients examine and experiment with new methods and innovations for handling cyberattacks [4].

Patients' data should be available on time to the authorized people. The data breach can lead to unavailability of the patient data which further leads to a decrease in the quality of patient care and reduced effectiveness of treatment. The security breach can cause economic and social loss to both the patients and institutions. For example, a ransomware attack in 2020 on a University Hospital in Germany led to the unavailability of data preventing the hospitals to accept emergency patients for a short period of time which led to the death of at least one patient and their ambulance was diverted to the other hospital delaying the treatment for an hour [5].

The privacy of patients is legal and ethical in healthcare. Because confidentiality builds trust, patients are more willing to divulge information that is necessary for a proper diagnosis and course of therapy. As healthcare has become data-driven, the privacy of traditional boundaries is tested. The increase in data sharing has mainly the leverage of artificial intelligence (AI), machine learning (ML), and big analytics have increased the potential for medical breakthroughs. These advances in the dataset's accessibility contain patient information that can be identified [4, 5].

The privacy challenges of healthcare are not determined by a specific economy or region, it shows global concern. Data security presents challenges for developing nations, whose healthcare systems are frequently underfunded and dependent on outdated equipment. Old technologies, limited resources, and insufficient regulatory framework can cause breaches in patient information. Healthcare firms can protect patient data by implementing cloud-based solutions, which include robust encryption, security and access controls, redundancy, and certification for compliance [6, 7]. Healthcare systems globally face the dual challenges of safeguarding data privacy while leveraging advanced technologies like AI and machine learning. Previous studies have highlighted vulnerabilities in outdated infrastructures and the need for regulatory compliance frameworks like HIPAA and GDPR.

Method

Research Design

A systematic review of 36 studies was conducted using databases like Scopus and PubMed. Inclusion criteria focused on secure healthcare technologies, with data extraction emphasizing scalability, privacy, and efficiency. To conduct this study, it used the key databases which included Scopus and PubMed, were explored to extract relevant literature. The design highlights considering technologies enhancing security and privacy in health information systems. In addition, it also focuses on specific themes like secure access control, data sharing, and storage.

Literature Search

The literature search included keywords such as "medical data," "privacy," "security," and "health information systems." This study used databases such as Web of Science and IEEE were queried, targeting journal articles in English published from 2002 to 2022. Inclusion criteria ensured the relevance of selected studies, emphasizing secure technologies and methods for medical data management.

Inclusion and Exclusion Criteria

To conduct this study, I included articles that addressed secure technologies for health data privacy and security. On the other hand, this study excluded generic reports, incomplete study designs, and unrelated reviews. Articles were selected based on specific criteria, such as relevance to secure storage and sharing of medical data, with additional emphasis on solution-oriented approaches in health information systems.

Data Extraction

Data extraction followed structured protocols which focused on study objectives, methodologies, technologies, and outcomes. Tools such as EndNote facilitated the management of retrieved articles, while key data points related to secure access control, sharing, and storage were systematically tabulated for analysis. This ensured consistency and relevance in synthesized findings.

Results

Figure 2 depicts annually distributed studies with an unmistakable trend of progressive research activity over the years. There were only three studies in the year 2014, small but significant initial efforts into investigating the applications of technologies within healthcare. Five studies were then conducted in 2015, demonstrating increased interests and investments within this field. Following the trend was a single study in 2016, indicating a sharp decline, possibly owing to the shifting priorities that often come with adopting new technologies.

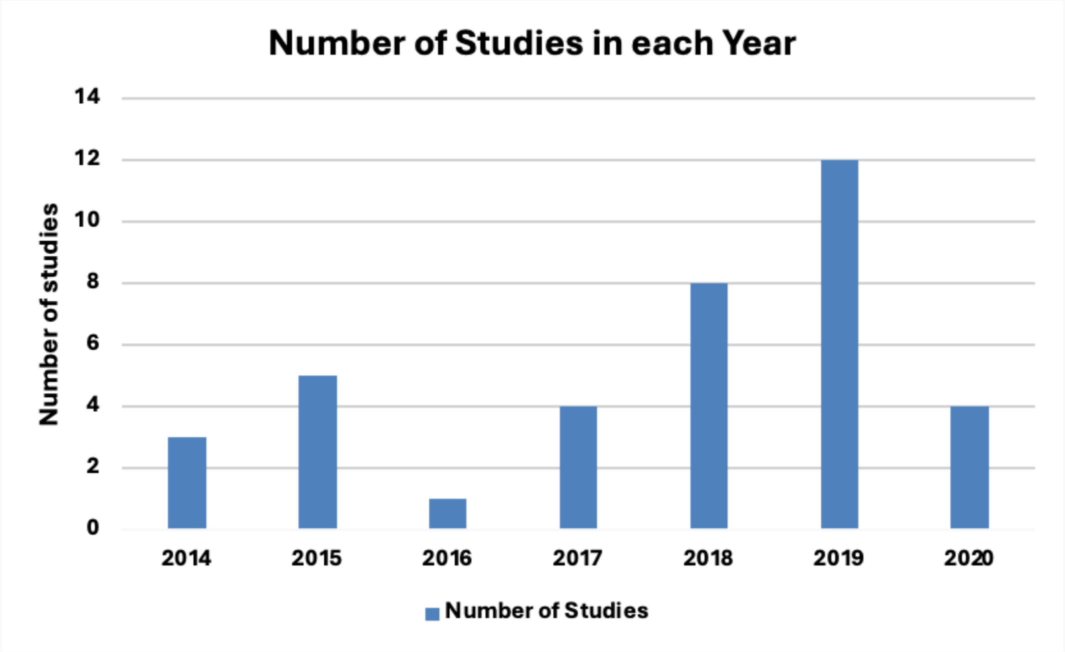

Figure 2: Number of studies with respect to year

Table 1 shows the included studies included in the research, their specific objectives, and the technological component that each research embraced is presented in Table 1. Using Mobile Health Applications, five studies ([8] – [12]) were carried out primarily on security frameworks, privacy preservation, and sensitive classification. These studies demonstrate how flexible mobile applications can be to accommodate a variety of aspects of secure healthcare data management.

IoT was one of the technologies that featured in seven ([13] – [19]) studies because of the benefit it brings in terms of creating privacy-aware infrastructures, energy-efficient security mechanisms, and lightweight authentication protocols. Blockchain ensures data integrity and decentralized access control, making it a preferred solution for secure patient data sharing. IoT, on the other hand, excels in real-time monitoring and availability, enhancing remote healthcare applications [20] to [28]. It covered everything from secure patient data sharing to decentralized health management. All this strengthens the uses of blockchain technology in assuring data integrity, access control, and solving problematics in medical data sharing. While blockchain offers high security, its computational demands make it less suitable for resource-constrained environments, unlike lightweight IoT protocols.

Table 1: Included Studies with their respective aims and technologies they utilized

Reference	Aim	Technology Used
[8]	Security framework	Mobile Health Application
[9]	Privacy-preserving data	Mobile Health Application
[10]	Secure certificate system	Mobile Health Application
[11]	Privacy preservation	Mobile Health Application
[12]	Sensitivity classification	Mobile Health Application
[13]	Privacy and data availability	IoT
[14]	Security reputation model	IoT
[15]	Authentication scheme	IoT
[16]	Privacy-aware infrastructure	IoT

[17]	Lightweight authentication protocol	IoT
[18]	Energy-efficient security	IoT
[19]	Secure health storage	IoT
[20]	Secure patient data sharing	Blockchain
[21]	Decentralized data solution	Blockchain
[22]	Secure health system	Blockchain
[23]	Blockchain challenges	Blockchain
[24]	Access control with blockchain	Blockchain
[25]	Secure data storage	Blockchain
[26]	Medical data-sharing scheme	Blockchain
[27]	Data management and sharing	Blockchain
[28]	Decentralized health management	Blockchain
[29]	Secure authentication protocol	Cloud Computing
[30]	Biometric authentication system	Cloud Computing
[31]	User-centric data sharing	Cloud Computing
[32]	Dynamic access control	Cloud Computing
[33]	Multi-agent security model	Other Technologies
[34]	Patient privacy method	Other Technologies
[35]	Hash-based integrity	Other Technologies
[36]	Federated learning for privacy	Other Technologies
[37]	Secure access control	Other Technologies
[38]	Lightweight HWBAN	Other Technologies
[39]	Sensor network privacy	Other Technologies
[40]	Privacy-preserving subprotocols	Other Technologies
[41]	Context-aware architecture	Other Technologies
[42]	Hybrid security solution	Other Technologies
[43]	5G secure healthcare	Other Technologies

Figure 3 provides an overview of the technologies most frequently used in the included studies, showcasing the diversity and prominence of specific approaches in healthcare research. Among the technologies, "Other Technologies" dominate with 11 studies, reflecting the breadth of alternative and innovative methods, such as multi-agent systems, federated learning, and lightweight encryption, being explored in this domain. Blockchain is the second most utilized technology, appearing in nine studies. Its popularity can be attributed to its ability to provide secure, decentralized data management and sharing solutions, addressing critical concerns like data integrity, transparency, and privacy in healthcare. IoT (Internet of Things) follows closely, featuring in seven studies. IoT technologies are pivotal in enabling real-time health monitoring and efficient data collection through interconnected devices, particularly in remote and mobile health applications. Mobile Health Applications, appearing in five studies, represent a growing area of interest, leveraging the ubiquity of mobile devices to provide accessible and user-friendly platforms for healthcare delivery and data collection. Finally, Cloud Computing is employed in four studies, emphasizing its role in offering scalable, on-demand computational resources for managing and analyzing large volumes of healthcare data. The distribution of technologies underscores the multifaceted approach researchers are taking to address various challenges in healthcare. While blockchain and IoT highlight the emphasis on security and real-time monitoring, mobile health applications and cloud computing focus on accessibility and scalability. The category of "Other Technologies" indicates the continuous exploration of emerging and complementary solutions to enhance the efficiency, security, and usability of healthcare systems.

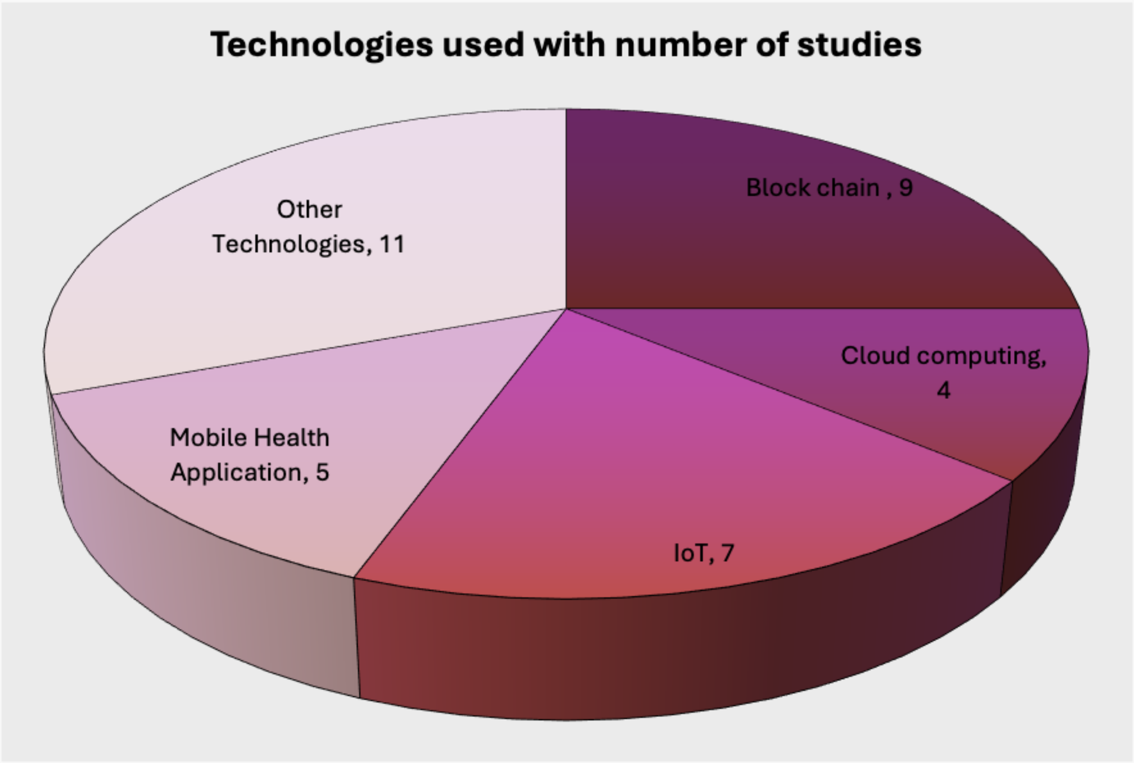

Figure 3: Frequently used Technologies in these included studies

The studies in this table demonstrate the diverse technologies applied in healthcare research. Technologies such as multi-agent systems ([33]) and NFC authentication ([41]) focus on enhancing user interaction and streamlining access control, making systems more user-friendly. On the other hand, Federated learning ([36]) and Hash-based BBS ([35]) prioritize high security and privacy, ensuring that sensitive medical data remains protected. Technologies like LR-ECC and EHGA-DLNN ([34]) and Edge cloud with Blockchain ([43]) provide high security with efficient data-sharing mechanisms, emphasizing robust cryptographic techniques. Meanwhile, Lightweight encryption and MAC generation ([39]) balance security with low computational costs, making them ideal for resource-constrained healthcare environments. Spring Framework and HTTP ([42]) integrate application-level infrastructure for secure data communication, whereas OBDD ([37]) reduces computational complexity through efficient decision-making algorithms (Table 3).

Table 3: Eleven studies with other Technologies used in the included studies

Reference	Technology Used
[33]	Multi-agent systems
[34]	LR-ECC, EHGA-DLNN
[35]	Hash-based BBS
[36]	Federated learning
[37]	OBDD
[38]	ECC, PUF
[39]	Lightweight Encryption, MAC generation
[40]	PPC, PPCC, PPSS, PPSU protocols
[41]	NFC authentication

[42]	Spring Framework, TSD, HTTP
[43]	Edge cloud, Blockchain

Table 4 presents the shared findings among the included studies, revealing critical priorities in healthcare technology applications. Data security and privacy emerged as the most prominent focus, with 14 studies emphasizing secure data transmission, confidentiality, and safeguarding sensitive information such as patient records. Scalability and efficiency, noted in six studies, underscore the importance of systems that can handle large data volumes while minimizing computational overhead and energy consumption. Five studies demonstrated high accuracy and prediction, showcasing reliable models for anomaly detection and diagnostic applications, enhancing decision-making processes in healthcare. Cost-effectiveness was also a notable finding in four studies, where resource usage was optimized without compromising performance or security, making these technologies suitable for real-world deployment. Decentralized and patient-centric access was evident in another four studies, reflecting a trend towards empowering patients with control over their healthcare data, which aligns with contemporary healthcare priorities. Enhanced data-sharing capabilities were also explored in four studies, ensuring efficient and secure communication between stakeholders. Efficient and lightweight protocols, noted in four studies, highlighted the development of cryptographic techniques that balance security with low computational requirements, particularly for IoT and mobile applications. Secure authentication mechanisms were observed in five studies, where robust methods ensured authorized access and data integrity. Finally, the practical application of these technologies in healthcare was evident in five studies, confirming their feasibility in real-world scenarios and their potential to address pressing challenges in the sector.

Table 4: Similar findings of the included studies and their respective explanation

Similar Findings	Number of Studies	References	Detailed Description
Data security and privacy	14	[8], [9], [13], [15], [17], [20], [21], [26], [27], [29], [31], [33], [39], [42]	Ensures secure data transmission, confidentiality, and privacy for patient records and sensitive information.
Scalability and efficiency	6	[9], [10], [13], [25], [30], [38]	Achieves high performance with minimal computational cost, energy consumption, and overhead.
High accuracy and prediction	5	[11], [22], [34], [36], [43]	Provides reliable prediction models, anomaly detection, and improved accuracy in healthcare applications.
Cost-effectiveness	4	[15], [19], [25], [29]	Reduces resource constraints and costs while maintaining high performance and security standards.
Decentralized and patient-centric access	4	[20], [24], [28], [32]	Supports decentralized architectures allowing patients control over access and management of their data.
Clustering and resource optimization	3	[16], [23], [26]	Improves clustering efficiency, minimizes resource usage, and enhances the utilization of medical resources.
Enhanced data sharing	4	[13], [20], [26], [43]	Facilitates secure, scalable, and efficient sharing of patient and healthcare data

			across entities.
Efficient and lightweight protocols	4	[18], [29], [37], [38]	Proposes lightweight cryptographic and network protocols for secure and efficient communication.
Secure authentication mechanisms	5	[10], [15], [17], [29], [41]	Implement robust authentication schemes to verify user access and maintain data integrity.
Practical application in healthcare	5	[8], [18], [19], [40], [43]	Demonstrates feasibility of systems in real-world healthcare scenarios, ensuring practical usability.

Table 5 shows the advantages of the studies utilizing "Other Technologies," revealing diverse benefits tailored to different aspects of healthcare systems. Efficient access control was a key feature, particularly in studies employing multi-agent systems and NFC authentication, which streamlined workflows and provided seamless user experiences. High security and accuracy were achieved through technologies like cryptographic methods, federated learning, and lightweight protocols, ensuring reliable protection of sensitive data. Privacy-friendly environments were also emphasized, ensuring that data sharing adhered to ethical and regulatory standards. Several studies demonstrated reduced computational costs, leveraging efficient algorithms like OBDD and ECC to optimize resource usage while maintaining robust performance.

Table 5: Advantages of studies using other technologies

Advantage	References
Efficient access control	[33], [41]
High security and accuracy	[34], [35], [36], [38], [39]
Privacy-friendly environment	[36], [39]
Reduced computational cost	[37], [38], [40]
Data confidentiality	[39], [43]
Secure data sharing	[42], [43]
Improved user interaction	[41]
Seamless healthcare workflow	[41]

Discussion”

A systematic review was done on the security and privacy of EHR. The EHR is shared among healthcare workers for achieving good quality health care and for achieving savings. In such cases, privacy is important as the patient may face problems if the information is disclosed. Standards and guidelines pertaining to security and privacy in EHR systems have been developed and issued in recent years [44].

Cybersecurity is the main concern of healthcare providers by adopting technologies to increase the quality of life in patients. WannaCry and ransomware are the recent cyber-attacks that cause destruction to healthcare due to these attacks [44,45]. A systematic review was done to assess the most commonly occurring factors that affect organizations due to the ignorance of the cyber threat in healthcare. They concluded that a standardized and collaborative approach for developing training programs, sharing information, and campaigns on cybersecurity attacks are required to strengthen the healthcare organizations against cyber threats [45,46].

Big data security protects the data of healthcare and maintains the confidentiality and privacy of the patient from unauthorized access. The two are essential for making sure that big data is used for research and individualized care in an effective manner without jeopardizing the privacy of medical information and healthcare data. As the amount of data increases in the health sector which makes it crucial for securing the sensitive data using big data analytics. A systematic review examines the challenges in association with the privacy and security of big data in healthcare and concludes that there is a significant increase in the healthcare security various challenges must be considered [47].

A review was done to assess the challenges and solutions associated with cybersecurity in the healthcare sector and the improvements needed to counteract the cyberattacks like ransomware, and phishing which are used by the cyber attackers to information. They found the most effective methods of cyberattacks that target healthcare during COVID-19 and the cybersecurity challenges that need improvement. During the COVID-19 pandemic and any potential future pandemics or epidemics, they gave the health sector valuable insights on cybersecurity challenges [48].

A study was to assess the clinicians' perspective on cybersecurity in healthcare and its effect on the safety of patients and organization functioning. It also assessed the challenges in association with cybersecurity implementation and the risks associated with it. To reduce these risks, healthcare system stability, maintain the trust of patients, and further save lives, cybersecurity shows top security in the healthcare sector. To effectively resist cyberattacks, a coordinated strategy is needed to enforce policies, change habits, and implement creative techniques [49].

To determine the changing risks, technological developments, and effectiveness of the cybersecurity solutions in place, a study thoroughly examines the relationship between cybersecurity and healthcare [46,47]. The study concludes that although there have been notable developments in healthcare cybersecurity, there are still issues with integrating new technologies, training medical personnel, and encouraging cooperation among stakeholders. Prioritizing cybersecurity as a fundamental aspect of healthcare delivery, funding education of cybersecurity, and promoting strict standards and laws are some strategic proposals for legislators and healthcare executives. They advance our knowledge of cybersecurity in healthcare, laying the groundwork for the next studies and strategic planning aimed at protecting private patient data and bolstering healthcare systems' ability to withstand cyberattacks [48,49].

To ensure patient information security, records of healthcare are extremely sensitive and should not be made accessible to unauthorized individuals. However, advanced technologies like cloud computing are susceptible to cyberattacks that compromise patient privacy and security of electronic health records. In these cases, wireless network security issues must be thoroughly understood and considered. A thorough investigation of the security issues with cloud computing was conducted. demonstrated that access control, permission, and authentication must be provided within the cloud's virtualized network to guarantee the security of healthcare data [47,49]. In underfunded healthcare systems, limited resources and outdated equipment hinder the adoption of advanced technologies. Scalable and cost-effective solutions like cloud computing are essential in such contexts. Challenges such as lack of funding, regulatory barriers, and insufficient training impede the effective implementation of cybersecurity strategies. Policymakers should prioritize investments in secure technologies and establish global standards for healthcare data protection.

Conclusion

The study concluded that integrating many technologies to address security, privacy, scalability, and efficiency is necessary to improve healthcare systems. Blockchain and IoT enabled secure data sharing and real-time monitoring, while mobile health apps and cloud computing improved data management. Federated learning, lightweight protocols, and other technologies reveal the possibility for decentralized, patient-centered solutions. Data security and scalability are essential for healthcare development. This study shows that healthcare systems must explore and integrate new technology to meet changing needs. AI, ML, and sophisticated cryptography can improve security and prediction.

References

1. Shojaei, P., & Chow, Y. (2024). Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review. *Computers*, *13*(2), 41. https://doi.org/10.3390/computers13020041
2. Thantilage, R. D., Le-Khac, N., & Kechadi, M. (2022). Healthcare data security and privacy in Data Warehouse architectures. *Informatics in Medicine Unlocked*, *39*, 101270. https://doi.org/10.1016/j.imu.2023.101270
3. Abbasi, Nasrullah & Smith, Derek. (2024). Cybersecurity in Healthcare: Securing Patient Health Information (PHI), HIPPA compliance framework and the responsibilities of healthcare providers. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online). 3. 278-287. 10.60087/jklst.vol3.n3. p.278-287.
4. Yigzaw, Kassaye Yitbarek & Olabarriaga, Sílvia & Michalas, Antonis & Marco-Ruiz, Luis & Hillen, Christiaan & Verginadis, Yiannis & Tuler de Oliveira, Marcela & Krefting, Dagmar & Penzel, Thomas & Bowden, James & Bellika, Johan & Chomutare, Taridzo. (2022). Health data security and privacy: Challenges and solutions for the future. 10.1016/B978-0-12-823413-6.00014-8.
5. Yusof, M. Mohd., Papazafeiropoulou, A., Paul, R. J., & Stergioulas, L. K. (2008). Investigating evaluation frameworks for health information systems. *International Journal of Medical Informatics*, *77*(6), 377–385. https://doi.org/10.1016/j.ijmedinf.2007.08.004
6. Mbonihankuye, S., Nkunzimana, A., & Ndagijimana, A. (2019). Healthcare data security technology: HIPAA compliance. *Wireless communications and mobile computing*, *2019*(1), 1927495.
7. Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, *46*(3), 541-562. https://doi.org/10.1016/j.jbi.2012.12.003.
8. Simplicio, M.A.; Iwaya, L.H.; Barros, B.M.; Carvalho, T.C.; Näslund, M. SecourHealth: A Delay-Tolerant Security Framework for Mobile Health Data Collection. IEEE J. Biomed. Health Inform. 2015, 19, 761–772. [CrossRef]
9. Medhanyie AA, Moser A, Spigt M, Yebyo H, Little A, Dinant G, Blanco R. Mobile health data collection at primary health care in Ethiopia: a feasible challenge. Journal of Clinical Epidemiology. 2015 Jan 1;68(1):80-6.
10. Ullah, I.; Amin, N.U.; Khan, M.A.; Khattak, H.; Kumari, S. An Efficient and Provable Secure Certificate-Based Combined Signature, Encryption and Signcryption Scheme for Internet of Things (IoT) in Mobile Health (M-Health) System. J. Med. Syst. 2020, 45, 4. [CrossRef]
11. Tong, Y.; Sun, J.; Chow, S.S.; Li, P. Cloud-Assisted Mobile-Access of Health Data with Privacy and Auditability. IEEE J. Biomed. Health Inform. 2014, 18, 419–429. [CrossRef]
12. Verma P, Sood SK. Cloud-centric IoT based disease diagnosis healthcare framework. Journal of Parallel and Distributed Computing. 2018 Jun 1; 116:27-38.

13. Singh S, Ra IH, Meng W, Kaur M, Cho GH. SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology. International Journal of Distributed Sensor Networks. 2019 Apr;15(4):1550147719844159.
14. Kong, F.; Zhou, Y.; Xia, B.; Pan, L.; Zhu, L. A Security Reputation Model for IoT Health Data Using S-AlexNet and Dynamic Game Theory in Cloud Computing Environment. IEEE Access 2019, 7, 161822–161830. [CrossRef]
15. Dhillon PK, Kalra S. Multi-factor user authentication scheme for IoT-based healthcare services. Journal of Reliable Intelligent Environments. 2018 Sep; 4:141-60.
16. Ullah, F.; Ullah, I.; Khan, A.; Uddin, M.I.; Alyami, H.; Alosaimi, W. Enabling Clustering for Privacy-Aware Data Dissemination Based on Medical Healthcare-IoTs (MH-IoTs) for Wireless Body Area Network. J. Healthc. Eng. 2020, 2020, 8824907. [CrossRef]
17. Santos A, Macedo J, Costa A, Nicolau MJ. Internet of things and smart objects for M-health monitoring and control. Procedia Technology. 2014 Jan 1; 16:1351-60.
18. Ray PP, Dash D, De D. Edge computing for Internet of Things: A survey, e-healthcare case study and future direction. Journal of Network and Computer Applications. 2019 Aug 15; 140:1-22.
19. Ding, R.; Zhong, H.; Ma, J.; Liu, X.; Ning, J. Lightweight Privacy-Preserving Identity-Based Verifiable IoT-Based Health Storage System. IEEE Internet Things J. 2019, 6, 8393–8405. [CrossRef]
20. Shackelford SJ, Mattioli M, Myers S, Brady A, Wang Y, Wong S. Securing the Internet of healthcare. Minn. JL Sci. & Tech. 2018; 19:405.
21. Patel V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health Informatics Journal. 2019 Dec;25(4):1398-411.
22. Kumari A, Tanwar S, Tyagi S, Kumar N, Parizi RM, Choo KK. Fog data analytics: A taxonomy and process model. Journal of Network and Computer Applications. 2019 Feb 15; 128:90-104.
23. Lim SY, Fotsing PT, Almasri A, Musa O, Kiah ML, Ang TF, Ismail R. Blockchain technology the identity management and authentication service disruptor: a survey. International Journal on Advanced Science, Engineering and Information Technology. 2018;8(4-2):1735-45.
24. Wang, S., Wang, X. and Zhang, Y., 2019. A secure cloud storage framework with access control based on blockchain. *IEEE access*, *7*, pp.112713-112725.
25. Kombe, C., Sam, A., Ally, M. and Finne, A., 2019. Blockchain technology in sub-saharan africa: Where does it fit in healthcare systems: A case of tanzania. *Journal of Health Informatics in Developing Countries*, *13*(2).
26. Liu J, Li X, Ye L, Zhang H, Du X, Guizani M. BPDS: A blockchain based privacy-preserving data sharing for electronic medical records. In2018 IEEE Global Communications Conference (GLOBECOM) 2018 Dec 9 (pp. 1-6). IEEE.
27. Reen, G.S., Mohandas, M. and Venkatesan, S., 2019, December. Decentralized patient centric e-health record management system using blockchain and IPFS. In *2019 IEEE conference on information and communication technology* (pp. 1-7). IEEE.
28. Liang, X., Shetty, S., Tosh, D., Bowden, D., Njilla, L. and Kamhoua, C., 2018. Towards blockchain empowered trusted and accountable data sharing and collaboration in mobile healthcare applications. *EAI Endorsed Transactions on Pervasive Health and Technology*, *4*(15).
29. Aslam MU, Derhab A, Saleem K, Abbas H, Orgun M, Iqbal W, Aslam B. A survey of authentication schemes in telecare medicine information systems. Journal of medical systems. 2017 Jan; 41:1-26.
30. Sharma S, Balasubramanian V. A biometric based authentication and encryption framework for sensor health data in cloud. InProceedings of the 6th International Conference on Information Technology and Multimedia 2014 Nov 18 (pp. 49-54). IEEE.

31. Qiu, H.; Qiu, M.; Liu, M.; Memmi, G. Secure Health Data Sharing for Medical Cyber-Physical Systems for the Healthcare 4.0. IEEE J. Biomed. Health Inform. 2020, 24, 2499–2505. [CrossRef] [PubMed]
32. Son, J.; Kim, J.D.; Na, H.S.; Baik, D.K. Dynamic access control model for privacy preserving personalized healthcare in cloud environment. Technol. Health Care 2015, 24 (Suppl. S1), S123–S129. [CrossRef] [PubMed]
33. Khan, F.; Reyad, O. Application of intelligent multi agent based systems for E-healthcare security. Inf. Sci. Lett. 2019, 8, 67–72.
34. Yang X, Lu R, Shao J, Tang X, Yang H. An efficient and privacy-preserving disease risk prediction scheme for e-healthcare. IEEE Internet of Things Journal. 2018 Nov 20;6(2):3284-97.
35. Yan F, Iliyasu AM, Le PQ. Quantum image processing: a review of advances in its security technologies. International Journal of Quantum Information. 2017 Apr 3;15(03):1730001.
36. Schneble W, Thamilarasu G. Attack detection using federated learning in medical cyber-physical systems. InProc. 28th Int. Conf. Comput. Commun. Netw. (ICCCN) 2019 Jul 29 (Vol. 29, pp. 1-8).
37. Edemacu K, Park HK, Jang B, Kim JW. Privacy provision in collaborative ehealth with attribute-based encryption: Survey, challenges and future directions. IEEE Access. 2019 Jun 27; 7:89614-36.
38. Yessad N, Bouchelaghem S, Ouada FS, Omar M. Secure and reliable patient body motion-based authentication approach for medical body area networks. Pervasive and Mobile Computing. 2017 Dec 1; 42:351-70.
39. Yi, X.; Bouguettaya, A.; Georgakopoulos, D.; Song, A.; Willemson, J. Privacy Protection for Wireless Medical Sensor Data. IEEE Trans. Dependable Secur. Comput. 2016, 13, 369–380. [CrossRef]
40. Rahman F, Bhuiyan MZ, Ahamed SI. Privacy preserving framework for RFID based healthcare systems. Future generation computer systems. 2017 Jul 1; 72:339-52.
41. Dzissah, D.A.; Lee, J.S.; Suzuki, H.; Nakamura, M.; Obi, T. Privacy Enhanced Healthcare Information Sharing System for Home-Based Care Environments. Healthc. Inform. Res. 2019, 25, 106–114. [CrossRef]
42. van der Weegen S, Essers H, Spreeuwenberg M, Verwey R, Tange H, de Witte L, Meijer K. Concurrent validity of the MOX activity monitor compared to the ActiGraph GT3X. Telemedicine and e-Health. 2015 Apr 1;21(4):259-66.
43. Hu J, Wu K, Liang W. An IPv6-based framework for fog-assisted healthcare monitoring. Advances in Mechanicalg Enineering. 2019 Jan;11(1):1687814018819515.
44. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2020). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors*, *21*(15), 5119. https://doi.org/10.3390/s21155119
45. Al Zaabi, M., & Alhashmi, S. M. (2024). Big data security and privacy in healthcare: A systematic review and future research directions. *Information Development*. https://doi.org/10.1177/02666669241247781
46. He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. *Journal of Medical Internet Research*, *23*(4), e21747. https://doi.org/10.2196/21747
47. Alanazi, A. T. (2023). Clinicians' Perspectives on Healthcare Cybersecurity and Cyber Threats. *Cureus*, *15*(10), e47026. https://doi.org/10.7759/cureus.47026
48. Layode, O., Naiho, H. N. N., Adeleke, G. S., Udeh, E. O., & Labake, T. T. (2024). The role of cybersecurity in facilitating sustainable healthcare solutions: Overcoming challenges to protect sensitive data. *International Medical Science Research Journal*, *4*(6), 668–693. https://doi.org/10.51594/imsrj.v4i6.1228

49. Mehraeen, E., Ghazisaeedi, M., Farzi, J., & Mirshekari, S. (2016). Security Challenges in Healthcare Cloud Computing: A Systematic Review. *Global Journal of Health Science*, *9*(3), 157. https://doi.org/10.5539/gjhs.v9n3p157