computers

MDPI

Review

Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review

Parisasadat Shojaei *, Elena Vlahu-Gjorgievska * and Yang-Wai Chow

School of Computing and Information Technology, University of Wollongong, Wollongong, NSW 2500, Australia; caseyc@uow.edu.au

* Correspondence: ps988@uowmail.edu.au (P.S.); elenavg@uow.edu.au (E.V.-G.)

Abstract: Health information systems (HISs) have immense value for healthcare institutions, as they provide secure storage, efficient retrieval, insightful analysis, seamless exchange, and collaborative sharing of patient health information. HISs are implemented to meet patient needs, as well as to ensure the security and privacy of medical data, including confidentiality, integrity, and availability, which are necessary to achieve high-quality healthcare services. This systematic literature review identifies various technologies and methods currently employed to enhance the security and privacy of medical data within HISs. Various technologies have been utilized to enhance the security and privacy of healthcare information, such as the IoT, blockchain, mobile health applications, cloud computing, and combined technologies. This study also identifies three key security aspects, namely, secure access control, data sharing, and data storage, and discusses the challenges faced in each aspect that must be enhanced to ensure the security and privacy of patient information in HISs.

Keywords: health information systems; healthcare; medical data; security; privacy

Citation: Shojaei, P.; Vlahu-Gjorgievska, E.; Chow, Y.-W. Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review. *Computers* **2024**, *13*, 41. https://doi.org/10.3390/computers13020041

Academic Editor: Paolo Bellavista

Received: 1 December 2023
Revised: 25 January 2024
Accepted: 25 January 2024
Published: 31 January 2024

1. Introduction

Described as comprehensive, technology-based systems, health information systems (HISs) are designed to manage and organize health data and information. These systems assist healthcare organizations in storing, retrieving, analyzing, and exchanging patient health information, thereby supporting clinical decision-making and enhancing patient care and outcomes. HISs typically include a range of software applications and tools for electronic health records (EHRs), health information exchange, clinical decision support (CDS), and administrative functions. These systems are versatile, being used in various settings such as hospitals, clinics, long-term care facilities, public health agencies, and even at home. HISs also play a pivotal role in enhancing data security and privacy, supporting compliance with regulations like the Health Insurance Portability and Accountability Act (HIPAA) [1].

The increase in digitalization of patient health information through electronic health records and personal health records has created new and serious threats to patient information security and privacy [2]. Medical data containing sensitive information about a patient's health and personal life, including medical history, diagnoses, treatments, and personal identifying information, are vulnerable to breaches. Such breaches can lead to serious consequences, including identity theft, fraud, and medical malpractice [3]. The security of patient data encourages individuals to share their personal health information for current or future care [3]. Furthermore, if healthcare professionals cannot trust an organization to protect records, they may be reluctant to record all information collected from patients [4]. Therefore, it is essential that HISs are designed and implemented with privacy and security as core considerations [4]. This includes using secure technologies for storing and transmitting data, implementing access controls, and providing training to healthcare professionals on best practices for ensuring patient security and privacy.

Moreover, ensuring the security and privacy of medical data, including confidentiality, integrity, and availability, is necessary to achieve high-quality healthcare services [3,4].

Table 1 provides an overview of the security and privacy technologies used in various HISs [3].

Table 1. Overview of various health information systems.

Health Information System	Security Technologies	Privacy Technologies	Advantages	Disadvantages
Electronic Health Records (EHRs)	Encryption, Access Control, Auditing	Data Masking, Patient Consent Mechanisms	Improved data integrity, Efficient access control	Complex implementation, High initial setup costs, Privacy concerns, Concerns over data breaches
Health Information Exchange (HIE)	Secure Data Transmission Protocols, Identity Management	Anonymization Techniques, Consent Management Systems	Enhanced interoperability and data sharing	Concerns over data breaches during exchange, Consent management challenges
Clinical Trial Management Systems	Secure Data Storage, Blockchain for Auditing	De-identification Methods, Informed Consent Platforms	Enhanced traceability, Immutable data records	Limited scalability, Ethical concerns related to consent

Previous literature reviews have mainly focused on the use of a particular type of technology, such as blockchain and the Internet of Things (IoT) [5,6]. So far, most of these studies have not comprehensively explained and reviewed the various technologies for ensuring the privacy and security of medical data. Therefore, the literature review presented in this paper attempts to perform a comprehensive review to evaluate the security and privacy aspects of different technologies used in health information systems and to analyze their advantages, limitations, and future directions.

This literature review includes studies that utilize various technologies to enhance the security and privacy of healthcare information. These technologies can be analyzed from three security aspects, namely, secure access control, secure data sharing, and secure data storage. To address data security and privacy, these technologies provide different secure schemes, such as secure frameworks, secure authentication protocols, privacy-preserving infrastructures, data storage, and access control models [7,8].

In this literature review, four current technologies are evaluated, namely, mobile health applications, the IoT, blockchain, and cloud computing, along with other methods that employ a combination of technologies. It should be noted that mobile applications and the IoT are different because they serve different purposes and have various characteristics, such as distinct features and functionalities, different access points, diverse operating systems, and varied threats, including different security and privacy risks and required security countermeasures. For instance, mobile devices may require additional encryption or multi-factor authentication for access to sensitive health information, while IoT devices may require additional controls to ensure the privacy and security of the data they collect and transmit.

The rest of this paper is structured as follows. Section 2 gives a brief overview of related concepts. Section 3 illustrates the research methodology. In Section 4, results from the literature review are presented. Section 5 presents a discussion and Section 6 concludes this paper.

2. Background

Security in the context of medical data and health information refers to the protection of sensitive patient information from unauthorized access, use, or disclosure. It encompasses various measures to safeguard the confidentiality, integrity, and availability of health

data [9]. Privacy, on the other hand, is a specific aspect of security that focuses on enforcing rules regarding how private information is stored and shared. Medical data privacy is important because it ensures that patients have control over who can access their health information and how it is used. This helps to maintain confidentiality and prevent the unauthorized use or disclosure of medical data, which can lead to identity theft, discrimination, and other negative consequences [9].

Therefore, attempts to create policies and regulations have been developed in various countries. For example, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 consists of federal laws that protect the privacy and security of health information in the U.S. These rules ensure that individuals have rights over their health information, and they require specific protections to safeguard electronic health information [10]. All companies operating in the healthcare industry in the U.S. must comply with HIPAA regulations. This includes healthcare providers, health plans, healthcare clearinghouses, and their business associates. The HIPAA provides a comprehensive set of guidelines for ensuring the privacy and security of health information [3]. The key guidelines comprise a security rule, privacy rule, breach notification rule, and enforcement rule. The security rule outlines the security standards to protect electronic protected health information (ePHI). It includes administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI. The privacy rule establishes national standards for protecting individuals' medical records and other personal health information. It governs the use and disclosure of PHI and grants a patient their rights over their own health information. In the event of a breach involving unsecured PHI, entities that comply with the HIPAA are required to notify affected individuals, the Secretary of Health and Human Services, and, in some cases, the media. Enforcement rules outline procedures for investigating complaints and the penalties for non-compliance with HIPAA regulations [3,11].

Accordingly, the privacy and security of HISs are crucial to ensure the confidentiality of a patient's personal information and to prevent potential security breaches that may compromise the integrity of the data. Additionally, access control tools and extensive training are essential for securing patient information and protecting confidentiality [10]. The organization and implementation of security and privacy in HISs can vary significantly depending on the country and the type of provider or user. This variation is primarily due to differences in legal frameworks, cultural attitudes toward privacy, technological infrastructure, and the specific needs of healthcare providers and users. For example, the European Union's General Data Protection Regulation (GDPR) is one of the most comprehensive and stringent privacy laws, impacting how companies worldwide handle the data of EU citizens [12]. In contrast, the United States has a more sector-specific approach, with laws like the HIPAA for healthcare data and the Children's Online Privacy Protection Act (COPPA) for protecting data for children. On the other hand, Australia's approach to health information privacy is outlined in the Privacy Act 1988, which includes the Australian Privacy Principles (APPs) [12]. These principles cover a broader spectrum of personal information compared to the U.S.'s HIPAA and apply to a wider range of entities, including all private health service providers [12].

In the context of HISs, approval and control of whether rules, requirements, and guidelines are followed, including the conducting of audits and inspections, are overseen by various regulatory bodies and government agencies. For instance, the HIPAA sets standards for the storage, sharing, and management of health information, and the Office of the Inspector General is involved in enforcing compliance through audits and investigations [13]. Furthermore, validation of HISs increasingly includes aspects of security and privacy. This is essential given the sensitive nature of health data and the evolving cybersecurity threat landscape. Modern validation methodologies for e-health systems focus on ensuring that security and privacy policies are effectively integrated and compliant with relevant regulations and standards. These methodologies typically involve a combination of technological advancements, adherence to legal frameworks, and the application of best practices in data security and privacy management. The goal is to ensure the confidentiality,

integrity, and availability of health data throughout its lifecycle, from collection to storage and processing. The validation process often includes rigorous testing and assessment of security measures, privacy protocols, and compliance with laws like the HIPAA in the U.S. or the GDPR in the EU. This approach is crucial to safeguarding patient data against unauthorized access, breaches, and other security incidents [13].

In the landscape of Health Information Systems (HISs), regulatory bodies such as the U.S. Food and Drug Administration (FDA) and the European Medicines Agency (EMA) play pivotal roles. These organizations are fundamental in establishing and enforcing standards that ensure the safety, efficacy, and privacy of health technologies. The FDA, in the United States, oversees the regulation of medical devices, which include software and hardware used in HISs. It sets forth guidelines that dictate how these technologies should be developed, tested, and implemented to protect patient data and ensure system integrity. Similarly, the EMA in the European Union performs an analogous function, focusing on the evaluation and supervision of medicinal products, thereby extending its influence to the technologies employed in healthcare settings across Europe [14].

These regulatory bodies also have a significant impact on how HIS technologies evolve and are adopted in healthcare practices. By setting stringent requirements for compliance, they influence the design and functionality of HIS technologies, prioritizing patient data security and privacy. Compliance with these regulations is not just a legal obligation but also a critical factor in gaining trust and acceptance among healthcare providers and patients. While these agencies primarily aim to protect public health, their guidelines also spur innovation, as developers and providers strive to create solutions that meet these rigorous standards without compromising on efficiency and user experience. Thus, the function and position of the FDA, EMA, and similar regulatory bodies are integral to the development and deployment of secure and privacy-compliant HIS technologies [14].

3. Materials and Methods

This systematic literature review followed the PRISMA guidelines [15], using an explicit and systematic search strategy and established inclusion and exclusion criteria. The search was conducted on five databases (Scopus, Web of Science, PubMed, Medline, and IEEE) to collect articles about the privacy and security of health information systems. During the querying phase, specific keywords were used to search for relevant articles. The search string used was (“medical date” OR “patient data” OR “health data”) AND (“privacy” OR “security” OR “data security”) AND (“health information systems” OR “information technology” OR “digital health” OR “health informatics”) with additional constraints: i.e., journal articles only, articles published in English, and articles published from 2002 to 2022.

As shown in Table 2, the search returned 1273 articles. All retrieved articles were imported to EndNote X20. At this stage, 559 duplicate references were removed, which left 714 papers for the initial screening process. During the initial screening stage, the titles and abstracts of all 714 research papers were assessed.

The research team developed a set of criteria to determine article eligibility for this review. The primary inclusion criteria for this research are the following: (1) articles describing the privacy and security of medical data in health information systems and (2) articles about secure technologies or solutions for storing and exchanging medical data. Additionally, (1) literature reviews, (2) articles that provide general information or generic reports related to medical data without describing solutions or methods for ensuring the privacy of medical data, and (3) articles that published their methodology or design for studies that have not been completed yet were excluded.

From the data in Table 2, based on the inclusion and exclusion criteria, a further 514 articles were removed, leaving 116 articles for full-text review. After filtering and selection, 36 studies were included in this review. Figure 1 summarizes the inclusion and exclusion criteria and the steps of the proposed search using the PRISMA flow diagram.

Table 2. Study selection process.

Database	Search Within	Result with No Constraints	Constraints	Result with Constraints	Result after Removing Duplicate Articles	Result after Removing Irrelevant Articles
Scopus	Article Title, Abstract, and Keywords	564	Article, English, Published from 2002 to 2022	247	129	17
Web of Science	All fields	464	Article, English, Published from 2002 to 2022	268	125	23
PubMed	All fields	349	Article, English, Published from 2002 to 2022	329	328	27
Medline	All fields	403	Article, English, Published from 2002 to 2022	375	78	22
IEEE	All fields	223	Article, English, Published from 2002 to 2022	54	54	27

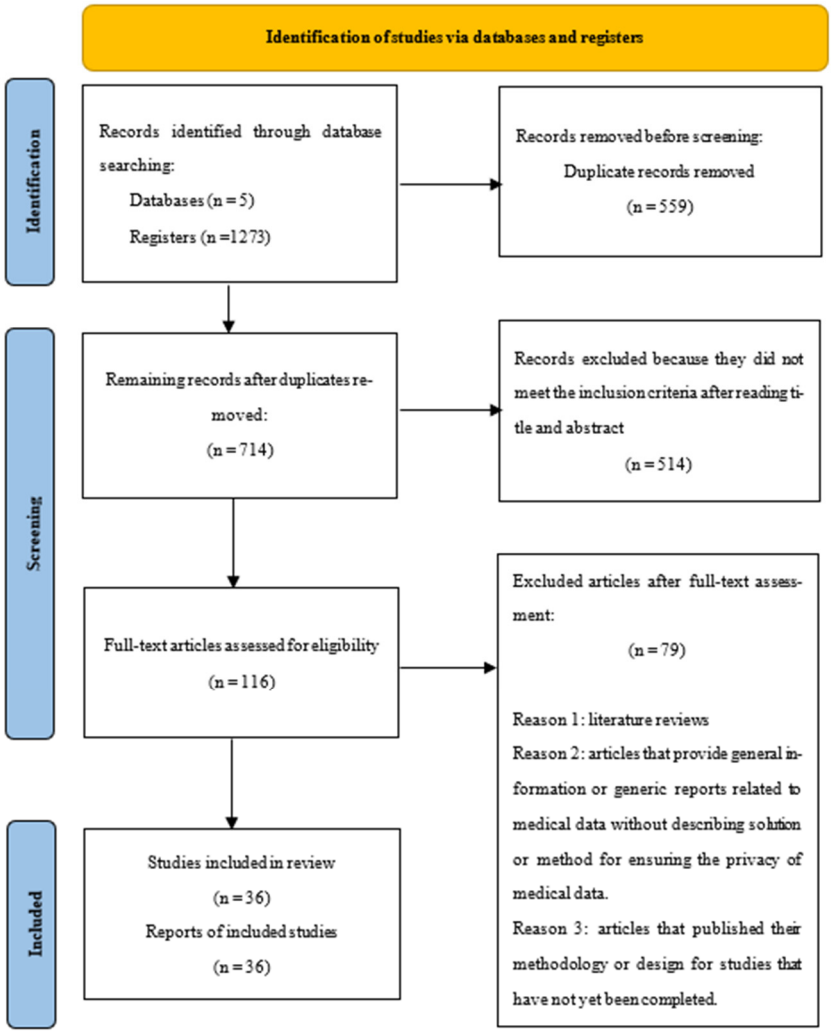

Figure 1. PRISMA flow diagram of how the systematic literature review was conducted. The diagram is divided into three phases: identification, screening, and inclusion.

4. Results

Each article was assessed based on whether it identified and evaluated existing approaches used to enhance data privacy and security in HISs. This resulted in a total of 36 relevant articles being selected for this systematic review.

As shown in Table 3, the technologies used in HISs include mobile applications, the IoT, blockchain, cloud computing, and other technologies. Furthermore, the articles reviewed revealed three key security aspects, namely, secure access control, secure data sharing, and data storage. Table 4 provides the main characteristics of the studies included in this review, focusing on approaches used to enhance the security and privacy of medical data.

Table 3. Technologies used in the included studies.

Technology Used	Count, *n*
Mobile Health Application	5
IoT	7
Blockchain	9
Cloud Computing	5
Other Technologies	10

Table 4. Characteristics of the studies included in this review.

Reference	Research Aim	Technology Used	Mentioned Factors	Main Findings	Empirical Evidence
[16]	Propose a lightweight security framework as a flexible solution for securing mobile health data collection systems, providing many security services for both stored and in-transit data	Mobile Health Application	Security Cost-effective	Tolerance to delays and lack of connectivity, Protection against device theft or loss, Secure data exchange between mobile device and server	The proposed mechanisms were integrated into an Android-based application. The experimental results show that it is possible to provide strong security for data while introducing minimal overhead to the collection process.
[17]	The proposed system offers salient features including efficient key management, privacy-preserving data storage, and retrieval, especially for retrieval in emergencies and auditability for misusing health data.	Mobile Health Application	Privacy Efficiency	Build privacy into mobile health systems with the help of a private cloud	The storage and communication efficiency were analyzed. The result indicates that the proposed scheme is efficient as well as scalable.
[8]	Propose an efficient and provable secure certificate-based combined signature, encryption, and signcryption (CBCSES) scheme	Mobile Health Application	Security (Resistant against attacks) Cost-effective	Offer the functions of both digital signature and encryption simultaneously as well as singly, Resistant against different attacks, Has better computational and communication costs	Detailed security analyses and a comparisons analysis of computational costs and communication overhead with the relevant existing schemes were carried out. The results obtained authenticate the superiority of the scheme with enhanced security.

Table 4. *Cont.*

Reference	Research Aim	Technology Used	Mentioned Factors	Main Findings	Empirical Evidence
[18]	Adopt an effective privacy-preserving technique to guarantee the sensitive information of people is secure. The proposed method uses anomaly detection based on wearable sensors in mobile cloud computing and a hash technique.	Mobile Health Application	Privacy Cost-effective	Achieves a good balance between anomaly detection accuracy and privacy-preservation capability, Minimizes privacy disclosure concerns	Simulated experiments were enacted and deployed to prove the feasibility of the proposal in terms of anomaly detection performances including accuracy, privacy preservation, and computational time in the cloud environment.
[7]	Facilitate the addition of security requirements into data collection processes. Propose a data sensitivity classification model in order to determine the sensitivity levels of form attributes depending on the context and sensitive parameters.	Mobile Health Application	Security	The security mitigations specified during form design are executed once the secure form is loaded on the mobile device during data collection.	Demonstrated the feasibility of this approach by implementing a prototype in an existing form designer tool for mobile health data collection
[19]	Handle sensitive data by preserving privacy and guaranteeing data availability without relying on a third party	IoT	Privacy Data availability	Good scalability and a modest impact on the performance of the application, Stakeholder always gains access to user data and avoids a single point of failure	Real-world experiments were and tested by connecting them with a modified IoMT application. The results obtained confirmed the feasibility of the proposed solution showing good scalability and a modest impact on the performance of the application.
[20]	Propose a security reputation model, based on a cloud environment, to protect the privacy of health data. Firstly, the text information of user health data was pre-classified by using the S-AlexNet convolutional neural network. Then, a recommendation incentive strategy based on dynamic game theory is proposed.	IoT	Security Privacy	Has reliable data recognition rate, convergence time, and recommendation efficiency, Mobile attacks are effectively resisted, The security factor of the user cloud service environment is improved	Experimental analysis on the Aliyun platform shows that the SCNN-DGT model is superior to the existing models.
[21]	Propose a new authentication scheme where the legitimate user can register through a trusted authority, which secures against prevailing attacks and key escrow problems	IoT	Security Cost-effective	Cost-effective with improved functionality, Secure against different notable attacks in the informal security analysis	Formal security analysis of the proposed protocol was performed using the Burrows–Abadi–Needham (BAN) logic and the real or random model. The security verification was performed using the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool, and a detailed comparative analysis of the communication cost is also included. The results prove that the proposed protocol is more effective and efficient compared to the other schemes.

Table 4. *Cont.*

Reference	Research Aim	Technology Used	Mentioned Factors	Main Findings	Empirical Evidence
[22]	Propose a clustering medical healthcare–IoT-based infrastructure with restricted access for privacy-aware data dissemination for wireless body area network	IoT	Privacy Cost-effective	Efficient cluster formation in minimal time, minimal information loss, and execution time for data dissemination, Increases the privacy of the patient's data in a better way	The efficiency of the proposed algorithm was evaluated against the state-of-the-art algorithm by performing extensive simulations. The results demonstrate the benefits of the proposed algorithms.
[23]	Develop a lightweight mutual authentication protocol for securing sensitive patient health information, Ensure the privacy of sensitive patient data while sharing with other smart community users	IoT	Security Privacy	Resists against all network attacks, Maintains patient data privacy in a multiuser scenario, Secures entity authentication to access the patient's stored cloud-based data, Has a high data encryption rate	A formal security analysis based on Burrows–Abadi–Needham (BAN) logic and a performance comparison of the proposed scheme with existing schemes were conducted. The proposed model is capable of maintaining the patient's data privacy, reducing service latency, and providing security from intruders through the authentication model.
[24]	Design an energy-efficient security mechanism using lightweight messaging protocol for exchanging medical data between client nodes and using lightweight cryptographic operations to encipher the sensitive data	IoT	Security Privacy Efficiency (energy)	Facilitates the mobility of patients while maintaining security and privacy in a particular monitoring area, Being energy-efficient, provides end-to-end data confidentiality and mobility support	It uses the Cooja simulator to create and analyze an e-health system scenario. The results show that the scheme is efficient compared to existing state-of-the-art mechanisms.
[25]	Lightweight secure health storage system preserving both the privacy and availability of patients' health data, preventing damage to patients' conditions from corrupted data and improving the reliability of the health storage system	IoT	Security Cost-effective	Reduces the system's computational cost and management burden of third-party verifiers	A functionalities comparison of the proposed scheme and other schemes and an evaluation of the computational cost and communication cost through numerical analysis and simulated experiment were conducted. The results indicate that the proposed system is feasible.
[26]	Ensure secure sharing of patient data among participating hospitals in the network, by proposing Internet-of-Healthcare Systems which provides the highest level of storage and access security possible, overcoming the security and data administration problems by using blockchain	Blockchain	Security Privacy Data confidentiality	Provides greater functionality, Addresses the security of data transmission, data processing, and secure data storage	Used real data from 157 hospitals. The system addressed the security of data transmission, data processing, and secure data storage.

Table 4. *Cont.*

Reference	Research Aim	Technology Used	Mentioned Factors	Main Findings	Empirical Evidence
[27]	Provide a decentralized solution for data communication, combining two decentralized technologies, a solid ecosystem and blockchain technology, to tackle all potential security issues using solidity-based smart contracts	Blockchain	Security	Mitigates threats posed to data while using the traditional approach. Healthcare data are kept confidential to secure personal information and medical history, Interoperability issues were addressed by introducing a decentralized solution to the healthcare domain	Performance evaluation was conducted using Ganache, JMeter, and manual observations. Latency was proven to increase as the size of files increased and the number of users accessing resources increased.
[28]	Design a secure system for optimized protection and privacy criteria of health data management, suggesting a secure and energy-efficient e-health system that would use IoMT to reduce energy usage and increase data provision.	Blockchain	Security Privacy	Achieves high accuracy, prediction, less delay, latency, and response time, Can authenticate each node by establishing public and private keys	Performance metrics were considered, such as the accuracy ratio, prediction ratio, response time, delay time, and latency range. The experimental results are based on the collected samples from a healthcare institution. The results show that the proposed model is effective and secure.
[29]	Address the fundamental issues, limitations, and challenges in blockchain, Hyperledger, and the IoT, and provide a design of an efficient distributed architecture	Blockchain	Security Privacy Cost-effective	Reduces the resource constraints and increases security and privacy with secure and protected protocols for medical ledger preservation, Minimizes resource consumption throughout service delivery,	The proposed serverless e-healthcare application was evaluated and examined. The experimental results demonstrate an efficient performance of the proposed blockchain Hyperledger fabric-enabled consortium network called BIoMT.
[30]	Build a dynamic access control framework based on a smart contract, which is built on top of a distributed ledger (blockchain), to secure the sharing of EMRs among different entities involved in the smart healthcare system	Blockchain	Security Efficient for real-time Cost-effective	The proposed access control is efficient for real-time IoT-enabled smart healthcare systems and enables all the entities to share electronic medical records (EMRs) with the permission of the patient, and it allows a new entity to be added at any time, making it more practical and dynamic.	The performance of the access mechanism was evaluated. The performance evaluation and efficiency analysis demonstrate the feasibility of the proposed scheme in a real-time smart healthcare system for a secure, decentralized, distributed, and patient-centric access control.
[31]	Develop a system with secure data storage architecture to address cybersecurity storage challenges through private data collection to guarantee data privacy	Blockchain	Security Efficiency (performance)	Provides secured data storage, with higher overall performance, Cost-effectiveness of secured data storage and low energy consumption	The performance and cost of the architecture was evaluated. The results show that Hyperledger Fabric blockchain architecture shows higher overall performance compared to Ethereum.

Table 4. *Cont.*

Reference	Research Aim	Technology Used	Mentioned Factors	Main Findings	Empirical Evidence
[32]	Propose a new data-sharing scheme for medical scenarios, which breaks system boundaries and realizes cross-hospital diagnosis using attribute-based encryption technology to encrypt patient medical data	Blockchain	Privacy	Efficient, correct, and well adapted in medical scenarios, Realize medical data sharing and improve the utilization of social medical resources on the premise of protecting medical privacy	Theoretical analysis and experiments of a prototype implementation were conducted. The results show that the scheme solves the contradiction between the privacy preservation of medical data and the necessity of data sharing.
[33]	Develop a system that will facilitate secure, trustable management, sharing, and aggregation of electronic health data, ensuring patient privacy protection and security with respect to the requirements for healthcare data management, including the access control policy specified by the patient	Blockchain	Security Cost-effective	Ensures privacy, security, availability, and granular access control over highly sensitive patient data	Implementation of a prototype was used. The results demonstrate that the methodology is general and can be easily extended to support other types of patient care.
[34]	Design and build an ecosystem that provides efficient and effective decentralized health data management and exchange operations by applying a prototype blockchain and smart contract to a patient device	Blockchain	Security Efficiency (data management)	Enabled not only at the overall personal health record or resource level but also at the granular data element and data value levels, Demonstrates that blockchain is a suitable software tool that safely and efficiently performs the required data verification and decentralized data backup processes	Three use cases were utilized, demonstrating that health data access control and authenticity verification of personal health record data were enabled not only at the overall personal health record or resource level but also at the granular data element and data value levels.
[35]	Propose a secure authentication protocol to ensure the privacy of health data, utilizing blockchain technology to guarantee data integrity in the cloud server and applied consortium blockchain for scalability and low computational cost	Cloud computing	Security Cost-effective	Has lower computational and communication costs, Provides more security features	Informal analysis was used and computation blue and communication costs compared. The results demonstrate that the proposed protocol is efficient and has better safety compared to the related protocols.
[36]	Present a cloud-based biometric authentication system having two different components to handle the ever-growing data of the health sector and to provide security to different users	Cloud computing	Security Efficiency (time and speed)	Has less time to run and high speed	Validation was performed through experiments and performance comparison. Experiments performed on this system revealed that it achieves a speedup of 9x which is better than other systems implemented in recent works.

Table 4. *Cont.*

Reference	Research Aim	Technology Used	Mentioned Factors	Main Findings	Empirical Evidence
[37]	Design a user-centric data storage and sharing method to protect the safety and privacy of users' data which could protect data safety and privacy even when both cloud servers and keys are compromised	Cloud computing	Security Privacy Efficiency (time)	Can avoid data leakage even if the keys are compromised, Has high speed	The feasibility of this system based on mobile edge computing (MEC) was evaluated in a smartphone scenario to prove the improvement in efficiency compared with standard encryption algorithms and evaluate the method with statistical and performance analysis. According to the evaluation, the proposed method is approximately 2.3 times faster than the baseline method.
[38]	Propose a dynamic access control model for preserving data privacy, with a key feature of the proposed model being that it can deal with the healthcare domain and dynamic access control in a cloud environment	Cloud computing	Privacy	Access control can be dynamically determined by changing the context information such that even for a subject with the same role in the cloud, access permission is defined differently depending on the context information and access condition.	The article verified the ability of the proposed model to provide correct responses by representing dynamic access control through a use case scenario. The results show that the proposed model can deal with the healthcare domain and dynamic access control in a cloud environment.
[39]	Propose a novel model based on multi-agents (user interface agent, authentication agent, connection establishment agent, and connection management agent) to maintain security and privacy while accessing the electronic health data between the users	Other Technologies	Security Privacy Efficiency (communication)	Provides effective and secure e-health security services Make ease of use and effective communication between users and the e-service providers.	The proposed model for providing security in e-health data was compared with the existing approaches. The results show that the proposed method is effective and secure.
[40]	Provide an effective method for protecting patient privacy, utilizing log of round value-based elliptic curve cryptography (LR-ECC) to enhance the security level during data transfer after the initial authentication phase.	Other Technologies	Security Privacy	High security and accuracy, Superior to that of the prevailing systems for disease prediction and provides better privacy and security	Performance analysis of secure data transmission and classification were conducted. The experimental outcome displays the proposed work's performance provides better privacy and security.
[41]	Propose a new hash-based BBS (HBBS) pseudo-random bit generator to achieve integrity and security in the transmission of medical data	Other Technologies	Security Efficiency	Has high security and good efficiency to be suitable for smart health applications and telemedicine	Multiple metrics and analyses were conducted. The proposed scheme outperforms other encryption techniques, representing a secure alternative to encrypting and decrypting medical images.

Table 4. *Cont.*

Reference	Research Aim	Technology Used	Mentioned Factors	Main Findings	Empirical Evidence
[42]	Secure patient's health records by maintaining user privacy and data integrity with a federated learning-based decentralized artificial intelligence model that trains data locally in hospitals and globally at research centers	Other Technologies	Security Privacy	The federated learning model performs well in accuracy, sensitivity, and specificity compared to the traditional centralized model.	The evaluation was based on the performance of the federated learning model. The results show that the scheme is suitable for promoting a secure and privacy-friendly environment for sharing data with clinical research centers for biomedical research.
[43]	Propose a novel access control scheme for secure sharing of health data in collaborative e-health systems, aiming to achieve immediate attribute/user revocation, collusion resistance, forward security, backward security, efficiency, and expressiveness	Other Technologies	Security Data confidentiality Efficiency	Achieves data confidentiality and fine-grained access control, Resistant to collusion attacks, Achieves both forward and backward security	The proposed scheme was simulated and a comparative analysis in relation to similar schemes was conducted. The security and performance analysis show that the proposed scheme is secure, expressive, and efficient.
[44]	Provide a secure and lightweight healthcare wireless body area network (HWBAN) scheme by using fewer elliptic curve cryptography (ECC) operations and a physically unclonable function (PUF) to enhance security and efficiency at the same time	Other Technologies	Security Efficiency Cost-effective	Meets more security and usability requirements, Takes less computational and communication costs	The computational and communication costs were analyzed. The results show that the scheme is more practical for smart medical applications, allowing users to obtain their health status directly through their phones.
[45]	Investigate the security and privacy issues in the medical sensor data collection and present a solution for privacy-preserving medical sensor networks	Other Technologies	Security Privacy Data confidentiality Data integrity	Achieves data confidentiality, authenticity, and integrity, Preserves patient data privacy as long as one of the three data servers is not compromised	Security and privacy analysis shows that the protocols are secure against both outside and inside attacks if one data server is not compromised. Performance analysis shows that the protocols are practical as well.
[46]	In the proposed scheme, several secure and privacy-preserving subprotocols were designed to ensure privacy in the e-healthcare system, and then it adopted the greedy algorithm in a secure manner to perform the query and the min-heap technology to improve efficiency.	Other Technologies	Privacy Cost-effective	Practical and efficient in terms of computational cost and communication overhead.	Experiments were conducted and the performance of the scheme evaluated, in terms of the communication overhead and computational cost. The experimental results show that the scheme is applicable to different clinical scenarios.
[47]	Develop a context-aware architecture to achieve accountability, privacy, and enhanced security in distributed home-based care systems	Other Technologies	Privacy	Enhances healthcare data access and secure information delivery to preserve user's privacy, Enhances the workflow of users and integrates it into a seamless access control process	A prototype of the system was deployed for testing on a local network with an Android smartphone as the medical personnel terminal, confirming its feasibility.

Table 4. *Cont.*

Reference	Research Aim	Technology Used	Mentioned Factors	Main Findings	Empirical Evidence
[48]	Develop a hybrid security solution to secure the collection and management of personal health data, providing secure hosting and operation of application services, collection, storage, processing, and provisioning of data.	Other Technologies	Security	Effectively protects the application programming interface (API) and personal health data	The technology was validated with theoretical evaluation and experimental testing, and the test results were compared with related studies qualitatively for the efficient evaluation of the implemented security solution The results show that his study can be used as a services for sensitive data (TSD) integration manual to protect personal health data in healthcare research.
[49]	Present a framework for 5G-secure smart healthcare monitoring to achieve fast and accurate identification of context-aware health situations, a blockchain-based secure data sharing mechanism, and low-latency services for emergent patients	Other Technologies	Security Efficiency (latency and mobility)	Obtains high accuracy while significantly reducing the latency and improving the data-sharing security	A prototype system was implemented to monitor hypertensive heart disease, confirming its effectiveness with respect to a real scenario.

4.1. Mobile Health Application

Mobile devices play an important role in the management of medical data in health information science. However, organizations must ensure that appropriate security and privacy measures are in place to protect sensitive information from unauthorized access or theft. These privacy and security measures align with the proposals of Ref. [7], who suggest threat modelling to identify potential threats and possible mitigations. By integrating security policies, defining sensitivity levels of form fields, and corresponding security mechanisms, data security can be catered to as early as the design phase. In addition, articles [8,16–18] implement secure models to strengthen the privacy and security of medical data within mHealth applications. These models aim to protect sensitive health information throughout its lifecycle, from collection and transmission to storage and access. For instance, Ref. [16] suggests a lightweight security framework for securing mHealth data collection systems, relying on lightweight and low-cost mechanisms to secure data exchanged with servers. These findings emphasize the importance of implementing strong encryption techniques for both data in transit and data at rest. This includes encrypting communication channels between devices and servers, as well as storing medical data on mobile devices and in the cloud [8]. For example, Ref. [8] proposes a scheme called an Efficient and Provable Secure Certificate-Based Combined Signature, Encryption, and Signcryption (CBCSES) scheme. This scheme not only provides encryption and signcryption but also offers an encryption or signature model when needed.

Moreover, mHealth applications can be designed using a secure framework for data collection, minimizing the risk of unauthorized access or theft of information. This contributes to securing the data exchanged with the server and includes key features such as tolerance to delays and lack of connectivity [7,16]. A previous study identified the need to use secure cloud storage for storing data, which can provide additional backup and security measures [17]. The system proposed in [17] offers salient features including efficient key management, privacy-preserving data storage and retrieval—particularly effective in emergency situations—and auditability to prevent misuse of health data. Furthermore, an approach presented in [18] utilized privacy-aware anomaly detection methods. These

prioritize the security of health data by identifying abnormal patterns and ensuring the privacy of individual users, thus helping to maintain the confidentiality and integrity of sensitive health information [18].

4.2. IoT

The Internet of Things (IoT) has the potential to transform healthcare by enabling data collection and exchange from various devices and sensors. IoT devices feature built-in security measures, including encryption and authentication, to protect data in transit and storage while ensuring access is restricted to authorized parties [28].

IoT devices can store and organize medical data, simplifying access and analysis for healthcare professionals [19]. A new shared, agnostic, and permissioned decentralized data layer enhances data availability. This architecture has been implemented in a real-world Internet of Medical Things (IoMT) application [19], effectively handling sensitive data by preserving privacy and ensuring data availability without third-party reliance. Additionally, the IoT enhances data security and privacy through encryption, robust authentication, and access control, ensuring that sensitive health data are accessible only to authorized parties, thereby making unauthorized access more challenging [20–24].

It is important to note that IoT applications in healthcare offer cost reduction and efficiency benefits. These applications streamline operations, minimize errors and waste, and reduce system costs [21]. The focus in [21] was on avoiding the key escrow problem and establishing a new session key between servers and personal digital assistants (PDAs) for future communication, enhancing cost-effectiveness, and security against various attacks. Remote monitoring contributes to shorter hospital stays and fewer readmissions, improving treatment outcomes and reducing healthcare costs [21,25]. Furthermore, Ref. [25] discusses using an edge server to compute data authenticators to verify data integrity, significantly reducing computational costs and the management burden on third-party verifiers.

4.3. Blockchain

Extensive research has established that blockchain technology offers a secure, transparent, and tamper-proof method for storing and sharing medical data, which is crucial for maintaining patient privacy and security within HISs. Operating on a decentralized network, blockchain technology lacks a central authority controlling the data. This approach mitigates the risk of a single point of failure or a single entity accessing sensitive information, addressing potential security issues inherent in centralized storage systems [28]. Additionally, Ref. [28] discovered that blockchain technology can overcome challenges related to interoperability, security, confidentiality, privacy protection, and secure storage. Similarly, Ref. [27] integrated two decentralized technologies, the Solid ecosystem and blockchain, using solidity-based smart contracts to resolve security issues, thereby providing a secure, patient-centric design for complex, developing electronic health record (EHR) data exchange.

Blockchain technology can also create secure private networks for sharing sensitive medical data (transferred and distributed) exclusively among authorized parties [33,49]. For example, Ref. [33] proposes a permissioned blockchain-based system for EHR data sharing and integration, employing public key infrastructure-based asymmetric encryption and digital signatures to secure EHR data. This system ensures patient privacy protection and adheres to healthcare data management requirements, including the access control policy specified by the patient. Similarly, Ref. [32] introduced a privacy-preserving medical data-sharing scheme that balances the need for privacy with the necessity of data sharing. This perspective aligns with Ref. [49], who utilized a blockchain-based secure data sharing mechanism for the safe uploading and sharing of health data. The study by Ref. [31] developed a blockchain-based system with a secure data storage architecture to tackle cybersecurity storage challenges, employing private data collection to ensure privacy and decentralizing nodes in the network to prevent storage complications. This method also addresses other security challenges typically associated with centralized systems. Further-

more, blockchain technology enables the creation of smart contracts that automate data sharing under predefined conditions, ensuring that data are only shared with authorized parties. In line with this, Ref. [30] developed an access control framework based on smart contracts, which is built on a distributed ledger (blockchain), to secure the sharing of electronic medical records among various entities in the smart healthcare system.

In the context of blockchain applications in HISs, patient autonomy is a central theme, allowing individuals to have ownership and control over their personal health data. This empowerment is crucial, yet it poses challenges, particularly when patients are cognitively impaired or unable to manage their data. In such cases, the use of advanced directives or legally authorized representatives could be integrated into blockchain systems to ensure responsible data management [26]. Moreover, blockchain's decentralized nature and cryptographic techniques provide robust security for health data [27]. However, challenges arise in maintaining consistent permissions, especially in emergency situations where swift access to patient data is crucial. Smart contracts and cryptographic keys within blockchain networks can be employed to manage permissions seamlessly, ensuring healthcare professionals have necessary access while maintaining patient privacy and data integrity [30].

Furthermore, the legal implications of using blockchain in HISs under different jurisdictions, such as the potential access by the U.S. government to cloud-stored data under U.S. law, raise significant privacy concerns. While blockchain offers many benefits for healthcare data security, its integration into existing healthcare systems must be approached with caution, ensuring adherence to regulations like the HIPAA and addressing potential privacy issues related to decentralized data storage. This necessitates a careful balance between technological innovation and compliance with legal and regulatory standards.

4.4. Cloud Computing

Cloud computing offers multiple advantages for ensuring the security and privacy of medical data in HISs. By adopting cloud-based solutions, healthcare organizations benefit from strong security controls, encryption, access controls, redundancy, and compliance certifications, all aimed at safeguarding patient data. The findings of this review indicate that cloud computing providers can implement robust access control mechanisms. These include multi-factor authentication and role-based access control, ensuring that only authorized personnel can access sensitive medical data, thereby enhancing security measures [36,38].

Moreover, cloud computing can be more cost-effective compared to maintaining an on-premises IT infrastructure. This efficiency comes from eliminating the need for expensive hardware and software, allowing healthcare organizations to reduce costs and improve their overall financial performance [36]. Cloud computing also guarantees data recovery following a disaster, further bolstering data security and privacy [17,37]. For instance, a study by Ref. [37] describes a secure encryption algorithm (SE) combined with fragmentation and dispersion for storage. This method is designed to protect data even if both the key and the public fragment of EHR data on clouds are compromised. This aligns with other research demonstrating that storing EHR in the cloud significantly enhances security and protects patient information from unauthorized access [50].

4.5. Other Technologies

In addition to the technologies mentioned earlier, several studies have examined methods that employ a variety of technologies to enhance the security and privacy of medical data. Table 5 presents an overview of these technologies.

Table 5. Overview of other technologies used in HISs.

Reference	Technology Name	Security and Privacy Features	Primary Functions	Advantages
[39]	Multi-agent-based systems (user interface agent, authentication agent, connection establishment agent, and connection management agent)	Security Privacy	These intelligent agents make ease of use and effective communication between patients/users and the e-service providers.	Simple and efficient access control mechanism based on the agents' functionalities, Provides effective and secure e-health security services
[40]	Log of round value-based elliptic curve cryptography (LR-ECC) Herding genetic algorithm-based deep learning neural network (EHGA-DLNN)	Security Privacy	Enhance the security level during data transfer after the initial authentication phase	High security and accuracy
[41]	Hash-based BBS (HBBS)	Security	For integrity purposes, the hash value is generated using secure hash algorithm SHA-256 and is hidden in the least significant bit (LSB) of the extracted pseudo-random bits for the purpose of generating multiple keystreams.	Has high security and good efficiency
[42]	Decentralized federated learning-based convolutional neural network	Security Privacy	Presents a privacy-friendly and secure EHR scheme for medical cyber-physical systems.	Securing valuable hospital biomedical data useful for clinical research organizations, Suitable for promoting a secure and privacy-friendly environment for sharing data with clinical research centers for biomedical research
[43]	Ordered binary decision diagram (OBDD)	Security	Achieves immediate attribute/user revocation, collusion resistance, forward security, backward security, efficiency, and expressiveness	The efficiency of the scheme can be attributed to the use of prime-order groups, minimized hashing operations, and reduced amount of exponentiation operations.
[44]	Elliptic curve cryptography (ECC) operations Physically unclonable function (PUF)	Security	Improve security and efficiency at the same time, Strict formal security proof is provided to demonstrate the proposed scheme meets the security and reliability requirements	Meets more security and usability requirements and takes less computational and communication costs than related protocols proposed recently
[45]	Lightweight encryption scheme Message authentication code (MAC) generation scheme	Security Privacy	Secures the communication between medical sensors and data servers	Achieves data confidentiality, authenticity, and integrity between each medical sensor and each data server
[46]	Subprotocols as building blocks, such as PPC, PPCC, PPSS, and PPSU protocols	Privacy	It first designs secure and privacy-preserving several subprotocols to ensure privacy in the e-healthcare system, then it adopts the greedy algorithm in a secure manner to perform the query and the min-heap technology to improve efficiency.	Practical and efficient in terms of computational cost and communication overhead
[47]	Near-field communication (NFC) authentication mechanism	Privacy	To generate a trustworthy source of visit records, the article uses a system that supplies concrete evidence that healthcare personnel visited a patient's residence.	Using the NFC tag enhances the workflow of users and integrates it into a seamless access control process. It helps improve user interaction by eliminating user input tasks.

Table 5. *Cont.*

Reference	Technology Name	Security and Privacy Features	Primary Functions	Advantages
[48]	Spring Framework services for sensitive data (TSD) Hypertext Transfer Protocol (HTTP (H))	Security	Providing secure hosting and operation of application services, collection, storage, processing, and provisioning of data	A key element of Spring is application-level infrastructure support. It effectively protects the application programming interface (API) and personal health data.
[49]	Edge cloud blockchain	Security	The edge cloud performs context-aware health situation identification and utilizes a blockchain-based secure data sharing mechanism to facilitate secure uploading and sharing of health data.	It identifies the health situation based on a similarity measure in the edge cloud. A blockchain-based securing data sharing mechanism is used to achieve secure sharing of health data among patients and health service providers.

The study by Ref. [48] developed a hybrid security solution using the Spring Framework, services for sensitive data (TSD) as a service platform, and Hypertext Transfer Protocol (HTTP) security methods. This solution provides secure hosting and operation of application services, as well as the collection, storage, processing, and provisioning of data. The results demonstrate that the adopted digital solution effectively protects APIs and personal health data. Another study by Ref. [41] presents a new hash-based BBS (HBBS) pseudo-random bit generator to ensure the integrity and security of data, making it suitable for smart health applications and telemedicine. This study also proposes an encryption technique aimed at achieving robust security during the transmission of medical data. Furthermore, Ref. [44] introduces a secure and lightweight approach using fewer elliptic curve cryptography (ECC) operations and a physically unclonable function (PUF), improving security and efficiency with lower computational and communication costs. The study by Ref. [45] proposes a privacy-preserving encryption approach that incorporates an innovative data collection protocol. This method involves dividing patient data into three parts and storing them across three data servers to maintain privacy.

Additionally, Ref. [46] designed several secure and privacy-preserving subprotocols to ensure privacy in an e-healthcare system, adopting a secure greedy algorithm for query performance and min-heap technology to enhance efficiency. The method in [47] offers an architecture that improves the reliability of data exchange between healthcare personnel by providing a security layer that supports accountability through context-aware services, enabling appropriate data access for users. Ref. [40] proposes a secure method for preserving privacy in healthcare data, specifically for disease prediction in modern healthcare systems. This system uses cryptography during data transfer and allows authorized healthcare staff to securely access patient data for disease prediction using a herding genetic algorithm-based deep learning neural network. Ref. [43] suggests a secure, expressive, and efficient access control scheme with immediate attribute/user revocation in collaborative e-health systems, based on the ordered binary decision diagram (OBDD) access structure. It binds user keys to user identities, therefore creating resistance to collusion attacks. Additionally, Ref. [39] highlights a model based on a multi-agent system comprising various intelligent agents such as a user interface agent, authentication agent, connection establishment agent, and connection management agent. This model provides effective and secure e-health security services, facilitating ease of use and effective communication between users and e-service providers.

Various studies have demonstrated the relationship between secure solutions for storing and sharing sensitive health information and ensuring the security and privacy of data in HISs. For instance, Ref. [42] proposed a secure scheme using a decentralized federated learning-based convolutional neural network, private and public interplanetary file systems (IPFS), a consortium blockchain network, and smart contracts. This scheme

is ideal for promoting a secure and privacy-friendly environment for data sharing. In a study by Ref. [49], a framework for 5G-secure smart healthcare monitoring (5GSS) was employed for fast and accurate identification of context-aware health situations, along with a blockchain-based secure data sharing mechanism and low-latency services for emergent patients.

5. Discussion

In this systematic literature review, the articles on data privacy and security for HISs that were reviewed focused on various technologies, such as the IoT, blockchain, mHealth applications, and cloud computing. This section first discusses the challenges and future directions of these technologies in relation to HISs. From this, three fundamentally distinct security aspects could be identified, namely, secure access control, data sharing, and data storage within HISs. These aspects will be discussed in the subsequent subsections.

5.1. Challenges and Future Directions of the Technologies Used in HISs

5.1.1. Mobile Health Applications

In the realm of mHealth applications, the privacy and security of medical data can be significantly enhanced through the use of robust encryption techniques. These techniques are crucial in preventing unauthorized access and are resistant to various attacks. Consequently, even if unauthorized individuals gain access to the data, it remains indecipherable without the appropriate decryption keys [7]. These findings are in line with those reported in [51], which also emphasized the need for efficient measures to mitigate privacy and security risks in mHealth. This highlights the significance of encryption in safeguarding data against breaches.

A challenge identified in this review is the lack of adequate backup mechanisms in many mHealth applications. Some applications do not have sufficient data backup and recovery systems, which poses a challenge in restoring data following a security breach or other data loss events. The article by Ref. [52] underscores the essential need for comprehensive data backup and recovery mechanisms in mHealth applications and points out the potential vulnerabilities in many current applications. This concern is echoed in [53].

Therefore, the development of a framework for ensuring the privacy and security of data in mHealth applications should encompass strategies aimed at minimizing risks. Such strategies include employing strong encryption techniques to prevent unauthorized access, implementing comprehensive data backup and recovery mechanisms, ensuring secure storage, and maintaining clarity and ease of use for the end-user.

5.1.2. IoT

Many IoT devices used in healthcare are not designed with security as a primary concern, and often feature weak password mechanisms or other vulnerabilities that are susceptible to exploitation by attackers [54]. Additionally, these devices and systems frequently collect and transmit substantial amounts of personal and medical data, presenting risks of unauthorized access, use, or disclosure [21,25]. This concern aligns with the findings of Ref. [55], that underscore the necessity of a secure and resilient operating environment for critical IoT systems in healthcare to mitigate potential threats. Consequently, addressing these security vulnerabilities is imperative for the healthcare sector to ensure patient safety and system integrity [56].

To bridge these gaps and overcome limitations, the healthcare sector should adopt appropriate technical and organizational measures for data protection, implement effective authentication mechanisms, and deploy security protocols alongside privacy-preserving solutions for tracking, monitoring, and analytics. Furthermore, research that focuses on designing IoT devices with standardized protocols to address the interoperability and standardization challenges in IoT and healthcare systems is essential [57].

5.1.3. Blockchain

Besides the significant benefits of using blockchain technology to control access to sensitive medical information [58], achieving complete data privacy and confidentiality in healthcare systems remains a considerable challenge that must be addressed effectively [49]. These findings align with Ref. [59], who suggests that blockchain-based health systems must establish robust mechanisms to protect patient data and ensure privacy. Other concerns include the scalability of blockchain technology and the management of shared healthcare records, which can affect their capacity to ensure the security and privacy of health information [60]. Additionally, the processing speed and capacity of blockchain systems may not be sufficient for the demands of real-time healthcare data management [32], which is a concern that was also raised in other studies [61,62].

Considering this, further research and development focusing on enhancing the scalability and performance of blockchain networks, strengthening measures for data privacy and confidentiality, addressing interoperability challenges, and considering the societal and security implications of blockchain-based health systems, is required.

5.1.4. Cloud Computing

One of the findings of this review is the security concerns associated with cloud computing. Cloud computing systems are vulnerable to hacking and data breaches, potentially exposing sensitive medical information to unauthorized parties [35]. This concern aligns with findings from Ref. [63], who indicate that healthcare organizations are hesitant to adopt cloud computing due to concerns over patient information confidentiality, privacy, and service costs. Ensuring the security of patient data and compliance with regulations such as the HIPAA and GDPR remain a significant challenge in cloud-based HISs [64].

The potential exposure of sensitive health information and the need for robust backup and disaster recovery mechanisms are significant areas of concern for healthcare organizations [63]. Medical institutions may have limited control over the security and privacy of their data when utilizing cloud computing systems, and they often depend on the security measures implemented by the cloud provider [17,37]. This finding is consistent with [64], highlighting the challenges in maintaining control over data, which also encompasses issues related to data interception and ownership in cloud computing.

Based on this analysis, while cloud computing offers numerous benefits for healthcare, such as improved collaboration, cost savings, and scalability, it also presents critical limitations and challenges. Overcoming security concerns, ensuring data privacy and confidentiality, and addressing the reluctance to adopt cloud technology are essential for the successful implementation of cloud computing in healthcare. These are crucial issues for future research. Furthermore, data protection methods should be designed to suit real-world clinical settings [37].

5.2. Secure Access Control

Numerous articles have emphasized the importance of secure access control as a vital component of HISs, regardless of the technology used. This is essential to ensuring the privacy and security of sensitive patient data. Secure access control is instrumental in preventing data breaches by regulating access to sensitive patient data. This approach effectively reduces the risk of data theft, cyberattacks, and other security threats [21,30,35,39,41,43]. Moreover, it ensures that only authorized individuals can access sensitive patient information, thereby protecting patient privacy and preventing unauthorized access to information that can be exploited for malicious purposes [23,38–40,44]. Implementing secure access controls is crucial in preventing data breaches, which can be both costly and damaging to healthcare organizations. By restricting access to sensitive data, the likelihood of data breaches can significantly be minimized. Most studies suggest that secure access control not only reduces communication and computational costs but also enhances security [21,30,35]. From an efficiency standpoint, some articles highlight that certain systems are effective for real-time healthcare systems [30,35,44], while others suggest that certain models, particu-

larly those based on agent-based systems, provide effective and secure e-health security services [39].

This study has identified secure access control as being critical for ensuring the privacy and security of medical data. However, several challenges exist in implementing secure access control in HISs. HISs typically involve multiple levels of access control, including user authentication, authorization, and audit logging. Managing and configuring these controls can be complex, with a risk of misconfiguration or loopholes that can lead to security breaches. Additionally, HISs are often intricate and may involve various systems handling large volumes of data and users. Consequently, integrating different systems and ensuring that they all have the necessary access controls is challenging. Furthermore, there are numerous regulations and standards, such as the HIPAA, HITECH, and GDPR, which must be adhered to in the healthcare industry [10].

When integrating blockchain and cloud computing to facilitate decentralized access control, healthcare organizations must adopt a comprehensive and proactive strategy for securing access to HISs. This strategy may include implementing multi-factor authentication, encryption, and user training and awareness programs, along with conducting regular security audits and assessments. Furthermore, healthcare organizations should stay informed about the latest security best practices and emerging threats, adjusting their access controls as necessary.

According to the literature, several limitations are associated with providing secure access control. Technical limitations pertain to the technical infrastructure of HISs, such as vulnerabilities in software or hardware, potentially compromising system security and permitting unauthorized access to sensitive data. Human factors also pose a threat, as employees might intentionally or unintentionally misuse sensitive patient data, leading to data breaches or other security incidents.

Addressing the identified weaknesses in secure access control of HISs requires a multifaceted approach to effectively enhance security and protect sensitive patient data. A key strategy is the strengthening of the technical infrastructure. This involves regular updates and patches to both software and hardware components of HISs, which help fix vulnerabilities and enhance a system's overall security. Another crucial aspect is the enhancement of employee training and awareness. Implementing comprehensive training programs focused on data security and privacy practices increases employees' awareness of potential risks. This education is vital for reducing the likelihood of data breaches resulting from human error or misuse. Further fortification of HIS security includes implementing advanced authentication mechanisms, such as multi-factor authentication. This significant step, coupled with regular audits of access, will ensures that only authorized personnel access sensitive patient data, thereby minimizing the risk of unauthorized breaches. Additionally, conducting regular system audits and security assessments is indispensable. These periodic reviews assist in identifying and mitigating potential threats to HISs. Continuous monitoring and assessment of the security landscape allow proactive addressing of potential vulnerabilities. By focusing on these critical areas—upgrading technical infrastructure, enhancing employee awareness and training, implementing robust authentication processes, and conducting regular security audits—the security of HISs can significantly be improved. This comprehensive approach reduces the likelihood of unauthorized access and strengthens the protection of patient data.

5.3. Secure Data Sharing

Another aspect of security discussed in the literature is the facilitation of secure data sharing in HISs. One method for achieving secure data sharing involves utilizing decentralized solutions [19,29,32–34]. Implementing lightweight and cost-effective mechanisms can enhance efficiency by minimizing time and resource consumption, thereby reducing expenses for healthcare organizations [24,29,46]. Other approaches offer secure data sharing by enabling a centralized system, which is simpler to monitor and secure compared to multiple disparate systems [16,17,20,21,33,35]. Studies, such as [33], demonstrate that

secure and trustworthy data sharing empowers patients to manage their own data, including having complete control over sharing permissions. Furthermore, Ref. [37] introduces a data sharing system from a user-centric perspective, which not only improves medical treatment but also safeguards individual safety and privacy.

Based on analysis, achieving secure data sharing in HISs is a complex and ongoing process that demands constant vigilance. However, implementing robust authentication and authorization mechanisms is challenging, particularly in large healthcare organizations with multiple systems and databases. A further challenge arises from the fact that HISs often operate across various technologies and standards, complicating data exchange and potentially leading to incomplete patient records, thus hindering secure information sharing. One significant challenge for healthcare organizations is to prevent data breaches, which can lead to the theft or exposure of sensitive patient data. Protective measures may include firewalls, intrusion detection systems, and other security protocols. Additionally, HIS staff must be thoroughly trained and made aware of the importance of data privacy and security. They should understand the risks associated with data breaches and be educated on prevention strategies.

Previous studies on secure data sharing in HISs highlight its essential role in enhancing patient care but also point out several limitations that must be addressed. A primary limitation is the lack of interoperability, which hampers data sharing across different systems. This can create barriers to secure health information sharing, leading to incomplete patient records, especially when patients receive care from multiple providers or organizations. Another critical limitation is the vulnerability of HISs to cybersecurity attacks and technical failures due to their complex technical infrastructure. These incidents can compromise the confidentiality, integrity, and availability of sensitive health information. Furthermore, regulatory and legal barriers can prevent data sharing between different healthcare providers and organizations, limiting the benefits of data sharing in healthcare outcomes. Technical constraints also pose significant challenges to secure data sharing. Some HISs may lack the capacity for large-scale data sharing or the necessary security features to safeguard data during transmission. Additionally, most schemes for secure data sharing are not designed with real-world clinical settings in mind. Finally, the lack of standardization in HISs can impede the accuracy and consistency of shared data, further complicating the secure sharing process.

In response to the challenges encountered in secure data exchange within HISs, several principal recommendations have been identified as best practices. First, there is an increasing agreement on the need to enhance interoperability. This involves developing and adopting standardized protocols and formats, which are essential for enabling smooth data transfer across various HIS platforms. Equally critical is the strengthening of cybersecurity measures. To protect HISs against cyber threats and technical mishaps, the implementation of advanced security protocols is crucial. In conjunction, regular security audits and system updates are necessary to ensure robust defenses against potential cyberattacks. Another key aspect is addressing the regulatory and legal barriers that impede efficient data sharing. A coordinated effort to harmonize regulations can facilitate data exchange across different jurisdictions while ensuring secure and compliant operations. Improving the technical infrastructure of HISs is also a priority. This includes upgrading systems to not only support large-scale data sharing but also to integrate enhanced security features for data protection. These upgrades are necessary to meet the growing demands and complexities of modern healthcare data management. Additionally, the design of secure data sharing systems should consider the practical needs and workflows of real-world clinical settings. Customizing these systems to integrate seamlessly into the daily operations of healthcare providers is essential for their effective adoption and use. Finally, the standardization of data is vital. Promoting and implementing uniform standards in data recording and sharing is crucial to ensuring accuracy and consistency across different systems. This uniformity is key to improving the quality of patient care while maintaining the integrity and privacy of health data.

5.4. Secure Data Storage

Various studies have discussed the importance of secure data storage in HISs for ensuring data privacy and security. An analysis of these studies reveals that implementing secure data storage can be cost-effective in the long run, as it reduces the risk of costly data breaches for healthcare organizations [8,25]. Another significant finding is that utilizing decentralized solutions helps address potential security issues through solidity-based smart contracts [26,31,36]. It is also noted that secure data storage ensures patient data confidentiality, allowing only authorized personnel access [7,18,41,45,48]. This practice helps prevent data breaches and unauthorized access to sensitive health information [20,28,31]. As indicated in the literature, secure data storage builds trust between patients and healthcare providers. Patients are more inclined to trust providers who take their data's security and privacy seriously, potentially leading to better patient outcomes and higher satisfaction [17,22]. Additionally, secure data storage maintains the integrity of patient data by preventing tampering or alteration, ensuring data accuracy and reliability, which is critical for making important medical decisions [65]. Overall, secure data storage is essential for maintaining patient data privacy and security, and healthcare organizations that prioritize it can benefit from improved compliance, reduced costs, and increased trust.

In general, secure data storage in HISs requires a comprehensive approach that addresses key challenges to ensure the confidentiality, integrity, and availability of patient data. This involves implementing stringent user authentication and authorization protocols, ensuring that storage data are accessed only by authorized personnel. Furthermore, employing a multi-layered security approach that includes firewalls, encryption, and intrusion detection systems can further strengthen data storage security against a wide array of cyber threats. Maintaining the accuracy and completeness of patient data is critical for effective patient care and medical decision-making, so utilizing reliable protocols for data verification and validation can support data integrity. Additionally, implementing data backup and recovery mechanisms can help mitigate the risk of data loss. Addressing these recommendations will significantly improve the security and reliability of data storage within HISs.

These improvements are not only beneficial for the protection of data but also play a pivotal role in enhancing the overall quality of patient care.

6. Limitations

The literature review presented here has a few limitations. Initially, only papers published in English were included, thereby excluding articles reported in other languages. Furthermore, the review was restricted to journal articles to ensure its quality. Consequently, other types of publications, such as conference papers, books, white papers, and organizational reports, were not considered. This exclusion may have resulted in missing additional insights that could have been valuable for this review. Therefore, it is possible that some security issues not mentioned in the selected articles were overlooked.

7. Conclusions

This study systematically reviews the literature on health information systems (HISs) in relation to medical data privacy and security. It contributes to existing research by identifying various related technologies and addressing security and privacy aspects. This study highlights the necessity for a secure HIS that not only meets organizational objectives but also ensures the protection of patient data. HISs offer significant benefits to healthcare organizations in terms of storing, retrieving, analyzing, exchanging, and sharing patient health information. These systems must both serve the needs of patients and health practitioners, while safeguarding the security and privacy of medical data. Therefore, HISs must be designed and implemented with privacy and security as primary considerations. This involves employing secure technologies for data storage and sharing, enforcing access controls to restrict data viewing or modification, and educating healthcare professionals on best practices for patient data privacy and security.

In conclusion, this review has explored the significant advancements and challenges in the realm of health information systems (HISs), focusing on key technologies such as blockchain, mobile health applications, cloud computing, and secure data sharing and storage. As we look toward the future of HISs, it is important to consider the evolving landscape of health data management frameworks. In this context, openEHR emerges as a noteworthy framework. While not the primary focus of this review, openEHR's approach to standardized data models and archetypes for electronic health records presents potential synergies with the technologies discussed. Its emphasis on interoperability, security, and patient-centered data management aligns with the broader objectives of enhancing HISs. Future research could beneficially explore the integration of openEHR with current technologies to address the evolving needs of healthcare systems, ensuring a comprehensive and secure approach to managing health information. The continuous evolution of HISs requires adaptable and forward-thinking solutions, and openEHR represents a key area for future exploration and development in this field.

Author Contributions: Conceptualization, methodology, analysis P.S., E.V.-G. and Y.-W.C.; formal analysis, P.S.; investigation, P.S.; writing—original draft preparation, P.S.; writing—review and editing, E.V.-G. and Y.-W.C.; supervision, E.V.-G. and Y.-W.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Yusof, M.M.; Papazafeiropoulou, A.; Paul, R.J.; Stergioulas, L.K. Investigating Evaluation Frameworks for Health Information Systems. *Int. J. Med. Inform.* **2008**, *77*, 377–385. [CrossRef] [PubMed]
2. Vora, J.; Italiya, P.; Tanwar, S.; Tyagi, S.; Kumar, N.; Obaidat, M.S.; Hsiao, K.F. Ensuring Privacy and Security in E-Health Records. In Proceedings of the International Conference on Computer, Information and Telecommunication Systems (CITS), Colmar, France, 11–13 July 2018.
3. Mbonihankuye, S.; Nkunzimana, A.; Ndagijimana, A. Healthcare Data Security Technology: HIPAA Compliance. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 1927495. [CrossRef]
4. Qayyum, A.; Qadir, J.; Bilal, M.; Al-Fuqaha, A. Secure and Robust Machine Learning for Healthcare: A Survey. *IEEE Rev. Biomed. Eng.* **2020**, *14*, 156–180. [CrossRef] [PubMed]
5. Agbo, C.C.; QMahmoud, H.; Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare* **2019**, *7*, 56. [CrossRef] [PubMed]
6. Mohamad Jawad, H.H.; Bin Hassan, Z.; Zaidan, B.B.; Mohammed Jawad, F.H.; Mohamed Jawad, D.H.; Alredany, W.H.D. A Systematic Literature Review of Enabling IoT in Healthcare: Motivations, Challenges, and Recommendations. *Electronics* **2022**, *11*, 3223. [CrossRef]
7. Katarahweire, M.; Bainomugisha, E.; Mughal, K.A.; Ngubiri, J. Form-based security in mobile health data collection systems. *Secur. Priv.* **2021**, *4*, e155. [CrossRef]
8. 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]
9. Keshta, I.; Odeh, A. Security and privacy of electronic health records: Concerns and challenges. *Egypt. Inform. J.* **2021**, *22*, 177–183. [CrossRef]
10. Harman, L.B.; Flite, C.A.; Bond, K. Electronic Health Records: Privacy, Confidentiality, and Security. *Am. Med. Assoc. J. Ethics* **2012**, *14*, 712–719.
11. Basil, N.N.; Solomon, A.; Chukwuyem, E.; Ekokobe, F. Health Records Database and Inherent Security Concerns: A Review of the Literature. *Cureus* **2022**, *14*, e30168. [CrossRef]
12. Fathima Shah, W. Preserving Privacy and Security: A Comparative Study of Health Data Regulations—GDPR vs. HIPAA. *Int. J. Res. Appl. Sci. Eng. Technol.* **2023**, *11*. [CrossRef]
13. Amato, F.; Casola, V.; Cozzolino, G.; De Benedictis, A.; Mazzocca, N.; Moscato, F. A Security and Privacy Validation Methodology for e-Health Systems. *ACM Trans. Multimed. Comput. Commun. Appl.* **2021**, *17*. [CrossRef]
14. Joppi, R.; Bertele, V.; Vannini, T.; Garattini, S.; Banzi, R. Food and Drug Administration vs European Medicines Agency: Review times and clinical evidence on novel drugs at the time of approval. *Br. J. Clin. Pharmacol.* **2020**, *86*, 170–174. [CrossRef]

15. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G.; The PRISMA Group. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *PLoS Med.* **2009**, *6*, e1000097. [CrossRef]
16. 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]
17. 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]
18. Xie, Y.; Zhang, K.; Kou, H.; Mokarram, M.J. Private anomaly detection of student health conditions based on wearable sensors in mobile cloud computing. *J. Cloud Comput.* **2022**, *11*. [CrossRef] [PubMed]
19. Bigini, G.; Lattanzi, E. Toward the InterPlanetary Health Layer for the Internet of Medical Things With Distributed Ledgers and Storages. *IEEE Access* **2022**, *10*, 82883–82895. [CrossRef]
20. 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]
21. Agrahari, A.K.; Varma, S.; Venkatesan, S. Two factor authentication protocol for IoT based healthcare monitoring system. *J. Ambient Intell. Humaniz. Comput.* **2023**, *14*, 16081–16098. [CrossRef]
22. 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]
23. Shreya, S.; Chatterjee, K.; Singh, A. A smart secure healthcare monitoring system with Internet of Medical Things. *Comput. Electr. Eng.* **2022**, *101*, 107969. [CrossRef]
24. Bashir, A.; Mir, A.H. Lightweight Secure MQTT for Mobility Enabled e-health Internet of Things. *Int. Arab. J. Inf. Technol.* **2021**, *18*, 773–781. [CrossRef]
25. 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]
26. Yongjoh, S.; So-In, C.; Kompunt, P.; Muneesawang, P.; Morien, R.I. Development of an Internet-of-Healthcare System Using Blockchain. *IEEE Access* **2021**, *9*, 113017–113031. [CrossRef]
27. Ghayvat, H.; Sharma, M.; Gope, P.; Sharma, P.K. SHARIF: Solid Pod-Based Secured Healthcare Information Storage and Exchange Solution in Internet of Things. *IEEE Trans. Ind. Inform.* **2022**, *18*, 5609–5618. [CrossRef]
28. Arul, R.; Al-Otaibi, Y.D.; Alnumay, W.S.; Tariq, U.; Shoaib, U.; Piran, M.J. Multi-modal secure healthcare data dissemination framework using blockchain in IoMT. *Pers. Ubiquitous Comput.* **2021**. [CrossRef]
29. Khan, A.A.; Wagan, A.A.; Laghari, A.A.; Gilal, A.R.; Aziz, I.A.; Talpur, B.A. BIoMT: A State-of-the-Art Consortium Serverless Network Architecture for Healthcare System Using Blockchain Smart Contracts. *IEEE Access* **2022**, *10*, 78887–78898. [CrossRef]
30. Saini, A.; Zhu, Q.; Singh, N.; Xiang, Y.; Gao, L.; Zhang, Y. A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System. *IEEE Internet Things J.* **2021**, *8*, 5914–5925. [CrossRef]
31. Mnyawi, R.; Kombe, C.; Sam, A.; Nyambo, D. Blockchain-based Data Storage Security Architecture for e-Health Care Systems: A Case of Government of Tanzania Hospital Management Information System. *Int. J. Comput. Sci. Netw. Secur.* **2022**, *22*, 364–374.
32. Xu, G.; Qi, C.; Dong, W.; Gong, L.; Liu, S.; Chen, S.; Liu, J.; Zheng, X. A Privacy-Preserving Medical Data Sharing Scheme Based on Blockchain. *IEEE J. Biomed. Health Inform.* **2022**, *27*, 698–709. [CrossRef]
33. Dubovitskaya, A.; Baig, F.; Xu, Z.; Shukla, R.; Zambani, P.S.; Swaminathan, A.; Jahangir, M.M.; Chowdhry, K.; Lachhani, R.; Idnani, N.; et al. ACTION-EHR: Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care. *J. Med. Internet Res.* **2020**, *22*, e13598. [CrossRef]
34. Kim, H.J.; Kim, H.H.; Ku, H.; Yoo, K.D.; Lee, S.; Park, J.I.; Kim, H.J.; Kim, K.; Chung, M.K.; Lee, K.H.; et al. Smart Decentralization of Personal Health Records with Physician Apps and Helper Agents on Blockchain: Platform Design and Implementation Study. *JMIR Med. Inform.* **2021**, *9*, e26230. [CrossRef]
35. Son, S.; Lee, J.; Kim, M.; Yu, S.; Das, A.K.; Park, Y. Design of Secure Authentication Protocol for Cloud-Assisted Telecare Medical Information System Using Blockchain. *IEEE Access* **2020**, *8*, 192177–192191. [CrossRef]
36. Shakil, K.A.; Zareen, F.J.; Alam, M.; Jabin, S. BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. *J. King Saud Univ.-Comput. Inf. Sci.* **2020**, *32*, 57–64. [CrossRef]
37. 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]
38. 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]
39. Khan, F.; Reyad, O. Application of intelligent multi agent based systems for E-healthcare security. *Inf. Sci. Lett.* **2019**, *8*, 67–72.
40. Padinjappurathu Gopalan, S.; Chowdhary, C.L.; Iwendi, C.; Farid, M.A.; Ramasamy, L.K. An Efficient and Privacy-Preserving Scheme for Disease Prediction in Modern Healthcare Systems. *Sensors* **2022**, *22*, 5574. [CrossRef] [PubMed]
41. Reyad, O.; Karar, M.E. Secure CT-Image Encryption for COVID-19 Infections Using HBBS-Based Multiple Key-Streams. *Arab. J. Sci. Eng.* **2021**, *46*, 3581–3593. [CrossRef] [PubMed]
42. Salim, M.M.; Park, J.H. Federated Learning-based secure Electronic Health Record sharing scheme in Medical Informatics. *IEEE J. Biomed. Health Inform.* **2022**, *27*, 617–624. [CrossRef] [PubMed]
43. Edemacu, K.; Jang, B.; Kim, J.W. Collaborative Ehealth Privacy and Security: An Access Control With Attribute Revocation Based on OBDD Access Structure. *IEEE J. Biomed. Health Inform.* **2020**, *24*, 2960–2972. [CrossRef] [PubMed]

44. Jiang, Z.; Liu, W.; Ma, R.; Shirazi, S.H.; Xie, Y. Lightweight Healthcare Wireless Body Area Network Scheme With Amplified Security. *IEEE Access* **2021**, *9*, 125739–125752. [CrossRef]
45. 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]
46. Zhang, M.; Chen, Y.; Susilo, W. PPO-CPQ: A Privacy-Preserving Optimization of Clinical Pathway Query for E-Healthcare Systems. *IEEE Internet Things J.* **2020**, *7*, 10660–10672. [CrossRef]
47. 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]
48. Chatterjee, A.; Gerdes, M.W.; Khatiwada, P.; Prinz, A. SFTSDH: Applying Spring Security Framework With TSD-Based OAuth2 to Protect Microservice Architecture APIs. *IEEE Access* **2022**, *10*, 41914–41934. [CrossRef]
49. Hu, J.; Liang, W.; Hosam, O.; Hsieh, M.Y.; Su, X. 5GSS: A framework for 5G-secure-smart healthcare monitoring. *Connect. Sci.* **2022**, *34*, 139–161. [CrossRef]
50. Roehrs, A.; Da Costa, C.A.; da Rosa Righi, R.; De Oliveira, K.S.F. Personal Health Records: A Systematic Literature Review. *J. Med. Internet Res.* **2017**, *19*, e5876. [CrossRef]
51. Mirza, A.B. Potential of Mobile Devices in New Zealand Healthcare. In *Masters of Engineering in Software*; Massey University: Albany, Auckland, New Zealand, May 2008.
52. Dogtown Media. Data Backup and Disaster Recovery Strategies for Healthcare App Data Storage. Available online: https://www.dogtownmedia.com/data-backup-and-disaster-recovery-strategies-for-healthcare-app-data-storage/ (accessed on 12 January 2024).
53. Arora, S.; Yttri, J.; Nilse, W. Privacy and Security in Mobile Health (mHealth) Research. *Alcohol. Res.* **2014**, *36*, 143–151.
54. Elhoseny, M.; Thilakarathne, N.N.; Alghamdi, M.I.; Mahendran, R.K.; Gardezi, A.A.; Weerasinghe, H.; Welhenge, A. Security and Privacy Issues in Medical Internet of Things: Overview, Countermeasures, Challenges and Future Directions. *Sustainability* **2021**, *13*, 11645. [CrossRef]
55. Thapa, S.; Bello, A.; Maurushat, A.; Farid, F. Security Risks and User Perception towards Adopting Wearable Internet of Medical Things. *Int. J. Environ. Res. Public Health* **2023**, *20*, 5519. [CrossRef] [PubMed]
56. Tandon, R.; Cupta, P.K. Security and Privacy Challenges in Healthcare Using Internet of Things. In *IoT-Based Data Analytics for the Healthcare Industry*; Singh, S.K., Singh, R.S., Pandey, A.K., Udmale, S.S., Chaudhary, A., Eds.; Academic Press: London, UK, 2021; pp. 149–165.
57. Kelly, J.T.; Campbell, K.L.; Gong, E.; Scuffham, P. The Internet of Things: Impact and Implications for Health Care Delivery. *J. Med. Internet Res.* **2020**, *22*, e20135. [CrossRef] [PubMed]
58. Yinka, O.T.; Haw, S.C.; Yap, T.T.V.; Subramaniam, S. Improving the data access control using blockchain for healthcare domain. *F1000 Res.* **2021**, *10*, 901. [CrossRef]
59. Kiania, K.; Jameii, S.M.; Rahmani, A.M. Blockchain-based privacy and security preserving in electronic health: A systematic review. *Multimed. Tools Appl.* **2023**, *82*, 28493–28519. [CrossRef] [PubMed]
60. Sanka, A.I.; Cheung, R.C.C. A systematic review of blockchain scalability: Issues, solutions, analysis and future research. *J. Netw. Comput. Appl.* **2021**, *195*, 103232. [CrossRef]
61. Zhang, R.; Xue, R.; Liu, L. Security and Privacy for Healthcare Blockchains. *IEEE Trans. Serv. Comput.* **2022**, *15*, 3668–3686. [CrossRef]
62. Ghosh, P.K.; Chakraborty, A.; Hasan, M.; Rashid, K.; Siddique, A.H. Blockchain Application in Healthcare Systems: A Review. *Systems* **2023**, *11*, 38. [CrossRef]
63. Mehrtak, M.; SeyedAlinaghi, S.; MohsseniPour, M.; Noori, T.; Karimi, A.; Shamsabadi, A.; Heydari, M.; Barzegary, A.; Mirzapour, P.; Soleymanzadeh, M.; et al. Security challenges and solutions using healthcare cloud computing. *J. Med. Life* **2021**, *14*, 448. [CrossRef]
64. AI-Issa, Y.; Ottom, M.A.; Tamrawi, A. eHealth Cloud Security Challenges: A Survey. *J. Healthc. Eng.* **2019**, *2019*, 7516035.
65. Attarian, R.; Hashemi, S. An anonymity communication protocol for security and privacy of clients in IoT-based mobile health transactions. *Comput. Netw.* **2021**, *190*, 107976. [CrossRef]