applied sciences

MDPI

Review

Centralized vs. Decentralized Cloud Computing in Healthcare

Mona Abughazalah [1,*], Wafaa Alsaggaf [1], Shireen Saifuddin [1] and Shahenda Sarhan [2,3]

[1] Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia; waalsaggaf@kau.edu.sa (W.A.); ssaifuddin@kau.edu.sa (S.S.)
[2] Faculty of Computer and Information, Mansoura University, Mansoura 35516, Egypt; sh_sarhan@mans.edu.eg
[3] University of Economics and Human Sciences, 01-043 Warsaw, Poland
[*] Correspondence: mabughazaleh@kau.edu.sa

Abstract: Healthcare is one of the industries that seeks to deliver medical services to patients on time. One of the issues it currently grapples with is real-time patient data exchange between various healthcare organizations. This challenge was solved by both centralized and decentralized cloud computing architecture solutions. In this paper, we review the current state of these two cloud computing architectures in the health sector with regard to the effect on the efficiency of Health Information Exchange (HIE) systems. Our study seeks to determine the relevance of these cloud computing approaches in assisting healthcare facilities in the decision-making process to adopt HIE systems. This paper considers the system performance, patient data privacy, and cost and identifies research directions in each of the architectures. This study shows that there are some benefits in both cloud architectures, but there are also some drawbacks. The prominent characteristic of centralized cloud computing is that all data and information are stored together at one location, known as a single data center. This offers many services, such as integration, effectiveness, simplicity, and rapid information access. However, it entails providing data privacy and confidentiality aspects because it will face the hazard of a single point of failure. On the other hand, decentralized cloud computing is built to safeguard data privacy and security whereby data are distributed to several nodes as a way of forming mini-data centers. This increases the system's ability to cope with a node failure. Thus, continuity and less latency are achieved. Nevertheless, it poses integration issues because managing data from several sites could be a problem, and the costs of operating several data centers are higher and complex. This paper also pays attention to the differences in aspects like efficiency, capacity, and cost. This paper assists healthcare organizations in determining the most suitable cloud architecture strategy for deploying secure and effective HIE systems.

Keywords: cloud computing; health information exchange; centralized cloud computing; decentralized cloud computing

check for updates

Citation: Abughazalah, M.; Alsaggaf, W.; Saifuddin, S.; Sarhan, S. Centralized vs. Decentralized Cloud Computing in Healthcare. *Appl. Sci.* **2024**, *14*, 7765. https://doi.org/10.3390/app14177765

Academic Editor: Enno van der Velde

Received: 9 July 2024
Revised: 7 August 2024
Accepted: 26 August 2024
Published: 3 September 2024

1. Introduction

Medical records are essential in any healthcare center since they hold all the important details of a particular patient, their health profile, the medical timeline, and records of every consultation. Patients' records are also a prominent component for enhancing the accuracy and quality of healthcare service because records are the main system for storing patients' information, enhancing communication, and follow-up investigations [1].

In the past, hospitals were able to save patient information on paper [2], a mode of record keeping that has numerous demerits even though it remains typical in the medical field. Disasters such as fire, flood, or pests can easily destroy papers or make them inaccessible through water damage or rodents. Moreover, paper records can take a lot of space in healthcare centers; it becomes a major issue for storage. Furthermore, it might be time-consuming to search for the necessary documents needed when retrieving data for the staff. Some challenges faced with paper records include lost data; poor record keeping, since some writings may be hard to read; data being accessible by a single user; and the physical burden of paper [3,4].

To solve the problem, electronic medical records (EMRs) [5] have gradually replaced paper records for recording patients' information to allow hospitals to store patients records electronically where necessary. They have several benefits. They present documents with a standard format with easy access and retrieval. This not only results in the efficient and accurate documentation of patient information but also reduces hospital expenses. In addition, it enhances patient safety by documenting important information that would include drug–drug interactions and allergic reactions to ensure that all medical procedures adhere to the recommended guidelines to avoid adverse effects [6,7].

Nevertheless, one of the demerits that comes with EMRs is that the patient care offered through the EMR system is limited to the specific healthcare facility, with no connection to any other facility [8]. With the improvement of the healthcare systems, there was a demand for integrated and community-wide health information, leading to the definition of EHRs. They are advanced versions of EMRs that provide not only the consolidated record of the patient but also the record of health information from a number of healthcare organizations and comprise data received from various sources, including medical records, laboratory results, reports on radiology, and data on pharmacy. They are supposed to be seamless in order to support HIE and the exchange of patient information within and across the participating healthcare centers [9].

HIE [10] is an IT platform that facilitates the exchange of health-related data between and among healthcare organizations, which includes hospitals, clinics, laboratories, and pharmacies among others; HIE is related to EHRs as it provides a platform through which data can be exchanged, while EHR provides a comprehensive record of patients. This is especially crucial during disasters because information about a patient could mean the difference between life and death [11].

A number of benefits are provided by EHR systems that enable the smooth sharing of patient data between hospital systems. However, healthcare organizations must also consider certain drawbacks, especially regarding the storage of sensitive patient health information. This requires strict privacy and security measures to protect the patient data from unauthorized access, breaches, or cyberattacks [12,13]. In this regard, cloud-based solutions are advantageous over traditional on-premise EHR systems, in terms of HIE [14], as cloud providers implement strong security measures to protect patient data, including encryption, access controls, and regular security audits. Cloud-based HIE solutions leverage these security features to ensure the secure transmission and storage of sensitive patient information [15]. In addition to this, HIE systems that implement cloud technology are flexible since they can accommodate the level of need for sharing information more so when established to suit the set standards. These platforms also provide enhanced integration on the account of providing standard interfaces and protocols for real-time data sharing and interoperability. This makes it possible for a provider to obtain the most current patient information as they need it [16].

Previous research categorized cloud technology solutions under two primary types: centralized and decentralized. In the centralized cloud architecture, all the HIE infrastructure and services involved are hosted and managed in a single, centralized cloud environment. This enables all of the participating healthcare organizations to connect to and access the HIE platform via the central cloud infrastructure. In contrast, in the decentralized cloud architecture, the HIE infrastructure and services are distributed across multiple cloud instances [17]. Our role is to assist healthcare organizations in making informed decisions regarding the most suitable cloud architecture to meet their health information exchange (HIE) requirements. This includes carefully evaluating the advantages and disadvantages of centralized cloud computing architecture versus decentralized architecture. We offer a thorough analysis and assessment of both cloud computing solutions for healthcare architecture, which are considered the primary contributions of our paper.

This paper discusses both centralized and decentralized cloud computing in healthcare by addressing the following research questions:

- RQ1: What are the benefits and limitations of the use of centralized cloud computing in healthcare that aims to improve HIE?
- RQ2: What are the benefits and limitations of the use of decentralized cloud computing in healthcare that aims to improve HIE?
- RQ3: What are the differences between centralized and decentralized cloud healthcare solutions regarding the system's performance, response times, latency, the privacy of patient data, and cost efficiency?
- RQ4: What are the research gaps within centralized cloud healthcare solutions?
- RQ5: What are the research gaps within decentralized cloud healthcare solutions?

The aim of this study was to assess and compare centralized and decentralized cloud computing architecture solutions for the development of healthcare systems. The objective was to determine how these different cloud computing approaches can provide hospitals with the best possible performance and cost efficiency while also ensuring the maintenance of patient privacy and data security.

The rest of this paper is organized as follows: Section 2 briefly discusses HIE and its relationship with cloud technology in healthcare systems. Section 3 will explain what cloud computing is, its types, and the deployment of the cloud in the healthcare sector. The analysis of the research methodology is presented in Section 4. This paper's Section 5 reviews earlier literature reviews on centralized and cloud computing efforts. In Section 6, this paper also presents a literature review of what has been achieved in the decentralized and cloud computing domains in the past. Section 7 also looks at the differences between both models of cloud computing. Section 8 provides the conclusion of this survey, and Section 8 is the last section of this paper.

2. Health Information Exchange

HIE is a healthcare delivery approach that enables the sharing of important patient information among different healthcare systems. In today's ever-changing digital health landscape, HIE is crucial for enhancing the coordination and continuity of care. By leveraging electronic data exchange, HIE enables the secure transmission of patient health records, diagnostic test results, medication histories, and other relevant information among healthcare organizations [18]. This interconnected system empowers healthcare providers with comprehensive insights into a patient's medical history, engendering more informed clinical decisions, better treatment outcomes, and increased overall efficiency in healthcare service delivery. As HIE continues to evolve, it plays a vital role in advancing patient-centered care, reducing redundancies, and realizing a more interconnected and efficient healthcare ecosystem, thereby improving patient health outcomes [19,20].

The integration of HIE with cloud technology represents a significant advancement in the accessibility, scalability, and efficiency of healthcare information management [21]. Utilizing cloud infrastructures in HIE, healthcare organizations, providers, and patients can benefit from increased accessibility, enhanced scalability, and improved efficiency. The introduction of cloud technology in HIE presents many opportunities for healthcare stakeholders to better manage and deliver healthcare services [22,23].

Cloud-based HIE allows healthcare professionals to access patient information securely from anywhere online, facilitating timely decision making, especially in emergencies [24]. Due to its scalability, cloud technology enables healthcare organizations to adjust HIE systems on demand, accommodating variations in data volume and user requirements [25]. The use of this cost-effective alternative to traditional methods of record storage and sharing can help to evolve healthcare. Cloud service providers ensure the security of patient health information via encryption, access controls, and regular security audits of the HIE sphere. The use of cloud-based HIE promotes collaboration and interoperability across healthcare organizations via standardized data formats and communication protocols [26]. Hence, the use of HIE and cloud technology promises to create a more connected and efficient healthcare ecosystem [27].

3. Cloud Computing

The internet-based delivery of sophisticated services and data exchange is increasingly relying on the growing trend of cloud-based technologies [28]. Services like Gmail, Google Docs, and Dropbox have propelled this technology into global prominence. The rapid expansion of internet-based technologies is represent by cloud systems, which offer economic benefits and swift data retrieval across widespread networks [29]. Building upon grid computing principles, this technology enhances the concept by layering resources and services over the underlying hardware framework. Web technologies like HTML, CSS, PHP, AJAX,.NET, and SOAP form the foundation for cloud-based applications, fostering user engagement. This model facilitates flexible, as-needed utilization of computing assets, encompassing software, services, and data storage [30,31].

3.1. Cloud Computing Deployment Models

Cloud infrastructure implementations fall into four distinct categories: private cloud, public cloud, hybrid cloud, and community cloud [27,32].

The private cloud is exclusively controlled and centrally managed by a single entity, sometimes termed 'corporate cloud', as it operates under proprietary ownership. While external service providers can maintain private cloud servers, most enterprises opt for on-premise hardware, allowing internal teams to directly oversee and administer the infrastructure within their own data facilities [33].

Public cloud models are widely recognized as a standard cloud offering. They are publicly accessible platforms and are frequently employed for web-based applications, collaborative file distribution, and the storage of non-sensitive information. For collaborative endeavors and software creation, open-access cloud infrastructures are often advised. These systems rely on extensive hardware resources, owned and maintained by service vendors in large-scale computing facilities. In the realm of software engineering and quality assurance, openly accessible cloud platforms play a crucial role. Engineering teams frequently leverage these virtual ecosystems for their affordability, rapid deployment, and ease of configuration, making them ideal for developmental stages and test scenarios [34].

Integrating public and private cloud systems, hybrid infrastructures facilitate seamless interoperability between platforms. This fusion enables efficient data management and application performance across diverse environments. Enterprises with specific industry- or scale-related requirements often find this integrated approach ideal, as it caters to their need for both public and private cloud elements. Typically evolving from private infrastructures, hybrid cloud systems incorporate one or more public cloud services. This architecture proves advantageous for organizations facing data sensitivity concerns or regulatory constraints that demand specific protection, storage, and handling protocols [35].

Catering to groups with aligned interests or shared objectives, community cloud platforms offer specialized services to a network of affiliated users or entities. Participants in these ecosystems typically operate under common governance structures, adhere to similar security protocols, and follow unified policy frameworks. These collaborative digital environments can be deployed through various configurations: housed within a participating organization's facilities, maintained at a peer entity's location, managed by a single service provider, or distributed across a combination of these arrangements [36].

The structure of cloud computing ecosystems incorporates multiple essential elements: a front-end platform, back-end servers, network service, and a cloud-based delivery service. Figure 1 illustrates cloud architecture components. User interaction with cloud computing platforms occurs through front-end–client-side interfaces, serving as the entry point for accessing and utilizing cloud-based applications and services. Back-end infrastructure elements, including virtualized environments, processing units, data repositories, and security frameworks, form the core of cloud service operations. This back-end ecosystem, overseen by service providers, supplies the necessary resources for distributed computing functionalities [37].

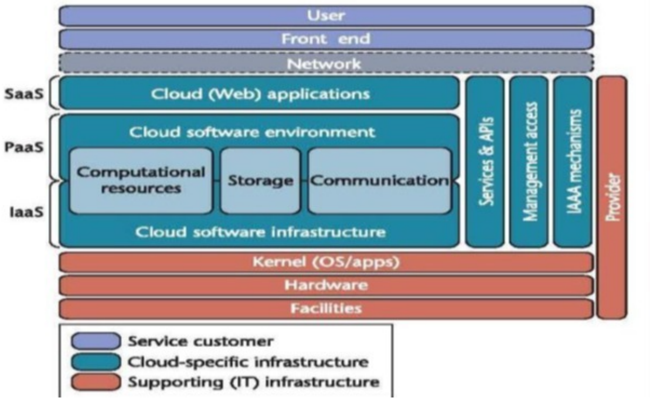

Figure 1. Cloud architecture components [37].

The front-end encompasses web browsers, like Chrome, Firefox, and Opera; clients; and mobile devices. User interaction with cloud-based services occurs through visual digital interfaces, forming the foundation of client-side infrastructure. Network connectivity serves as the conduit linking user interfaces with core infrastructure, facilitating data exchange and operational synergy between these two domains [38]. Cloud-based software and platforms, accessible on demand, comprise the suite of services sought by end-users. Based on user requirements, the service orchestration layer determines and regulates access to specific cloud offerings. The virtualized execution framework provides operational support for cloud-based instances. A crucial element in cloud computing infrastructure is the expansive data repository system, offering substantial capacity for information storage and administration within the cloud environment. Cloud systems provide multi-tiered services encompassing host environments, network infrastructure, and application platforms. A central orchestration layer coordinates these elements, overseeing operational aspects from software deployment to data storage. In the back end, this management framework also implements robust security protocols, safeguarding user resources, digital assets, and underlying infrastructure across the entire ecosystem [39,40].

3.2. Cloud Computing in Healthcare

The medical sector is evolving constantly with the advancements in technology, and the demand for optimal patient care continues to grow. Cloud computing plays a significant role in transforming healthcare information technology (IT) operations [41]. It provides a dynamic and flexible approach for the management, storage, and access of critical medical information. Leveraging cloud computing technologies, healthcare organizations can redefine how they operate and unlock unprecedented opportunities for collaboration, innovation, and patient-centric care. Cloud computing enables secure access to patient data and medical records anywhere, anytime, promoting informed decision making and timely care [42]. It promotes seamless communication and collaboration between healthcare systems and applications, exceeding the abilities of traditional databases. This increases interoperability and improves the means of sharing information within the continuum of the linked healthcare delivery system. Vendors of cloud services adhere to established sector guidelines, like the Health Insurance Portability and Accountability Act (HIPAA) [43,44], to protect sensitive patient data in cloud environments.

Hence, cloud solutions are also cheaper than traditional infrastructures in healthcare organizations, since investing in costly on-premise hardware and the maintenance of their own infrastructure can be replaced with investing more in patients and advanced solutions [23,45].

Integrating cloud computing and health information exchange (HIE) into the healthcare industry represents a new and transformative approach for the sector. This partnership revolutionizes the management and use of patient information. Bridging the gap between these two technologies makes it possible to address the challenges of interoperability, data accessibility, and collaborative care [46]. This collaborative approach promises a future in which healthcare delivery is more connected and efficient and prioritizes the patient's needs and preferences above all else in healthcare decisions [20].

4. Research Methodology

This study's methodology draws upon guidance from [47], which encompassed a trio of key stages: planning, conducting, and reporting:

1. The planning phase included the following:
   - The identification of the research problem;
   - The determination of the research questions.
2. The conducting phase included the following:
   - The determination of the search strategy;
   - The determination of the study selection criteria;
   - The determination of the study selection process.
3. The reporting phase included the following:
   - The definition of the dissemination strategy;
   - The formatting of the report;
   - The evaluation of the report.

Figure 2 illustrates the research methodology.

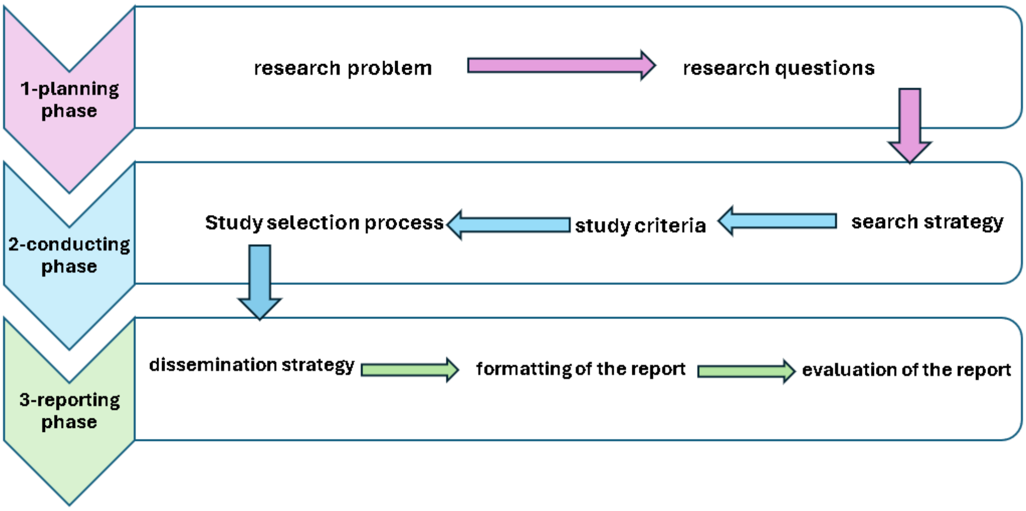

Figure 2. Research methodology.

4.1. Planning Phase

4.1.1. Defining the Need for a Paper

This paper aimed at (i) examining how prior research dealt with issues associated with system response time latency, patient data privacy, and cost considerations in centralized and decentralized cloud healthcare care systems and (ii) the review and analysis of previous studies' recommendations that can help in identifying directions for developing solutions for the existing gaps in centralized and decentralized cloud health systems, specifically in terms of their performance issues, patient data privacy, and cost.

4.1.2. Determining the Research Questions

Specific research questions were established for this paper, depending on the concerns that this paper aimed at addressing.

4.2. Conducting Phase

This section aims to identify the procedures followed in the completion of this paper. The search strategy included the identification of the papers, inclusion and exclusion criteria, and the data extraction and synthesis required to inform this paper. In addition, it provides an overview of the quality measures applied in this paper to evaluate the reviewed studies.

4.2.1. Search Strategy

The initial phase involved implementing a targeted retrieval process to identify pertinent research aligning with the study's goals. This approach included the following:

1. Scholarly databases and open-access platforms formed the foundation of this paper, including the following: IEEE Xplore, ACM Digital Library, SpringerLink, Elsevier, and MDPI. These papers were selected based on the most renowned and trusted publishers that researchers widely rely on. They provide subscriptions and free access to the majority of papers;
2. To locate pertinent data on cloud computing systems in HIE, specific terminological queries were formulated: "Cloud computing", "health information exchange in Cloud computing", "centralized Cloud computing in healthcare", "decentralized Cloud computing in healthcare", "Healthcare Integration", "Electronic Health Records (EHR) Integration", "Unified Healthcare Records". Alternative spellings were also taken into consideration while searching through the names of the libraries; the libraries' basic search operators used OR and AND to allow for a broader search. The keywords in each group were connected using the OR operator, while between the groups of keywords, the connection was made using the AND operator.

4.2.2. Study Selection Criteria

This phase narrowed the literature pool, isolating studies not addressing the research questions. This refinement process employed the following criteria:

- When choosing the best scientific paper from a pool of research papers, the process involves critically evaluating and refining the set of papers to include only those that are most relevant, high-quality, and suitable for the specific research objectives, which is essential for establishing the criteria for including or excluding them. These criteria usually consider factors such as the following:
  - The paper is relevant to the research questions;
  - The paper is highly related to the topic;
  - Methodological rigor and validity of investigative approaches;
  - The investigation focused on scholarly works disseminated, spanning from 2011 to 2024.

  The following ensured that the papers included in this review are relevant and met a certain level of quality:
- Redundant entries and cross-database duplicates were eliminated, ensuring a unique representation of each scholarly work in the final literature pool;
- Bibliographic analysis was conducted to find additional related articles.

4.2.3. Study Selection Process

After excluding the duplicate studies, the primary studies published between 2011 and 2024 were analyzed. Table 1 illustrates the selection process through a series of filtering stages, each contributing to the progressive improvement of the body of literature. The sequential procedure comprised the following:

1. The initial phase involved querying predetermined terminological parameters to generate an initial foundational research set. We used Google Scholar to reach the research papers in famous journals. And for identifying the papers, we performed it two ways manually and using RAYYN. Over 324 original articles were reviewed

after examining several models adopted by previous researchers. In order to obtain a reasonable number of reviewed articles, over 57 articles from the ACM digital library were downloaded, 73 articles from the IEEE digital library, 64 from MDPI, 49 from ELSEVER, and 81 from Springer. A small number of articles from less popular journals were also included. The articles reviewed were refined to 183, due to the similarity observed in some researchers' models and approaches. Figure 3 illustrates the PRISMA flow diagram.

2. In step two, the study titles were analyzed, the duplicates removed, and the inclusion/exclusion criteria were applied. In total, 141 studies were excluded, due to their irrelevant titles and because they were duplicates or included outdated solutions.
3. In the third step, the resulting 98 studies were selected as their abstract and keywords complied with the selection criteria.
4. In the fourth step, following a thorough full-text analysis, 53 studies were selected for this paper.

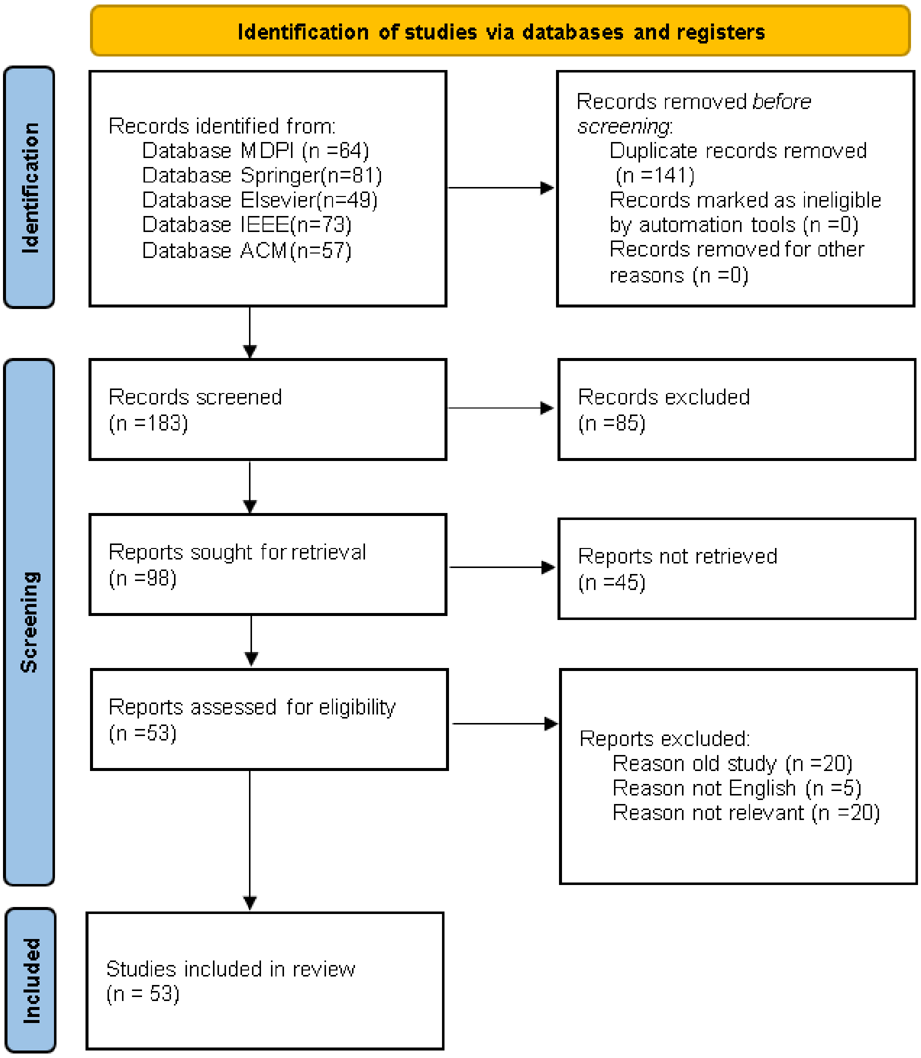
Identification of studies via databases and registers
Identification
Screening
Included
Records identified from:
Database MDPI (n =64)
Database Springer(n=81)
Database Elsevier(n=49)
Database IEEE(n=73)
Database ACM(n=57)
Records removed *before screening*:
Duplicate records removed (n =141)
Records marked as ineligible by automation tools (n =0)
Records removed for other reasons (n =0)
Records screened (n =183)
Records excluded (n =85)
Reports sought for retrieval (n =98)
Reports not retrieved (n =45)
Reports assessed for eligibility (n =53)
Reports excluded:
Reason old study (n =20)
Reason not English (n =5)
Reason not relevant (n =20)
Studies included in review (n = 53)

Figure 3. PRISMA flow diagram.

Table 1. The cumulative count of research selected at each phase.

Steps	Libraries	Total Number of Studies per Library	Total Number of Studies Selected
First: Manual Search on Libraries	MDPI	64	324
	Springer	81	
	Elsevier	49	
	IEEE	73	
	ACM	57	
Second: Analysis of Titles and Duplicate	MDPI	31	183
	Springer	47	
	Elsevier	33	
	IEEE	50	
	ACM	22	
Third: Analysis of Abstract	MDPI	19	98
	Springer	21	
	Elsevier	15	
	IEEE	31	
	ACM	12	
Fourth: Full-Text Analysis	MDPI	9	53
	Springer	11	
	Elsevier	9	
	IEEE	23	
	ACM	4	

4.3. Reporting Phase

The analytical phase comprised a triad of primary procedures:

- The definition of the dissemination strategy;
- Adherence to standardized documentation protocols in manuscript preparation;
- The assessment of the document's accuracy and academic quality is thorough and rigorous.

The culminating phase synthesized findings to elucidate the comparative impact of centralized and decentralized cloud infrastructures in medical informatics, highlighting their respective contributions to healthcare advancement.

5. Centralized Cloud Computing

Centralized cloud computing has gained prominence in contemporary information technology landscapes, due to its ability to transform the way in which organizations handle and deliver computing resources and services [17]. This model concentrates computing power, storage, and other resources in a central data center, or group of data centers. Users and organizations can configure their computing resources over the Internet, according to their needs. This centralized model offers flexibility to users and organizations alike, enabling them to streamline their operations and achieve their goals more efficiently [48]. Data centers play a crucial role in centralized cloud computing as they help businesses to save cost and to optimize resource management utilizing resources efficiently. Users can manage computing resources like virtual machines, storage, and applications directly, which is a flexible and scalable approach that can improve operational efficiency. Cloud systems can adjust resources quickly to adapt to changing demands, making it easier for organizations to respond to business requirements [49].

Several previous studies employed centralized cloud computing in their model. For instance, ref. [50] proposed a framework for analyzing big data in healthcare. A centralized cloud hosts patient information and provides healthcare services. The EHR component integrates patient records from pharmacies, hospitals, and laboratories with a data analytical component for identifying new patterns. A Care Delivery Organization (CDO) component represents healthcare organizations in various locations, sharing data using the HL7 protocol [51]. The framework employs a centralized cloud shared with different CDOs nationwide. The framework outlined in the paper leverages mobile cloud computing to enhance access to patient data and optimize system response times. By consolidating patient records in a cloud-based EHR system, healthcare providers can eliminate the need to maintain individual EMR systems, potentially reducing overall costs. However, the paper does not provide much detail on data transmission security, but it does mention the use of security measures like encryption algorithms and authentication techniques used to safeguard the inviolability and restricted access of health-related data.

Meanwhile, ref. [52] introduced a new cloud-based model for sharing medical data across healthcare units in Indonesia. The software developed can be used by various entities, like medical centers, physicians, and patients. All the patient data are stored in one centralized cloud-based EMR. By hosting the EMR application in the cloud, the system benefits from scalable resources for faster response times and dynamic resource scaling. It eliminates large upfront costs, offers a pay-per-use model, and ensures patient privacy and compliance through the use of ICD-10 [53] and HL7. protocols for secure data exchange, centralized data storage and security measures. However, the storage of patients' sensitive data in a system that utilizes Software as a Service (SaaS) technology involves security concerns.

A solution for the management of patient data in rural healthcare systems via a private cloud model was proposed in [54]. The private cloud architecture stores and accesses patient data locally within the rural healthcare organization, eliminating the need for a centralized public cloud. This reduces network latency and improves the system's response time for accessing patient records. Hosting the private cloud eliminates the need to transmit data over long distances to a remote cloud, further enhancing response time. In order to ensure data security, the system proposed has two databases, one for patient files and the other for personal identification data. Health-related information resides within secure virtual machine, integrated into the consolidated private network architecture, which delivers processing capabilities, data storage solutions, and connectivity infrastructure for health information management. However, the building and maintenance of a private cloud infrastructure can be costly, especially for rural healthcare systems operating on limited budgets. The expense associated with hardware, software, and the skilled personnel required for a system's implementation and maintenance can pose significant barriers to the adoption of private cloud solutions by rural healthcare systems.

Meanwhile, ref. [55] discussed the topic of scoliosis and its effects on patients, emphasizing the creation of a clinical data cloud system to improve pediatric patient care within the Shriners Children's Hospital system. The primary goals of the infrastructure development were to establish a consolidated data repository and enhance data interoperability. The infrastructure aims to consolidate and standardize diverse data from several locations and modalities, facilitating the retrieval and accessibility of data for clinical and research reasons. The authors employed the Fast Healthcare Interoperability Resources (FHIR) standard to include clinical data from several hospital sites [56]. This standard aims to enable fast data exchange and reduce latency in data access and retrieval. It also ensures secure data storage to protect the confidentiality of patient information. Their team engineered a SMART-on-FHIR application with a friendly graphical user interface (GUI). This platform enables the efficient retrieval of unified clinical information for users without technical expertise. The application incorporates role-based access controls to enforce selective entry protocols, restricting data visibility and interaction with the patient data. The clinical data infrastructure for pediatric patient care is efficacious for improving patient outcomes in actual clinical cases. However, creating SMART-on-FHIR apps is resource-intensive, as it involves time, money, and expertise. Moreover, patient data privacy concerns can be a barrier.

The authors of [57] highlighted the absence of automation in healthcare management systems. The paper emphasized the significance of centralized and automated healthcare systems, specifically in relation to the COVID-19 pandemic. The authors proposed a framework that collects patient details from wearable devices or testing centers and stores them in a central repository accessible to any hospital. This approach enables faster and more efficient handling of patient cases. The use of a doctors' forum in the framework enables quick decision making and treatment suggestions, improving the overall response time for patient care. Patient data are stored on the cloud as audio files to prevent unauthorized access. However, storing audio files in the cloud can be challenging, due to their larger size compared to text files. It is, therefore, essential to consider the impact on storage space to ensure seamless access to important files. Automation can decrease the necessity for manual tasks and human involvement, resulting in lower operational expenses.

Similarly, ref. [58] explored the potential of using centralized cloud computing to improve emergency healthcare services in India, proposing the use of palm vein pattern recognition to provide secure access to patient records, optimal medical accuracy, a quick admissions process, and the development of cloud-based services for the healthcare industry. This biometric authentication provides a higher level of security and privacy compared to traditional methods like smart cards or magnetic stripe cards. In their analysis, the authors compared the response times of cloud and web services to client queries, finding that the cloud demonstrated a faster response time and could handle more queries than web services. While the framework proposed was undoubtedly innovative, the reliance on palm vein pattern recognition can be an expensive technology compared with the alternatives.

In addition, ref. [59] presented a conceptual framework for a cloud-based emergency healthcare service paradigm that sought to provide a healthcare application to assist patients in emergencies. The system proposed storing individuals' medical histories in a centralized cloud database, enabling easy retrieval in an emergency. A prototype of the system proposed was implemented using fingerprint matching to obtain concise medical records in a unified document from the centralized server. The system integrates users' biometric details with unique reference numbers and employs multi-document summarization to create a single medical record. The suggested model has improved the system response time and reduced latency by centralizing patient medical data in the cloud. This enables the faster retrieval of information during emergencies. Patient data privacy is enhanced using stringent security criteria such as cryptography, multi-layered access control, and harmonized information safeguarding frameworks. The model is also cost-effective as it leverages cloud computing benefits, including pay-as-you-go pricing, shared resources, and integration with existing government identification systems. However, the implementation of the model might be challenging, due to the system's reliance on biometric data to protect sensitive patient data.

Finally, ref. [60] explored the utilization of an 'eHealth Cloud' in the healthcare sector. This cloud-based application was designed to store electronic medical records in a three-tier architecture. The application has been created with the RIA (Rich Internet program) as the client, SimpleDB cloud as the server, and a logic layer. Through offloading processor-intensive tasks to the cloud server, the burden on client devices is reduced, leading to improved overall system responsiveness. The use of REST (Representational State Transfer) interfaces between client and server tiers enables efficient data transfer and reduced latency. The logic layer, situated between the client and server, enforces rules and security measures to safeguard data privacy and control access. The government ministry manages the logic layer and enforces data privacy regulations. It integrates insurance and pharmaceuticals while protecting patient data privacy. However, it does not specify the security mechanisms and protocols for safeguarding patient data confidentiality and integrity. The SimpleDB cloud has limited data storage for the growing volume of EMR data. This causes issues that would be quickly exhausted by large EMR datasets and requires careful planning and management. The paper does not detail how the "eHealth Cloud" model addresses cost in cloud-based healthcare but mentions the cost-effectiveness of cloud computing as a key benefit.

Table 2 summarizes the previously mentioned research in relation to their strengths and limitations.

Table 2. Summary of the extant centralized cloud computing studies.

Ref	Year	Proposed Model	Strengths	Limitations
[52]	2011	Mobile cloud computing framework for secure big data analytics in healthcare systems.	• Accessible via a mobile app. • Enables faster response times. • Use healthcare standards ICD-10 and HL7. • Offers a pay-per-use model.	• Utilizes SaaS technology, which involves security concerns.
[58]	2012	Implement palm vein recognition technology to securely access patient records and improve emergency healthcare in India through cloud computing.	• Faster response time. • The cloud can quickly handle many queries. • Optimal medical accuracy. • Quick admissions process.	• Palm vein recognition is an expensive technology.
[59]	2013	A cloud-based architecture for an emergency healthcare service matches fingerprints to retrieve summarized clinical data in a single document.	• Real-time access to patient data. • Quick access to a patient's medical history during emergencies.	• Relying on biometric data to protect sensitive patient data may not be secure.
[50]	2014	Mobile cloud computing framework for secure big data analytics in healthcare systems.	• Leverages mobile cloud computing. • Enhance access to patient data. • High response times. • Utilizes big data analytics for timely, critical decision making.	• Lack of details on data transmission security
[60]	2014	The eHealth Cloud is a cloud-based application with three tiers that aims to augment conventional documentation-centric medical practices.	• REST interfaces enable efficient data transfer and reduced latency.	• Simple DB has data storage limits.
[54]	2018	The implementation of a private cloud solution for the purpose of safeguarding and overseeing patient data in rural healthcare facilities in India.	• Two databases for medical records and biometric information, providing services for managing health data and improving security for patient data.	• Private cloud is expensive for rural healthcare.
[57]	2020	A centralized and automated healthcare system, specifically regarding the COVID-19 pandemic.	• The patient's data are stored as audio files using steganography for increased security.	• Audio files require more storage and resources than text, leading to increased operational and costs.
[55]	2022	A cloud-based centralized data repository for pediatric patient care at Shriners Children's Hospital system to simplify data management.	• User-friendly interface. • FHIR enable fast data exchange and reduce latency in data access and retrieval. • Real clinical cases.	• Developing SMART on FHIR apps is expensive and time-consuming, with privacy concerns about patient data being a major issue.

6. Decentralized Cloud Computing

Decentralized cloud computing is an advanced and novel approach where computing resources are spread out over several nodes or locations instead of being concentrated in one data center [61]. This revolutionary approach offers a range of benefits that can significantly improve the performance of cloud computing systems. Decentralized cloud computing has the potential to revolutionize the cloud computing industry [62]. This new technology utilizes distributed technologies and collaborative networks to offer increased resilience, transparency, trust, and privacy in cloud services [63]. As research and development in this field advances, it is likely that innovative decentralized cloud solutions will arise that reshape how we use and benefit from cloud computing resources [64,65].

Several previous studies used decentralized cloud computing in their model. For instance, ref. [61] proposed a decentralized model for storing students' health data on a campus health information system. The model distributes information repositories to personalized student pods to help avoid the performance bottleneck of a centralized server, reduce system response time, and allow for parallel processing, improving overall system responsiveness. The model's key advantage is the decentralized storage of student data in personal pods, mitigating the possibility of significant data leaks. In using decentralized authentication and access control methods, students gain autonomous oversight of their medical information while robust safeguards maintain confidentiality and data integrity. The decentralized model can reduce IT costs by distributing the storage burden to individual student devices. This eliminates the need for a centralized server infrastructure and may also eliminate the need for a dedicated data center or cloud service. It leverages existing student devices, reducing the need for additional hardware investments. Student devices may lack the security controls and maintenance of enterprise-grade hardware, making them more vulnerable to security risks and unauthorized access, potentially compromising the confidentiality of personal health data stored in the pods.

In the meantime, ref. [66] presented the concept of a wider distributed patient health information exchange framework utilizing smartphone application technology to establish a nationwide health information exchange (NHIE) and a mobile Personal Health Record (mPHR) deployed on the mobile devices of patients for the local storage of health data, leveraging a patient's data and secure access by multiple healthcare systems. The framework utilizes mobile Personal Health Records (mPHRs) stored on the smartphones of patients for local health data storage. This enables quick access without depending on centralized servers. Special interfaces allow real-time data exchange with minimal latency between the mPHR and healthcare provider systems. The framework empowers patients to manage their health data by keeping the mPHR on their personal devices, enabling them to control data sharing with healthcare providers. This ensures better privacy and security through secure communication protocols and techniques such as encryption and authentication. The distributed nature of the framework reduces implementation and maintenance costs. It can be deployed cost-effectively by leveraging smartphones and using standardized interfaces to minimize integration costs for healthcare providers. Yet, the architecture relies on the capabilities of smartphones, which may be constrained by restrictions in storage, computing power, and battery capacity, particularly for managing large volumes of medical data, which will affect the performance of the system. It also relies on Near-Field Communication (NFC) to facilitate data transmission between end-user interfaces and peripheral hardware. However, implementing NFC data exchange can be challenging as it requires the patient's physical presence. If data are missing, the patient must return to the provider to collect it.

In contrast, ref. [67] presented MedShare, a hybrid cloud architecture developed to share medical resources among healthcare providers who operate autonomously and may be disconnected. This architecture allows for quicker data retrieval and exchange among healthcare providers, improving system response time, enhancing computational efficiency through localized data processing, and eliminating centralized information relay requirements. The private clouds of healthcare providers securely hold patient data, while only indexes and pointers are saved on the public cloud. Data sharing requires a two-way authorization process and patient consent to address privacy concerns. The MedShare system uses existing legacy EHR systems and data repositories of healthcare providers without the need for a complete infrastructure overhaul. Its hybrid cloud architecture efficiently utilizes resources, with private clouds managing data retention and computational operations of sensitive patient medical records and the public cloud handling indexing and patient information exchange services. The modular and scalable design of the MedShare system allows healthcare providers to join the network without significant upfront investments, making it a cost-effective solution. Nevertheless, performance analysis revealed computational constraints, with data retrieval processes demonstrating less-than-ideal response metrics and elevated failure rates. This was attributed to the transfer of medical information between private hospital clouds.

Meanwhile, ref. [68] introduced the retrieval and storage-based indexing framework (RSIF), designed for distributed cloud computing environments, to improve healthcare data access and concurrency. The RSIF uses a replication-free and continuous indexing approach to decrease the duration needed for simultaneously accessing and retrieving data. Utilizing deep learning techniques to classify data restrictions for augmentation and updates helps approximate the optimal indexing and ordering, further reducing retrieval time. To assess the efficacy of the RSIF, the study authors performed a comparative investigation of the method of retrieval using four distinct metrics: ICNNDLA, IPO-PAS, BAS-LS, and RSIF. The mean retrieval time and cost factor were evaluated for each metric, and an analysis of the data yielded evidence suggesting that the RSIF metric performed better than the other metrics, exhibiting the lowest average retrieval time of 0.066 s and a cost factor of 0.153. The simulation analysis conducted also showed that the framework proposed was reliable. Yet, the paper does not explicitly discuss patient data privacy mechanisms in the RSIF model. However, continuous indexing can slow down other processes, especially for large datasets like patient data, and can consume significant computing resources such as CPU, memory, and I/O.

In contrast, ref. [69] discussed how healthcare systems might integrate with distributed cloud storage and hybrid image compression. The hybrid image compression technique, combining lossless and lossy compression, helps reduce the data size and transmission bandwidth requirements, leading to faster data retrieval and transfer, which leads to improved system performance. With the suggested appliance, it underlines the importance of data compression in reducing redundancy and saving storage space and bandwidth. While hospitals employ teleradiology to diagnose X-rays remotely, the transmission of a 10 MB image using a high-speed modem during emergencies can take up to half an hour. Therefore, compression not only concerns storage costs, but also involves transmission time and the utilization of imaging apparatus. The hybrid image compression technique reduces storage requirements, leading to cost savings in cloud storage. Combining distributed cloud storage and hybrid image compression can help healthcare organizations optimize their data storage and management costs. Yet, the paper does not discuss specific mechanisms for ensuring patient data privacy in detail, such as encryption, access control, and data segregation.

The authors of [70] discussed the advantages of utilizing distributed cloud technology in mobile healthcare systems to improve data storage and organization, proposing a Distributed Data Analytics and Organization Model (DDAOM) to minimize errors and inefficiencies involved in managing large amounts of data. The model uses federated learning to perform calculations for multiple services with different input and output data assignments. This method reduces delays in storage and processing, as well as varying service provision and backlogs. By managing state maintenance through realistic learning iterations, the model ensures the smooth deployment of services, reducing latency. In federated learning, past states' memory is utilized to allocate local input from different edges Through decentralized processing paradigms, ensuring the confidentiality of health-related personal information and preventing mining in certain areas to better protect sensitive patient information. Federated learning also allows for decentralized storage and processing, eliminating the need for a centralized and expensive infrastructure. An empirical evaluation of the DDAOM demonstrated enhancements in data retention latency, analytical processing speed, service dissemination efficacy, task queue management, and resource distribution equilibrium. Specifically, it achieved 9.86% less storage delay, 10.72% less mining delay, a 10.76% higher service distribution, 9.45% fewer backlogs, and a 8.4% higher allocation ratio than the Mobility-aware Task Scheduling and Allocation Approach (MobMBAR), retrieval and storage-based indexing framework (RSIF), and Effective Training Scheme for Deep Neural Networks (ETS DNN). However, relying on federated learning and state management techniques may introduce inherent latency.

As [71] highlighted, the healthcare industry faces significant challenges in the management and processing of large amounts of data using traditional database management systems. The authors proposed a solution to manage both structured and unstructured data effectively by combining the scalability of non-relational databases (NoSQL) services with the capabilities of a Relational Database Management System (RDBMS). The RDBMS is utilized for the efficient management of structured data by offering robust querying and transaction capabilities, ensuring optimal performance for structured data operations. NoSQL databases are used to manage unstructured and semi-structured data. They are highly scalable and provide low-latency access, which is essential for handling significant quantities of health-related digital assets encompassing diagnostic imagery, auditory records, and video graphic documentation. By combining RDBMS and NoSQL, the model can achieve improved overall system response time and latency. The model uses a hybrid cloud architecture, where patient data of a sensitive nature are stored in a private cloud to provide heightened protection and management, whilst public data are maintained in a public cloud for general healthcare information. NoSQL databases offer cost savings and scalability. They can handle larger data volumes at a lower cost and with less infrastructure. However, combining RDBMS and NoSQL databases to implement a distributed storage system is complex and requires expertise in both technologies. This may increase system complexity, making maintenance and troubleshooting more challenging. The document discusses the challenges of managing large volumes of structured and unstructured data using traditional DBMS. However, it does not quantify the performance improvements achieved by the proposed hybrid RDBMS-NoSQL approach.

Meanwhile, ref. [72] highlighted the significance of secure data storage in healthcare databases hosted on decentralized cloud storage systems. The implementation of a backup proxy server for ad hoc data recovery contributes to faster data access and retrieval, as the system can quickly recover data from the proxy server if needed. The system employs robust encryption methods, such as AES-256 and Paillier encryption, to secure patient data for storage on distributed servers. Role-based access control (RBAC) and attribute-based encryption (ABE) guarantee that only authorized individuals may retrieve the encrypted patient data, preserving privacy. Data are dispersed among numerous servers, and hashing methods are used to enhance security and prevent unwanted access or tampering with the data. The backup proxy server approach offers a cost-effective solution for data recovery and redundancy. It can utilize more economical storage options compared to the primary data servers. However, introducing the backup proxy server may result in an additional step in the data access process, potentially increasing latency based on the server's location and performance. However, the creation of an RBAC system for secure data access is time-consuming, and large AES 256 encryption key sizes can slow data access, which delays efficient communication for the end users.

In [73], a community cloud architecture was designed to improve the accessibility of healthcare data. The platform allows clinicians, researchers, and data scientists to access datasets from multiple sources easily. The architecture employs a cloud-based design configuration to ensure fast processing and scalable data analytics. Cloudlets are small-scale cloud infrastructures deployed near end-users, providing low-latency access to data and applications. The architecture was intentionally designed to not store or cache any sensitive data to prevent potential attacks. Instead, the data are removed from the cloud after the termination of each remote desktop session. The architecture ensures compliance with security standards such as HIPAA and NIST [74], which are crucial for protecting sensitive patient health data's confidentiality and integrity. The secure gateway component provides a mechanism for secure data transformation and access control, ensuring that patient data are properly anonymized and access is exclusively allowed to individuals who have been approved. The use of Virtual 641 Desktop Infrastructure (VDI) and thin-client access further enhances data privacy by keeping sensitive data centralized and limiting the exposure of raw data on end-user devices. The design based on cloudlets and the VDI approach enables efficient resource utilization 644 and scalability, leading to reduced overall infrastructure and maintenance costs. However, the system utilizes a query parallelization mechanism that allows users to run multiple queries simultaneously. However, this has led to an increase in hardware costs and power 647 consumption.

Table 3 summarizes the studies discussed above, in terms of their advantages and limitations.

Table 3. Summary of the extant decentralized cloud computing studies.

Ref	Year	Proposed Model	Strengths	Limitations
[69]	2013	The architecture synthesizes decentralized data repositories with an advanced visual information processing algorithm.	• Enables the efficient storage and transmission of large medical image datasets.	• The document does not cover specific methods for ensuring the privacy of patient data
[71]	2013	An integrated data management framework for digital health platforms, leveraging both the RDBMS and NoSQL database paradigms across a decentralized infrastructure.	• Efficiently handles diverse data types. • Provides improved performance and scalability. • Optimizes storage utilization. • Improves security and privacy.	• Combining RDBMS and NoSQL is complex and requires expertise in both technologies.
[66]	2017	A decentralized ecosystem facilitating medical data interoperability, leveraging ubiquitous mobile computing platforms.	• Quick access to patient data. • Real-time data exchange with minimal latency.	• The capabilities of smartphones are limited by storage, processing power, and battery life.
[67]	2018	An innovative hybrid cloud infrastructure, termed “MedShare,” orchestrates the collaborative utilization of medical resources across autonomous healthcare entities.	• The integration and interoperability of legacy EHR systems. • MedShare is free to use and share.	• High response time and timeouts in the query-record step between private clouds.
[73]	2019	A community cloud architecture that aims to balance data accessibility and security compliance for healthcare big data applications.	• Fast processing and scalable data analytics. • Low-latency access to data.	• Query parallelization increases hardware costs and power usage.
[68]	2020	Design of a retrieval and storage-based indexing framework (RSIF) for distributed cloud computing environments.	• Low mean retrieval time.	• Continuous indexing slows down processes and consumes significant computing resources for large datasets like patient data.
[61]	2021	Decentralized personal cloud data model integrated into the Campus Health Information System (CHIS) for storing and managing student health data.	• Avoids the performance bottleneck.	• Student devices may lack security controls and maintenance, making them more vulnerable to security risks and unauthorized access. This could potentially compromise the confidentiality of personal health data stored on them.
[72]	2021	This framework seeks to enhance data integrity and confidentiality safeguards for health-related information within a distributed digital repository ecosystem.	• Quickly recover data from the proxy server.	• Large AES 256 encryption key sizes slow down data access and delay efficient end-user communication.
[70]	2023	The DDAOM is a model for efficiently managing large healthcare data in mobile cloud computing.	• Reduces storage delays. • Ensures proper service distribution. • Less backlogs.	• Using federated learning and state management techniques may result in high latency.

7. Results

The papers discussed in the previous two sections were analyzed according to this study's research questions, presented in the introduction.

7.1. RQ1: What Are the Benefits and Limitations of the Use of Centralized Cloud Computing in Healthcare That Aims to Improve HIE?

Centralized cloud computing has been developed for the healthcare sphere to improve HIE. It offers several benefits and limitations, as discussed below.

7.1.1. Benefits of the Use of Centralized Cloud Computing in Healthcare

In the healthcare industry, it is crucial to have accurate, easily accessible, and secure information. Centralized cloud computing transforms how medical data are managed, shared, and utilized [60]. This innovative approach merges vast computational resources, medical records, and applications within centralized data centers, creating an environment in which healthcare providers can use digital technologies to enhance therapeutic outcomes and operational efficiency [55]. Centralized cloud computing in healthcare centralizes patient data, streamlines access, and enables comprehensive patient care [55]. It also provides frameworks for secure data exchange, safeguarding patient information, and enabling timely decision making [59]. Centralized cloud environments promote standardized data formats, enhancing communication between healthcare systems and facilitating seamless data exchange throughout the healthcare ecosystem [75,76]. One significant benefit of centralized cloud computing is that it allows healthcare providers, practitioners, and patients to access and exchange health information anytime, anywhere [50]. This promotes fast response times for the access and retrieval of healthcare data, enhancing the accessibility and availability of patient data, facilitating better care coordination, and engendering informed decision making [57]. Moreover, by centralizing healthcare data in the cloud, different information sources and healthcare organizations can be integrated, offering a comprehensive perspective of an individual's health trajectory [60]. These integrated data enhance the continuity of care and enable healthcare providers to enhance the precision of diagnosis and treatment recommendations. Additionally, the cloud infrastructure provides scalability, enabling healthcare organizations to scale their data storage and computing resources up or down, according to their needs [52]. This approach yields economic efficiencies by minimizing spatial infrastructure demands and attenuating ongoing operational expenditures [77]. Digital infrastructure vendors deploy multilayered safeguarding protocols to ensure health information privacy and preserve data integrity. These mechanisms encompass cryptographic systems and granular access management frameworks [78].

7.1.2. Limitations of Centralized Cloud Computing in Healthcare

Centralized cloud computing for HIE relies on reliable and high-speed network connectivity. Healthcare providers can face difficulties with the access and exchange of patient data in areas with limited or unstable internet access, hindering HIE efforts [57]. Therefore, healthcare organizations must have a robust internet connection to maintain seamless access to cloud services, and to avoid latency issues and slower response times that can negatively impact the overall performance of HIE [54]. Despite rigorous protective protocols implemented by digital infrastructure vendors, vulnerabilities persist regarding the unauthorized retrieval of sensitive health information and potential compromise of data confidentiality [57]. Therefore, healthcare organizations should select trustworthy cloud providers and implement additional security measures in order to safeguard the confidentiality of patient information [79,80].

7.2. RQ2: What Are the Benefits and Limitations of the Use of Decentralized Cloud Computing in Healthcare That Aims to Improve HIE?

This section highlights the fact that while the utilization of decentralized cloud computing in healthcare can improve HIE, there are also limitations.

7.2.1. Benefits of the Use of Decentralized Cloud Computing in Healthcare

Decentralized cloud computing is a concept in which the data of healthcare can be segmented and can be stored in various servers; therefore, control, security, and privacy can be enhanced [61]. In a centralized architecture, data are generally exchanged farther from the healthcare providers, which provides the throughput and latency of the system. In addition, this strategy can facilitate healthcare companies in decentralizing processing and utilizing the cloud on demand. It allows them to adjust the extent to which they rely on centralized computing and a single cloud architecture, enabling flexibility in scaling up or down. Available horizontal scalability indicates that as an organization seeks to add more nodes to the system, it is not necessary for it to have a detrimental effect on the organization, especially in terms of resource usage [71]. It is defined by the fact that it involves the direct transfer of information from node to node, and this means that it does not allow bottlenecks like a central server [66]. In addition, due to the decentralized applications and computation, it can also be available as the decentralized data storage and optimization of the large data centers. There is a decrease in vulnerability to a single point of failure as data circulation makes health information available from various nodes of a network; even if data are acquired in one node, the data can be retrieved in another node [81].

7.2.2. Limitations of Decentralized Cloud Computing in Healthcare

In decentralized cloud computing, there is always data transferred from multiple nodes to others, and hence, HIE can be a problematic area as it has to be synchronized correspondingly across various nodes [67]. Most often, decentralized architectures are even more complex to design, implement, and manage than centralized cloud computing [66]. In decentralized cloud computing, healthcare organizations must have reliable network connectivity to ensure seamless data exchange for HIE; any network problems can hinder its effectiveness [66]. Decentralized cloud computing requires strong security measures at each node in order to safeguard patient data and ensure privacy, ensuring adherence to data protection rules across all nodes might provide difficulties, requiring careful planning and continuous monitoring [72]. Decentralized cloud computing may require a higher initial investment than a centralized approach. This is due to the setup and maintenance of multiple nodes, the assurance of their synchronization, and the management of the distributed resources, which can incur additional expenses [82].

7.3. RQ3: What Are the Differences between Centralized and Decentralized Cloud Healthcare Solutions Regarding the System's Performance (Response Times, Latency), the Privacy of Patient Data, and Cost Efficiency?

This survey examined two different cloud computing models: centralized and decentralized. The analysis of these models demonstrated that each has unique advantages and disadvantages. The healthcare industry faces challenges in deciding which model to choose, as both models impact significantly how healthcare data are stored, secured, accessed, and shared. The choice between centralized and decentralized architectures depends on various factors, including the specific requirements, scalability needs, data locality, and security considerations of the applications and services deployed. The comparison below highlights their differences in architecture, data management, system performance and latency, security and privacy of patient data, and cost efficiency.

7.3.1. Architecture

The centralized model in healthcare means that all the related information is hosted at the central server or data center. This model belongs to the client–server type of model, in which the clients are the healthcare workers and the patients who require the services of the server [52]. This model has been implemented to offer the best performance in processing healthcare information, especially within major healthcare institutions [54]. As for decentralized cloud computing, such a system can be described as a set of nodes. This type of cloud computing is configured throughout the world. This model is a peer-to-peer model where every node is both a client and a server sending and receiving data. This means that the network does not deploy a single point of control, but the entirety of nodes in the network work harmoniously in handling data. This system does not require a network control server to control and oversee the network and assets in the network [83].

7.3.2. Data Management

A centralized model is a patient database that is centrally located and controlled from one server, thus making the healthcare data organization easy. This way, data that could have been scattered across several dashboards can now be accessed by the care health provider in one single place for analysis [57]. This feature is also very useful due to its ability to chain related healthcare organizations and enable the easy sharing of information between them. This system also recaps all patients' details, physical assessments, tests, and scans comprehensively in the analysis and diagnosis helping in facilitating the correct selection of the solution at the right time and with the shortest time [50]. Despite the above benefits of the centralized healthcare systems, they have their demerits. However, the main disadvantage of the approach is the concentration of resources in one location. If the main server is damaged, when there is a failure in the servers' hardware or software or due to any other technicalities, it goes down [84]. Then, hospitals and patient care, which depend on the central IT system, lose their services, and this disrupts patients' treatment, data retrieval, and key processes [85]. However, decentralized models use a data storage technique whereby the data are stored in several nodes, which has more benefits than storing the data in a central place, such as high redundancy and fault tolerance [61]. Every node keeps a part of the data. This makes it possible for the data to be retrievable from the other nodes in case one node in the network fails; hence, this is a more secure system. On the same note, distributed data storage is not without its drawbacks regarding consistency and synchronization in the distributed network. If existing data are updated or some changes are made, then this option may involve consensus mechanisms or synchronization protocols, which can complicate the process or even add a certain amount of time to it [67].

7.3.3. System Performance and Latency

One of the most significant factors in managing patient records and diagnosing results in the healthcare sector is easy and fast access to the record. If latency is high, then it will take more time to deliver these services, which are very important in handling these cases and providing them appropriate treatment at the earliest. The centralization model means that data are collected, stored, and made easily retrievable from a central server [52]. These systems facilitate the optimal allocation of computational assets, encompassing processing capacity, memory allocation, data storage volumes, and network throughput. Aspects such as load disbursal, the organization of tasks, the scheduling of algorithms, and pattern analysis for the appropriate distribution of resources at the central server attenuate the response time [50]. However, the response time is contingent upon the client's location in relation to the centralized server. Thus, it would take a shorter duration, possibly because the client is situated near the central server. However, centralized structures may face problems related to overload in the network when many clients want to direct their requests to the central server simultaneously. In addition, the centralized models largely rely on the connectivity and availability of the network, which at times, slows down the response time [54]. On the other hand, in a decentralized cloud, the nodes are more dispersed to various regions compared to those in centralized clouds [61]. This is beneficial since the nodes can be closer to the healthcare organizations, and thus, the delivery of data is faster. Better data transmission latency enables faster data transmission whenever the nodes are placed nearer to the healthcare organizations since healthcare organizations need faster data access, quicker response time, and real-time interaction [66]. This is even more important in health, especially where quick access to data belonging to the patient or critical information that can be useful for diagnosis and treatment can make a difference. In this case, for decentralized models, the performance and the latency are dependent on the service of the network. Thus, a response should be given as soon as possible with low latency, which requires good connection quality, meaning high speed, better bandwidth, and low packet loss [72]. The clients ought to be well connected to the network through appropriate transmission means to the decentralized nodes in the healthcare organizations to avoid such delays.

7.3.4. Security and Privacy of Patient Data

Such models are classified as centralized cloud computing models in healthcare and store a vast amount of patient data in one location; they are vulnerable to cyber threats and hackers because patient data are highly valuable to hackers if compromised. In the case of an efficient breach, the unauthorized disclosure or theft of a patient's personal information can have significant adverse consequences on their lives. It is crucial to implement sufficient steps to safeguard patients' information against unauthorized access [54,58]. Decentralized cloud computing, in contrast, offers a method of storing data on several nodes or servers that are spread across different networks [61]. This approach has several advantages in relation to confidentiality and security since data fragmentation and any other methods of encryption can further the goal of keeping data away from prying eyes. In employing this technique, data are scaled down and distributed into fragments residing in different nodes so that no unlawful invader can penetrate them too easily [71]. In addition, there is encryption that implements measures to safeguard the information in case it is intercepted. It also makes the nodes more secure and private, which is ideal for processing patient-sensitive information and crucial healthcare entities.

7.3.5. Cost Efficiency

Centralized cloud computing can be beneficial to extend for healthcare organizations since it helps to avoid the investments and maintenance in on-premise infrastructure, which results in considerable expenditure [50]. Some healthcare organizations may expand the resources up or down on demand, meaning that when a healthcare organization requires more computing or storage, it can hire for it. This kind of flexibility enables healthcare organizations to only pay for the requirement of the resources needed, hence avoiding the aspect of having to purchase more resources than required, and therefore cutting down the costs [52]. However, cloud computing centralization models entail some form of data download and upload to the cloud infrastructure that may attract charges relating to the amount and type of data and the bandwidth used. Healthcare organizations should, thus, assess the costs involved in data transfer and endeavor to enhance data transmission with their associated costs. Nevertheless, in decentralized cloud computing, healthcare organizations do not have to invest a lot for infrastructure like big data centers or buy and maintain large servers for every healthcare center as the infrastructure is distributed over many nodes or servers, thus having reduced costs compared to traditional systems [66]. Consequently, in decentralized cloud computing, data can also be stored and processed near their usage locales; hence, there is less needed to move data so far. The computer communication bandwidth costs can be lower when data are to be conveyed within a dispersed network, especially when a heavy amount of traffic is required for data processing or interchange. However, decentralized cloud computing is slightly different and more advanced than the centralized cloud models; there is a need for additional technical know-how and infrastructural support, thus involving a higher cost of establishment, maintenance, and the human resources trained specifically for the job [66,72]. However, another drawback of cloud computing that may become serious when the network is expanding is that it may become rather slow, as all the applications are decentralized. The maintenance of a predictable quality can be technically disruptive, and the facility may need to spend more on the desired quality. In a decentralized environment, the acquiring and maintenance of data consistency and coordination among queryable nodes is not an easy task, and it also requires consensus, which involves additional cost and technical advancements; unused resources also demand additional costs [86].

Table 4 delineates key distinctions between centralized and decentralized cloud infrastructures within the healthcare information exchange paradigm.

Table 4. Comparison of centralized and decentralized cloud computing in context of HIE.

Comparison Criteria for HIE	Centralized Cloud Computing	Decentralized Cloud Computing
Capabilities	• Centralizes patient data in a single cloud repository. • Enables seamless data exchange and integration between healthcare providers and systems.	• Distributes patient data across multiple nodes. • Requires data exchange and synchronization across nodes to facilitate HIE.
Accessibility	• Provides fast and easy access to patient data for healthcare providers. • Enhances availability and continuity of care.	• Potential latency issues due to data transfer between nodes • Healthcare providers may need to access data from multiple nodes
Security and Privacy	• Digital infrastructure providers implement rigorous protective protocols to preserve health information integrity.	• Security and privacy measures required at each node. • Compliance with data protection regulations across all nodes can be complex.
Cost-Effectiveness	• Cost-effective through the elimination of the requirement for costly infrastructure and maintenance on the premises.	• Higher initial investment due to the setup and maintenance of multiple nodes and ensuring their synchronization.
Reliability	• Relies on stable and high-speed network connectivity to access cloud services.	• Decreased vulnerability to single point of failure, as data are available across multiple nodes.
Availability	• Provides a unified and consolidated view of patient data. • Enables comprehensive patient care and information exchange.	• Data are replicated and stored across multiple nodes, providing redundancy. • If one node is unavailable, data can be retrieved from other nodes.

As shown in Table 5 the primary differences between centralized and decentralized cloud computing is summarized.

Table 5. Comparative analysis of centralized versus decentralized cloud computing.

Centralized Cloud Computing	Decentralized Cloud Computing
Architecture	
Client–server architecture.	Peer-to-peer architecture
Data Management	
Data are stored and managed on a central server, ensuring a unified and consistent repository	Distribute data across nodes for redundancy and fault tolerance
System Performance	
Fast response time is achieved because all patient data are stored on a single central server, allowing quick access. However, this method has limitations as it relies on network speed and availability and can face network bottlenecks when multiple clients access the central server simultaneously.	All nodes are distributed across different regions, enabling healthcare organizations to be closer to the nodes to improve the speed of response time and data transfer efficiency. However, it depends on the connectivity and reliability of the network concerned.
Latency	
Higher latency for distant users.	Reduces latency by placing resources closer to users.
Security	
Security is usually centralized in the server or data center for easy management and monitoring.	Distributes encryption, access controls, and consensus algorithms across multiple nodes for data security and privacy.
Cost	
Low cost	High cost

7.4. RQ5: What Are the Research Gaps within Centralized Cloud Healthcare Solutions?

This section identifies the current research gaps in centralized cloud healthcare solutions. The first gap concerns data privacy and security. While existing research endeavors in this domain have aimed to bolster information security and fortify data confidentiality measures in centralized cloud healthcare solutions, gaps remain in ensuring robust protection against unauthorized access, data breaches, and privacy violations. Therefore, further research is required to develop advanced encryption techniques, access control mechanisms, and privacy-enhancing algorithms to enhance the security of patient data stored and processed in the cloud.

The second gap concerns the lack of coordination and integration in the exchange of data. There are still drawbacks in the interoperability and exchange of data between healthcare information systems and cloud information systems. Further, more effort needs to be placed into identifying the right correspondence for use in patient data exchange that allows the proper exchange of healthcare information across the varied systems while simultaneously preserving data consistency and semantic integration.

The third gap is associated with the opportunity to optimize performance. Centralized cloud healthcare solutions should be effective in catering to real-time applications and cited healthcare services with a large capacity and quick response time. However, new studies have to be conducted in order to increase the efficiency of supplied resources, data processing algorithms, and network topologies to exclude delays and enhance the effectiveness of the systems, especially in those applications where they are utilized, like telemedicine, remote patient monitoring, and many others.

Last of all, cost optimization and sustainability are the fourth are of a gap in the research in this field. Returning to cost optimization, this concerns healthcare centralized cloud solutions achieving sustainable results. More work must be conducted in cost models, optimization techniques, and energy-conscious computer architectures and protocols to reduce infrastructural costs, the costs of storing data, and energy usage while concurrently enhancing the system and functional ability, as well as addressing data security issues.

7.5. RQ6: What Are the Research Gaps within Decentralized Cloud Healthcare Solutions?

This section overviews the existing research gaps of decentralized cloud healthcare solutions that cause a number of unavoidable issues to make sure that such solutions will be able to scale, be interoperable, maintain privacy and security, use energy efficiently, and be integrated with real-world applications.

The first of these voids relates to the effectiveness of distributed data storage and processing tools, load-sharing methods, and resource control solutions that will be adequate for accommodating large datasets and rolling user intensities without compromising response times.

The second gap refers to the lack of interoperability between cloud healthcare systems and platforms that are decentralized and that may widely differ and use different protocols and systems. For the sharing of data and information, standardized protocols and data formats are needed, as are necessary networks, to achieve the promotion of safe and effective message transmission and data exchange between decentralized networks, while also ensuring that there is privacy of data and also integrity of the inputs fed to the system.

The third gap relates to the more significant issue of patient privacy in decentralized cloud healthcare solutions, and consequently, there is a need to work on privacy-enhancing technologies like secure multiparty computation, zero-knowledge proofs, and differential privacy. These should help to control the processing of patient data in a cooperative way without infringing the privacy of the patients and should also be efficient for a distributed system of different nodes. Fourth, basic problems such as trust and security of distributed systems need to be resolved using identity management, access control, data origin authentication, and audits of the distributed network. The positive impact of smart contract technologies is that they enhance the decentralized healthcare system’s dependability.

Other dimensions that should be discussed in the context of decentralized cloud healthcare solutions are energy efficiency and sustainability; consequently, future studies should investigate energy-conscious algorithms, resource provisioning and management, and distributed energy management mechanisms that minimize the energy consumption and, thereby, the lifecycle costs of decentralized healthcare solutions.

Also, additional extensive empirical real-world research and pilot implementations are needed to assess decentralized cloud healthcare solutions' feasibility, efficiency, and ergonomic properties. Future works include both large-scale experiments and system performance evaluations in various healthcare settings as well as more elaborate user feedback to support the confirmation of decentralization's feasibility and advantages.

8. Conclusions

This study presented an in-depth analysis of the differences between centralized and decentralized cloud computing architectures in the specific context of healthcare and HIE systems. Centralized cloud computing provides advantages, including integration, efficiency, and simplicity. It also provides quick access to data since all data are stored at a single centralized server in the cloud. However, this has the aspect of having a single point of failure and becomes a subject of data privacy/security if the central repository is an issue. On the other hand, decentralized cloud computing involves a collection of nodes and is considered more secure and private compared to centralized cloud computing by avoiding a single point of failure. However, the decentralized cloud computing architectural strategy leads to integration issues and increased operational expenses because of managing several geographically dispersed data centers. This paper also compares the pros and cons of adopting centralized or decentralized cloud computing architecture systems for the implementation of HIE systems. Centralized cloud computing is convenient and easy to use, while decentralized cloud computing ensures the security of patient's sensitive information. Healthcare organizations must consider various performance, data privacy, and security aspects, as well as cost requirements, before choosing the right cloud architecture for their HIE needs. In this regard, the analysis offers useful help to healthcare practitioners in making appropriate decisions about utilizing cloud computing technologies. Such approaches should enhance the security, efficiency, and effectiveness of the respective HIE systems, which, in turn, should lead to the enhancement of patient care coordination, as well as the outcomes. The findings provided in this analysis will also be useful for designing further research studies to improve the solutions associated with cloud-based HIE. These solutions should be designed to provide advantages similar to those of the centralized and decentralized models.

Author Contributions: Conceptualization, M.A. and S.S. (Shahenda Sarhan); methodology, M.A.; software, M.A.; validation, M.A., W.A. and S.S. (Shahenda Sarhan); formal analysis, M.A.; investigation, M.A., W.A., S.S. (Shahenda Sarhan), S.S. (Shireen Saifuddin); resources, M.A.; data curation, M.A.; writing—original draft preparation, M.A.; writing—review and editing, W.A., S.S. (Shahenda Sarhan), and S.S. (Shireen Saifuddin); visualization, M.A.; supervision, W.A., S.S. (Shahenda Sarhan) and S.S. (Shireen Saifuddin); project administration, W.A., S.S. (Shahenda Sarhan) and S.S. (Shireen Saifuddin); funding acquisition, W.A. All authors have read and agreed to the published version of the manuscript.

Funding: This Project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, under grant no. J: 76-612-1442.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy.

Acknowledgments: The authors acknowledge with thanks to DSR technical and financial support.

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

References

1. Lorkowski, J.; Pokorski, M. Medical records: A historical narrative. *Biomedicines* **2022**, *10*, 2594. [CrossRef]
2. Pai, M.M.; Ganiga, R.; Pai, R.M.; Sinha, R.K. Standard electronic health record (EHR) framework for Indian healthcare system. *Health Serv. Outcomes Res. Methodol.* **2021**, *21*, 339–362. [CrossRef]
3. Tertulino, R.; Antunes, N.; Morais, H. Privacy in electronic health records: A systematic mapping study. *J. Public Health* **2024**, *32*, 435–454. [CrossRef]
4. Ayaad, O.; Alloubani, A.; ALhajaa, E.A.; Farhan, M.; Abuseif, S.; Al Hroub, A.; Akhu-Zaheya, L. The role of electronic medical records in improving the quality of health care services: Comparative study. *Int. J. Med. Inform.* **2019**, *127*, 63–67. [CrossRef]
5. Sadoughi, F.; Nasiri, S.; Ahmadi, H. The impact of health information exchange on healthcare quality and cost-effectiveness: A systematic literature review. *Comput. Methods Programs Biomed.* **2018**, *161*, 209–232. [CrossRef]
6. Hettige, B.; Wang, W.; Li, Y.F.; Le, S.; Buntine, W. MedGraph: Structural and temporal representation learning of electronic medical records. In *ECAI 2020*; IOS Press: Amsterdam, The Netherlands, 2020; pp. 1810–1817.
7. Alsahafi, Y. Understanding Healthcare Consumers Intention to Use the Integrated Electronic Personal Health Record System in Saudi Arabia. Ph.D. Thesis, University of Technology Sydney, Ultimo, NSW, Australia, 2021.
8. Zhuang, Y.; Sheets, L.R.; Chen, Y.W.; Shae, Z.Y.; Tsai, J.J.; Shyu, C.R. A patient-centric health information exchange framework using blockchain technology. *IEEE J. Biomed. Health Inform.* **2020**, *24*, 2169–2176. [CrossRef]
9. Anshari, M. Redefining electronic health records (EHR) and electronic medical records (EMR) to promote patient empowerment. *Int. J. Inform. Dev.* **2019**, *8*, 35–39. [CrossRef]
10. Osei-Tutu, K.; Song, Y.T. Enterprise Architecture for Healthcare Information Exchange (HIE) Cloud Migration. In Proceedings of the 2020 14th International Conference on Ubiquitous Information Management and Communication (IMCOM), Taichung, Taiwan, 3–5 January 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–8.
11. Pai, D.R.; Rajan, B.; Chakraborty, S. Do EHR and HIE deliver on their promise? Analysis of Pennsylvania acute care hospitals. *Int. J. Prod. Econ.* **2022**, *245*, 108398. [CrossRef]
12. Argaw, S.T.; Troncoso-Pastoriza, J.R.; Lacey, D.; Florin, M.V.; Calcavecchia, F.; Anderson, D.; Burleson, W.; Vogel, J.M.; O'Leary, C.; Eshaya-Chauvin, B.; et al. Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Med. Inform. Decis. Mak.* **2020**, *20*, 146. [CrossRef]
13. Karacic Zanetti, J.; Nunes, R. To Wallet or Not to Wallet: The Debate over Digital Health Information Storage. *Computers* **2023**, *12*, 114. [CrossRef]
14. Chenthara, S.; Ahmed, K.; Wang, H.; Whittaker, F. Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE Access* **2019**, *7*, 74361–74382. [CrossRef]
15. Sivan, R.; Zukarnain, Z.A. Security and privacy in cloud-based e-health system. *Symmetry* **2021**, *13*, 742. [CrossRef]
16. Koutsoukos, K.; Symvoulidis, C.; Kiourtis, A.; Mavrogiorgou, A.; Dimopoulou, S.; Kyriazis, D. Emergency Health Protocols Supporting Health Data Exchange, Cloud Storage, and Indexing. In Proceedings of the 15th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2022), Online, 9–11 February 2022; Volume 5: HEALTHINF, pp. 597–604.
17. Sriram, G. Edge computing vs. Cloud computing: An overview of big data challenges and opportunities for large enterprises. *Int. Res. J. Mod. Eng. Technol. Sci.* **2022**, *4*, 1331–1337.
18. Premarathne, U.; Abuadbba, A.; Alabdulatif, A.; Khalil, I.; Tari, Z.; Zomaya, A.; Buyya, R. Hybrid cryptographic access control for cloud-based EHR systems. *IEEE Cloud Comput.* **2016**, *3*, 58–64. [CrossRef]
19. Spanakis, E.G.; Sfakianakis, S.; Bonomi, S.; Ciccotelli, C.; Magalini, S.; Sakkalis, V. Emerging and established trends to support secure Health Information Exchange. *Front. Digit. Health* **2021**, *3*, 636082. [CrossRef]
20. Symvoulidis, C.; Mavrogiorgou, A.; Kiourtis, A.; Marinos, G.; Kyriazis, D. Facilitating health information exchange in medical emergencies. In Proceedings of the 2021 International Conference on e-Health and Bioengineering (EHB), Iasi, Romania, 18–19 November 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–4.
21. Campelo, R.; Casanova, M.; Guedes, D.; Laender, A.H. A brief survey on replica consistency in cloud environments. *J. Internet Serv. Appl.* **2020**, *11*, 2020. [CrossRef]
22. Wu, D.C.; Lin, H.L.; Cheng, C.G.; Yu, C.P.; Cheng, C.A. Improvement the Healthcare Quality of Emergency Department after the Cloud-Based System of Medical Information-Exchange Implementation. *Healthcare* **2021**, *9*, 1032. [CrossRef]
23. Al-Marsy, A.; Chaudhary, P.; Rodger, J.A. A model for examining challenges and opportunities in use of cloud computing for health information systems. *Appl. Syst. Innov.* **2021**, *4*, 15. [CrossRef]
24. Sarkar, I.N. Health Information Exchange as a Global Utility. *Chest* **2023**, *163*, 1023–1025. [CrossRef]
25. Andreas, A.; Mavromoustakis, C.X.; Mastorakis, G.; Do, D.T.; Batalla, J.M.; Pallis, E.; Markakis, E.K. Towards an optimized security approach to IoT devices with confidential healthcare data exchange. *Multimed. Tools Appl.* **2021**, *80*, 31435–31449. [CrossRef]
26. Sa, I.P.; Mb, V.P. Secure ehealth cloud framework for patients' EHR storage and sharing for Indian Government healthcare model. *Proc. Est. Acad. Sci.* **2020**, *69*, 266–276.
27. Payne, T.H.; Lovis, C.; Gutteridge, C.; Pagliari, C.; Natarajan, S.; Yong, C.; Zhao, L.P. Status of health information exchange: A comparison of six countries. *J. Glob. Health* **2019**, *9*, 020427. [CrossRef] [PubMed]

28. Eze, B.; Kuziemsky, C.; Peyton, L. A configurable identity matching algorithm for community care management. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *11*, 1007–1020. [CrossRef]
29. Gkika, E.C.; Anagnostopoulos, T.; Ntanos, S.; Kyriakopoulos, G.L. User preferences on cloud computing and open innovation: A case study for university employees in Greece. *J. Open Innov. Technol. Mark. Complex.* **2020**, *6*, 41. [CrossRef]
30. Sunyaev, A.; Sunyaev, A. Cloud computing. In *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 195–236.
31. Gourisaria, M.K.; Samanta, A.; Saha, A.; Patra, S.S.; Khilar, P.M. An extensive review on cloud computing. In *Data Engineering and Communication Technology: Proceedings of 3rd ICDECT-2K19*; Springer: Singapore, 2020; pp. 53–78.
32. Raj, R.; Choudhary, S.P. Cloud Computing for Medical Application and Health Care. *Int. Res. J. Eng. Technol.* **2022**, *9*, 541–546.
33. Breitgand, D.; Glikson, A. Global enterprise cloud transformation: Centralize, distribute or federate? In Proceedings of the 2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013), Ghent, Belgium, 27–31 May 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 892–895.
34. Benkhelifa, E.; Hani, A.B.; Welsh, T.; Mthunzi, S.; Guegan, C.G. Virtual environments testing as a cloud service: A methodology for protecting and securing virtual infrastructures. *IEEE Access* **2019**, *7*, 108660–108676. [CrossRef]
35. Azumah, K.K.; Maciel, P.R.M.; Sørensen, L.T.; Kosta, S. Modeling and simulating a process mining-influenced load-balancer for the hybrid cloud. *IEEE Trans. Cloud Comput.* **2022**, *11*, 1999–2010. [CrossRef]
36. Souravlas, S.; Anastasiadou, S.D. On Implementing Social Community Clouds Based on Markov Models. *IEEE Trans. Comput. Soc. Syst.* **2022**, *11*, 89–100. [CrossRef]
37. Kumar, S.; Goudar, R. Cloud computing-research issues, challenges, architecture, platforms and applications: A survey. *Int. J. Future Comput. Commun.* **2012**, *1*, 356. [CrossRef]
38. Mathur, P.; Nishchal, N. Cloud computing: New challenge to the entire computer industry. In Proceedings of the 2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010), Solan, India, 28–30 October 2010; IEEE: Piscataway, NJ, USA, 2010; pp. 223–228.
39. Jadeja, Y.; Modi, K. Cloud computing-concepts, architecture and challenges. In Proceedings of the 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), Nagercoil, India, 21–22 March 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 877–880.
40. Jawed, M.S.; Sajid, M. A comprehensive survey on cloud computing: Architecture, tools, technologies, and open issues. *Int. J. Cloud Appl. Comput.* **2022**, *12*, 1–33. [CrossRef]
41. Sachdeva, S.; Bhatia, S.; Harrasi, A.A.; Shah, Y.A.; Anwer, K.J.; Philip, A.K.; Shah, S.F.A.; Khan, A.; Halim, S.A. Unraveling the role of cloud computing in health care system and biomedical sciences. *Heliyon* **2024**, *10*, e29044. [CrossRef] [PubMed]
42. Masud, M.; Gaba, G.S.; Choudhary, K.; Alroobaea, R.; Hossain, M.S. A robust and lightweight secure access scheme for cloud based E-healthcare services. *Peer-Peer Netw. Appl.* **2021**, *14*, 3043–3057. [CrossRef]
43. Reid, G.A. Improving HIPAA Compliance Efforts with Modern Cloud Technologies. Ph.D. Thesis, Capitol Technology University, Laurel, MD, USA, 2021.
44. Lee, T.F.; Chang, I.P.; Su, G.J. Compliance with hipaa and gdpr in certificateless-based authenticated key agreement using extended chaotic maps. *Electronics* **2023**, *12*, 1108. [CrossRef]
45. Aceto, G.; Persico, V.; Pescapé, A. Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0. *J. Ind. Inf. Integr.* **2020**, *18*, 100129. [CrossRef]
46. Kumar, P. Literature Based Study on Cloud Computing for Health and Sustainability in View of COVID-19. Core. Ac. Uk. 2020. Available online: https://core.ac.uk/download/pdf/327105038.pdf (accessed on 5 August 2024)
47. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; EBSE Technical Report, Ver. 2.3; Department of Computer Science, Keele University: Durham, UK, 2007.
48. Ahmad, M.O.; Khan, R.Z. The cloud computing: A systematic review. *Int. J. Innov. Res. Comput. Commun. Eng.* **2015**, *3*, 4060–4075.
49. Feuerlicht, G.; Govardhan, S. Impact of cloud computing: Beyond a technology trend. *Syst. Integr.* **2010**, *2*, 262–269.
50. Youssef, A.E. A framework for secure healthcare systems based on big data analytics in mobile cloud computing environments. *Int. J. Ambient. Syst. Appl.* **2014**, *2*, 1–11. [CrossRef]
51. Thiess, H.; Fiol, G.D.; Malone, D.C.; Cornia, R.; Sibilla, M.; Rhodes, B.; Boyce, R.D.; Kawamoto, K.; Reese, T.J. Coordinated use of Health Level 7 standards to support clinical decision support: Case study with shared decision making and drug-drug interactions. *Int. J. Med. Inform.* **2022**, *162*, 104749. [CrossRef]
52. Pardamean, B.; Rumanda, R.R. Integrated model of cloud-based E-medical record for health care organizations. In Proceedings of the 10th WSEAS International Conference on e-Activities, Island of Java, Indonesia, 1–3 December 2011; pp. 157–162.
53. Almagro, M.; Unanue, R.M.; Fresno, V.; Montalvo, S. ICD-10 Coding of Spanish Electronic Discharge Summaries: An Extreme Classification Problem. *IEEE Access* **2020**, *8*, 100073–100083. [CrossRef]
54. Ganiga, R.; Pai, R.M.; MM, M.P.; Sinha, R.K. Private cloud solution for securing and managing patient data in rural healthcare system. *Procedia Comput. Sci.* **2018**, *135*, 688–699. [CrossRef]
55. Hornback, A.; Shi, W.; Giuste, F.O.; Zhu, Y.; Carpenter, A.M.; Hilton, C.; Bijanki, V.N.; Stahl, H.; Gottesman, G.S.; Purnell, C.; et al. Development of a generalizable multi-site and multi-modality clinical data cloud infrastructure for pediatric patient care. In Proceedings of the 13th ACM International Conference on Bioinformatics, Computational Biology and Health Informatics, New York, NY, USA, 7–10 August 2022; pp. 1–10.

56. Duda, S.N.; Kennedy, N.; Conway, D.; Cheng, A.C.; Nguyen, V.; Zayas-Cabán, T.; Harris, P.A. HL7 FHIR-based tools and initiatives to support clinical research: A scoping review. *J. Am. Med. Inform. Assoc.* **2022**, *29*, 1642–1653. [CrossRef] [PubMed]
57. Moorthy, R.; Udupa, S.; Bhagavath, S.A.; Rao, V. Centralized and automated healthcare systems: A essential smart application post COVID-19. In Proceedings of the 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 3–5 December 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 131–138.
58. Karthikeyan, N.; Sukanesh, R. Cloud based emergency health care information service in India. *J. Med. Syst.* **2012**, *36*, 4031–4036. [CrossRef] [PubMed]
59. Banerjee, A.; Agrawal, P.; Rajkumar, R. Design of a cloud based emergency healthcare service model. *Int. J. Appl. Eng. Res.* **2013**, *8*, 2261–2264.
60. Biswas, S.; Akhter, T.; Kaiser, M.; Mamun, S. Cloud based healthcare application architecture and electronic medical record mining: An integrated approach to improve healthcare system. In Proceedings of the 2014 17th International Conference on Computer and Information Technology (ICCIT), Dhaka, Bangladesh, 22–23 December 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 286–291.
61. Weng, X.; Wu, H.; Pan, Y.; Chen, H. Decentralized Personal Cloud Data Model and its Application in Campus Health Information System. In Proceedings of the 2021 IEEE International Conference on Dependable, Autonomic and Secure Computing, IEEE International Conference on Pervasive Intelligence and Computing, IEEE International Conference on Cloud and Big Data Computing, IEEE International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Calgary, AB, Canada, 25–28 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 879–883.
62. Pires, A.; Simão, J.; Veiga, L. Distributed and decentralized orchestration of containers on edge clouds. *J. Grid Comput.* **2021**, *19*, 36. [CrossRef]
63. Wang, X.; Liu, X.; Fan, L.; Jia, X. A decentralized virtual machine migration approach of data centers for cloud computing. *Math. Probl. Eng.* **2013**, *2013*, 878542. [CrossRef]
64. Ferrer, A.J.; Marquès, J.M.; Jorba, J. Towards the decentralised cloud: Survey on approaches and challenges for mobile, ad hoc, and edge computing. *ACM Comput. Surv. (CSUR)* **2019**, *51*, 1–36. [CrossRef]
65. Pavani, V.; Narayana, V.L. Multi-level authentication scheme for improving privacy and security of data in decentralized cloud server. In Proceedings of the 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 7–9 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 391–394.
66. Abdulnabi, M.; Al-Haiqi, A.; Kiah, M.L.M.; Zaidan, A.; Zaidan, B.; Hussain, M. A distributed framework for health information exchange using smartphone technologies. *J. Biomed. Inform.* **2017**, *69*, 230–250. [CrossRef] [PubMed]
67. Yang, Y.; Li, X.; Qamar, N.; Liu, P.; Ke, W.; Shen, B.; Liu, Z. Medshare: A novel hybrid cloud for medical resource sharing among autonomous healthcare providers. *IEEE Access* **2018**, *6*, 46949–46961. [CrossRef]
68. Yan, S.; He, L.; Seo, J.; Lin, M. Concurrent healthcare data processing and storage framework using deep-learning in distributed cloud computing environment. *IEEE Trans. Ind. Inform.* **2020**, *17*, 2794–2801. [CrossRef]
69. Hussein, S.; Badr, S. Healthcare Cloud integration using distributed Cloud storage and hybrid image compression. *Int. J. Comput. Appl.* **2013**, *80*, 9–15.
70. Dhote, S.; Baskar, S.; Shakeel, P.M.; Dhote, T. Cloud computing assisted mobile healthcare systems using distributed data analytic model. *IEEE Trans. Big Data* **2023**, 1–12. [CrossRef]
71. Weider, D.Y.; Kollipara, M.; Penmetsa, R.; Elliadka, S. A distributed storage solution for cloud based e-Healthcare Information System. In Proceedings of the 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013), Lisbon, Portugal, 9–12 October 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 476–480.
72. Pokharkar, S.T.; Vishwamitra, L. Securing data in decentralized cloud storage for authorized encrypted search with privacy-preserving on healthcare databases. In Proceedings of the 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, India, 18–19 June 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 755–760.
73. Valluripally, S.; Raju, M.; Calyam, P.; Chisholm, M.; Sivarathri, S.S.; Mosa, A.; Joshi, T. Community cloud architecture to improve use accessibility with security compliance in health big data applications. In Proceedings of the 20th International Conference on Distributed Computing and Networking, Bangalore, India, 4–7 January 2019; pp. 377–380.
74. Choquette, S.J.; Duewer, D.L.; Sharpless, K.E. NIST Reference Materials: Utility and Future. *Annu. Rev. Anal. Chem.* **2020**, *13*, 453–474. [CrossRef]
75. Sharma, D.K.; Boddu, R.S.K.; Bhasin, N.K.; Nisha, S.S.; Jain, V.; Mohiddin, M.K. Cloud computing in medicine: Current trends and possibilities. In Proceedings of the 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), Coimbatore, India, 8–9 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–5.
76. Al-Issa, Y.; Ottom, M.A.; Tamrawi, A. eHealth cloud security challenges: A survey. *J. Healthc. Eng.* **2019**, *2019*, 7516035. [CrossRef] [PubMed]
77. Ahmadi, M.; Aslani, N. Capabilities and advantages of cloud computing in the implementation of electronic health record. *Acta Inform. Medica* **2018**, *26*, 24. [CrossRef]
78. Javaid, M.; Haleem, A.; Singh, R.P.; Rab, S.; Suman, R.; Khan, I.H. Evolutionary trends in progressive cloud computing based healthcare: Ideas, enablers, and barriers. *Int. J. Cogn. Comput. Eng.* **2022**, *3*, 124–135. [CrossRef]

79. 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]
80. Dang, L.M.; Piran, M.J.; Han, D.; Min, K.; Moon, H. A survey on internet of things and cloud computing for healthcare. *Electronics* **2019**, *8*, 768. [CrossRef]
81. Liang, P.; Zhang, L.; Kang, L.; Ren, J. Privacy-preserving decentralized ABE for secure sharing of personal health records in cloud storage. *J. Inf. Secur. Appl.* **2019**, *47*, 258–266. [CrossRef]
82. Atieh, A.T. The next generation cloud technologies: A review on distributed cloud, fog and edge computing and their opportunities and challenges. *ResearchBerg Rev. Sci. Technol.* **2021**, *1*, 1–15.
83. Alamouti, S.M.; Arjomandi, F.; Burger, M. Hybrid edge cloud: A pragmatic approach for decentralized cloud computing. *IEEE Commun. Mag.* **2022**, *60*, 16–29. [CrossRef]
84. Rimal, B.P.; Van, D.P.; Maier, M. Mobile-edge computing versus centralized cloud computing over a converged FiWi access network. *IEEE Trans. Netw. Serv. Manag.* **2017**, *14*, 498–513. [CrossRef]
85. Agapito, G.; Cannataro, M. An overview on the challenges and limitations using cloud computing in healthcare corporations. *Big Data Cogn. Comput.* **2023**, *7*, 68. [CrossRef]
86. Ramanan, P.; Yildirim, M.; Gebraeel, N.; Chow, E. Large-scale maintenance and unit commitment: A decentralized subgradient approach. *IEEE Trans. Power Syst.* **2021**, *37*, 237–248. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.