The rapid development of the Internet of Medical Things (IoMT) technology has resulted in various advances in the smart healthcare field; it improves healthcare systems to offer more complicated real-time services and provides an efficient patient motioning system. However, despite the brilliant side of IoMT, several concerns continue to undercut its adoption. In fact, collecting, transmitting, storing, and using data in IoMT applications raises issues regarding privacy and data protection, especially with the multitude of stakeholders involved during the whole data life cycle. Motivated from these facts, this article is devoted to perform a Systematic Literature Review (SLR) of privacy-preserving solutions used in the smart healthcare ecosystem. The recent research papers disseminated between 2017 and 2021 are selected from multiple databases and a standardized SLR method is conducted. A total of 100 papers were reviewed and a critical analysis was conducted on the selected papers. Moreover, this review study attempts to highlight the limitation of the current approaches and aims to find possible solutions to them. Thus, a detailed analysis was carried out on the selected papers in terms of the privacy techniques they deployed, the data life cycle phase they addressed, the stakeholders needs they met, and the privacy principles they covered according to privacy laws and regulations. Finally, we summarize our results showing privacy-preserving trends and identifying recommendations to involve privacy principles coverage in smart healthcare applications.

1. Introduction

In recent years, smart healthcare is one of the fastest-growing technologies that provide an opportunity for accurate and efficient prevention of several diseases. The Internet of Medical Things (IoMT) is a connected infrastructure of medical devices, health systems, and services. The IoMT [1] enables the connection, communication, capture, and exchange of Electronic Medical Records (EMR) between entities. The EMR includes sensitive health data, whereas the implementation of any Internet of Things Technology usually comes with various concerns about privacy and data protection. When it comes to patient privacy, the things to consider are even more. Hence, data security and privacy issues have become the biggest concerns of people in smart healthcare field. For example, a patient usually expects that his or her EMRs, such as blood pressure and pulse rate, can only be accessed by authorized professional health caregivers and with his or her consent and control.

Recently, several researchers have shown interest in security and privacy preservation in a smart healthcare environment. Yet, understanding the current security and privacy issues of the IoMT system is essential. Moreover, it is significant to know the effectiveness of the offered solutions. We found that little attention has been paid in the literature to elaborate on these issues. Therefore, in this work, a Systematic Literature Review (SLR) [2] is presented.

1.1. Scope. Recently, Many surveys have been conducted which highlighted the privacy-preserving issues in healthcare environments. Most of these surveys have given an
insight into the privacy issues and their solutions in different areas of the healthcare field. In the proposed survey, we have given a comprehensive overview of different privacy-preserving approaches in the smart healthcare ecosystem which use many smart technologies (Cloud Computing, Fog Computing, Internet of Things, and telehealthcare technologies) to share data between various stakeholders. To this end, the current systematic literature review is intended to address privacy-preserving solutions in IoMT considering different needs of stakeholders, the whole data life cycle, and limitations in terms of privacy criteria coverage view.

One of the most recent survey papers of privacy-preserving in healthcare environments was performed by Hameed et al. [3]. In this paper, the authors highlighted a systematic literature review around the IoMT security and privacy issues and how machine learning techniques are applied to solve these problems.

Within the scope of another study, performed by Tanriverdi [4], blockchain-based studies on the preservation of medical data sharing privacy were analyzed. In this study, information about the research publications in the literature and possible issues that can be examined in the future were discussed. In another study, Iwaya et al. [5] reviewed, analyzed, and synthesized the related literature on the security and privacy of m/uHealth systems using an evidence-based software engineering methodology, a Systematic Mapping Study (SMS).

Another exhaustive survey on security and privacy issues in Healthcare 4.0 was carried out by Hathaliya and Tanwar [6]. The authors explored the blockchain-based solution to give insights to researcher communities. The technology used, the problem formulation, the parameters to handle the security, and privacy issues were implemented in a comparative analysis of the existing survey on security and privacy in Healthcare 4.0.

A review of security and privacy in the medical Internet of things was conducted by Sun et al. [7]. The authors surveyed the existing solutions for security and privacy in the IoMT; the proposed solutions are focusing on data encryption, access control, trusted third party auditing, data search, and data anonymization. It had also highlighted the future challenges of security and privacy in IoMT.

1.2. Motivation. The motivation of this paper was as follows:

(i) Importance of privacy preserving in the smart healthcare field is one of the key criteria to explore this area.

(ii) The existing literature mainly discussed some privacy aspects of smart healthcare such as technical aspects; IoT-based and machine learning–based solutions. Many other emerging areas of privacy in smart healthcare, such as compliance with privacy laws, in accordance with patient’s preferences and privacy preserving in the whole data life cycle were not explored to their full potential. So, there is a need to write a survey that considers the integration of all these aspects as mentioned above.

(iii) This systematic literature review is intended for new researchers in the field, and for those who are keen to know about recent advances and limitations of privacy-preserving in a smart healthcare environment. In addition, this kind of study enables the identification of research trends, raising the most discussed aspects and open issues, indicating possibilities of research in less discussed aspects.

1.3. Contributions. In this paper, we make the following contributions:

(i) We discuss the background and the importance of privacy in smart healthcare.

(ii) We identify several aspects that should be considered while treating privacy issues on smart healthcare systems.

(iii) We identify 3425 primary studies that present privacy-preserving solutions in the smart healthcare sector.

(iv) We further select 100 primary studies that meet the inclusion and exclusion criteria we set for the paper screening phase.

(v) We conduct an in-depth assessment through a critical analysis of the 100 selected papers and present the research ideas, techniques, and the adopted aspects and considerations in the field of privacy in IoMT.

(vi) We make different combinations of the prespecified privacy aspects in the form of bubble charts to conclude the state of privacy principles coverage and security requirement fulfillment by the primary studies.

(vii) Finally, we summarize the lessons learned from this SLR and identify the recommendations that lead toward a holistic approach to preserve privacy in smart healthcare applications.

1.4. Organization of the Paper. The remainder of the paper is structured as follows: Section 2 presents a general background about IoMT, state of art, and terminologies of privacy in smart healthcare. Section 3 describes the methodology with which the primary studies were systematically selected for analysis. The findings of all the primary studies selected are presented in section 4, followed by the discussion of the results in Section 5. Section 6 presents recommendations to upgrade toward a holistic approach to preserve privacy. Section 7 concludes the paper and presents some future research directions.

2. Background

In this section, we present background knowledge about privacy, security, and smart healthcare, by defining each concept, and presenting the existing privacy-preserving techniques, laws, and criteria; we also provide an overview of
smart healthcare, and the existing IoMT categories and architectures.

2.1. Privacy Definitions and Techniques

2.1.1. Definitions: Privacy VS. Security. Privacy and security are two different concepts, yet they are frequently misunderstood or conflated by the concerned users and organizations while dealing with Internet services and personal data. Thus, it is mandatory to rectify the meaning of each and discuss their differences.

Privacy is related to the right to have control over information, identity, and activity of oneself, and take part in data processing decisions, such as disclosure, retention, and erasure, whilst security is related to how the data is protected, and the measures to follow against the different threats.

In other words and according to Ref. [8], the difference between security and privacy can be represented as: “Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction so that the confidentiality, integrity, and availability of information are maintained. In contrast, privacy ensures that user’s data are stored, used and disclosed fairly according to the data owner’s preferences.”

2.1.2. Privacy-Preserving Techniques. Not any privacy-preserving techniques are suitable for all sorts of applications [9]; Herein, we present a few techniques that are effectively used to preserve privacy in the smart healthcare sector:

(i) **Access Control**: The intent behind these techniques is to restrict access to only authorized parties [10]. Its mechanisms can take many forms depending on the adopted approach while granting permissions; assigning permissions based on roles designated as Role-Based Access Control (RBAC), and based on attributes designated as Attribute-Based Access Control (ABAC).

(ii) **Cryptography**: Various cryptographic techniques are being applied in order to preserve privacy, They can be classified into three main collections: Secret Key Cryptography (SKC) which uses the same key for encryption and decryption, i.e., DES, Public Key Cryptography (PKC), a system in which two different keys are used, i.e., RSA, Hash Function, which is an irreversible function that generates an output data with fixed size from an unfixed input size [11].

(iii) **Anonymization**: This technique is commonly performed before the distribution and analysis processes with the aim of data sanitization, also known as de-identification [11]; it makes the data less precise and hides the identity of patients.

(iv) **Blockchain**: Recently, blockchain has extended beyond the financial sector and has become a trending solution for decentralization, and privacy issues in the smart healthcare domain, due to its numerous features [12], namely, Decentralization; Transparency; Open-source; Autonomy; Immutability; and Anonymity.

2.1.3. Data Access Management. The use of smart health has become the key source of data breaches since medical data are more sensitive than the other types. The 2021 Mid-Year Data Breach Quick View Report published by Risk-Based Security affirmed that 238 healthcare data breaches were reported in the first 6 months of 2021, which makes the healthcare sector in the top position as the most breached economic sector [13] (Figure 1); moreover, “Hacking” or Unauthorized Access is considered the number one breach type (Figure 2), which points to the importance of data access management.

Many techniques are being used for this purpose, including the aforementioned techniques, Access Control and Cryptography; authentication process is also used as a solution to provide secure access to the medical data.

With the emergence of blockchain, new technologies are added to this block, namely, permissioned blockchain and smart contracts. Permissioned blockchain requires an access control layer, which makes it provide an additional level of security over the typical blockchain, while smart contracts are being applied to manage the permissions to a patient’s HER [14].

2.2. Smart Healthcare Overview. In our SLR, we are interested in privacy-preserving solutions, particularly in the smart healthcare sector. With that being said, in this section, we will clarify the status of this sector in the field of health as a whole, and its different actors.

2.2.1. Electronic Health (e-Health). E-health is an emerging field at the intersection of classical health, and Information and Communication Technologies (ICT), for instance, the use of Electronic Health Records (EHR) or databases that store medical information of patients.

Nevertheless, an article published in the Journal of Medical Internet Research [15] claims that the definition of e-health has a broader sense, as the “e” does not simply mean electronic, but implies several other “e’s,” which combine to provide a full definition of e-health; these “10 e’s,” are the following: Efficiency, Enhancing Quality, Evidence-Based, Empowerment, Encouragement, Education, Enabling, Extending, Ethics, and Equity.

2.2.2. Mobile Health (m-Health). More recently the emergence of smartphones has led to their recognition as a great help in the healthcare sector, hence the emergence of mobile healthcare. Known as m-health.

M-health is a subsection of e-health and defined by The World Health Organization (WHO) in collaboration with the Global Observatory for eHealth as “medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices” [16]. M-health
applications facilitate the communication between patients and caregivers. Moreover, they allow remote and real-time monitoring.

2.2.3. Smart Health (s-Health). The abiding progression of ICT has led to a new concept named context-aware environments, such as smart homes and smart cities, which are built with high sensing, analyzing, and decision-making capabilities. The implementation of these context-aware environments along with both e-health and m-health has engendered the term smart health (or s-health).

2.2.4. S-Health VS. m-Health. S-health and m-health are distinct in terms of the underlying infrastructure. Ref. [17] stated that “the concept of s-health could be considered an augmentation of m-health with the sensing capabilities of smart cities,” and summarizes the differences in two points; differences in information sources as the data may come from different sources not only from patients which exceed m-health, and differences in information flows as the collected data may be processed by several parties, hence it is beyond the user-centric approach and beyond m-health.

2.2.5. Key Stakeholders of s-Health. To ensure full coverage of privacy in s-health, it is mandatory to define the different actors as well as the needs of each of them:

(i) Patients: are the data owners; therefore, they have the complete right to take control over their data, in terms of access, modification, retention, erasure, disclosure... In other words, the patients’ preferences must be considered by the smart healthcare systems.

(ii) Services providers: are the actors who provide smart healthcare and well-being services, such as doctors, service developers, and cloud providers.

(iii) Governmental bodies: are either the organizations that define privacy regulations and laws, such as the European Data Protection Law, or the organizations that supervise the legitimacy of data processing in the smart healthcare sector.

To summarize, a solution that preserves privacy in a way that satisfies the various stakeholders’ needs is a solution that respects both the patient’s preferences and the service provider’s privacy policy, while complying with the privacy laws and regulations.

2.3. IoMT: Data Life Cycle, Categories, and Architectures

2.3.1. Data Life Cycle. Wireless body area networks (WBAN) [18] and IoMT collect data streams such as heart rate, blood pressure, ECG from sensors, actuators, which are then transmitted to different units, i.e., mobile devices, hospital data centers, etc. These data streams are then stored in cloud servers, databases, ready for any further processing or use. That being said, the data life cycle can be assembled in 4 global stages, namely, collection, transmission, storage, and process.

In our SLR, we are targeting IoMT data protection and patient’s privacy-preserving solutions in s-health, and since privacy must be protected in each data phase, we are joining the data life cycle to the adopted aspects to assess the proposed studies.
2.3.2. Categories of IoMT. Different categories of IoMT are being adopted by the privacy-preserving solutions in the s-health. We present them as follows:

(i) **Fog/Edge/Cloud-based**: Cloud computing allows the data to be stored on multiple servers and accessed from different locations. Yet, despite the recent efforts to make data closer to the user, fog and edge computing have overlapped to enhance the velocity of data processing. In edge computing, the data are stored in the device itself or closer to the device and not sent to the cloud [19]; similarly, fog computing provides an additional intermediate layer where the data are processed within a node, gateway, or router and then transferred to the proper devices [20].

(ii) **Blockchain-based**: As we already mentioned in the privacy techniques section, blockchain technology becomes hugely implemented in the s-health domain in order to address privacy issues and maintain seamless accessibility of data by the different stakeholders; it is built on public-key cryptography which is used to conduct transactions among nodes; these transactions are then stored on a shared ledger [1]. Once the data are recorded in the blockchain, they cannot be modified or removed.

(iii) **Policy-based**: A privacy policy is another facet that should be concerned about while dealing with privacy issues in s-health since they are the main intersection point between the multiple actors on the patients’ data, i.e., service providers, governmental organizations, etc., wherein every actor expresses his needs on how the data should be used, when, and how. Many privacy-preserving solutions have followed privacy by design approach, yet they fail to cover the needs of all the stakeholders.

2.3.3. Architectures of IoMT. Based on the aforementioned categories, we can distinguish 4 architectures for the IoT in the healthcare domain, namely, *centralized architecture*, *decentralized architecture*, *hybrid architecture*, and *third parties architecture*, as illustrated in Table 1.

### 2.4. Privacy-Preserving in s-Health: Laws, Policies, and Preferences

#### 2.4.1. Privacy Legislation

Privacy preservation is a common responsibility among the different stakeholders; hence, they are attempting to manage it by applying many mechanisms; however, they only rely on the technical perspective while neglecting the perspective of legitimacy and law compliance. In this section, we will promote the existing and relevant laws and regulations of protecting data and personal health information (PHI).

As shown in Figure 3, since 1988, countries are attempting to put boundaries on data usage, and allow citizens to have control over their data, furthermore setting penalties on any violation behavior of personal privacy. A comparative study of major privacy laws and regulations is surveyed in Ref. [21].

The most relevant data protection legislation enacted to date is the EU law General Data Protection Regulation (GDPR), which is not only restricted to European-based companies and service providers but also deals with international parties that are involved in processing the data of the EU citizens. For that reason, many recent privacy laws consider the adoption of GDPR, for instance, the Consumer Privacy Act (CCPA) in California, enacted in June 2018 and took effect in January 2020, the General Data Protection Law (LGPD) in Brazil passed in 2018 and goes into effect in February 2020 [22], and the Consumer Data Protection Act (CDPA) in Virginia enacted on March 2, 2021.

Besides the EU GDPR, the International Standard ISO/IEC 29100 defines 11 privacy principles to help organizations define their privacy safeguarding requirements related to personally identifiable information (PII) [23], namely: Consent and choice; Purpose legitimacy and specification; Collection limitation; Data minimization; Use, retention, and disclosure limitation; Accuracy and quality; Openness, transparency, and notice; Individual participation and access; Accountability; Information security; and Privacy compliance. The principles are described in Ref. [23].

#### 2.4.2. Privacy Policies and Patients’ Preferences

As stated in section 2.3.2, a Privacy Policy is a statement wherein an organization clarifies how it will handle the collected Personal Health Information (PHI); however, it may not necessarily satisfy the patients’ preferences. In order to prevent this kind of conflict, the Privacy Policy must be written understandably and mostly natural languages are used for this purpose, while at the same time allowing patients to express their preferences beforehand. In fact, this approach is proceeding toward a mutual agreement among the s-health stakeholders regarding privacy preservation, yet it provokes many challenges particularly the agreement process and the conflicting policies.

### 3. Systematic Literature Review

To choose and subsequently analyze a series of scientific articles, the methodology used to conduct the literature search and the selection of the studies to be included in our analysis has been presented in this section. An SLR is composed of five phases, namely: (i) **definition of Research Scope**, (ii) **Selection of primary studies**, (iii) **Inclusion and exclusion criteria**, (iv) **Selection results**, and (v) **Data analysis**.

#### 3.1. Step1: Definition of the Research Scope

The first step to perform an SLR is identifying the need to uncover gaps and trends related to the privacy-preserving aspects addressed in this study. Therefore, it is necessary to identify some research questions (RQ) to be answered from the inputs provided by the analysis of relevant studies, which will constitute the primary studies.
The purpose of this research was to analyze existing studies and their solutions, to summarize the efforts of research on privacy-preserving in smart healthcare applications from an end-to-end view (Different needs of stakeholders and whole data life cycle), and to discover limitations in terms of privacy criteria coverage view. Therefore, to achieve these objectives, we have chosen three research questions as listed in Table 2.

### Table 1: Architectures of IoMT.

| Architectures | Entities participation | Storage type | Pros | Cons |
|---------------|------------------------|--------------|------|------|
| Centralized   | N                      | Centric      | Efficiency: All data are managed in one place; affordable to maintain | Single point of failure; no control over data usage |
| Decentralized | Y                      | Distributed  | Secure storage; control over data usage | Higher maintenance costs |
| Third-party   | N                      | Centric      | Cost-effective | Data disclosed to untrusted third party; no control over data usage |
| Hybrid        | N/Y                    | Centric/Distributed | Takes advantage of the pros of each architecture | Difficulty in management |

Figure 3: Privacy laws and regulations.

The purpose of this research was to analyze existing studies and their solutions, to summarize the efforts of research on privacy-preserving in smart healthcare applications from an end-to-end view (Different needs of stakeholders and whole data life cycle), and to discover limitations in terms of privacy criteria coverage view. Therefore, to achieve these objectives, we have chosen three research questions as listed in Table 2.

### 3.2. Step 2: Selection of Primary Studies

In this phase, we will identify the source bases and the source strings used to select the primary studies for our study. To form our research query, we used the Boolean operators AND and OR to combine the multiple keywords describing our research subject, the final result is the following:

(Privacy OR Cybersecurity OR “Cyber security” OR security) AND (“smart healthcare” OR “smart health” OR “digital healthcare” OR “medical Internet of things” OR “medical IoT” OR “Internet of medical things”)

We have submitted this query in various relevant databases, namely: Science Direct, Scopus, Web of Science, and Springer Link. The obtained results were then filtered through the inclusion and exclusion criteria defined in section 2.3; afterward, we conducted the snowballing technique to the new set of results, including both forward and backward processes.

### 3.3. Step 3: Inclusion and Exclusion Criteria

After the initial selection from the previously mentioned databases, the next step is the paper screening, which consists of checking the eligibility of each article according to many criteria for inclusion and exclusion, as presented in Table 3, to retrieve only the most relevant studies that present a privacy-preserving solution in the smart healthcare environment.

### 3.4. Step 4: Selection Results

The initial query search in the selected databases provided us with an amount of 3425 articles as shown in Figure 4; after removing the duplicated studies, the number was reduced to 3391; these studies are then examined through the inclusion/exclusion criteria and reduced to 59. An additional 8 and 33 studies were identified by forward and backward snowballing, respectively, making the outcome of the papers to be included in our systematic literature review equal to 100 papers.

### 4. Result and Finding

After selecting the primary studies, in this section, two types of analysis were performed to evaluate and synthesize the primary studies—bibliometric analysis and technical analysis, as discussed in the following subsections.

#### 4.1. Bibliometric Analysis

After the paper screening phase, in this section, we focused on the evaluation of the primary studies in terms of their publishers and publication year. According to Figure 5, an important number of primary studies (51%) was published by Science Direct, and 33% was published by Scopus; moreover, a percentage of 21% was published by Web of Science, while the least number of papers was found in SpringerLink (4%).

It is worth mentioning that the researchers’ concern about security in smart healthcare and privacy of medical data is constantly growing, as seen in Figure 6; the published primary studies went from 9 percent in 2017 to 29 percent in 2021. The increasing adoption of telemedicine, usage of the
### Table 2: Research questions for our systematic literature review.

| Research questions                                                                 | Goals                                                                                                                                 |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| **RQ1:** What are the proposed solutions to preserve privacy according to the different stakeholders' needs (patients, providers, government bodies) while considering data-access management? | This question aims at identifying the existing solutions to preserve privacy from different stakeholders’ points of view; therefore, it will help to know the missing stakeholders’ needs that require more interest in the future. |
| **RQ2:** What are the privacy criteria that have been considered by the proposed solutions, and in which data life cycle phase? | This question aims at identifying the privacy criteria coverage stated by the existing solutions, as well as the phase of the data life cycle that should be more enhanced. |
| **RQ3:** How and what are the techniques used by published papers to preserve privacy in smart healthcare, and in which architecture and category? | This question aims to identify the privacy-preserving techniques and their impact on the architecture choice. |

### Table 3: Inclusion and exclusion criteria.

| Inclusion criteria                                                                 | Exclusion criteria                                                                 |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| The paper must present a privacy-preserving solution related to smart healthcare   | Duplicated articles                                                               |
| The paper must be a research article published in a peer-reviewed journal or conference | Articles published before 2017                                                     |
| We suppose that relevant articles should have at least one citation per year if the publication year is between 2017 and 2019. For example, if an article is published in 2017, it should have at least 4 citations | Articles that are written in a language other than English                          |
|                                                                                 | Articles that present a previous version of a complete research study               |
|                                                                                 | The study is a survey                                                              |

### Figure 4: Number of articles included and excluded through paper screening.

- **ScienceDirect**  
  N = 1651

- **Scopus**
  N = 817

- **Web of Science**
  N = 589

- **Springer Link**
  N = 368

- **Total** = 3425
- **Total removed** = 558  
  Duplicated articles are removed. Articles published before 2017 are removed.

- **Total** = 2867
- **Total removed** = 1368  
  The papers aren’t a research articles. The papers haven’t enough citation.

- **Total** = 1499
- **Total removed** = 1440  
  The papers out of our research topic. The papers that are not written in English.

- **Total** = 59
- **Total added** = 41  
  Articles included after the Snowballing.
Internet of medical things by different stakeholders, and cyber awareness of patients, imply that in the next few years, the research will be further enriched by studies that arise in the context of privacy-preserving in digital healthcare.

4.2. Technical Analysis. This step consists of defining a classification scheme composed of different privacy aspects in order to compare the different solutions based on a comprehensive analysis. We define seven privacy aspects for our study as follows:

- **(i) Architecture:** Centralized, Decentralized, Third party, and Hybrid.
- **(ii) Category:** Fog-/Edge-/Cloud-based, Blockchain-based and Policy-based.
- **(iii) Data access management and privacy-preserving technique:** Access Control, Blockchain, Authentication, Cryptography, and Anonymization.
- **(iv) Stakeholders’ needs:** Patient Preferences, Privacy Policy, and Privacy laws.
- **(v) Data Life Cycle:** Collection, Transmission, Storage, and Process/Use.
- **(vi) ISO Privacy Principle:** P1: Consent and choice; P2: Purpose legitimacy and specification; P3: Collection limitation; P4: Data minimization; P5: Use, retention, and disclosure limitation; P6: Accuracy and quality; P7: Openness, transparency, and notice; P8: Individual participation and access; P9: Accountability; P10: Information security; P11: Privacy compliance.

In this phase, we will classify the papers into four classes (centralized, decentralized, third party, and hybrid) based on the architecture privacy aspect. Furthermore, an in-depth assessment will be accomplished through a critical analysis of the selected papers based on the other privacy aspects: category, data access management and privacy-preserving technique, stakeholders’ needs, data life cycle, and ISO privacy principle. In the following subsections, we present the findings of the aforementioned analysis.

4.2.1. Centralized Architecture. In this subsection, we present the main features and limitations of the relevant papers in a centralized architecture, while the detailed results are summarized in Table 4.

Kumar et al. [24], proposed a Secure Addressing and Mutual Authentication protocol (SAMA) scheme to protect the network from multiple attacks by modifying the standard IPv6 protocol, and by establishing a secure session key and mutual authentication.

In another work carried out by de Oliveira et al. [25], a dynamic revocable data access control protocol for Acute Care teams (AC-AC) was proposed, by adding a security mechanism that enables break-glass access to the Electronic Medical Records (EMR) with dynamic revocation to provide access to a patient’s encrypted EMR during acute care.

In the same context, and using Hyperelliptic Curve Cryptosystem (HECC), authors proposed in Ref. [81] a secure and efficient software-defined healthcare-enabled WBANs architecture. More explicitly, authors integrated the SDN technology into the proposed solution while separating the control and data planes in an efferent manner. Hence, convenient results were obtained in terms of security, computation, communication, and storage costs.

On the other hand, Zhong et al. [26] proposed an efficient attribute-based encryption (ABE) scheme that out-sources part of the encryption and decryption to the edge nodes and supports attribute updates, enabling flexible right control. This scheme is tested and evaluated in different security levels and proves that it is more efficient for resource-constrained devices than the traditional ABE schema. Furthermore, in a study reported by Onesimut al. [27], a privacy-preserving data collection scheme was implemented based on the clustering-based anonymity mode for IoT-based healthcare services and formulates the threat model as client-server-to-user to ensure privacy on both ends.

In the same context, an integrated privacy-preserving framework in IoT-based smart healthcare was suggested in Ref. [29]; the particularity of this solution is its ability to allow patients making pragmatic data sharing deals with smart services by indicating the data items that can be shared or used along with their precision.

Izza et al. [28] proposed an IoT-based Radio Frequency Identification (RFID) authentication scheme for Wireless Body Area Networks (WBAN), which is an improved version of the RFID authentication scheme for IoT proposed by Naeem et al. This study focused on solving the remaining security challenges of the previous protocol during the transmission phase.
| Primary studies | Category | Privacy techniques | Data-access management | Stakeholders needs | Data life cycle | Privacy criteria (ISO/IEC 29100) |
|----------------|----------|--------------------|------------------------|-------------------|----------------|----------------------------------|
| [24]           | Cloud-based | Cryptography anonymization | Cryptography authentication process | No | Transmission | P6; P10; P11 |
| [25]           | Cloud-based | Cryptography | Cryptography access control | No | Transmission storage process | P1; P2; P5; P6; P8; P10 |
| [26]           | Edge/Cloud-based | Cryptography access control | Access control | No | Transmission storage process | P6; P10; P11 |
| [27]           | Cloud-based | Anonymization | | No | Collection | P5; P6; P7; P10; P11 |
| [28]           | Cloud-based | Cryptography \ Anonymization | Cryptography | No | Transmission | P6; P10; P11 |
| [29]           | Cloud-based | Anonymization | Access control | Patient preferences privacy policy | | P1; P3; P5; P7; P8; P11 |
| [30]           | Edge-based | Cryptography | Access control | Patient preferences privacy policy | | P1; P3; P4; P6; P8; P10; P11 |
| [31]           | Cloud-based | Cryptography access control | Access control | Privacy policy | | P2; P8; P6; P9; P10; P11 |
| [32]           | Cloud-based | Cryptography access control | Cryptography access control | Privacy policy | | P1; P2; P5; P8; P9; P11 |
| [33]           | Cloud-based | Anonymization access control | Cryptography access control authentication process | No | Storage process | P6; P7; P10; P11 |
| [34]           | Cloud-based | Cryptography anonymization | Cryptography authentication process | No | Transmission storage process | P6; P7; P11 |
| [35]           | Cloud-based | Access control | Cryptography | Privacy policy | | P2; P5; P10; P11 |
| [36]           | Privacy-based | Cloud-based | Anonymization | No | Storage process | P2; P5 | P5; P9; P10 |
| [37]           | Privacy-based | Cloud-based | Authentication process | No | Process | P2; P5; P6; P8 |
| [38]           | Cloud-based | Cryptography | Authentication process | No | Privacy process | P6; P10; P11 |
| [39]           | Cloud-based | Cryptography anonymization | Cryptography authentication | No | Collection transmission storage process | P2; P3; P4 | P10; P11 |
| [40]           | Cloud-based | Cryptography access control | Access control authentication process | No | Transmission storage process | P6; P10; P11 |
| [41]           | Cloud-based | Cryptography | No | No | Storage process | P6; P9; P10; P11 |
| [42]           | Cloud-based | Cryptography | No | No | Storage process | P6; P9; P10; P11 |
| [43]           | Cloud-based | Cryptography access control | Access control | No | Storage process | P6; P8; P10; P11 |
| [44]           | Privacy-based | Anonymization access control | | No | Storage process | P6; P10; P11 |
| [45]           | Cloud-based | Cryptography | Cryptography | Patient preferences privacy policy | | P1; P4; P7; P5; P3; P6; P9; P10 |
| [46]           | Cloud-based | Cryptography access control | Access control authentication process | Patient preferences | | P2; P5; P8; P9; P10 |
| [47]           | Cloud-based | Cryptography | Cryptography | | Transmission storage process | P6; P7; P10; P11 |
| [48]           | Cloud-based | Cryptography anonymization | Cryptography authentication process | No | Process | P6; P7; P10; P11 |
| [49]           | Cloud-based | Cryptography | Cryptography authentication process | No | Process | P6; P7; P10; P11 |
| [50]           | Cloud-based | Cryptography | Cryptography | | Collection transmission storage process | P6; P10; P11 |
| Primary studies | Category | Privacy techniques | Data-access management | Stakeholders needs | Data life cycle | Privacy criteria (ISO/IEC 29100) |
|-----------------|----------|--------------------|------------------------|-------------------|----------------|---------------------------------|
| [51]            | Cloud-based | Cryptography access control | Cryptography access control | Privacy policy | Collection storage process | P1; P4; P7; P2 |
| [52]            | Cloud-based | Cryptography | Cryptography authentication process | No | Transmission storage | P7; P8; P10 |
| [53]            | Cloud-based | Cryptography access control | Cryptography access control | Privacy policy | Storage process | P9; P10; P11 |
| [54]            | Cloud-based | Cryptography anonymization access control | Cryptography access control authentication | Privacy policy | Transmission storage process | P6; P10; P11 |
| [55]            | Cloud-based | Cryptography anonymization | Cryptography authentication process | No | Transmission | P5; P7; P10; P11 |
| [56]            | Cloud-based | Cryptography anonymization access control | Cryptography access control | Patient preferences | Storage process | P1; P5; P8; P10; P11 |
| [57]            | Edge/Cloud-based | Cryptography | Cryptography authentication process | Patient preferences | Transmission storage process | P1; P2; P5; P8; P9 |
| [58]            | Cloud-based | Cryptography access control | Access control | No | Collection process | P1; P2; P8; P11 |
| [59]            | Privacy-based | Access control | Authentication process | No | Transmission process | P6; P10; P11 |
| [60]            | Cloud-based | Cryptography | Cryptography | Privacy policy | Process | P2; P5; P9; P10 |
| [61]            | Cloud-based, Fog/Edge/Cloud-based | Access control | Access control | Patient preferences | Collection transmission | P1; P3; P4; P7; P8; P11 |
| [62]            | Cloud-based | Cryptography anonymization | Smart contracts | No | Transmission process | P2; P5; P10 |
| [63]            | Cloud-based | Cryptography | Cryptography | Patient preferences | Transmission/Storage | P7; P5; P8; P9; P10 |
| [64]            | Policy-based | Anonymization access control | Access control | Privacy policy | Transmission storage process | P1; P6; P7; P8; P10; P11 |
| [65]            | Cloud-based, distributed data | Anonymization | No | Privacy policy | Collection storage | P3; P4; P7; P10 |
| [66]            | Cloud-based | Cryptography | No | No Patient preferences/Privacy policy | Transmission | P6; P10; P11 |
| [67]            | Privacy-based | Cryptography access control | Access control | No | Transmission | P2; P10; P11 |
| [68]            | Cloud-based | Cryptography access control | Access control | No | Transmission storage | P6; P9; P10; P11 |
| [69]            | Cloud-based | Anonymization | Access control | No | Storage process | P6; P10; P11 |
| [70]            | Cloud-based | Cryptography anonymization access control | Access control | No | Storage process | P7; P8; P10; P11 |
| [71]            | Privacy-based | Cryptography anonymization | Cryptography authentication process | No | Process | P5; P9; P10 |
| [72]            | Cloud-based | Anonymization | No | No | Collection | P3; P4; P9; P10; P11 |
| [73]            | Cloud-based | Cryptography | No | Privacy policy | Storage process | P2; P5; P10; P11 |
| [74]            | Privacy-based | Cryptography | Access control | Compliant with laws privacy policy | Collection process | P1; P2; P3; P7; P8; P11 |
| [75]            | Cloud-based | Cryptography | Cryptography | No | Transmission storage | P7; P8; P10 |
| [76]            | Edge/Cloud-based | Cryptography | No | Privacy policy | Collection | P5; P6; P7; P10; P11 |
| [77]            | Cloud-based | Cryptography anonymization access control | Cryptography access control authentication | No | Storage process | P6; P9; P11 |
Moreover, Alraja et al. [29] focused on protecting the privacy of the IoT users, and helping them make pragmatic data-sharing deals with smart services and data consumers by determining the existing privacy risks concerning each data sharing.

Singh and Chatterjee [30] designed a smart healthcare system based on edge computing architecture which consists of an intermediary layer called an edge computing layer responsible for maintaining the network latency and preserving the privacy of the patient data.

The emerging healthcare Industrial Internet of Things (HealthIIoT) faces several fundamental security and privacy challenges, such as secure fine-grained data delivery, privacy-preserving keyword-based ciphertext retrieval, and malicious key delegation. For these challenges, Sun et al. [31] proposed a Privacy-aware and Traceable Fine-grained System (PTFS) in cloud-assisted HealthIIoT, which enables secure fine-grained data delivery, privacy-preserving data retrieval, efficient encryption, and decryption operations.

Sathya and Raja [32] proposed a Euclidean L3P-based Multiobjective Successive Approximation (EMSA) algorithm, a powerful measure of privacy in the smart healthcare environment, Based on the critical foundation for the storage of sensitive data in cloud environments, the role-based encryption keys.

Furthermore, other research groups and Ogundoyin et al. [33] proposed a lightweight privacy-preserving authentication and fine-grained access control scheme (PAASH) for smart health. This study addresses the security, efficiency, and privacy challenges of smart healthcare in smart cities.

Furthermore, Vineela et al. [34] proposed an authentication scheme for preserving the security and privacy of the big data in a cloud environment; this schema follows a mutual authentication and performs encryption operation between user and cloud environment.

A human-in-the-loop-aided (HitL-aided) scheme was designed by Zhou et al. [35] to preserve privacy in smart healthcare. They employed a block design technique to obfuscate various health indicators from the hospitals and the smart devices. They also introduced a human-in-the-loop (HitL) to enable privacy access of the health reports from the smart healthcare platform.

In addition, in a study made by Krall et al. [36], a new approach for preserving privacy in the framework of predictive modeling was proposed. This solution meets the requirement of differential privacy while mitigating the risk of model inversion.

Based on machine learning techniques to detect deviated user access against Electronic Health Records (EHR), and to maintain the privacy of healthcare data, Hussain Seh et al. [37] defined an efficient framework for securing the privacy and confidentiality of healthcare data proactively. On the other hand, He et al. [38] presented a password strength meter that takes into account users’ personal information. It helps users to select passwords with a higher degree of security.

Furthermore, in another recent work performed by Ibaida et al. [39], a novel privacy-preserving and efficient technique was proposed, that implements a lightweight shallow neural network to reduce the burden on the network while ensuring the privacy of the Electrocardiogram signals (ECG).

For the same purpose, another recent work carried out by El Zouka et al. [40] defined a secured healthcare monitoring system using fuzzy logic-based decision support (FBIS) systems to get the status of the patient. The proposed model consists of a trusted environment that is responsible for collecting authenticated physiological data.

Furthermore, a secure certificateless searchable public-key encryption (SPE) scheme for SHS was defined by Ma et al. [41], named SCF-CLSPE scheme, and it can resist keyword guessing attacks (KGA) and chosen keyword attacks (CKA) under the standard model. This scheme was also tested and proved that it has lower computation and communication costs.

Jayaram and Prabakaran [42] presented an edge-level privacy-preserving additive homomorphic encryption for secure data processing and filtering nonsensitive data in the edge layer. Also, an adaptive weighted probabilistic classifier model is proposed in the cloud layer for onboarding disease prediction and rehabilitation of remote patients.

Also, many healthcare-based solutions, including Refs. [82–84], focus on predicting serious disease using deep learning, machine learning, or a combination of the two. These works aim to analyze and monitor patient health to prevent severe health complications. Yet, these works focus more on patients’ data while little attention is given to the patient’s privacy. Contrary to these propositions, the work performed by Ge et al. [43] while aiming to predict disease by using deep learning also assured the data deletion approach by the data owner to limit access to their health data.
Toward the identification of anomalous behaviors within electronic patient record (EPR) datasets, researchers Hurst et al. [44] presented an investigation methodology. The proposed framework uses the LOF algorithm to detect unusual data patterns, labeling points as normal or anomalous, under the consideration of an HIL approach.

Moreover, Abdo et al. [45] used machine learning techniques for classifying a user’s-health state and crowdsensing for collecting information about a person’s privacy preferences. They proposed a novel cloud-based secure location privacy-preserving mobile healthcare framework with securely storing, processing, and decision-making capabilities.

Furthermore, to provide users with secure and efficient access to their data, a lightweight user authentication system was designed by Kaul et al. [46]. In order to prevent unauthorized users from accessing the data, a proposed authentication describes a lightweight data access control process.

Moreover, with the intent to protect a patient’s images from a compromised broker, Hamza et al. [47] proposed a privacy-preserving chaos-based encryption cryptosystem. They proposed a fast probabilistic cryptosystem to secure medical keyframes that are extracted from wireless capsule endoscopy procedures using a prioritization method.

Hathaliya et al. [48] proposed a mobile-based healthcare system with a biometric authentication approach, to ensure the security and privacy of electronic healthcare records in the Healthcare 4.0 era. For the same purpose, researchers Hathaliya et al. [49] previously proposed a biometric-based authentication scheme to ensure secure access of the patient’s EHR from any location. The proposed scheme is tested and validated by the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool.

Furthermore, in a study reported by Xie et al. [50], iCLAS was presented, which is an improved certificateless aggregate signature scheme that can resist all kinds of security attacks and can ensure patient privacy protection.

A privacy preservation framework was presented by Azad et al. [51] within smart context-aware healthcare emphasizing privacy assurance challenges within Electronic Transfer of Prescription. They proposed an enhancement to the widely used Salford model to achieve privacy preservation against masquerading and impersonation methods.

An anonymity-based user authentication protocol is preferred to resolve the privacy preservation issues in the IoMT. For this purpose, Deebak et al. [52] proposed a Secure and Anonymous Biometric Based User Authentication Scheme (SAB-UAS) to ensure secure communication in healthcare applications.

Moreover, in Yang et al. [53], a privacy-preserving smart IoT-based healthcare big data storage system with self-adaptive access control was defined. This solution aims at solving the following challenges: privacy of patients’ medical data, access control in emergency scenarios, and optimization of data storage in big data systems. In another recent work by the same group, Yang et al. [54] proposed a privacy-preserving e-health system, where it defines a noninteractive and authenticated key distribution procedure for the medical IoT network, as well as a novel keyword match-based policy update mechanism. Also, note that this system is a fusion of Internet-of-things (IoT), big data, and cloud storage.

Furthermore, in a study reported by Aghili et al. [55], the limitations of the previously proposed lightweight RFID mutual authentication (LRMI) protocol were presented, to eventually propose a new secure and lightweight mutual RFID authentication (SclLAP) protocol that provides secure communication and preserves privacy in the smart medical systems. The proposed security features are verified using the BAN logic.

Greene et al. [56] proposed ShareHealth, an end-to-end system for secure sharing of the collected medical data, by allowing the data owners to specify access-control policies and to cryptographically enforce those policies.

In addition, with the aim of solving the problem of limited computation ability of sensors on a patient in a smart healthcare system, Ding et al. [57] proposed a lightweight secure smart healthcare storage system that employs edge servers to compute data authenticators and verify data integrity.

MPPDS, a novel collaborative eHealth system that supports Multilevel Privacy-Preserving Data Sharing, was developed by Kim et al. [58]. The proposed system gives the data owner the possibility to share his or her health data with several data users within a collaborative eHealth system, under different levels of privacy protection.

Huang et al. [59] presented a practical scheme that can reliably authenticate patients with biometric authentication; electrocardiogram (ECG) signals, and provide differentially private protection simultaneously.

Furthermore, intending to protect patients’ sensitive data while the smart health platform needs to do some analysis over these data, researchers Wang et al. [60] proposed a privacy-preserving outsourced computation scheme in the healthcare system. They enhanced the security of this scheme by splitting the decryption permissions into both servers.

A fog-based access control model was proposed by Wang et al. [61], to ensure high-level privacy protection without reducing the efficiency in cloud/fog computing, especially on the Internet of medical things IoMT.

Zhang et al. [62] defined a secure smart healthcare system based on a leakage-resilient anonymous HIBE scheme in the bounded leakage model. It can protect the patient’s privacy well, even when the private key is partially leaked. It also achieves the safe transmission of the patient’s electronic health records (EHR) in the case of leakage attacks.

Based on multi-party random masking and polynomial aggregation techniques, Kaur et al. [63] proposed a PPCF scheme. Privacy-Preserving Collaborative Filtering scheme on Arbitrary Distributed Data (ADD), where two phases are considered namely: off-line model generation and online prediction generation.

Vora et al. [64] presented an approach to preserve the identity and to protect the privacy of clinical data using an ARCANA encryption scheme. They also discussed an
authorization framework using access of varying degrees. Moreover, they had implemented the AT&T scheme for managing the access control mechanism of patients’ data.

A practical framework called PrivacyProtector was defined by Luo et al. [65]. The proposed framework is a patient privacy-protected data collection, intending to prevent collision attacks and data leakage. PrivacyProtector includes the ideas of secret sharing and shares repairing for patients’ data privacy.

In another study made by Elhoseny et al. [66], a hybrid security model was proposed. This model aims to secure the diagnostic test data in medical images. They also developed through integrating 2-D discrete wavelet transform 1 level (2D-DWT-1L) steganography technique with a proposed hybrid encryption scheme.

An attribute-based credential (ABC) was presented by Maria de Fuentes et al. [67], to cope with smart health privacy issues and to set the stage for the further adoption in other privacy-aware IoT-based smart cities’ services.

Zhang et al. [68] introduced PASH, a privacy-aware s-health access control system, in which the key ingredient is a large universe ciphertext-policy attribute-based encryption (CP-ABE) with access policies partially hidden.

In another work, Zhang et al. [69], the authors, have introduced SSH, a Secure Smart Health system with privacy-aware aggregate authentication and access control in IoT. This solution is built on an anonymous certificateless aggregate signature and an anonymous CP-ABE scheme.

An efficient work carried out by Zheng et al. [70] presented a medical data sharing scheme in cloud storage. To solve the privacy issues in users’ data sharing, they utilize attribute-based encryption to enable data sharing. And, they use the attribute bloom filter to hide all the attributes in the access control structure.

Zhang et al. [71] provided a privacy protection mechanism offering biometric authentication that allows the server to authenticate users with a biometric template. The user’s anonymity is maintained during the authentication and key negotiation process.

A novel method for preserving the privacy of the collected data in the healthcare environment was developed by Kim et al. [72]. The proposed method is characterized as temporal data collected at fixed intervals by leveraging local differential privacy.

Practical privacy-preserving analytics in healthcare information systems was developed by Sharma et al. [73]. The study is based on kHealth, a personalized digital healthcare information system that is being developed and tested for disease monitoring.

Furthermore, with the aim of proposing the requirements and the practical approaches that should be considered when designing and developing IoT for data collection and data sharing within the healthcare domain, O’Connor et al. [74] define a “Privacy by Design approach.”

A methodology to secure patients’ medical big data MBD in the healthcare cloud was proposed by Al Hamid et al. [75], using the decoy technique with a fog computing facility. It is based on the bilinear pairing cryptography that can generate a session key among the participants and communicate among them securely.

A pioneer work carried out by Bhuiyan et al. [76] investigated the concerns with privacy-protected data collection. For this purpose, a new secret sharing scheme and a share reconstruction scheme were defined for patient data privacy. They consider a distributed database consisting of multiple edge servers and each server receives a share of the patient data.

A new schema named OOABS was defined by Liu et al. [77] to replace the traditional Mobile Internet Devices (MIDs), and embedded Devices (EDs) of the electronic Health systems, to overcome their limitations in terms of storage space, power supply, and computational capacity.

Yang et al. [78] proposed a new solution to preserve privacy in e-health. This solution is based on the dynamic searchable symmetric encryption scheme with forwarding privacy and delegated verifiability for periodically generated healthcare data.

Rahman et al. [79] designed a security framework named PriSens-HSAC. The proposed framework is the first framework that provides increased privacy for Radio Frequency Identification (RFID) based healthcare systems, using RFID authentication along with access control techniques.

Moreover, Zhang et al. [80] defined a secure smart healthcare system that fulfills fine-grained access control on smart healthcare cloud data and hence ensures users’ privacy protection. The key technique is a promising cryptographic primitive called ciphertext-policy attribute-based encryption.

### 4.2.2. Decentralized Architecture

Each primary research paper of this class was read in full, and relevant data were extracted and summarized in Table 5. The main idea of each paper is also recorded below in the following section.

Chelladurai et al. [85] proposed a Patient-Centric secure EHR Management system using blockchain technology, to provide a regulated solution to the requirements of patients, doctors, and health service providers with integrity management. The proposed system provides high security and integrity through cryptographic hash functions. Lee et al. [86] proposed a blockchain-based medical data preservation scheme for telecare medical information systems (TMISs), which consists of a medical sensor area authentication protocol (WBAN) and a social network information transfer protocol. A Double Blockchain Telemedicine Diagnosis (DBTMD) scheme was proposed by Wang et al. [87] for privacy protection, which constructs a public chain Userchain and a consortium Medicalchain. It also develops an identity authentication chain to ensure the real-time accuracy of the doctor’s identity information. This study reduces the communication costs of keys’ transactions.

Furthermore, Wang et al. [88] proposed a data privacy protection, efficient retrieval, and analysis service scheme of IoT based on low-cost fog computing. The fog computing system is set between the IoT and cloud services, and
Table 5: Summary of studies reported on decentralized architecture.

| Primary studies | Category               | Privacy techniques | Data-access management | Stakeholders needs | Data life cycle                          | Privacy criteria (ISO/IEC 29100) |
|-----------------|------------------------|--------------------|------------------------|--------------------|------------------------------------------|----------------------------------|
| [85]            | Blockchain-based       | Cryptography       | Access control         | No                 | Collection transmission storage process  | P1; P6; P7; P8; P10               |
|                 |                       | blockchain         | smart contracts        |                    | Collection transmission storage          |                                 |
| [86]            | Blockchain-based       | Cryptography       | Cryptograph            | No                 | Transmission storage process             | P1; P6; P10                     |
|                 |                       | blockchain         | access control         |                    |                                          |                                 |
| [87]            | Blockchain-based       | Cryptography       | Cryptography            | No                 | Transmission storage process             | P1; P4; P5; P6; P7; P8; P10; P11  |
|                 |                       | blockchain         | access control         |                    |                                          |                                 |
| [88]            | Blockchain-based       | Cryptography       | Cryptograph            | No                 | Transmission storage process             | P4; P5; P6; P7; P8; P10; P11     |
|                 |                       | smart contracts    | authenticity process   |                    |                                          |                                 |
| [89]            | Blockchain-based       | Blockchain access  | Smart contracts        | No                 | Collection transmission storage process  | P1; P5; P6; P7; P10               |
|                 |                       | control            |                        |                    |                                          |                                 |
| [90]            | Blockchain-based       | Cryptography       | Cryptograph            | No                 | Transmission storage process             | P1; P5; P6; P7; P10               |
|                 |                       | blockchain         | access control         |                    |                                          |                                 |
| [91]            | Fog/Cloud-based        | Cryptography       | No                     | No                 | Transmission storage process             | P6; P10                          |
|                 |                       | Smart contracts    |                        |                    |                                          |                                 |
| [92]            | Blockchain-based       | Cryptography       | Cryptography            | No                 | Transmission storage process             | P5; P6; P7; P8; P10; P11          |
|                 |                       | blockchain         | smart contracts        |                    |                                          |                                 |
| [93]            | Blockchain-based       | Smart contracts    |                        | No                 | Transmission storage process             | P1; P3; P4; P5; P7; P8; P10; P11  |
|                 |                       | blockchain         |                        |                    |                                          |                                 |
| [94]            | Blockchain-based       | Cryptography       | Smart contracts        | Patient preferences| Storage process                          | P1; P3; P7; P8; P10; P11          |
|                 |                       | blockchain         | smart contracts        | Patient preferences|                                          |                                 |
| [95]            | Blockchain-based       | Blockchain access  | Smart contracts        | Patient preferences| Storage process                          | P1; P3; P7; P8; P10; P11          |
|                 |                       | control            |                        | Compliant with     |                                          |                                 |
| [96]            | Blockchain-based       | Access control     | Smart contracts        | Patient preferences| Storage process                          | P1; P2; P3; P5; P7; P8; P9; P10; P11| Compliant with laws patient preferences | P1; P2; P3; P5; P7; P8; P9; P10; P11 | Storage process |
|                 |                       | smart contracts    |                        |                  |                                          |                                 |
| [97]            | Blockchain-based       | Smart contracts    |                        | Patient preferences| Storage process                          | P1; P3; P4; P5; P7; P8; P10; P11  |
|                 |                       | blockchain         |                        | Patient preferences|                                          |                                 |
| [98]            | Blockchain-based       | Cryptography       |                        | No                 | Transmission storage process             | P1; P3; P7; P8; P10; P11          |
|                 |                       | blockchain         |                        | No                 |                                          |                                 |
| [99]            | Blockchain-based       | Cryptography       |                        | No                 | Transmission storage process             | P7; P10; P11                     |
|                 |                       | blockchain         |                        | No                 |                                          |                                 |
| [100]           | Blockchain-based       | Cryptography       |                        | No                 | Storage                                  | P6; P10; P11                    |
|                 |                       | blockchain         |                        | No                 |                                          |                                 |
| [101]           | Blockchain-based       | Cryptography       | Smart contracts        | Patient preferences| Storage process                          | P1; P5; P7; P8; P10; P11          |
|                 |                       | smart contracts    | authentication process | Compliant with     |                                          |                                 |
| [102]           | Blockchain-based       | Cryptography       | Smart contracts        | Compliant with     | Transmission storage process             | P1; P2; P6; P7; P8; P9; P10; P11  |
|                 |                       | blockchain         | Compliant with         | laws                |                                          |                                 |
| [103]           | Blockchain-based       | Smart contracts    | Authentication process | No                 | Storage                                  | P2; P5; P6; P7; P8; P10; P11     |
|                 |                       | blockchain         | Authentication process | No                 |                                          |                                 |
| [104]           | Blockchain-based       | Smart contracts    | Authentication process | No                 | Transmission storage process             | P2; P5; P6; P7; P8; P10; P11     |
|                 |                       | blockchain         | Authentication process | No                 |                                          |                                 |
| [105]           | Blockchain-based       | Cryptography       | Authentication process | No                 | Transmission storage process             | P2; P5; P6; P7; P8; P10; P11     |
|                 |                       | blockchain         | Authentication process | No                 |                                          |                                 |
| [106]           | IOTA-based             | Cryptography       | Access control         | Patient preferences| Transmission storage process             | P5; P6; P7; P8; P10; P11          |
|                 |                       | smart contracts    | authentication process | Patient preferences|                                          |                                 |

Security and Communication Networks
provides low latency, high computing efficiency, and decentralization.

Moreover, in a research paper made by Kumar et al. [89], a smart contract-enabled consortium blockchain network was defined, which is built on the interplanetary file systems (IPFS) cluster node and smart contracts for authentication of patients and medical devices.

Furthermore, in a study reported by Zhang et al. [90], the PTBM scheme was proposed, a contact tracing scheme in 5G-integrated and Blockchain-based Medical applications, which enables patients’ location tracking and checking in a privacy-preserving manner.

Wang et al. [91] define a computation transferable authenticated key agreement protocol without an online registration center for smart healthcare. The proposed scheme adopts certificateless public-key cryptography, which can solve the problems of certificate management and key escrow. For the same intent, researchers Wang et al. [92] previously proposed GuardHealth, a decentralized blockchain system for data privacy-preserving and sharing. The proposed system manages confidentiality, authentication, data preserving, and data sharing when handling sensitive information.

A blockchain-based knapsack system has been proposed by Ranjith and Mahantesh [93]. The proposed blockchain method was evaluated on medical data to analyze the performance. The results show that the proposed method has less computation time and memory use compared to the existing methods. For the same purpose, in a pioneer work carried out by Dai et al. [94], a blockchain-enabled IoMT was proposed to increase the security and privacy concerns of IoMT systems. They also discuss the solutions brought by blockchain-enabled IoMT to COVID-19 from five different perspectives.

Moreover, with the aim to access control over individual health data, Jaiman and Urovi [95] presented a blockchain-based data-sharing consent model by using smart contracts. The dynamic consent model extends to two ontologies: The Data Use Ontology (DUO), which models the individual consent of users, and the Automatable Discovery and Access Matrix (ADA-M), which describes queries from data requesters.

Zhuang et al. [96] presented a blockchain model that achieves patient-centric HIE to protect data security and patients’ privacy, ensure data provenance, and provide patients full control of their health records, by personalizing data segmentation and an “allowed list” for clinicians to access their data.

Uddin et al. [97] proposed a blockchain leveraged decentralized architecture for eHealth. This architecture comprises three layers, the sensing layer (Body Area Sensor Network), the NEAR processing layer (the Fog), and the FAR processing layer (the Cloud).

Furthermore, a study was performed by Aruna Sri and Lalitha Bhaskari [98] aiming at analyzing blockchain-based encryption for patients’ data and proposes a consensus mechanism to validate Proof of Word and Interoperability for data discovery and access.

Sun et al. [99] defined an attribute-based encryption scheme for secure storage and efficient sharing of electronic medical records in an InterPlanetary File System (IPFS) storage environment. The proposed model includes fine-grained and flexible access control, revocability of consent, auditability, and tamper resistance.

Tripathi et al. [100] proposed the Smart and Secured Healthcare System (S2HS), which is a two-level blockchain-based smart healthcare systems (SHS) framework to provide intrinsic security and integrity of the system.

Moreover, Usman and Qamar [101] presented a blockchain-based records management system that implements permissioned blockchain platform “Hyperledger” for efficient management and sharing of electronic medical records (EMRs).

In a research paper made by Hylock and Zeng [102], HealthChain was presented, a novel patient-centered blockchain framework to support immutable logging, promote patient engagement, and facilitate secure mediated information exchange between patients and providers.

Existing solutions on retrieval of electronic medical records either fail to protect sensitive data or are limited to a single image data provider. To resolve these challenges, Shen et al. [103] proposed a medical encrypted image retrieval scheme based on blockchain for privacy protection. They presented the layered architecture and threat model of the proposed scheme, using the emerging blockchain techniques.

In another study made by Xu et al. [104], the Healthchain scheme was proposed, a large-scale health data privacy-preserving scheme based on blockchain technology, where health data are encrypted to conduct fine-grained access control.

| Primary studies | Category                  | Privacy techniques                                           | Data-access management                  | Stakeholders needs                                     | Data life cycle                  | Privacy criteria (ISO/IEC 29100) |
|-----------------|---------------------------|-------------------------------------------------------------|----------------------------------------|--------------------------------------------------------|----------------------------------|----------------------------------|
| [107]           | Blockchain-based          | Cryptography blockchain                                      | Smart contracts                        | Compliant with laws patient preferences                 | Transmission storage process     | P1; P2; P5; P6; P7; P8; P10; P11 |
| [108]           | Blockchain-based          | Cryptography smart contracts                                 | Cryptography smart contracts           | No                                                     | Transmission storage process     | P5; P6; P10; P11                  |
Daraghmi et al. [105] designed a MedChain system for medical records access management, where the timed-based smart contracts can interact with the various demands of health providers, patients, and third parties.

To provide a storage solution while preserving privacy for users, Li et al. [106] proposed a novel blockchain-based data preservation system (DPS) for medical data. With the proposed system, users can preserve important data in perpetuity, and the originality of the data can be verified if tampering is suspected.

Furthermore, Dagher et al. [107] proposed a framework named Ancile, which utilizes smart contracts in an Ethereum-based blockchain to define heightened access to medical records by the different stakeholders while preserving the privacy of patients’ sensitive information.

In another work carried out by Brogan et al. [108], the role of distributed ledger technologies in ensuring security within electronic health was highlighted and proposes a Masked Authenticated Messaging (MAM) module of the IOTA protocol, which focuses on the transport of health activity data generated by wearable and embedded devices to a distributed ledger.

In order to handle the aim of protecting health information (PHI) generated by IoMT devices, Griggs et al. [109] proposed utilizing blockchain-based smart contracts to facilitate secure analysis and management of medical sensors. Using a private blockchain based on the Ethereum protocol.

Zhang et al. [110] proposed a BSPP scheme, blockchain-based secure and privacy-preserving personal health information (PHI) sharing scheme for diagnosis improvements in eHealth systems. The scheme is constructed using two blockchains, private blockchain for storing the PHI and consortium blockchain for maintaining the records of its secure indexes.

In a pioneer work carried out by Al Omar et al. [111], a MediBchain was presented, a patient-centric healthcare data management system by using blockchain as storage to attain privacy. Pseudonymity is ensured by using cryptographic functions to protect patients’ data.

While a lot of blockchain-based solutions for smart healthcare focusing on the nature of the network architecture as a first step toward ensuring patients’ privacy, some recent contributions give a particular attention to the protection of the communication contents and real identities of the nodes in a blockchain-based environment.

In this context, an interesting work was proposed in Ref. [112] where authors suggest a large-scale and efficient batch verification scheme based Elliptic Curve Digital Signature Algorithm (ECDSA) and group testing technology. Indeed, contrary to many recent propositions, this research paper does not only focus on improving the efficiency of batch verification algorithms but also considers the problem of invalid signatures identification. By doing so, this paper resolves the problem of performance degradation in case the batch verification fails. Another research work [113] emphasizes the importance of considering the open communication channel between patients and healthcare professionals in an (IoMT)-based environment. In particular, and based on the blockchain technology, authors propose a lightweight and reliable authentication protocol while trying to address the problem of physical layer security and over-centralized server in wireless medical sensor networks.

4.2.3. Third-Party Architecture. Herein, the main results of the papers where a public institution or a private corporation is responsible for the data management are given followed by a summarized illustration of the studies, as shown in Table 6.

In a work performed by Larrucea et al. [114], the Healthcare Industry architecture reference model was extended, with a set of tools dealing with consent management and data hiding tools, while considering the legal aspects such as general data protection regulation (GDPR).

In addition, a done made by Zhang et al. [115] proposes an efficient and privacy-preserving disease prediction system, called PPDP. In PPDP, patients’ historical medical data are encrypted and outsourced to the cloud server, which can be further utilized to train prediction models by using the Single-Layer Perceptron learning algorithm in a privacy-preserving way.

Moreover, the CP-ABSC scheme was proposed by Rao [116], a Ciphertext-Policy Attribute-Based Signcryption, with a public ciphertext verifiability framework, that achieves essential security goals of an attribute-Based Encryption (ABE) and Attribute-Based Signatures (ABS) schemes such as data confidentiality, unforgeability, and signcryption privacy.

4.2.4. Hybrid Architecture. In this section, results and analysis of the relevant papers that combine several architectures are given, while the main points and limitations of the related papers are summarized in Table 7.

In the research made by Chen et al. [117], a medical data information system model was proposed. The proposed model is based on blockchain, the Internet of Things, cloud storage, and proxy re-encryption algorithm to realize the reliable collection, safe storage, and sharing of medical data.

In another recent work done by Wang et al. [118], a novel handover authentication model of ITS with multi-server edge computing architecture was defined, a handover authentication scheme that allows the authenticated server to assist users to subsequently authenticate with another server and blockchain technology to preserve user’s privacy.

Furthermore, Ngabo et al. [119] proposed a public-permissioned blockchain security mechanism using the elliptic curve crypto (ECC) digital signature that supports a distributed ledger database to provide an immutable security solution, transaction transparency and prevent the patient electronic health records from tampering at the IoMT fog layer.

Healthcare facilities and insurance companies ought to guarantee authenticity before offering any assistance to an individual. Therefore, Al Omar et al. [120] had implemented a blockchain framework to safeguard patients’ sensitive data and insurance policy. They defined a solution for the healthcare system that provides data privacy and transparency. Data privacy is shielded with cryptographic
mechanisms, and insurance policies are included in blockchain via the Ethereum platform.

Moreover, Egala et al. [121] had introduced a blockchain-based novel architecture that affords a decentralized EHR and smart-contract-based service automation without settling with the system’s security and privacy. In the proposed architecture, they had proposed the hybrid computing model with the blockchain-based distributed data storage system to overcome blockchain-based cloud-centric IoMT healthcare system disadvantages.

In another work carried out by Robles et al. [122], a new trustworthy personal data protection mechanism was presented for well-being services, based on privacy-by-design technologies. This mechanism is based on Blockchain networks and indirection functions and tokens.

Besides, in a study reported by Sun et al. [123], lightweight policy-hiding ciphertext-policy attribute-based encryption CP-ABE scheme was defined, for the IoT-oriented smart health application.

Liu et al. [124] designed a cooperative privacy preservation scheme for wearable devices with identity authentication and data access control considerations in the time and space contexts. In the time-aware cloud computing mode, ciphertext policy attribute-based encryption is applied for
fine-grained access control, and a bloom filter is used to achieve an efficient data structure without privacy exposure. In the space-aware edge computing mode, secret sharing and MinHash-based authentication is designed to enhance privacy preservation along with similarity computing without revealing sensitive data.

Moreover, another research group Dwivedi et al. [125] proposed a modified blockchain model suitable for IoT devices that rely on their distributed nature and other additional privacy and security properties of the network to provide secure management and analysis of healthcare big data.

Furthermore, with the intent to support a tamper resistance feature, Thwin and Vasupongayya [126] proposed a blockchain-based personal health record system (PHR system). The proposed model employed proxy re-encryption and other cryptographic techniques to preserve privacy.

Natgunanathan et al. [127] proposed a location privacy protection mechanism in which location privacy is protected while maintaining the utility of the location data. The MPU has the necessary data and processing ability to decide whether the patient is in a critical state or not.

Several solutions have been introduced to control the consequence of attacks using the decentralized method, but these solutions somehow failed to assure the overall privacy of patient-centric systems. Therefore, Omar et al. [128] presented a patient-centric healthcare data management system that uses blockchain technology to store and protect their data. They use cryptographic functions to encrypt patients’ data and to ensure pseudonymity.

5. Discussion

This section aims at answering the research questions, by combining the different aforementioned privacy aspects. It should be noted that the systematic review results may have been impacted by multiple parts such as selection of databases, researchers’ ideas, and time restrictions.

RQ1: What are the proposed solutions to preserve privacy according to the different stakeholders’ needs while considering data-access management?

To answer this question, we combine stakeholders’ needs with data-access management. According to our study, few solutions (35%) are found to cover at least one stakeholder’s needs. Figure 7 shows that the most addressed stakeholder need by the studied papers is the patient preferences (35 publications), followed by the privacy policy (31 publications). The compliance with laws is the least addressed by papers (22 publications). Access control (28 publications) is the most used data access management technique in the currently proposed solutions for each stakeholder’s needs. Furthermore, smart contracts (20 publications) and cryptography (19 publications) have also emerged in the stakeholders’ needs.

RQ2: What are the privacy criteria that have been considered by the proposed solutions, and in which data life cycle phase?

The result of combining the privacy criteria and the data life cycle facets is shown in Figure 8. According to our analysis, we can observe the privacy criteria coverage by the different studies. Thus, the most covered criterion is the “information security (16.23%)” followed by the ‘Privacy compliance” criteria (12.52%). Moreover, Accuracy and quality (11.99%); Openness, transparency, and notice (11.52%); and Individual participation and access (11.4%) have also emerged in the whole data life cycle. This can be explained by the relationship between these principles and the most addressed data life cycle phases, such as storage and process. However, “Data minimization” (3.59%) is the least considered criterion.

It seems that few of the existing solutions (7%) address the whole data life cycle. Figure 9 shows that the most addressed data phase by the studied publications is the storage phase (75 publications), followed by the process phase (66 publications). The collection phase is the least enhanced by publications (20 publications).

RQ3: How and what are the techniques used by published papers to preserve privacy in smart healthcare, and in which architecture and category?

To answer the above research question, privacy-preserving techniques, category, and architecture used and reported in the reviewed studies are analyzed. As shown in Figure 10, cryptography is the dominant technique in most of the proposed solutions that helps to preserve privacy in several architectures. This blockchain-based category is used with 37% of the total publications.

Figure 11 shows that the most addressed architecture by the studied papers is the centralized architecture (58 publications), followed by the decentralized architecture (27 publications). Third-party architecture gives full trust to the third party for the whole data management and does not control data usage. Therefore, it is the least architecture (3 publications) addressed by the proposed solutions.

6. Toward a Holistic Approach to Preserve Privacy: Discussion and Future Directions

By integrating new and innovating technologies such as mobile and smart IoT solutions or favorizing decentralized healthcare systems over traditional health infrastructures, we guarantee that healthcare services are delivered faster and in an efficient way to patients. Still, as demonstrated throughout the proposed SLR, there are challenges to address, mainly the lack of a holistic approach that considers privacy all along the data lifecycle and the stakeholders’ needs.

Protecting patients from any privacy violation becomes even harder since privacy has to be taken into ground during the collection, transmission, usage, and storage of patient’s sensitive data. Nevertheless, what if we consider privacy even before developing such smart and innovative solutions? What if instead of trying harder to enhance actual smart IoT-based solutions for healthcare we emphasize the importance of privacy before even these systems come into existence?

We believe that privacy together with possible best practices to preserve it have to be designed before the development of smart solutions. To illustrate this, we consider
the classification previously suggested in section 2 (Fog/Edge/Cloud-based, blockchain-based, and policy-based) and we compare them according to the privacy-by-design principles. As stated in Ref. [129], the seven privacy-by-design principles are summarized in Table 8.

6.1. Discussion. Table 9 gives a clear picture of how the development in technologies for healthcare is significantly helping in protecting patients’ privacy. At the same time, these same technologies and new architectures need to be enhanced in order to meet patients’ privacy needs as well as the different stakeholders’ needs. We believe that it is a difficult equation to solve. Still, by encouraging organizations and project holders to follow best practices and raising their awareness about the different privacy risks, we guarantee that privacy risks and invasions can be reduced or prevented even before they happen. Therefore, the seven privacy-by-design principles were adopted as criteria or requirements that when met by a specific type of architecture (one of three proposed classes) reflects nothing but how much this architecture or solution considers the user’s privacy and also the other actors’ privacy needs. For instance, in cloud-based solutions by applying practices such as “least privilege,” which consists on granting only the required permissions to complete a task, we prevent unauthorized access which then leads to a proactive approach (P1). From another line, Cloud providers such as Amazon Web Services (AWS) make security a shared responsibility between the service provider and the service consumer. This makes the design of privacy aligned with a win-win approach (P3).

In blockchain-based solutions, the fidelity and security of data are guaranteed, and trust is generated without the need for a trusted third party. This makes the exchange of private data performed in a transparent manner (P6). In addition to that, the architecture of a blockchain network and the adoption of schemes such as Zero-knowledge proof make this kind of solution highly secure while preserving user privacy (P3). To achieve this, data owners’ privacy is protected by the use of encrypted keys instead of divulging the real identity of users (P7).

In policy-based solutions, the way patients’ data are collected, stored, and shared is detailed by the means of formalized policies/preferences. Hence, patients can be reassured about who, when, and how these data are being used, stored, and shared (P6). Notably, the most important parameter in the third class (policy-based solution) is policy/preferences. That said, by involving the patient in the decision-making, we are indirectly protecting him or her from unauthorized use or disclosure (P7).

6.2. Recommendations and Future Directions. Health data are very private and can have a huge impact on patients’
health and outcomes. Hence, and in order to be reassured about the safety of their data, patients have the right to know what and how much data are collected, why are collected, and for what purposes these data are going to be used for. As a first step toward this aim, patients’ privacy preferences have to be well explained, formalized, and then shared across all the involved parties. Notably, both patients’ and third parties’ policies have to be accessible, clear, and regularly updated.

Next, as a second-best recommendation, it is of utmost importance to identify third parties that have access to patients’ data, especially when data are gathered from different sources. For instance, in IoT-based health solutions, medical data are generated from different wearable IoT devices and are then sent to different sources for processing and storage. Therefore, and since it is directly related to a patient’s life, these data have to be carefully used and shared \[119\]. Indeed, as stated in Ref. \[130\], Blockchain is a good solution to safeguard sensitive medical data generated by these IoT devices. First, thanks to its nature of decentralization, data are not owned nor managed by one single entity. Second, and particularly in private blockchains, it is possible to control who can access the blockchain network and may also control the type of access rights each entity has. Above this, personal data have to be kept anonymous so that they cannot be divulged—by mistake—to a specific person.

Apart from restricting access to patients’ data and respecting patients’ preferences when using and sharing data, it is highly recommended not to ask for more information than necessary from patients. These kinds of practices are strongly considered in healthcare cloud-based solutions.
Privacy-preserving Techniques

- Access Control
- Anonymization
- Cryptography
- Blockchain

Centralized 58%
Decentralized 27%
Hybrid 12%
Third Party 3%

Figure 10: Papers distribution by the privacy-preserving techniques, categories, and architectures.

Figure 11: Storage architecture VS Number of Publications.

Table 8: Summary of the seven privacy-by-design principles.

| The principal                          | Definition                                                                                                                                 |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Proactive not reactive                 | It refers to the ability of a system to anticipate and prevent privacy risks before they happen                                           |
| Privacy as the default setting         | This principle seeks to ensure a higher degree of personal data protection by enforcing privacy default settings.                           |
| Privacy embedded into design           | This way, privacy remains intact even if the user does not follow any privacy practices                                                  |
| Positive-sum, not zero-sum             | This principle means that privacy has to be considered as an essential component or functionality of any system                             |
| End-to-end security                    | Designing privacy follows a “win-win” approach where privacy can be reached by compromising other concepts. (e.g., security)            |
| Visibility and transparency            | This principle means that security, considered as an important concept for protecting patients’ data, has to be taken into grounded during the entire lifecycle of the data, from start to finish. |
| Respect for user privacy               | By respecting this principle, we make sure that all stakeholders are able to see how information moves through the system                |
|                                        | This principle encourages organizations and solution architects to design user-centric solutions where both the owner of data as well as the other stakeholders play an active role |
In this research, we conducted a Systematic Literature Review (SLR), where we presented an exhaustive study of the existing privacy-preserving solutions in the smart healthcare environment. By analyzing the content of the primary studies based on several aspects, i.e., the implemented privacy techniques, privacy principles, IoMT architecture, stakeholders’ needs, etc., the designated research questions were answered. The findings of this study revealed that among one hundred primary studies, more than 70 percent had neglected the stakeholders’ needs, especially the compliance with patient privacy preferences and privacy laws; moreover, the data collection is the least considered phase, which translates the neglecting of the two criteria: data collection limitation and data minimization. Many other limitations are cited in the previous sections, which all point out the lack of a holistic approach that aims to preserve privacy all along the data life cycle and according to the different stakeholders’ needs. We believe that our systematic literature review will be of great help to researchers targeting privacy preservation in the IoMT field, as they can rely on the aforementioned limitations, to propose further scientific contributions.

In our ongoing research, we aim to propose a blockchain-based solution for privacy-preserving in IoMT, which overcomes the limitations of the prior solutions and considers the whole privacy aspects adopted in the previous analysis, to ensure full coverage of privacy and security.

### Data Availability

The data used to support the findings of this paper are available from the corresponding author upon request.

### Conflicts of Interest

The authors declare that they have no conflicts of interest.

### Table 9: Comparison of the categories of MIoT and the privacy-by-design principles.

| Class          | P1 | P2   | P3    | Principle | P4 | P5 | P6 | P7 |
|----------------|----|------|-------|-----------|----|----|----|----|
| Cloud-based    | +  |    - |       | +/-       | +  |    - | +/- |   |
| Blockchain-based| +  | +/−  |       |           | +  |    - | +/- |   |
| Policy-based   | +/-|      |       |           | +  |    - | +/- |   |

### References

[1] N. Dilawar, M. Rizwan, and F. Ahmad, “Blockchain: securing internet of medical things (IoMT),” *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 1, p. 31, 2019.

[2] Y. Xiao and M. Watson, “Guidance on conducting a systematic literature review,” *Journal of Planning Education and Research*, vol. 39, no. 1, pp. 93–112, 2019.

[3] S. S. Hameed, W. H. Hassan, L. A. Latiff, and F. Ghabban, “A systematic review of security and privacy issues in the internet of medical things: the role of machine learning approaches,” *Peer J Comput. Sci.*, vol. 7, p. e414, 2021.

[4] M. Tanriverdi, “A systematic review of privacy preserving healthcare data sharing on blockchain,” *Journal of Cybersecurity and Information Management*, vol. 5, pp. 31–37, 2020.

[5] L. H. Iwaya, A. Ahmad, and M. A. Babar, “Security and privacy for mHealth and uHealth systems: a systematic mapping study,” *IEEE Access*, vol. 8, pp. 150081–150112, 2020.

[6] J. J. Hathaliya and S. Tanwar, “An exhaustive survey on security and privacy issues in Healthcare 4.0,” *Computer Communications*, vol. 153, pp. 311–335, 2020.

[7] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, “Security and privacy in the medical internet of things: a review,” *Security and Communication Networks*, vol. 2018, Article ID e5978636, 9 pages, 2018.

[8] Z. El Ouazzani, H. El Bakkali, and S. Sadki, “Privacy preserving in digital health: main issues, technologies, and solutions,” *Research Anthology on Privatizing and Securing Data*, IGI Global, Hershey, Pennsylvania, pp. 1503–1526, 2021.

[9] W. Fang, X. Z. Wen, Y. Zheng, and M. Zhou, “A survey of big data security and privacy preserving,” *IEEE Technical Review*, vol. 34, no. 5, pp. 544–560, 2017.

[10] C. S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand, “Security techniques for the electronic health records,” *journal of Medical Systems*, vol. 41, no. 8, p. 127, 2017.

[11] Z. El Ouazzani and H. El Bakkali, “A classification of non-cryptographic anonymization techniques ensuring privacy in big data,” *International Journal of Communication Networks and Information Security*, vol. 12, pp. 142–152, 2020.

[12] D. Preethi, N. Khare, and B. K. Tripathy, “Security and privacy issues in blockchain technology,” in *Blockchain Technology and the Internet of Things*, Apple Academic Press, New Jersey, NJ, USA, 2020.

[13] Risk Based Security, “2021 Mid year data breach QuickView report,” Risk Based Security, Richmond, VA, USA, https://pages.riskbasedsecurity.com/hubsfs/Reports/2021%20Mid%20Year%20Data%20Breacht%20QuickView%20Report.pdf, 2021.

[14] M. Verdonck and G. Poels, “Decentralized Data Access with IPFS and Smart Contract Permission Management for Electronic Health Records,” in *Proceedings of the...*
G. Eysenbach, “What is e-health?” Journal of Medical Internet Research, vol. 3, no. 2, p. e833, 2001.

Indicato Metadata Registry Details, “Indicator Metadata Registry Details,” 2021, https://www.who.int/data/gho/indicator-metadata/irmr-details/4774.

M. T. de Oliveira, H.-V. Dang, L. H. A. Reis, H. Zhong, Y. Zhou, Q. Zhang, and Y. Xu, J. Cui, “An efficient medical records,” in Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, pp. 113–115, New York, NY, USA, June 2015.

P. Shalini, D. Dharmin, P. Reema, and D. Nishant, “Security and privacy issues in cloud, fog and edge computing,” Procedia Computer Science, vol. 160, pp. 734–739, 2019.

D. C. Kloneff, “Fog computing and edge computing architectures for processing data from diabetes devices connected to the medical internet of things,” J Diabetes Sci Technol, vol. 11, no. 4, pp. 647–652, 2017.

D. E. Majdoubi and H. E. Bakkali, “A survey of major data privacy laws, languages and approaches in smart cities environments,” in Proceedings of the 4th International Conference on Smart City Applications, pp. 1–8, New York, NY, USA, October 2019.

The four most internationally significant recent privacy laws, “The four most internationally significant recent privacy laws,” TechGenix, vol. 26, 2019.

Online Browsing Platform, “Online Browsing Platform (OBP),” 2021, https://www.iso.org/obp/ui.

P. Kumar and L. Chouhan, “A privacy and session key based authentication scheme for medical IoT networks,” Computer Communications, vol. 166, pp. 154–164, 2021.

M. T. de Oliveira, H.-V. Dang, L. H. A. Reis, H. A. Marquering, and S. D. Olabarriaga, “AC-AC: Dynamic revocable access control for acute care teams to access medical records,” Smart Health, vol. 20, Article ID 100190, 2021.

H. Zhong, Y. Zhou, Q. Zhang, and Y. Xu, J. Cui, “An efficient and outsourcing-supported attribute-based access control scheme for edge-enabled smart healthcare,” Future Generation Computer Systems, vol. 115, pp. 486–496, 2021.

J. A. Onesimiu, J. Karthikeyan, and Y. Sei, “An efficient clustering-based anonymization scheme for privacy-preserving data collection in IoT based healthcare services,” Peer-to-Peer Netw., Peer-to-Peer Netw Appl, vol. 14, no. 3, pp. 1629–1649, 2021.

S. Izza, M. Benssalah, and K. Drouiche, “An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment,” Journal of Information Security and Applications, vol. 58, Article ID 102705, 2021.

M. N. Alraja, H. Barhamgi, A. Rattrout, and M. Barhamgi, “An integrated framework for privacy protection in IoT—applied to smart healthcare,” Computers & Electrical Engineering, vol. 91, Article ID 107060, 2021.

A. Singh and K. Chatterjee, “Securing smart healthcare system with edge computing,” Computers & Security, vol. 108, Article ID 102353, 2021.

J. Sun, D. Chen, N. Zhang et al., “A privacy-aware and traceable fine-grained data delivery system in cloud-assisted healthcare IIoT,” IEEE Internet of Things Journal, vol. 8, no. 12, pp. 10034–10046, 2021.

A. Sathyas and S. K. S. Raja, “Privacy preservation-based access control intelligence for cloud data storage in smart healthcare infrastructure,” Wireless Personal Communications, vol. 118, no. 4, pp. 3595–3614, 2021.

S. O. Ogundoyin and I. A. Kamal, “PAASH: a privacy-preserving authentication and fine-grained access control of outsourced data for secure smart health in smart cities,” Journal of Parallel and Distributed Computing, vol. 155, pp. 101–119, 2021.

A. Vineela, N. Kasiviswanath, and C. Shobabindu, “Theoretical analysis on applications aspects of smart materials preserving the security and privacy in medical big data and cloud,” Materials Today Proceedings, 2021.

T. Zhou, J. Shen, D. He, P. Vijayakumar, and N. Kumar, “Human-in-the-Loop-Aided privacy-preserving scheme for smart healthcare,” IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 6, pp. 1–10, 2020.

A. Krall, D. Einke, and H. Yang, “Mosaic privacy-preserving mechanisms for healthcare analytics,” IEEE Journal of Biomedical and Health Informatics, vol. 25, no. 6, pp. 2184–2192, 2021.

A. Hussain Seh, J. F. Al-Amri, A. F. Subahi, A. Agrawal, R. Kumar, and R. Ahmad Khan, “Machine learning based framework for maintaining privacy of healthcare data,” Intelligent Automation & Soft Computing, vol. 29, no. 3, pp. 697–712, 2021.

D. He, R. Ye, S. Chan, M. Guizani, and Y. Xu, “Privacy in the internet of things for smart healthcare,” IEEE Communications Magazine, vol. 56, no. 4, pp. 38–44, 2018.

A. Ibaida, A. Abuadhbba, and N. Chilamkurti, “Privacy-preserving compression model for efficient IoMT ECG sharing,” Computer Communications, vol. 166, pp. 1–8, 2021.

H. A. El Zouka, M. M. Hosni, Secure IoT communications for smart healthcare monitoring system,” Internet of Things, vol. 13, Article ID 100036, 2021.

M. Ma, D. He, S. Fan, and D. Feng, “Certificateless searchable public key encryption scheme secure against keyword guessing attacks for smart healthcare,” Journal of Information Security and Applications, vol. 50, Article ID 102429, 2020.

R. Jayaram, S. Prabakaran, Onboard disease prediction and rehabilitation monitoring on secure edge-cloud integrated privacy preserving healthcare system,” Egyptian Informatics Journal, vol. 22, 2020.

C. Ge, C. Yin, Z. Liu, L. Fang, J. Zhu, and H. Ling, “A privacy preserve big data analysis system for wearable wireless sensor network,” Computers & Security, vol. 96, Article ID 101887, 2020.

W. Hurst, A. Boddy, M. Merabti, and N. Shone, “Patient privacy violation detection in healthcare critical infrastructures: an investigation using density-based benchmarking,” Future Internet, vol. 12, p. 100, 2020.

M. A. Abdou, A. A. Abdel-Hamid, and H. A. Elzouka, “A cloud-based mobile healthcare monitoring framework with location privacy preservation,” in Proceedings of the 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), pp. 1–8, Sakheer, Bahrain, December 2020.

S. D. Kaul, V. K. Murty, and D. Hatzinakos, “Secure and privacy preserving biometric based user authentication with data access control system in the healthcare environment,” in Proceedings of the 2020 International Conference on Cyberworlds (CW), pp. 249–256, Caen, France, September 2020.
R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, and F. Titouna, “A privacy-preserving cryptosystem for IoT E-healthcare,” *Information Sciences*, vol. 527, pp. 493–510, 2020.

J. J. Hathaliya, S. Tanwar, and R. Evans, “Securing electronic healthcare records: a mobile-based biometric authentication approach,” *Journal of Information Security and Applications*, vol. 53, Article ID 102528, 2020.

J. J. Hathaliya, S. Tanwar, S. Tyagi, and N. Kumar, “Securing electronics healthcare records in Healthcare 4.0: a biometric-based approach,” *Computers & Electrical Engineering*, vol. 76, pp. 398–410, 2019.

Y. Xie, X. Li, S. Zhang, and Y. Li, “ICLASS: an improved certificateless aggregate signature scheme for healthcare wireless sensor networks,” *IEEE Access*, vol. 7, pp. 15170–15182, 2019.

M. A. Azad, I. Arshad, S. Mahmoud, K. Salah, and M. Imran, “A privacy-preserving framework for smart context-aware healthcare applications,” *Transactions on Emerging Telecommunications Technologies*, Article ID e3634, 2019.

B. D. Deebak, F. Al-Turjman, M. Aloqaily, and O. Alfandi, “An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT,” *IEEE Access*, vol. 7, pp. 135632–135649, 2019.

Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, “Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system,” *Information Sciences*, vol. 479, pp. 567–592, 2019.

Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, “Privacy-preserving fusion of IoT and big data for e-health,” *Future Generation Computer Systems*, vol. 86, pp. 1437–1455, 2019.

S. F. Aghili, H. Mala, P. Kaliyar, and M. Conti, “SecLAP: Secure and lightweight RFID authentication protocol for Medical IoT,” *Future Generation Computer Systems*, vol. 101, pp. 621–634, 2019.

E. Greene, P. Proctor, and D. Kotz, “Secure sharing of mHealth data streams through cryptographically-enforced access control,” *Smart Health*, vol. 12, pp. 49–65, 2019.

R. Ding, H. Zhong, J. Ma, X. Liu, and J. Ning, “Lightweight privacy-preserving identity-based verifiable IoT-based health storage system,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8393–8405, 2019.

J. W. Kim, K. Edemacu, and B. Jang, “MPPDS: Multilevel privacy-preserving data sharing in a collaborative eHealth system,” *IEEE Access*, vol. 7, pp. 109910–109923, 2019.

P. Huang, L. Guo, M. Li, and Y. Fang, “Practical privacy-preserving ECG-based authentication for IoT-based healthcare,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9200–9210, 2019.

Q. Wang, D. Zhou, S. Yang, P. Li, C. Wang, and Q. Guan, “Privacy preserving computations over healthcare data,” in *Proceedings of the 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 635–640, Atlanta, GA, USA, July 2019.

X. Wang, L. Wang, Y. Li, and K. Gai, “Privacy-aware efficient fine-grained data access control in internet of medical things based fog computing,” *IEEE Access*, vol. 6, pp. 47657–47665, 2018.

Y. Zhang, P. Lang, D. Zheng, M. Yang, and R. Guo, “A secure and privacy-aware smart health system with secret key leakage resilience,” *Security and Communication Networks*, vol. 2018, Article ID e7205298, 13 pages, 2018.

H. Kaur, N. Kumar, and S. Batra, “An efficient multi-party scheme for privacy preserving collaborative filtering for healthcare recommender system,” *Future Generation Computer Systems*, vol. 86, pp. 297–307, 2018.

J. Vora, I. Prit, S. Tyagi, N. Kumar, M. Obaidat, and K. F. Hsiao, “Ensuring privacy and security in E-health records,” in *Proceedings of the 2018 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp. 1–5, Alasce, Colmar, France, July 2018.

M. Elhoseny, G. Ramirez-Gonzalez, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, “Secure medical data transmission model for IoT-based healthcare systems,” *IEEE Access*, vol. 6, pp. 20596–20608, 2018.

J. Maria de Fuentes, L. Gonzalez-Manzano, A. Solanas, and F. Veseli, “Attribute-based credentials for privacy-aware smart health services in IoT-based smart cities,” *Computer*, vol. 51, no. 7, pp. 44–53, 2018.

Y. Zhang, D. Zheng, and R. H. Deng, “Security and privacy in smart health: efficient policy-hiding attribute-based access control,” *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2130–2145, 2018.

Y. Zhang, R. H. Deng, G. Han, and D. Zheng, “Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things,” *Journal of Network and Computer Applications*, vol. 123, pp. 89–100, 2018.

D. Zheng, A. Wu, Y. Zhang, and Q. Zhao, “Efficient and privacy-preserving medical data sharing in internet of things with limited computing power,” *IEEE Access*, vol. 6, pp. 28019–28027, 2018.

L. Zhang, Y. Zhang, S. Tang, and H. Luo, “Privacy protection for E-health systems by means of dynamic authentication and three-factor key agreement,” *IEEE Transactions on Industrial Electronics*, vol. 65, no. 3, pp. 2795–2805, 2018.

J. W. Kim, B. Jang, and H. Yoo, “Privacy-preserving aggregation of personal health data streams,” *PLOS ONE*, vol. 13, no. 11, Article ID e0207639, 2018.

S. Sharma, K. Chen, and A. Sheth, “Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems,” *IEEE Internet Computing*, vol. 22, no. 2, pp. 42–51, 2018.

Y. O’Connor, W. Rowan, L. Lynch, and C. Heavin, “Privacy by design: informed consent and internet of things for smart health,” *Procedia Computer Science*, vol. 113, pp. 653–658, 2017.

H. A. Al Hamid, S. S. M. Rahman, M. S. Hossain, A. Almogren, and A. Alamri, “A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography,” *IEEE Access*, vol. 5, pp. 22313–22328, 2017.

M. Z. A. Bhuiyan, M. Zaman, G. Wang, T. Wang, and J. Wu, “Privacy-protected data collection in wireless medical sensor networks,” in *Proceedings of the 2017 International Conference on Networking, Architecture, and Storage (NAS)*, pp. 1–2, Shenzhen, China, August 2017.

J. Liu, J. Ma, W. Wu, X. Chen, X. Huang, and L. Xu, “Protecting mobile health records in cloud computing: a secure, efficient, and anonymous design,” *ACM Transactions on Embedded Computing Systems*, vol. 16, no. 2, pp. 1–20, 2017.
[87] L. Yang, Q. Zheng, and X. Fan, "RSPP: A reliable, searchable and privacy-preserving e-healthcare system for cloud-assisted body area networks," in *Proceedings of the IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, pp. 1–9, Atlanta, GA, USA, May 2017.

[88] F. Rahman, M. Z. A. Bhuiyan, and S. I. Ahamed, “A privacy preserving framework for RFID based healthcare systems,” *Future Generation Computer Systems*, vol. 72, pp. 339–352, 2017.

[89] Y. Zhang, J. Li, D. Zheng, X. Chen, and H. Li, “Towards privacy protection and malicious behavior traceability in smart health,” *Personal and Ubiquitous Computing*, vol. 21, no. 5, pp. 815–830, 2017.

[90] J. Iqbal, M. Adnan, Y. Khan et al., “Designing a healthcare-enabled software-defined wireless body area network architecture for secure medical data and efficient diagnosis,” *Journal of Healthcare Engineering*, vol. 2022, Article ID 9210761, 19 pages, 2022.

[91] R. Bharti, A. Khamparia, M. Shabaz, G. Dhiman, S. Pande, C. Zhang, C. Xu, K. Sharif, and L. Zhu, “Privacy-preserving healthcare system for cloud-empowered secure data management and Graph Convolutional Network enabled anomaly detection in smart healthcare,” *Journal of Parallel and Distributed Computing*, vol. 142, pp. 1–12, 2020.

[92] Z. Wang, N. Luo, and P. Zhou, “GuardHealth: blockchain empowered secure data management and Gra...
A. Zhang and X. Lin, “Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain,” *Journal of Medical Systems*, vol. 42, no. 8, pp. 1–18, 2018.

A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, “MediBchain: a blockchain based privacy preserving platform for healthcare data,” in *Proceedings of the International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, pp. 534–543, Guangzhou, China, December 2017.

H. Xiong, C. Jin, M. Alazab et al., “On the design of blockchain-based ECDSA with fault-tolerant batch verification protocol for blockchain-enabled IoMT,” *IEEE Journal of Biomedical and Health Informatics*, 2021.

C. Zhang, L. Zhu, C. Xu, and R. Lu, “A transparent and privacy-preserving healthcare platform with novel smart contract for smart cities,” *IEEE Access*, vol. 9, pp. 90738–90749, 2021.

B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, “Fortified-chain: a blockchain-based framework for security and privacy-ensured internet of medical things with effective access control,” *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11717–11731, 2021.

T. Robles, B. Bordel, R. Alcarria, and D. Sánchez-de-Rivera, “Enabling trustworthy personal data protection in eHealth and well-being services through privacy-by-design,” *International Journal of Distributed Sensor Networks*, vol. 16, no. 5, Article ID 1550147720911210, 2020.

H. Liu, X. Yao, T. Yang, and H. Ning, “Cooperative privacy preservation for wearable devices in hybrid computing-based smart health,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1352–1362, 2019.

A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, “A decentralized privacy-preserving healthcare blockchain for IoT,” *Sensors*, vol. 19, no. 2, Article ID 2, 2019.

T. T. Thwin and S. Vasupongayya, “Blockchain-based access control model to preserve privacy for personal health record systems,” *Security and Communication Networks*, vol. 2019, Article ID e8315614, 15 pages, 2019.

I. Natgunanathan, A. Mehmoody, X. Xiang, L. Gao, and S. Yu, “Location privacy protection in smart health care system,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3055–3069, 2019.

A. A. Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, “Privacy-friendly platform for healthcare data in cloud based on blockchain environment,” *Future Generation Computer Systems*, vol. 95, pp. 511–521, 2019.

F. Khan, J. H. Kim, L. Mathiassen, and R. Moore, “Data breach management: an integrated risk model,” *Information & Management*, vol. 58, no. 1, Article ID 103392, 2021.