blockchains

MDPI

Review

Blockchain-Based Privacy-Enhancing Federated Learning in Smart Healthcare: A Survey

Zounkaraneni Ngoupayou Limbepe [1], Keke Gai [1,*] and Jing Yu [2,*]

[1] School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing 100081, China; ngoupayou.limbepe@bit.edu.cn
[2] School of Information Engineering, Minzu University of China, Beijing 100081, China
* Correspondence: gaikeke@bit.edu.cn (K.G.); jing.yu@muc.edu.cn (J.Y.)

Abstract: Federated learning (FL) has emerged as an efficient machine learning (ML) method with crucial privacy protection features. It is adapted for training models in Internet of Things (IoT)-related domains, including smart healthcare systems (SHSs), where the introduction of IoT devices and technologies can arise various security and privacy concerns. However, as FL cannot solely address all privacy challenges, privacy-enhancing technologies (PETs) and blockchain are often integrated to enhance privacy protection in FL frameworks within SHSs. The critical questions remain regarding how these technologies are integrated with FL and how they contribute to enhancing privacy protection in SHSs. This survey addresses these questions by investigating the recent advancements on the combination of FL with PETs and blockchain for privacy protection in smart healthcare. First, this survey emphasizes the critical integration of PETs into the FL context. Second, to address the challenge of integrating blockchain into FL, it examines three main technical dimensions such as blockchain-enabled model storage, blockchain-enabled aggregation, and blockchain-enabled gradient upload within FL frameworks. This survey further explores how these technologies collectively ensure the integrity and confidentiality of healthcare data, highlighting their significance in building a trustworthy SHS that safeguards sensitive patient information.

Keywords: federated learning; privacy protection; blockchain; privacy enhancing technologies; smart healthcare

Academic Editor: Hamed Taherdoost

Received: 5 November 2024
Revised: 21 December 2024
Accepted: 24 December 2024
Published: 1 January 2025

Citation: Ngoupayou Limbepe, Z.; Gai, K.; Yu, J. Blockchain-Based Privacy-Enhancing Federated Learning in Smart Healthcare: A Survey. *Blockchains* **2025**, *3*, 1. https://doi.org/10.3390/blockchains3010001

1. Introduction

In the digital era, the adoption of IoT technologies has catalyzed a transformative shift in various sectors, most notably in healthcare. The burgeoning network of interconnected devices, collectively known as the *Internet of Medical Things* (IoMT), has fundamentally enhanced the capabilities of *smart healthcare systems* (SHSs) by enabling sophisticated data analytics and real-time patient monitoring [1–3]. With an estimated 30 billion IoT devices projected by 2030 [4,5], the healthcare sector is on the brink of a data revolution, poised to significantly improve medical diagnostics and patient care through *Artificial Intelligence* (AI) and *machine learning* (ML) [6].

However, the exponential growth of data within SHSs introduces complex privacy and security challenges [7]. The highly sensitive nature of personal health information requires robust mechanisms to protect data against unauthorized access and breaches, in accordance with strict regulations like the *General Data Protection Regulation* (GDPR) [8] and the *Health Insurance Portability and Accountability Act* (HIPAA) [9]. In response, FL [10] has emerged as an innovative solution that enables decentralized model training on diverse

devices without the need to share their sensitive raw data. Although it inherently embraces privacy by design, solely relying on its basic privacy features proves insufficient to ensure comprehensive privacy in smart healthcare [11]. According to [12,13], FL is vulnerable to attacks such as membership inference [14,15], model reconstruction [8,16], and model inversion [8,17], which can lead to significant privacy risks. In addition, the introduction of FL into SHSs also raises some privacy concerns [18]. To enhance its privacy-preserving capabilities, the augmentation of FL with advanced technologies like *Differential Privacy* (DP), *Homomorphic Encryption* (HE), and *Secure Multi-Party Computation* (SMPC) upon the concept of *Privacy-Preserving Federated Learning* (PPFL) is actively explored [19]. PPFL has thus evolved into a compelling paradigm for enhancing both privacy and security in SHSs [7,20]. Moreover, blockchain [21–23] with its features seems to be another serious option for enhancing both privacy and security in an FL context. In fact, incorporating blockchain into FL enhances privacy and trust throughout the process, especially in sensitive operations involving health data [24]. Blockchain technology augments FL by providing an immutable, transparent ledger for gradients upload, aggregation processes, and model storage, thus enhancing trust and privacy assurance throughout the FL lifecycle.

Although the potential advantages of integrating FL with PETs and blockchain for privacy protection in SHSs are considerable, significant challenges remain. On one hand, the challenge lies in the diversity of privacy threats in SHSs and the rapidly increasing number of new threats. For instance, the adoption of FL-enabled SHS introduces numerous privacy threats arising from both technical vulnerabilities and malicious users. On the other hand, the challenge aligns with the technical intricacies associated with seamlessly integrating these technologies into SHSs for privacy protection. Actually, it is crucial to investigate the best possible combination between these technologies to mitigate the effects of threats on user privacy by considering factors such as compatibility, efficiency, and communication overhead. Therefore, it is important to explore how PETs and blockchain mechanisms can empower FL for privacy protection, particularly in the burgeoning landscape of smart healthcare. In this regard, addressing these challenges requires not only technological innovation but also a reevaluation of regulatory frameworks to facilitate the effective adoption of these advanced solutions [25].

Motivated by the promising features and recent developments of FL, researchers have conducted many studies to survey the potential of integrating PETs and blockchain to enhance privacy protection in FL-based systems including FL-based smart healthcare. For example, the work in [26] reviewed the applications of FL in healthcare, highlighting its effectiveness across several domains such as mammogram analysis, COVID-19 classification, and wearable health monitoring. However, it does not explore the potential of the integration of PETs and blockchain with FL to enhance its privacy capacity in SHSs. Similarly, the works in [27,28] have explored the potential of combining FL with PETs for privacy enhancement, but the study does not explore the application in SHSs. In addition, ref. [29] comprehensively surveyed the application of FL in SHSs, highlighting its ability to enhance privacy in remote health monitoring, medical imaging, COVID-19 detection and electronic health records. However, it lacks emphasizing the potential of integrating FL with PETs and blockchain, which could significantly enhance data privacy and security in SHSs. In the work by [12], a systematic review of privacy-preserving methods that integrate blockchain and FL in telemedicine is provided, highlighting their potential to enhance data security and trustworthiness in remote healthcare systems. However, the study does not adequately explore the implications of combining PETs with these frameworks, which could further strengthen privacy measures and address existing vulnerabilities in SHSs. The summary of the comparison with other surveys is given in Table 1.

Table 1. Existing surveys and our contributions.

Ref.	FL-SHSs	PETs-FL	BC-FL	PETs and BC-FL in SHSs	Contributions
Briggs *et al.* [27]	✗	✓	✗	✗	A review of PPFL in IoT environments, emphasizing methods for enhancing privacy.
Moon *et al.* [26]	✓	✓	✗	✗	A comprehensive review of FL applications in healthcare, highlighting its role in privacy-preserving medical imaging and wearable healthcare systems.
Yin *et al.* [28]	✗	✓	✓	✗	A comprehensive survey on PPFL, proposing a novel 5W-scenario-based taxonomy to systematically analyze privacy risks.
Nguyen *et al.* [29]	✗	✓	✗	✗	A survey of PPFL emphasizing compliance with GDPR requirements.
Hiwale *et al.* [12]	✓	✓	✓	✗	A review of PP methods integrating blockchain and FL, analyzing their applications in telemedicine.
Our survey	✓	✓	✓	✓	A comprehensive survey on PETs and blockchain-based methods in SHSs, emphasizing blockchain–FL and PETs' ability to protect privacy in SHSs, especially for health data management, remote health monitoring, medical imaging, and health finance management.

Notations: FL-SHSs: FL-enabled SHSs; PETs-FL: PETs-enabled FL; BC-FL: blockchain-enabled FL; GDPR: General Data Protection Regulation.

Given the aforementioned limitations of existing surveys and the fast-ever development of FL, we find it necessary to conduct a comprehensive survey that reviews the most recent findings, identifies the gap, and suggests the future research directions related to PPFL in SHSs. Therefore, this survey uniquely examines the technical integration of PETs and blockchain in FL frameworks, providing a comprehensive analysis of how these technologies can collectively enhance privacy and security in SHSs. We first review the privacy concerns in SHSs and find out a classification of privacy threats. Then, we conduct an extensive review of PPFL and its integration in SHSs. We finally examine the potential of the integration of blockchain and PETs with FL to enhance privacy in SHSs. We focus on some specific applications of smart healthcare such as health data management, remote health management, medical imaging, and health finance management.

Through a systematic exploration of current studies and emerging technologies, this work aims to spur further research into robust, efficient, and scalable privacy-preserving frameworks, contributing to the evolution of smart healthcare into a domain where cutting-edge technology and stringent privacy protection coexist harmoniously.

This survey is built based on two main dimensions as shown in Figure 1: the augmentation of FL with PETs for enhancing privacy protection, and its integration with blockchain to further secure and decentralize healthcare data processes.

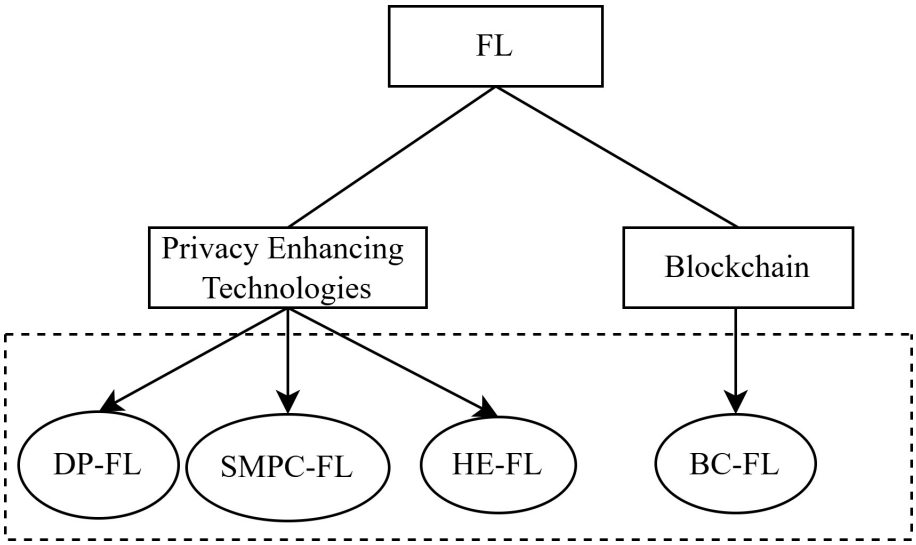

Figure 1. Survey map.

This work's contributions are fourfold:

- We investigate the main privacy threats currently in SHSs, elaborate on the main FL-based privacy mechanisms in SHSs, and propose a taxonomy of FL-based privacy mechanisms developed in recent studies.
- This survey meticulously explores the intersection of FL with DP, HE, and SMPC within SHSs. It outlines key contributions and performs a comparative analysis that focuses on privacy, scalability, computational efficiency, and the pros and cons of each technology, aiming to build robust and reliable SHSs.
- The survey analyzes the cutting-edge developments in integrating blockchain technology with PPFL within SHSs. We use three key technical dimensions: model storage, gradient upload, and aggregation, to succinctly summarize contemporary advancements and organize the discussion. In addition, we compare recent significant studies on the integration of blockchain technology in PPFL, evaluating each based on its respective advantages and limitations.
- Finally, we identify current deficiencies of PPFL and propose potential avenues for future research.

To ensure a comprehensive understanding of the intersection between FL, PETs, and blockchain in SHS, our survey is based on the literature published between 2018 and 2024. We consulted databases such as ACM Digital Library, IEEE Xplore, Scopus, and PubMed using keywords related to our core topics. Studies were included based on criteria such as relevance to the SHSs context, focus on privacy and security aspects, and use of FL, PETs, or blockchain. Data extraction focused on methods used, findings related to the effectiveness of technology implementations, and identified challenges. This approach allowed us to analyze trends and gaps in the current research landscape systematically. Table 2 presents the key acronyms used in this survey.

The organization of the remainder of this survey follows a logical structure starting with a discussion on privacy challenges in SHS in Section 2, followed by an overview of FL and its integration into SHS in Section 3. We then examine the major privacy-enhancing technologies integrated with FL aimed at increasing privacy preservation in smart healthcare in Section 4. Additionally, a study of existing works concerning the integration of blockchain in PPFL based on three technical dimensions is provided in Section 5. Discussions and future work are given in Section 6, and we conclude this survey in Section 7.

Table 2. List of key acronyms.

Acronyms	Definitions
FL	Federated Learning.
SHS	Smart Healthcare System.
PPFL	Privacy-Preserving FL.
PETs	Privacy-Enhancing Techniques.
DLT	Distributed Ledger Technology.
DP	Differential Privacy.
HE	Homomorphic Encryption.
BC	Blockchain.
SMPC	Secure Multiparty Computation.

2. Privacy Concerns in Smart Healthcare

In this section, we review the key concepts of privacy and address the privacy threats in SHSs. We start by clearly defining the concept of privacy and classifying privacy in SHSs. We then discuss the privacy threats in SHSs and provide a relevant classification.

Modern technologies have profoundly transformed healthcare systems, enhancing their efficiency, improving patient care, and also accelerating research in medical fields. In fact, wearable technology, *electronic health records* (EHRs) [3], and IoT devices are among the technologies upon which smart healthcare is built. These technologies generate a plethora of data that can be used for personalized treatment recommendations, illness diagnosis, remote health monitoring, enhancing elderly care, and predictive analytics [30,31]. These innovations, underpinned by IoT sensor technology [21,32], play a pivotal role in enabling smart hospital services and remote health monitoring, fundamentally redefining healthcare delivery [33–35].

Such advancements predicate the smart healthcare model, which is predicated on a patient-centric, interconnected ecosystem bolstered by AI and IoT for optimized health management and decision-making [36–38]. This system establishes a cohesive network for the secure transmission of health data, enhancing the integration of various healthcare platforms and community resources [39,40]. With the integration of AI and IoT in SHSs, vast amounts of data are produced, analyzed, stored, and shared [41]. In this process, it is essential to protect users' privacy.

Privacy, a multifaceted concept, has undergone nuanced definitions over time, reflecting the dynamic interplay between societal evolution and technological advancement. One of the earliest definitions, originating from a seminal law review, characterizes privacy as the fundamental right to "be let alone" [42]. This foundational definition has been echoed and elaborated upon in various domains, notably within the *Information and Technology* (IT) sector. Here, privacy is construed as the capacity to protect sensitive information from unauthorized access and use [43]. The *National Institute of Standards and Technology* (NIST) further refines this conception, defining privacy as the assurance of protecting the confidentiality of, and controlling access to, information pertaining to individuals or organizations [44].

Moreover, privacy is increasingly perceived as the prerogative of individuals to manage the dissemination of their personal data [45,46]. A recent study by Singh et al. [47] straightforwardly posits privacy as the fundamental mechanism for safeguarding sensitive information. Within the AI and FL field, ref. [48] elucidates privacy as the structured preservation of individualized data entities. Across these varied conceptualizations, a

common thread emerges: privacy assumes paramount importance within the *Information and Communication Technology* (ICT) landscape, necessitating specialized attention.

Notably, emerging technologies including blockchain and AI are leveraged for protecting privacy, employing diverse techniques to enhance the efficacy of safeguarding sensitive information. These advancements underscore the ongoing efforts to fortify privacy frameworks amidst the evolving technological landscape.

2.1. Types of Privacy

In [49], Ding et al. proposed five types of privacy in SHSs, including identity, location, query, owner, and footprint privacy. Zhu et al. [21] also described five main types of privacy associated with IoT systems, including identity, location, trajectory, query, and report privacy. In the above works, location, query, and identity privacy are commonly discussed by researchers. Moreover, Chen et al. [50] classified privacy in three main categories, namely identity-based privacy, data-based privacy, as well as location privacy. While identity privacy refers to protecting personal identifiers, location privacy consists of protecting the user's location data such as geographic position and its parameters [21] from disclosure. As well, data privacy entails the protection of the user's personal data. Most recently, Wang et al. [51] proposed two main types of privacy in SHSs, identity privacy and data privacy. Data privacy consists of a user or patient's physiological information, and identity privacy involves information about the identification of the participating clients. In the present study, we explore two distinct categories of privacy as shown in Figure 2, namely identity privacy and data privacy.

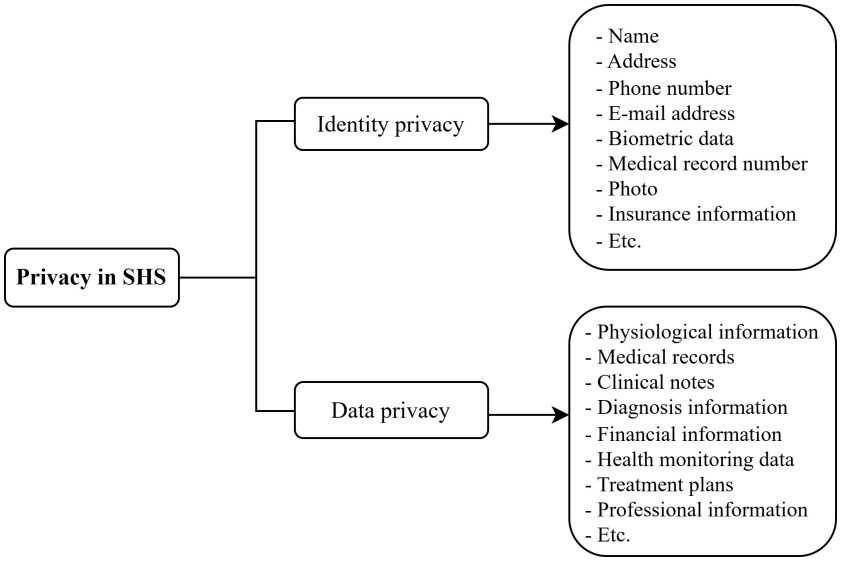

Figure 2. Types of privacy in SHSs.

Identity privacy refers to safeguarding the identifying information of users, encompassing data elements facilitating the unequivocal identification of an entity, including but not limited to name, date of birth, address, biometric details, photographic representations, among others. To mitigate identity privacy apprehensions within smart healthcare environments, Ali et al. [18] advocated for the adoption of anonymization techniques on users' *personal identifiable information* (PII). Furthermore, they proposed three distinct strategies aimed at strengthening user access to the system, encompassing login-based authentication, pseudonym use, and anonymity protocols, respectively. Still in addressing identity privacy concerns, the adoption of pseudonyms is commonly advocated by [21,49,50].

In contrast, *data privacy* refers to the protection of physiological data and other personalized information, such as medical records, clinical notes, diagnostic data, locational data,

professional particulars, and financial details. Various strategies, prominently including data encryption, have been deployed to uphold data privacy standards [50]. Moreover, safeguarding data privacy assumes paramount significance within the healthcare sector, particularly in the context of FL and AI applications [52]. As underscored by the literature [52], the imperative of data privacy in healthcare is multifaceted, encompassing considerations of patient trust and confidence, ethical obligations, regulatory compliance imperatives, and the deterrence of illicit data access.

2.2. Privacy Threats in Smart Healthcare

Privacy emerges as a paramount concern within SHSs owing to the exceedingly sensitive nature of the data they manage. While certain privacy concerns are shared with those encountered in IoT systems, others are specifically tailored to the domain of smart healthcare. Over the past decade, numerous scholars have extensively examined the literature concerning privacy preservation within SHSs, yielding diverse insights. Notably, Stojkov et al. [53] proposed a taxonomy that delineates privacy concerns within the healthcare domain, structured around the tripartite architecture of IoT. As a result of their investigation, a compendium of these concerns has been cataloged, as shown in Table 3.

Table 3. Privacy concerns in IoMT architecture.

IoT Layers	Privacy Concerns
Perception layer	Collection of more data than required without user consent, data and device tampering.
Network layer	Disclosure of device or user's identity or location, data tampering.
Application layer	Disclosure of user's personal information, user's movement analysis, behavioral analysis, lack of digital forgetting.

Ranjith et al. [54] carried out a comprehensive examination of the privacy challenges inherent in SHSs, elucidating a spectrum of security and privacy obstacles. These include RFID security vulnerabilities, *Distributed Denial of Service* (DDoS) attacks, man-in-the-middle attacks, intra-device authentication complexities, and secure communication protocols and key management methodologies. Additionally, Ali et al. [18] have delineated a series of potential privacy concerns and challenges specific to SHSs leveraging the IoMT. Principally, these concerns revolve around the integrity of the end user identities and their associated information. Notably, instances of data leakage may manifest during communication exchanges between healthcare practitioners and IoMT devices, or between healthcare providers and patients' personal devices. Prominent among the identified threats are eavesdropping attacks, falsified data dissemination to healthcare providers, and data flow analysis vulnerabilities [18].

The integration of advanced technologies and connectivity to improve medical services in SHSs also raises significant privacy concerns due to the sensitivity of the health-related data they handle. In this survey, as shown in Figure 3, we provide a classification of privacy threats in SHSs grouped in five key types including data breaches and unauthorized access, insider threats and social engineering, technical vulnerabilities, users privacy concerns, and regulatory compliance and data misuse.

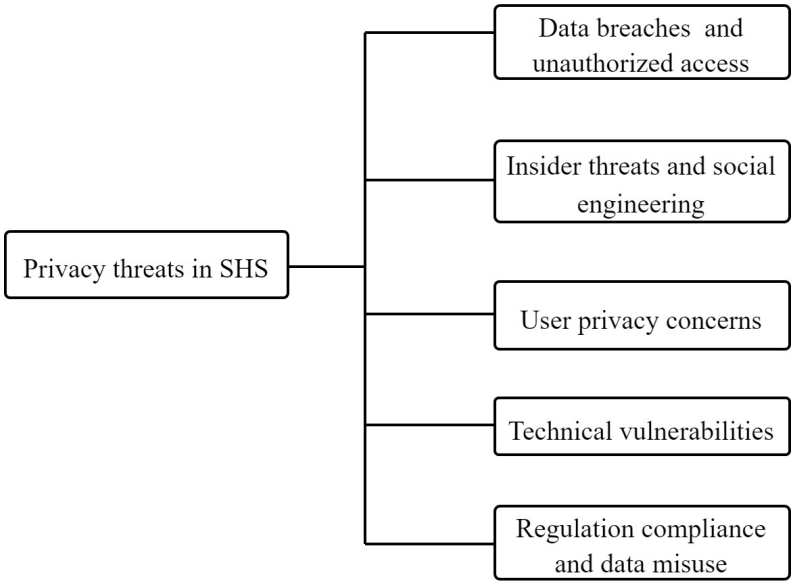

Figure 3. Classification of privacy threats in SHS.

Data breaches and unauthorized access: In an SHSs context, it refers to incidents where sensitive medical information is exposed or accessed by unauthorized individuals. The consequences of such threats are severe, as they compromise patient privacy, may lead to identity theft, financial fraud, violations of patient confidentiality, and can erode trust in healthcare providers. These incidents can occur in various ways including hacking, phishing, exploiting software vulnerabilities, cyberattacks, and insider threats [55]. These privacy threats can result in the exposure of patient identities, medical records, and other confidential data to malicious actors through various medical devices such as invasive, non-invasive, and active therapeutic devices as well as sensors (physiological, biological, and environmental) [56]. Despite sophisticated security measures, the prevalence of data breaches in healthcare facilities highlights the ongoing challenges in safeguarding sensitive information. To mitigate this type of privacy threat, it is critical to implement strong access controls, use encryption for data at rest and in transit, and perform frequent security audits.

Insider threats and social engineering: Insider threats [57] in healthcare refer to risks posed by individuals within a healthcare organization, such as employees, who have authorized access to the SHS and data. An insider can be former and current employees, business partners, or consultants [58]. These insiders may intentionally or unintentionally compromise security by accessing patient records without permission or engaging in data breaches. According to [57], several human factors such as awareness, selfishness, devotion, access, leadership, and caring are associated with insider threats. On the other hand, social engineering threats [59] involve manipulative operations employed by cyber criminals to trick users into revealing important personal information like passwords and other sensitive data. This can be performed through methods like phishing emails, where attackers impersonate trustworthy sources to trick victims into clicking malicious links or downloading harmful files. Both insider threats and social engineering attacks are significant cybersecurity concerns in the healthcare sector, requiring robust security measures and employee awareness. Implementing strict access controls and monitoring, conducting background checks, and training employees to recognize and resist social engineering tactics are crucial.

Technical vulnerabilities: SHSs involve the use of various devices and software in providing healthcare services [56]. Technical vulnerability threats are vulnerabilities within

the software, hardware, or network components of SHSs that can be utilized to gain unauthorized access or disrupt healthcare services [60]. These vulnerabilities may arise from unpatched software, outdated systems, or inadequately configured networks [57]. These can lead to data corruption, system downtime, or unauthorized data access, impacting patient care and data integrity. To mitigate these types of threats, robust system architecture, regular updates and patches, and comprehensive vulnerability assessments are essential.

Users privacy threats: It concerns threats related to data practices transparency and the autonomy of users over their data. Concerns often arise about how data are collected, used, shared, and stored within SHSs. Inadequate management of these concerns may result in a distrust of patients regarding healthcare providers, reluctance to share data, and potential non-compliance with privacy regulations. Implementing clear privacy policies, ensuring informed consent, and providing patients with easy access to their data and control over their use are crucial steps.

Regulatory compliance and data misuse: Adherence to the regulatory and legal frameworks is important to protect privacy in SHSs. Non-compliance and misuse of data for purposes other than those consented to by the patient fall under this category. Regulatory violations may result in legal penalties, loss of licenses, and damage to an organization's reputation. Data misuse can also infringe patient rights and trust. Healthcare providers must ensure that all SHS activities comply with applicable laws like HIPAA in the US, GDPR in Europe, and other local data protection regulations [8,9]. Regular compliance audits and ethical reviews of data usage practices are also recommended.

3. Federated Learning in Smart Healthcare Systems

This section presents the role of FL in SHSs starting with its foundational concepts of FL, followed by the integration of FL into SHSs and concluding with examining strategies to implement PPFL in SHSs to enhance privacy protection.

3.1. Background

The emergence of centralized-based ML models has heightened apprehensions regarding data privacy [48]. Centralizing data collection for training ML models poses a potential risk of exposing sensitive user information. FL was introduced as a new decentralized ML approach with promising features to mitigate privacy issues in traditional centralized ML models. Although some related work had previously been conducted, the FL approach was initially introduced by McMahan et al. in 2016 [10]. In their study, they explored a learning technique wherein users could collectively derive benefits from shared models trained on data, without necessitating a centralized data storage system. Following the work of [10], several studies have emerged, leading to the adoption of various definitions and concepts related to FL.

For instance, FL is defined as a form of a distributed ML approach where multiple participants can jointly train a model under the supervision of a cloud server while ensuring that their raw data are kept locally [61–63]. One important characteristic of FL is enabling the training process to occur on each participant's device, or partially at the server, as in split FL [64]. As a result, only the model parameters are transmitted to the central server to obtain the global model [10,65]. Consequently, both the server and the other participating devices are unable to directly access a particular client's raw data. This is presented as the main advantage of the FL methods. Hence, FL is called "a privacy-by-design approach" [48].

Originally proposed to address privacy concerns [61], FL also has the potential to reduce communication overhead and distribute computational tasks from the central server to clients. In previous works, the FL principle has been tackled in different ways. Qin et al. [61] defined a four-step FL basic principle that includes local update, weights upload,

global aggregation, and weights feedback. However, their proposition does not include one of the important steps, that is, the initialization. Mammen et al. [66] also proposed a four-step-based FL process with client selection and parameter broadcasting instead of weights upload and weights feedback. In addition, Kairouz et al. [62] proposed a typical FL training in five steps including client selection, model broadcast, clients' local computation, aggregation, and model update. However, in this typical training process presented, the weights upload is not outlined as a step but is very important in the process. To provide a comprehensive description of the whole FL process in this work, we consider the FL process in five steps including initialization and client selection, model broadcast, local training, gradients upload, and aggregation. Aside from the initialization step, which is performed once, the above-mentioned steps are executed repeatedly for a predefined number of global communications or when the model converges to an optimal point.

3.2. Federated Learning Integration into Smart Healthcare Systems

Alongside the significant benefits brought by the integration of IoT into healthcare systems, several challenges and concerns have emerged [67], including privacy and security concerns [68]. For instance, the proliferation and widespread adoption of IoMT devices, coupled with the inherent vulnerabilities that expose healthcare systems to privacy leakage, cyber attacks, and threats [47]. In addition, the need to access substantial quantities of sensitive patient data raises critical issues regarding the protection of the privacy [3,67]. Furthermore, data currently play a significant and pivotal role in SHSs, particularly growing prominence of big data and AI. The use of cutting-edge technologies, including IoT sensors, wearable devices, and EHRs, generates a huge volume of data that enables the understanding of individual health profiles and facilitates personalized care. Data, especially big data, play a crucial role in enabling personalized and efficient care, enhancing patient outcomes, and reducing medical expenses [38].

In response to the challenges highlighted above, FL seems to be a suitable approach. FL, a decentralized ML technique, facilitates collaborative ML model training over distributed healthcare facilities while ensuring the privacy of individual patient data [6,10]. Figure 4 illustrates the integration of FL in SHSs where FL nodes can represent various healthcare structures such as a smart hospital, smart mobile healthcare device, smart pharmacy, smart laboratory, etc. By allowing data to remain localized and eliminating the need for centralized data training, FL offers an efficient means of mitigating privacy risks inherent in conventional data-sharing approaches.

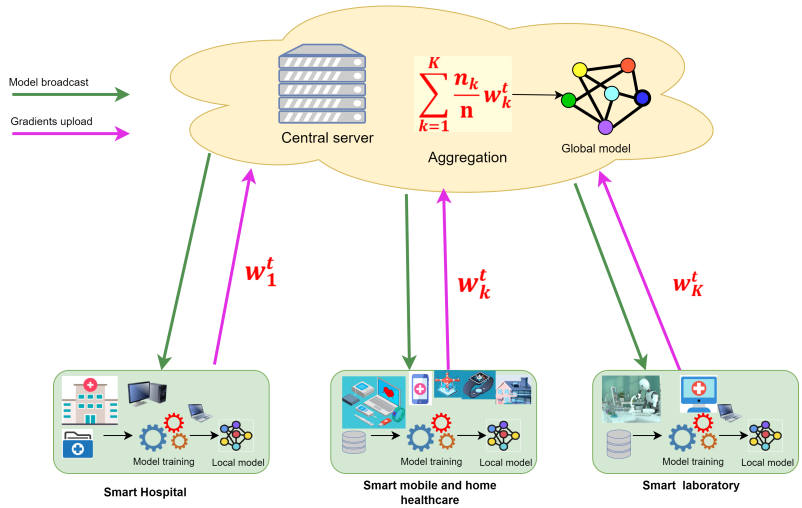

Figure 4. FL-enabled smart healthcare system (SHS).

3.3. Privacy-Preserving Federated Learning

Typically, in ML, privacy concerns can be grouped into two kinds, namely direct privacy breaches and indirect privacy disclosure [69]. Direct privacy breaches result from massive data collection and illegal use without owner's permission, while inadequate model generalization capacity leads to indirect privacy disclosure. Indirect privacy disclosure seems to be the main objective of ML privacy protection [69].

According to [8,10,63], privacy is the key feature of FL. Indeed, in the FL environment, clients usually communicate with the central server utilizing model parameters instead of raw data. This approach naturally ensures privacy by minimizing the transmission of sensitive information while still enabling collaborative model training [48,61].

However, it is crucial to recognize that FL provides only an incomplete resolution for protecting the privacy of AI and ML models [13,48], especially in SHSs. Although FL proved a great potential for enhancing privacy in SHSs, new privacy concerns targeting FL systems have emerged [51,70]. To overcome privacy concerns in the context of FL, PPFL has been introduced as a smart combination of FL and privacy preservation techniques [28]. It is designed to provide numerous significant enhancements aimed at boosting privacy and security in the design and implementation of FL systems. Its main challenge lies in striking a balance between preserving data privacy and maintaining data utility when integrating privacy preservation techniques in the FL context. Liu et al. [71] have used techniques such as *Trusted Execution Environment* (TEE) and *anti-Generative Adversarial Network* (GAN). While proposing the FL approach, ref. [10] also envisaged the possibility of combining it with SMPC and DP to mitigate privacy leakage. According to Jagar et al. [48], the key privacy technologies used in FL are HE, SMPC, DP, secure aggregation, and blockchain integration. Recent works [8,72] as well as [28,65,66] focused on PETs like HE, SMPC, and DP as the main and most explored techniques for enhancing privacy in FL.

In Figure 5, we propose a taxonomy of FL-based privacy mechanisms used in SHSs. The proposed taxonomy classifies FL-based privacy-preserving mechanisms in SHSs into three main groups, namely privacy-enhancing techniques, *Distributed Ledger Technology* (DLT), and hybrid techniques. Although PETs encompass several techniques such as cryptographic techniques, perturbation techniques, and anonymization techniques, for this study, we focus on DP, HE, and SMPC that are the key PETs integrated in privacy-preserving mechanisms within SHSs. We outline blockchain as the key DLT technique for enhancing privacy within the FL context, leveraging its inherent features [12] such as decentralized control, immutable records, and cryptographic security [73] to significantly strengthen privacy protection by preventing unauthorized data tampering and access. We describe each technique supported by some of its recent applications as follows.

3.3.1. Privacy-Enhancing Techniques

In this sub section, we describe the key categories of PETs that are cryptographic techniques, anonymization techniques, and perturbation techniques.

Cryptographic techniques: They are based on cryptography, that is, the study and application of techniques for safe communication [74]. Through encryption and decryption operations based on mathematical algorithms and computational techniques, cryptography serves as a cornerstone in safeguarding sensitive data and communication channels within various domains, including information technology, cybersecurity, and telecommunications. In the recent scientific literature, cryptographic techniques such as HE [75–77], SMPC [78,79], and secret sharing [80–82] mechanisms have emerged as promising solutions for strengthening privacy protection within FL frameworks.

Perturbation techniques: The fundamental concept behind these approaches is to introduce random noise to the initial dataset. This process enables statistical calculations

performed on the noisy data to remain indiscernible from those derived from the original dataset. The perturbation techniques used mainly in the FL context are DP-based techniques [83,84], such as global DP and local DP [85], etc.

Anonymization techniques: They are mechanisms applied to protect the privacy of users in a dataset by removing *personally identifiable information* (PII) [46]. The objective of these techniques is to make it impossible or extremely difficult to re-identify specific individuals within the data. For instance, Choudhury et al. [86] proposed an anonymization-based approach using the K-anonymity [87] technique to effectively enhance privacy preservation within the FL context while improving data utility.

3.3.2. DLT Techniques

The main DLT broadly adopted in the FL context for privacy preservation is blockchain technology. Leveraging its distinctive features, blockchain [21,23,88] holds the potential to empower FL frameworks, thereby enhancing privacy protection. Numerous blockchain-based approaches have been proposed in the scientific literature. These approaches, as elucidated in works by [23,89] as well as [70,90], represent concerted efforts to improve the privacy-preserving frameworks inherent in FL paradigms. In simple FL-based systems, privacy is protected by allowing local model training without sharing clients' data. In fact, blockchain encompasses technologies such as encryption and smart contracts that are utilized to enhance privacy protection in FL-based SHSs [91]. In blockchain-enabled FL frameworks, data are kept private by each client node and their privacy is ensured by the tamper-proof nature of blockchain. Furthermore, blockchain enhances privacy in FL-based frameworks by decentralizing trust and eliminating single points of failure. It ensures tamper-proof recording of model updates, enforces, and provides auditability to detect malicious behavior. Although blockchain is inherently a security-by-design technology, integration with FL can leverage its prominent features to provide strong security and somewhat contribute to enhancing privacy in FL-based frameworks. For example, Kasyap et al. [92] proposed a framework in which blockchain channels isolate sensitive data into secure groups, reducing exposure risks during training. Rahman et al. [93] introduced a framework with provenance tracking that leverages blockchain to track the origin, integrity, and updates of training data and models. This ensures that all data and updates are verified and traceable, preventing malicious data manipulation or leakage, thereby ensuring the integrity of data and updates while enforcing privacy through encryption. In addition, refs. [92,93] perform decentralized gradient aggregation where blockchain replaces the centralized aggregator with a decentralized gradient mining system. Each federated node performs local training, and encrypted gradient updates are aggregated using blockchain consensus mechanisms, ensuring privacy. Moreover, the scheme in [94] employs the auditability and incentives mechanism, which ensures that each update is recorded immutably on the blockchain, enabling participants to verify the integrity and provenance of the data used in model training. This ensures that malicious participants cannot introduce poisoned updates or tamper with the global model. Overall, it is worth noticed that, even though blockchain is not inherently a privacy technology, it has the potential to provide trustworthiness within FL systems, thereby indirectly enhancing privacy protection. To further enhance privacy in FL-based systems, it is essential to combine blockchain with PETs under the hybrid label.

3.3.3. Hybrid Techniques

Utilizing hybrid techniques in FL involves integrating two or more distinct technologies to mitigate privacy risks effectively. Each technique is carefully integrated, taking into account its unique features, benefits, and limitations, thereby enabling the global frame-

work to offer an efficient approach for privacy preservation. Numerous hybrid approaches have been advanced to protect privacy in SHSs within the FL framework, as evidenced by studies such as those by [24,95,96] for FL-based blockchain and DP, ref. [76] for FL-based HE and SS, ref. [97] for FL-based blockchain and SMPC, ref. [98] for FL-based blockchain, DP, and HE, and refs. [76,99] for FL-based HE and DP.

4. Federated Learning Meets Privacy-Enhancing Technologies

In this section, we explore privacy-enhancing technologies (PETs) that enhance FL for privacy protection. The discussed combinations include Differential Privacy-enabled FL, Secure Multi-Party Computation-enabled FL, and Homomorphic Encryption-enabled FL. Each subsection elaborates on the mechanisms, applications, and limitations of these PETs, with a focus on their relevance to smart healthcare data protection. We conclude with a comparison between the above PETs.

4.1. Differential Privacy-Enabled Federated Learning

DP [100] is a technique that consists of adding noise to data to mask individual contributions. It aims to ensure robust assurances about the privacy of individuals whose data serve for analysis or computation [101]. Specifically, given two adjacent datasets D_1 and D_2 which differ solely at one data point, applying the DP technique to perturb the original values can render the outputs of these datasets indistinguishable. Formally, DP can be defined as follows.

Definition 1 (ϵ-Differential Privacy [100])**.** *A randomized mechanism M satisfies ϵ-Differential Privacy (ϵ-DP) if, for any pair of neighboring datasets D_1 and D_2, and for any possible output $S \in Range(M)$,*

$$\Pr[M(D_1) \in S] \leq e^{\epsilon} \times \Pr[M(D_2) \in S] \tag{1}$$

where the parameter ϵ denotes the privacy budget, a mathematical concept that quantifies the maximum possible privacy loss. DP can be classified into two main types, including Global Differential Privacy (GDP) and Local Differential Privacy (LDP) [28]. While GDP focuses on adding noise centrally before sharing data, LDP perturbs data locally, allowing each client to protect their information independently. The problem of privacy preservation using DP in the FL context has been a focus of several research works. Abadi et al. [102] proposed a way of combining DP with deep learning to preserve privacy with some important results in terms of accuracy and privacy. Afterwards, various approaches tightly linked to the FL context have been proposed. In Table 4, we compare DP-based PPFL methods based on key metrics such as privacy level, key technologies, datasets, accuracy, and limitations.

Zheng et al. [83] proposed an approach to enhance privacy in the FL context that consists of injecting local DP noise into the model updates prior to transmission. Furthermore, they indicated that LDP primarily gains advantages from an extensive user community and requires fewer CPU/battery resources on portable devices while ensuring a robust level of privacy protection [83]. They obtained valuable insights from the proposed solution but suggested further and in-depth studies and experimentation to enhance the accuracy of the scheme. Li et al. [84] proposed ADDETECTOR, a privacy-preserving smart healthcare scheme designed for the early detection of Alzheimer's disease (AD) in an easy-to-use and cost-effective manner. The system addresses the challenges in remote AD detection and proposes a solution that utilizes IoT appliances and security protocols to ensure privacy. By employing FL and DP mechanisms, ADDETECTOR achieves high accuracy and low time overhead in AD detection trials, demonstrating its effectiveness and efficiency. However,

the ability of the proposed approach to overcome potential security threats and privacy breaches in real-world scenarios remains a critical challenge.

Table 4. DP-based PPFL approaches.

Schemes	Privacy Level	Key Technologies	Datasets	Accuracy (%)	Limitations
Zheng et al. [83]	High	FL, LDP	NYC Taxi, BR20009, Adult10	90	Client population dependency, privacy loss concerns
Yang et al. [103]	High	FL, DP, HFL, DNN	MNIST	78–98	Complexity of managing personalized privacy levels for each client, accuracy and privacy trade-off
Li et al. [104]	High	FL, SDG, PDP, FedSGD	MNIST and CIFAR-10	Not specified	Up to client to choose their privacy level
Weng et al. [101]	High	FL, LDP, CDP, GM, MA, SG, MGD	MNIST	LDP 97 LCDP 94.2	High communication overhead, system complexity
Khanna et al. [105]	High	FL, FL, DP, TP	iDASH 2020	97.5	Challenge of setting privacy budgets in differential privacy and the need for knowledgeable users to prevent potential privacy leakages
Maria et al. [106]	High	FFNN, ReLU, SGD, FedAvg, FL, DP	MNIST	92.5	Challenge of balancing accuracy and privacy, complexity of parameter tuning in differential privacy methods

Notations: FFNN: feed-forward neural network; TP: tensor flow–privacy; ReLU: rectified linear unit; PDP: personalized differential privacy; GM: Gaussian mechanism; MA: moment accountant; MGD: momentum gradient descent; SG: sparse gradient.

Yang et al. [103] proposed another approach, named PLU-FedOA, that optimizes FL with personalized local DP in mixed privacy preservation situations. Their algorithm consists of two components: PLU, that helps clients to transmit local updates under DP of individually chosen privacy degree, and FedOA, that allows the server to aggregate local parameters with optimized weight in combined privacy-preserving scenarios. Compared with other existing FL solutions like FedAvg, GDP-FL, and LDP-FL, PLU-FedOA has shown superior performance in a mixed privacy-preserving setting [103]. Although this solution is promising, its potential efficiency on various datasets and real-world applications still needs to be proved.

Li et al. [104] presented a novel FL scheme called PGC-FedSGD that integrates personalized LDP and the *Federated Stochastic Gradient Descent* (FedSGD) algorithm. In this solution, PGC-LDP is utilized by the clients to ensure local DP of the gradient, while FedSGD is used by the server for the aggregation. In this framework, users can choose their privacy levels regarding a FedSGD algorithm with LDP. The experiments on the MNIST and CIFAR-10 datasets demonstrated good results, as PGC-FedSGD has a simple architecture and algorithm design with a strong privacy assurance. However, the proposed approach, which results in clients uniformly selecting their privacy level within an empirical domain, appears unreasonable, as most participants tend to seek robust privacy guarantees if possible.

Unlike [103,104] approaches where DP is applied locally on the clients' side, Weng et al. [101] proposed another approach, in which DP is used by both the server and clients to obtain stronger privacy protection. Their scheme also applies sparse gradi-

ents and *momentum gradient descent* (MGD) to enhance accuracy performance and decrease communication overhead. The main findings include outperforming other DP-based FL schemes concerning model accuracy and providing a more robust privacy assurance [101]. The proposed scheme can achieve optimal accuracy performance while reducing communication costs by up to 90%. However, the potential degradation of accuracy performance due to the injection of noise for privacy protection and the need to choose the noise scale carefully to balance privacy protection and model performance are some limitations of this approach.

The work of Khanna et al. [105] proposed an FL algorithm that implements DP for ML model training on distributed healthcare data. The framework was tested for forecasting breast cancer status based on gene expression data and achieved similar accuracy and precision as a non-private model, demonstrating its effectiveness. However, there are still some challenges for their proposition including privacy concerns when models were trained on data from various institutions and hospitals and the need to set the privacy parameter by a user with expertise to mitigate potential privacy breaches.

Gu et al. [25] introduced a PPFL framework using DP for artificial IoT systems. Their approach includes two techniques, gradient perturbation and gradient permutation, to safeguard both the privacy of data and the identity of clients throughout the FL process. The gradient perturbation mechanism involves adding exponential noise to the computed gradient on the client side to satisfy data privacy, while the gradient shuffling mechanism guarantees that the server cannot discern which gradient belongs to which client, preserving the client's identity [25].

Maria et al. [106] introduced an Optimized DP (ODP) approach to safeguard the privacy of individual data points while facilitating the extraction of useful insights. Their scheme is evaluated on the MNIST dataset and analyzed with the FedAvg aggregator. The main findings include leveraging DP within FL to bolster privacy, experimentation with diverse DP parameters to optimize outcomes, and presentation of quantitative results detailing the accuracy of trained models alongside their corresponding privacy guarantees. Moreover, it demonstrates that maintaining constant epsilon values while varying noise levels and delta values leads to heightened privacy protections.

Nevertheless, strategies based on noise necessitate the algorithm to meticulously fine-tune the generation of noise to keep the model's performance, including accuracy. Failure to do so could significantly impair performance.

4.2. SMPC-Enabled Federated Learning

SMPC is an advanced cryptographic method that permits decentralized participants to collaboratively compute an objective function without disclosing their individual data [28]. It allows multiple users to collaborate when performing computations on their raw data without the need to share them. SMPC utilizes some advanced cryptographic protocols, such as secret sharing, garbled circuits, and HE, to facilitate confidential computations over private data.

While there is limited literature on integrating SMPC with FL for privacy preservation, some authors have explored this area. For instance, Kanagavelu et al. [78] introduced a two-phase mechanism using Multi-Party Computation (MPC) to enhance privacy in FL. The key findings of their approach include the successful integration of MPC for model aggregation in FL, enabling companies to collectively train models while preserving privacy. However, the limitations of the study involve high communication overhead and scalability issues with MPC-enabled model aggregation, the complexity introduced by the need for a small committee, and the focus on neural network models limiting generalizability to other machine learning models.

In addition, Tran et al. [79] proposed an approach called ComEnc-FL, a PPFL framework that leverages SMPC and parameter encryption for protecting privacy and reducing communication and computational costs. It surpasses typical SMC systems in training duration and data transfer capacity, matching the fundamental FL framework and outperforming DP-secure frameworks. However, while enhancing privacy and reducing computational and communication costs in FL, ComEnc-FL may still be susceptible to collusion between clients and the server, potentially compromising the model confidentiality. Overall, SMPC schemes prevent inquisitive or untrustworthy aggregators from inspecting private models without impacting accuracy [79]. SMPC schemes offer advantages in preventing unauthorized access to private models without compromising accuracy. However, challenges such as communication overhead, scalability issues, and susceptibility to collusion underscore the necessity of in-depth research and advancement to overcome the limitations and ensure robust privacy-preserving mechanisms within FL frameworks.

4.3. Homomorphic Encryption-Enabled Federated Learning

HE can be defined as a cryptographic mechanism that permits arithmetic operations on encrypted data without decryption requirement [11]. Thus, a fundamental property of HE is that decrypting the operated ciphertext should yield the same output as would be obtained by operating on the unencrypted data. This property allows to execute intricate mathematical operations on encrypted data while maintaining the security of the raw data.

HE encompasses a variety of encryption techniques capable of conducting diverse computations on encrypted data. It includes several types, such as partially homomorphic, somewhat homomorphic, and fully HE [11,107,108].

- Partially HE (PHE) enables computations involving a single type of operation, like addition or multiplication. PHE incurs lower computational costs compared to alternative forms of HE, yet its applicability remains limited [109].
- Somewhat HE (SWHE) enables both addition and multiplication but with restrictions on the number of operations permitted [11,110]. SWHE is more computational cost compared to PHE while providing enhanced functionalities [109].
- Fully HE allows an unlimited number of additions or multiplications on ciphertexts [68,110]. It allows unrestricted computations on encrypted data, including conditional operations, branching, and iterative processes [110–112].

This flexibility in conducting computations while maintaining data privacy makes HE an invaluable tool for scientific research and applications. Based on the encryption mechanism, this technique avoids sharing raw data and the model during the training process in FL between clients and the server. Therefore, it is very difficult for a third party to access user sensitive information. Several studies have proposed privacy-preserving solutions based on HE in the FL context. Table 5 compares HE-based PPFL methods based on key metrics such as privacy level, key technologies, datasets, accuracy, and limitations.

For instance, Park et al. [75] introduced a system that enables homomorphic operations with different encryption keys and the implementation of a system model involving a cloud server and multiple clients for secure model aggregation and averaging. They presented an algorithm for secure aggregation of local models which facilitates the update of the global model parameters by the server using local model parameters with noise that can be reversed out through participant collaboration. Their model involves a trusted key generation center, cloud server, computation provider, and multiple clients, ensuring data privacy through encryption and decryption processes [75]. The challenges addressed in [75] include the need for extra operations to enhance data privacy in FL-based frameworks, while limitations involve the balance between computational overhead and security level, especially with increasing key sizes.

Shi et al. [76] introduced a method that combines HE and secret sharing to ensure the confidentiality of local parameters, withstand collusion threats, and simplify aggregation without sharing keys. However, the proposed scheme faces challenges such as collusion threats among clients or with the server, network disruptions leading to communication issues, and the complexity of implementing encryption techniques in practical applications. Moreover, Wang et al. [77] propose a scheme using HE to secure model parameters in healthcare data applications, addressing privacy concerns and communication efficiency challenges. The scheme introduces client authentication mechanisms and access control to prevent attacks, ensuring data privacy and model performance while reducing communication overhead. However, the proposed scheme has some limitations including potential communication overhead due to users dropping out during training, hardware quality issues, network delays, and the need for an *Acknowledgment* (ACK) mechanism to handle unresponsive users, which may increase waiting delays and affect overall training progress.

Table 5. HE-based PPFL approaches.

Schemes	Privacy Level	Key Technologies	Datasets	Accuracy (%)	Limitations
Park et al. [75]	Very high	FL, HE	Not specified	90	Computational overhead, key sizes impact
Shi et al. [76]	Very high	FL, DP, HE, CNN,DNN	MNIST, CIFAR-10	Over 90	The need for a common key pair negotiation among clients and vulnerability to collusion attacks between clients and the server
Wang et al. [77]	Very high	FL, HE, AC Mechanism, ACK Mechanism	APTOS 2019 Blindness Detection, CIFAR-10	81.53	Time cost, communication overhead
Walskaar et al. [113]	Very high	FL, HE, xMK-CKKS	COVID-19 X-ray lung scans	93.8	High execution time, higher memory usage
Zhang et al. [114]	Very high	FL, HE, CNN	HAM10000	76.9	Communication overhead
Shen et al. [99]	High	FL, HE, SVM, DP	HCV and diabetes databases	86.4–98.6	High computational cost, communication overhead

Notations: AC: access control; ACK: acknowledgment mechanism; HCV: hepatitis C virus; SVM: support vector machine.

In addition, Walskaar et al. [113] also proposed another approach enhanced with *Ring Learning With Errors* (RLWE)-based multi-key HE. The proposed approach utilizes the xMK-CKKS scheme, a multi-key HE scheme based on the CKKS scheme, to ensure the data confidentiality during the training processes in untrusted environments while also addressing the shortcomings and trade-offs associated with privacy preservation in medical data analysis. Although [113] proposed a comprehensive and detailed method to addressing privacy concerns in the ML context for healthcare institutions by integrating multi-key HE within the FL framework, their approach presents some limitations, including the increased computational overhead and data expansion associated with homomorphic encryption, which can reduce system performance and require additional storage and communication resources. Additionally, the accumulation of noise in HE poses a significant challenge, potentially leading to undecryptable ciphertext over time, necessitating the use of noise management techniques to mitigate this issue.

Zhang et al. [114] developed a new masking scheme that integrates HE and SMPC for FL, which considers data quality in model aggregation and provides a dropout-tolerable and participants collusion-resistible solution. It also implements an FL prototype system for medical data, performing comprehensive experiments utilizing authentic skin cancer datasets to validate both the privacy preservation and the effectiveness of their approach.

However, the proposed approach has certain limitations such as the potential impact of HE on computational overhead, the need for further tuning in heterogeneous environments, and the lack of consideration for malicious server attacks and tampering of the aggregated model.

Shen et al. [99] introduced a privacy-preserving and efficient online diagnosis method for e-healthcare systems leveraging FL. The proposed scheme effectively protects patients' privacy, achieves high accuracy in clinical diagnosis, and demonstrates practicality for real-world SHSs. However, some limitations of the proposed scheme include potential damage to the raw data and model accuracy due to the use of DP, increased computational complexity from the complex HE algorithm, inefficient diagnosis result retrieval, and relatively low accuracy of the diagnosis model obtained using the SVM algorithm.

Kumar et al. [70] proposed a sophisticated scheme that integrates blockchain technology and HE with FL to address the challenges of privacy-preserving collaborative model aggregation for the analysis of the medical image, particularly for COVID-19 detection and classification. The proposed framework offers a novel approach to data sharing and collaborative training across multiple healthcare institutions, laying the groundwork for enhanced privacy, security, and accuracy in medical image analysis. However, the approach may face challenges in latency and scalability as a result of the decentralized nature of the blockchain network and the need for continuous updates to address new mutations of the COVID-19 virus. Recently, Liu et al. [115] introduced a novel framework wherein users encrypt their data using a joint public key determined by the server over three rounds of interactions. This scheme offers several advantages, including accommodating dynamic user participation, generating compact ciphertexts that remain independent of the number of participants involved, and reducing the number of interactions per round from three to two, thus mitigating concerns regarding user dropout during computation [115]. However, the security of the proposed scheme may be compromised in scenarios where all users collude with the server.

HE emerges as a pivotal technique for privacy preservation in FL systems within the healthcare domain. Offering the capacity of performing computations on encrypted data without decryption, HE provides a crucial opportunity to safeguard sensitive medical information while enabling collaborative model training. However, the diverse types of HE present trade-offs between computational costs and capabilities, necessitating careful consideration in system design. Despite the promising advancements and proposals of HE-based solutions to address privacy concerns, noise accumulation, computational overhead, as well as security vulnerabilities persist as challenges. Further studies and refinements are essential to overcome these obstacles to fully realize the potential of HE in FL-based smart healthcare applications.

4.4. Comparison of Key Privacy-Enhancing Technologies in FL

To compare the effectiveness of the aforementioned privacy-preserving techniques in FL, a comprehensive comparison is presented in Table 6, highlighting key aspects such as privacy guarantees, computational overhead, scalability, key features, and limitations between different methods.

Table 6. Comparison between main privacy-enhancing technologies in FL.

Privacy Techniques	Schemes	Privacy Level	Computation Overhead	Scalability	Function	Limitations
SMPC	[78,79]	Medium	Medium	High	Joint computation without revealing private inputs	High communication overhead

Table 6. *Cont.*

Privacy Techniques	Schemes	Privacy Level	Computation Overhead	Scalability	Function	Limitations
DP	[83,101,103–106]	High	Medium	High	Addition of calibrated noise to ensure individual privacy	Reduction in data utility due to noise addition
HE	[75,77,99,113,114]	High	High	Low	Operation directly on encrypted data	High communication overhead
FHE	[116]	Very High	High	Medium	Computation directly on encrypted data, flexibility in model training	High communication overhead, system complexity

The existing privacy protection frameworks for FL have certain limitations to varying degrees, rendering them unable to achieve a comprehensive resolution of all challenges within a single scheme. As shown in Table 6, we compare these technologies, focusing on aspects crucial for smart healthcare. SMPC is noted for its good privacy level and moderate computational overhead, offering the advantage of joint computation without exposing private inputs, albeit at the cost of high communication overhead. DP provides strong privacy but with a risk of reduced data utility. Data utility refers to the ability to maintain the usability and accuracy of data as well as preserving the validity and reliability of the insights derived from them after the application of a privacy protection mechanism [117]. Utility measures the ability of the system to maintain model performance. HE allows for computation on encrypted data, ensuring high privacy but suffering from high computational costs. Fully HE extends this capability with increased flexibility for model training but introduces system complexity and still retains considerable communication overhead. These insights are essential to determine the appropriate technology for a reliable smart healthcare system that balances privacy, efficiency, and practical limitations.

4.5. Privacy-Enhancing Technologies Meet FL-Based Smart Healthcare

In this section, we investigate the integration of PETs in FL-based SHSs, especially in health data management, remote health monitoring, medical imaging, and health finance management.

4.5.1. Application in Health Data Management

PETs such as DP, HE, and SMPC are often combined with FL in FL-based smart healthcare to enhance data privacy while training ML models. For example, the work in [118] presented a secure framework integrating SMPC and blockchain with FL to enable heterogeneous models to collaboratively learn from healthcare institutions' data while protecting users' privacy. In [84], authors proposed a privacy-preserving method that combines FL and DP for Alzheimer's disease detection based on patients' audio data collected by IoT devices. Authors in [6] developed a framework for disease prediction that combines FL, DP, and SMPC to protect users' data privacy during the training process. Similarly, ref. [119] employed DP-enabled FL for disease diagnosis in IoMT. Studies in [77,114] proposed homomorphic encryption-based FL schemes to protect the privacy of healthcare data in SHSs.

4.5.2. Application in Remote Health Monitoring

The rapid developments in IoT leading to Internet of Medical Things (IoMT) have boosted the expansion of remote health monitoring [120]. It consists of remote health services delivery through the Internet and IoT devices and sensors for remotely monitoring blood sugar levels, vital signs, heart rate, or other relevant health metrics. AI and FL have been introduced in this SHSs application field in several manners. Although FL by nature ensures privacy protection in this context, privacy enhancement measures are still needed, and several approaches using PETs are proposed. Shen et al. [99] introduced a privacy-preserving approach for remote disease diagnosis integrating HE with FL. HE is used to encrypt patients' physiological data during the training process. This application of smart healthcare is still evolving with further privacy-preserving FL methods from researchers to remotely monitor patients' health in various manners.

4.5.3. Application in Medical Imaging

Nowadays, medical imaging associated with AI is widely used in SHSs for many reasons, including disease prediction, disease diagnosis, and tumor classification. To enhance privacy during ML model training in medical imaging, several schemes that integrate PETs with FL have been proposed by researchers. For instance, ref. [121] proposed an adaptive DP-based FL method COVID-19 disease detection based on chest X-ray images. Similarly, ref. [122] introduced a DP-based FL approach for COVID-19 detection using a generative adversarial network and CT scan images. In [11], authors developed a framework integrating HE and FL for CNN-based COVID-19 detection.

4.5.4. Application in Health Finance Management

The management of medical finance is an important topic in SHSs since healthcare service providers are still looking for a more modern, reliable, and efficient system. AI has been introduced in this application of SHSs to improve financial transactions and efficiency. To the best of our knowledge, there is not yet a privacy-preserving FL method specifically tailored for financial transactions management in SHSs systems. However, regarding the fast-ever growing interest in AI-enabled healthcare, this field necessitates further attention from scholars.

5. Blockchain-Enabled Privacy-Preserving Federated Learning

In this section, we first review the foundational concepts of blockchain technology. We then discuss blockchain integration with FL based on three main aspects: blockchain-enabled model storage, blockchain-enabled aggregation, and blockchain-enabled gradient upload. Next, we compare some blockchain–FL schemes proposed in recent studies. Finally, we discuss the integration of blockchain in FL-based SHSs for health data management, remote health monitoring, medical imaging, and health finance management.

5.1. Background

Blockchain is a *Distributed Ledger-based Technology* (DLT) that stores transactions by packing them into chained blocks [21,23]. According to [95,123], blockchain refers to a shared, distributed, and decentralized ledger that is used to record transactions. The ledger is technically defined as a list of sequential and time-stamped transactions. This definition of blockchain outlines the capability of the blockchain technology to provide modern techniques of storing and sharing data with transparency in decentralized and distributed environments.

Blockchain has been revealed to the public along with Bitcoin in 2008 [88]. Initially linked to Bitcoin, blockchain has become a widely used technology in various fields of life.

Blockchains are thus widely believed to be impossible to be hacked due to the distributed consensus [124]. Overall, we simply define blockchain as a ledger-based, distributed, and decentralized technology of storing data into chained blocks. Its fundamental principles include cryptography, consensus algorithms, smart contracts, and peer-to-peer network as key technologies [125]. The basic general architecture of blockchain consists of six main layers, including the data layer, network layer, consensus layer, incentive layer, contract layer, and business or application layer [126]. The data layer contains the data blocks. A block consists of two main parts including the block header and the block body [21,127–129]. The former mainly contains the version number of the current block, the hash of the previous block, timestamp, nonce, the root value of the Merkle tree, the block size, and the block height. The Merkle tree serves as the generator of the hash value of all transactions in the block [127], and the hash of the previous block helps to link the current block with the previous one. A transaction can be defined as an atomic operation that the successful execution changes the state of a system.

According to [123], three types of records are stored on a blockchain, namely asset transactions, smart contract, and digital signature and certificates. A smart contract is a computer program that can perform a transaction with pre-specified instructions built into it [123]. As a revolutionary trustworthy technology for data storage and transaction verification, blockchain is progressively adopted through the internet. It provides platforms to conduct trusted transactions without the intervention of a third party [127]. Typically, blockchain can be classified into three main types [21,128]. These basic types are public blockchain, private blockchain and consortium blockchain. However, according to [123,130], there are four types of blockchain, including the three types cited above, and the fourth and added one, that is hybrid blockchain. In this section, we describe each of these four types of blockchain. In the public blockchain, any user can create, read, and submit transactions [123]. This type of blockchain generally fits with pure decentralized computing environment [21]. Each member of the public blockchain can publicly access the transactions, and his identity is anonymous [128]. In contrast to the process in public blockchain, only authorized users or organizations can create, read or submit transactions in private blockchain [21,128,130]. This type of blockchain is also called "permissioned blockchain" [130].

As a DLT, blockchain possesses some foundational technical characteristics which make its particularity. According to [126], blockchain has four main features including traceability, transparency, privacy, and high system reliability. In addition, ref. [128] listed five characteristics of blockchain such as anonymity, immutability, decentralization, transparency, and traceability. According to [21], there are four main characteristics of blockchain: auditability, persistency, decentralization, anonymity. Also, ref. [131] has defined four main characteristics of blockchain involving anonymity, immutability, decentralization, and transparency. Finally, in this section, we focus on the following characteristics that are the most cited in the literature on blockchain: anonymity, transparency [123,128], decentralization [21,127,128], auditability, persistency [21], traceability [129], and immutability [123,127].

5.2. Blockchain Integration into Federated Learning

Combining blockchain with FL introduces a promising approach to enhance privacy preservation, data security, and trust in decentralized ML systems. Blockchain technology [22,23], with its inherent characteristics such as decentralization, immutability, and transparency, offers solutions to privacy concerns within the FL context. Furthermore, its incorporation offers a more robust and protected FL process [23].

Concerning privacy preservation, the integration of blockchain with FL frameworks addresses privacy concerns by allowing clients to exchange model updates instead of raw data, thus safeguarding the privacy of sensitive information stored by the clients [132]. This method mitigates privacy violations associated with centralized processing and data falsification, which are common challenges in traditional FL systems [132]. Blockchain-enabled FL offers theories and techniques to improve FL performance from various perspectives, attracting significant attention from academia and industry. Wang et al. [128] were amongst the first to propose a blockchain-based FL approach for privacy protection. In this survey, we present and focus on five key advantages of the combination of blockchain with FL, which are described as follows.

Enhanced data privacy and security: Blockchain can securely manage access control [133] in FL by utilizing smart contracts, which are self-executing contracts with the terms of the agreement directly written into code [118,134]. These smart contracts [89] can enforce privacy-preserving data sharing and processing rules, ensuring the confidentiality and security of data throughout the learning process.

Improved trustworthiness and transparency: The blockchain's immutable ledger can record all FL activities, including data usage, model updates, and participant contributions [95]. This transparency ensures that any malicious or dishonest behavior is detectable, thereby improving trust among stakeholders [135,136]. Additionally, the ledger provides a verifiable and auditable trail [118] that ensures adherence to data regulations.

Incentive mechanisms: The integration of blockchain in FL can facilitate the implementation of token-based incentive mechanisms to encourage users to contribute their data and computational resources. By rewarding users with tokens for their contributions, the system can encourage more active participation, leading to improved model performance and faster convergence.

Decentralized model management: Blockchain is adapted for managing and storing FL models in a decentralized way [95], ensuring that no user has exclusive control over the global model and thereby avoiding the problem of a single point of failure and malicious poison of the server [89]. This not merely improves security and privacy but also promotes a democratic approach to model development and deployment.

Robustness against attacks: The decentralized and tamper-resistant feature of blockchain makes it more challenging for attackers to manipulate model updates or compromise data integrity [95]. This additional security is vital for applications in sensitive areas such as healthcare.

To comprehensively analyze the integration of blockchain into FL frameworks, our investigation centers on three key technical dimensions: aggregation, global model storage, and gradients upload. These dimensions are shown in Figure 6. Through a meticulous examination of these aspects, we aim to elucidate the implications, challenges, and potential benefits associated with integrating blockchain technology into FL.

5.3. Blockchain-Enabled Model Storage

As a digital ledger technology, blockchain ensures that stored data cannot be tempered. This feature makes blockchain technology a better way of storing the global model in the FL context. For example, Zhang et al. [24] put forth a privacy-preserving FL framework based on blockchain where the server in normal FL process is replaced by blockchain to avoid the risk of single point failure. Furthermore, for the proposed approach, blockchain stores the global model and the clients download the model for local training on their respective local data. Once the model parameters have stabilized, the training process can be halted, and then the final global model is transferred to the blockchain for permanent storage [24]. This approach ensures that the global model is securely stored and accessible to all client

nodes. Kumar et al. [70] proposed a scheme in which a blockchain ledger stores the global mode and also serves as a distributed ledger for aggregation. According to the approach proposed by Moulahi et al. [90], blockchain is also used to store the global model in order to protect it against attacks.

Furthermore, Lei et al. [137] developed an innovative blockchain-based client selection in FL. In their approach, blockchain also stores the global model and after each iteration, the updated model from the aggregation process is also stored in the blockchain. By using this storage, the model is protected from attacks and cannot be tempered. Almost in the same way, blockchain is used in many existing works to store the global model [138–140].

In conclusion, leveraging blockchain technology in FL for storing the global model emerges as a robust solution to ensure data integrity and prevent tampering. This approach is echoed in various existing schemes such as [24,70,90,91,141,142], highlighting its effectiveness. Using blockchain in place of the central server can significantly mitigate the chance of a single point of failure, enhancing security and reliability of FL. The decentralized nature of blockchain ensures that the global model is securely stored and readily accessible, showcasing its pivotal role in safeguarding FL processes against potential attacks.

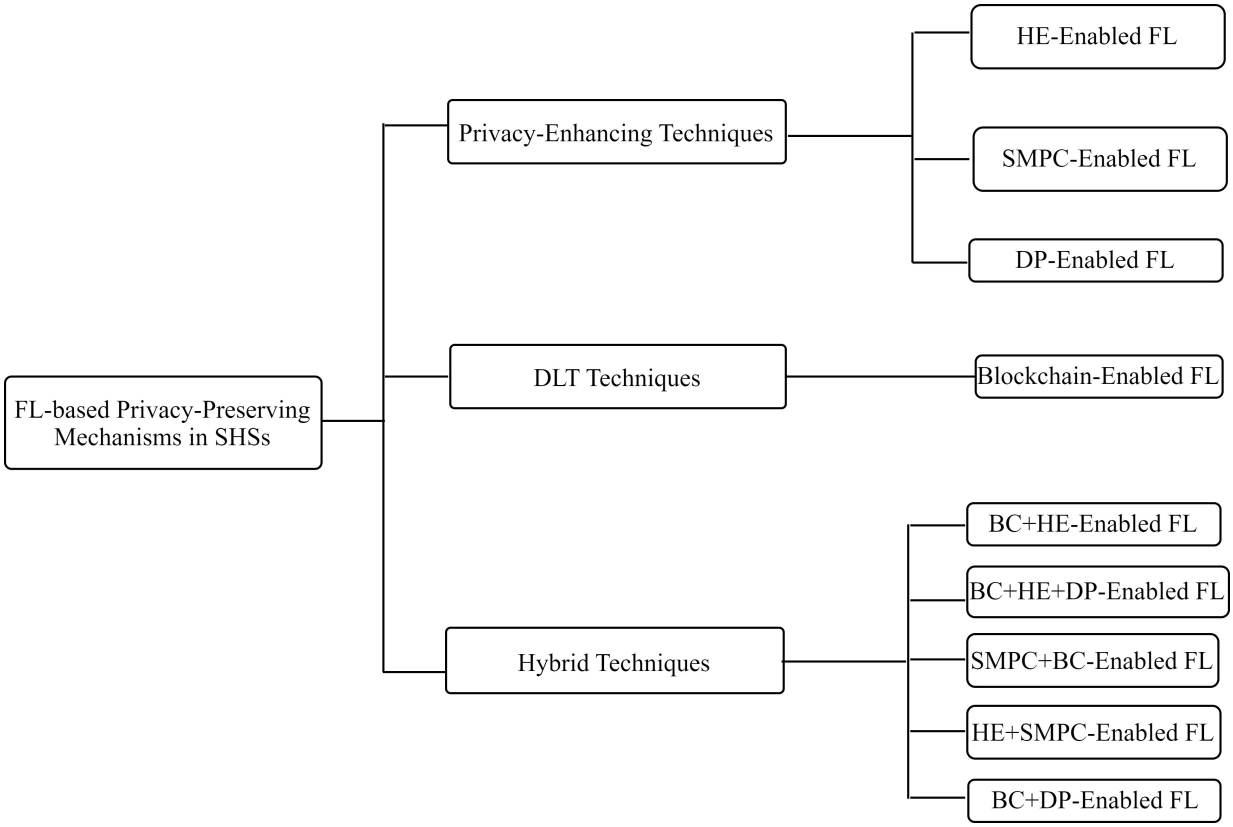

Figure 5. Taxonomy of FL-based privacy mechanisms in SHSs. SMPC-enabled FL (Abaoud *et al.* [6]), BC+HE+DP-enabled FL (Rahman *et al.* [93]), BC+DP-enabled FL (Ngan *et al.* [96]), SMPC+BC-enabled FL (Abou *et al.* [97]), HE-enabled FL (Shen *et al.* [99]), HE+SMPC-enabled FL (Zhang *et al.* [114]), DP-enabled FL (Stephanie *et al.* [118]), BC+HE-enabled FL (Shu *et al.* [139]), BC-enabled FL (Mazzocca *et al.* [143]).

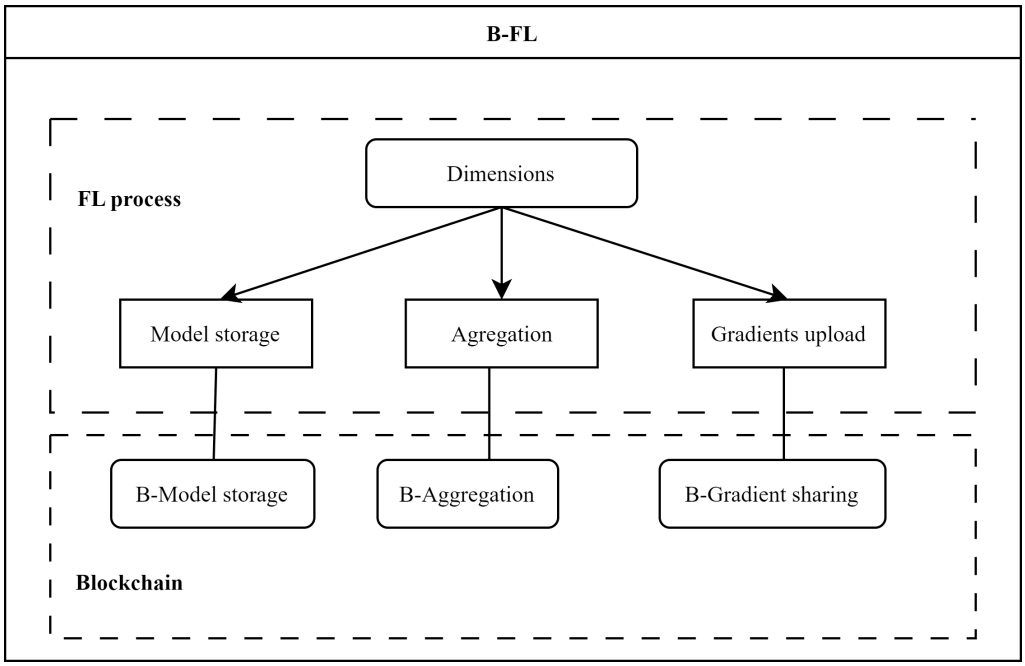

Figure 6. Technical dimensions of blockchain-enabled PPFL covered in this survey.

5.4. Blockchain-Enabled Aggregation

Many studies on blockchain-enabled PPFL proposed to use blockchain for model aggregation. Yang et al. [89] introduced a blockchain-based approach for trustworthy FL where blockchain is not used for aggregation. Their approach relies on several edge servers and clients that generate a blockchain linked by cryptography to confirm data correctness and immutability. The aggregation mechanism in this scheme involves the primary edge server validating local models, aggregating them into a global model using a smart contract, and packing them into a new block. This block is then distributed to edge servers, in charge of validating the correctness of the global model using consensus protocols like PoW and *Practical Byzantine Fault Tolerance* (PBFT). PBFT, along with *Proof of Work* (PoW), is employed across several edge servers to avoid model tampering from malicious servers, ensuring the trustworthiness of the global model aggregation platform while mitigating attacks and ensuring transparency and immutability in the gradient upload process [89]. Blockchain, through consensus protocols like PBFT, facilitates secure aggregation and validation, ensuring the trustworthiness of the aggregation platform. This approach ensures a trustworthy aggregation platform supported by distributed consensus protocols, mitigating single points of failure and malicious attacks on edge servers.

Kumar et al. [70] also proposed a B-PPFL approach in which is employed blockchain to gather the encrypted gradients from different client nodes and aggregates the local and global models using a *Directed Acyclic Graph* (DAG) with the PoW consensus algorithm. The blockchain performs the aggregation of the local and global models using the smart contract [70]. In this way, the adoption of blockchain provides a secure mechanism for various clients, enabling the aggregation of local model updates and providing authentication of the data. Moulahi et al. [90] developed a blockchain-based PPFL approach where the central server is replaced by blockchain technology. Furthermore, the aggregation is made by blockchain through a smart contract. Using a smart contract in blockchain for aggregation and global model storage leads to a secured and non-falsifiable mechanism. Liu et al. [69] also introduced a blockchain-based aggregation in the FL context using smart contracts combined with privacy technologies.

Significant contributions are made in FL-based healthcare systems by [93,94,143]. In their proposed framework, Passerat-Palmbach et al. [94] emphasized privacy protection in

FL-based electronic healthcare systems by leveraging blockchain for decentralized model aggregation and using secure multi-party computation and hardware-based encryption. Mazzocca et al. [143] proposed FRAMH, a middleware for healthcare combining FL and blockchain, where localized training ensures privacy, and blockchain secures model aggregation in risk-based healthcare applications. In addition, blockchain secures model updates, preventing tampering and maintaining data integrity in emergency and routine medical scenarios. Rahman et al. [93] proposed an *Internet of Health Things* (IoHT) framework in which blockchain replaces the centralized aggregator with a decentralized gradient mining system. Each federated client node performs local training, and encrypted gradient updates are aggregated using blockchain consensus mechanisms, ensuring privacy in Internet of Health Things.

Lei et al. [137] presented a method in which the aggregation is performed using smart contracts in blockchain. In fact, there is a control node in charge of collecting gradients uploaded by the the clients and after verification to ensure that they are not being tampered with, then the aggregation is performed using the criteria defined in the smart contract.

The utilization of blockchain in FL, specifically for aggregation, presents a significant advancement in ensuring data integrity, transparency, and security [12,69]. This method is increasingly recognized across various schemes, where blockchain not only facilitates secure aggregation through consensus protocols like PBFT and PoW but also enables a decentralized and trustworthy platform for FL. Such approaches mitigate risks of tampering and attacks, underscoring blockchain's role in enhancing the robustness and reliability of PPFL frameworks.

5.5. Blockchain-Enabled Gradient Upload

The combination of blockchain with FL also mitigates privacy and security concerns in gradient upload mechanisms. For instance, in the work by [89], the gradient upload process involves participants transmitting their local models to edge servers, which then disseminate the shared global model over wireless links. Blockchain integration ensures data authenticity and integrity through digital signatures, validating transactions, and guaranteeing that information is not tampered with [89]. In the approach proposed by [24], the gradient upload process involves participants locally training their models using FL, calculating the average gradient of their local data, and then adding Laplace noise to the locally updated model parameters. The updated model parameters are then sent to the *Interplanetary File System* (IPFS), and only the hashes calculated by IPFS are uploaded to the blockchain, ensuring the security and privacy of the uploaded gradients [24].

In their work, Lei et al. [137] proposed a scheme in which clients used a consortium blockchain to upload gradients after a round of local training on their raw data. Similarly, blockchain is used in many studies for gradients upload in the FL process [138–140,144,145].

The integration of blockchain into the FL process enhances the security and privacy of gradient uploads. By utilizing digital signatures and decentralized storage solutions like the IPFS, these approaches ensure data integrity and confidentiality across the network. This method guarantees that gradients are securely uploaded and protected from tampering, significantly bolstering the overall security and privacy framework of FL.

5.6. Comparison of Blockchain-Enabled Federated Learning Schemes

In the burgeoning field of FL, the quest for robust privacy preservation mechanisms is critical, especially within the sensitive domain of healthcare data. This section explores a comparison of contemporary schemes that integrate blockchain to fortify the FL process against privacy and security threats. Pioneering works such as those by Zhang et al. [24] and Kumar et al. [70] have paved the way for innovations that couple the immutable assur-

ance of blockchain with the collaborative essence of FL. Meanwhile, novel propositions like the privacy-focused methodologies in [90,142] and the energy-efficient frameworks in [98] illustrate the dynamic evolution of this interdisciplinary field. Each scheme contributes uniquely to the landscape, whether through enhancing data security or streamlining healthcare monitoring, marking significant strides toward a more secure and efficient FL paradigm. Through this lens, we examine the multifaceted contributions that not only bolster data protection but also navigate the inherent challenges posed by integrating blockchain, revealing a complex yet promising horizon for FL in healthcare. Table 7 presents a comparative analysis of recent works on *Blockchain enabled-Privacy-Preserving FL* (B-PPFL) in SHS, highlighting key contributions, privacy technologies, functionalities, and limitations. The reviewed schemes predominantly utilize FL in combination with blockchain and other privacy-preserving technologies such as DP, SMPC, and HE. These approaches aim to enhance data security and user privacy, offering benefits like improved scalability, secure collaboration, and efficient healthcare monitoring. However, they also face significant challenges, including high communication overhead, complex data management, scalability issues, and computational overhead. Addressing these limitations is crucial for the practical deployment of B-PPFL systems, suggesting a need for future research focused on optimizing communication efficiency, reducing computational burdens, and enhancing system scalability and real-world applicability.

Table 7. Comparative analysis of recent works on B-PPFL.

Schemes	Contribution	Key Technologies	Function	Limitations
Zhang et al. [24]	MPBC: blockchain-based privacy-preserving medical data-sharing scheme using FL	FL, DP	Hight privacy and security level, trustworthiness	Limited performance, scalability and throughput bottlenecks
Singh et al. [47]	A mechanism for privacy preservation of IoT healthcare data using FL and blockchain technology	FL	Privacy preservation, scalability improvement	Long communication delays, data management complexity
Zakaria et al. [97]	HealthFed: collaborative FL and blockchain framework for privacy protection in healthcare	FL, SMPC	Privacy preservation, secure collaboration, high accuracy	High communication overhead
Moulahi et al. [90]	A blockchain-based FL mechanism for privacy preservation of healthcare IoT data	FL	Privacy preservation, data security, efficient healthcare monitoring	Data heterogeneity, network connectivity issues, high latency
Singh et al. [98]	Blockchain-enabled FL mechanism for smart healthcare, emphasizing energy efficiency and privacy protection	FL, HE	Privacy protection, energy efficiency	Complexity in association formulation, NP-hardness of utility maximization problem
Yang et al. [142]	A medical data privacy protection framework by combining blockchain and FL	FL, HE	Privacy preservation, using SC to dynamically choose aggregation nodes instead of fixed server	High computational overhead
Alsamhi et al. [91]	Conceptual framework and technical synergy between FL and blockchain for privacy preservation in healthcare	FL, encryption	Privacy preservation, flexibility in model training	Lack of practical applications, system complexity

PT: privacy technologies.

5.7. Blockchain Enabled FL-Based Smart Healthcare

In this section, we review the latest developments on this topic regarding the four key applications of SHSs considered in this study.

5.7.1. Health Data Management

Nowadays, huge amounts of sensitive data are generated and managed in SHSs from various heterogeneous sources including labs databases, EHRs, and IoT sensors and devices. Managing such a health data warehouse is challenging and necessitates the combination of innovative technologies to ensure privacy and security. Several studies have tackled the integration of blockchain in FL-based SHSs to enhance privacy and security of health data. Ngan et al. [96] proposed PriFL-Chain, a privacy-preserving framework that integrates FL, DP and blockchain to address privacy and communication challenges in SHS. DP is utilized to ensure privacy of the user's sensitive data during local training, while blockchain is utilized to transparently track contributions and reward data owners, fostering collaboration. Despite its strengths, the proposed approach has shown potential limitations in computational overhead, ensuring fair rewards, and securing the IPFS storage system, which the authors suggest addressing through attribute-based encryption in future work. A blockchain-based FL proposed by [146] utilized the combined potential of FL and blockchain to protect the privacy of patients' data stored in EHRs. The work by [147] introduced an approach for protecting personal healthcare records by combining FL and blockchain. The proposed method leverages FL to preserve patient privacy during collaborative model training and uses blockchain technology to ensure secure and immutable storage of model updates. Although this combination improves privacy and security, it is constrained by the inherent scalability and latency challenges of blockchain systems. A blockchain-based FL framework tailored for SHSs, addressing privacy and energy efficiency challenges, is introduced by [98]. Key technologies include DP for securing sensitive data, HE for encrypted computations, and blockchain for decentralized and tamper-resistant model aggregation. Despite its innovative utility for an optimization strategy for WBANs and miners, the framework faces challenges in managing computational overhead due to HE and maintaining efficiency in highly heterogeneous networks. Authors in [148,149] have also proposed blockchain-based FL frameworks to share COVID-19 patient data in a privacy-preserving way.

5.7.2. Medical Imaging

Medical imaging has revolutionized SHSs by allowing researchers and health professionals to learn more about the human body. FL can enhance model training for disease detection and prediction through patterns identification in medical imaging. The association with blockchain can improve the framework by enhancing privacy, security, and transparency. Authors have tackled the topic in various ways. Kumar et al. [150] proposed a privacy-preserving framework that integrates blockchain with FL and deep learning for COVID-19 detection using CT imaging. While blockchain ensures secure data sharing and model authenticity, FL enables collaborative model training across hospitals without compromising data privacy. However, the proposed approach faces challenges related to computational overhead and scalability due to the integration of blockchain and the need for diverse, high-quality datasets. Similarly, ref. [70] introduced a blockchain-based FL framework for collaborative medical image analysis for COVID-19 detection using CT scans. By integrating blockchain, homomorphic encryption, and FL, the approach ensures secure, privacy-preserving data sharing and decentralized model training. Blockchain eliminates reliance on central servers and enhances trust, while homomorphic encryption safeguards gradient privacy. However, challenges remain about computational overhead and potential latency from blockchain operations. The authors in [151] presented a blockchain-enhanced FL framework for brain tumor segmentation, integrating FL with blockchain's decentralization, traceability, and tamper-proof features to ensure privacy, trust, and robustness in collaborative model training. This approach faces similar challenges as the above studies.

Authors in [152,153] also investigated the potential of combining FL and blockchain for secure medical imaging frameworks in SHSs.

5.7.3. Remote Health Management

Remote healthcare monitoring has revolutionized SHSs by enabling remote data collection and remote healthcare service delivery through various IoT and wearable devices. The integration of FL in RHM significantly improved data privacy, as users' data are kept locally. Few studies focused on integrating FL with blockchain to enhance privacy and security in the context of remote health monitoring. For example, ref. [154] introduced a BC-FL framework for remote disease detection. While FL serves for collaborative ML model training, blockchain ensures secure and transparent data sharing among users. The authors in [155] proposed a blockchain-integrated FL framework for real-time patient monitoring in the IoMT. While blockchain enhances data integrity and security by recording all model updates and device authentications, FL ensures privacy by keeping sensitive patient data localized. However, balancing energy efficiency with computational demands and addressing the scalability of the system in large-scale IoMT networks remains a challenge. In [156], authors developed a blockchain-enabled FL method for personalized healthcare using IoMT devices, combining FL for on-device data privacy and blockchain for secure, decentralized data management and communication. Specifically, blockchain ensures tamper-proof storage, data integrity, and secure access in remote healthcare monitoring systems, avoiding risks of single points of failure and enhancing trust. Authors in [20] proposed a secure health monitoring system in healthcare 5.0 that integrates blockchain with FL to detect malicious activities in a healthcare network and enable physicians to remotely monitor patients. FL and blockchain have been combined for COVID-19 detection through remote frameworks [150,157].

5.7.4. Health Finance Management

Blockchain [158] with its features including privacy, security, transparency, and immutability stands as a suitable approach to ensure trustworthiness in SHSs. Blockchain can ensure secure financial transactions through cryptocurrency payment in SHSs and considerably reduce administrative costs and eliminate financial frauds. For example, insurance service is one of the most frustrating for patients because insurers need to verify all the provided evidence to avoid fraudulent claims and fake documents. Blockchain can enhance the claim process by providing risk-free management and transparency and allowing the insurers to take ownership of assets to be insured for insurers [159]. The integration of blockchain technology in FL-based SHSs can significantly improve the financial services in many ways, including traceability in financial management, cryptocurrency payment, trustworthy insurance claim processing, audit, and billing.

6. Discussions and Future Work

In this section, a few findings and challenges are presented in Section 6.1 along with related opportunities in Section 6.2.

6.1. Discussions

Privacy-preserving FL holds substantial promise for revolutionizing healthcare systems by addressing the critical need for maintaining patient privacy while leveraging the collective intelligence of distributed data sources. Through our survey, several key insights emerged that shed light on the current landscape, opportunities, and challenges in this burgeoning field.

We classified privacy threats in SHSs into five main types, including data breaches, insider threats, technical vulnerabilities, user privacy concerns, and regulatory compliance

issues. These threats pose significant risks to patient privacy, data integrity, and trust in SHSs. We highlighted the complexities and challenges inherent in protecting sensitive health information and underscored the need for robust privacy-preserving mechanisms. After discussing FL principles and its potential benefits in SHSs, FL stands as a suitable solution to address privacy challenges in SHSs, facilitating collaborative model training while ensuring data integrity and confidentiality. However, as FL alone cannot ensure strong privacy protection, a new paradigm known as PPFL was discussed and a classification of FL-based privacy-enhancing mechanisms in SHSs was proposed. The proposed taxonomy relies on three main groups of techniques including PETs, DLT, and hybrid techniques, along with existing approaches and applications of each approach in SHSs.

On one hand, we identified DP, HE, and SMPC as the leading PETs that, when integrated with FL, significantly enhance privacy guarantees. Each technique presents unique strengths and challenges: DP is highly scalable but may suffer from utility loss; HE ensures robust security but incurs substantial computational overhead; SMPC provides strong security guarantees with moderate overhead. On the other hand, blockchain emerges as an efficient technology for addressing several inherent challenges in FL, particularly in decentralized and trustless environments. Blockchain enhances the integrity and transparency of FL processes, ensuring that model updates are tamper-proof and auditable. However, the integration of blockchain with FL also introduces challenges such as increased latency and computational requirements, which necessitate further optimization.

Furthermore, to comprehensively discuss the blockchain applications in FL for privacy protection, we focus on three key dimensions such as model storage, aggregation, and gradient upload, highlighting how blockchain's features can specifically address and mitigate privacy challenges in FL systems. The combination of blockchain with FL not only secures data transactions and model updates but also fosters a cooperative and reliable environment for participants across various sectors, particularly in SHSs, where data sensitivity is paramount. Although the reviewed schemes share common benefits in enhancing privacy and security, they face distinct challenges such as performance limitations, communication overhead, and computational intensity.

Another notable finding is the growing interest and adoption of PPFL methods within smart healthcare, especially for health data management, remote health monitoring, medical imaging, and health finance management. Researchers and practitioners alike are increasingly recognizing the significance of privacy-preserving techniques in safeguarding sensitive medical data, especially in light of strict regulatory requirements such as HIPAA and GDPR. The proliferation of PPFL frameworks specifically tailored for healthcare applications underscores the urgency and importance of addressing privacy concerns in this context.

Despite the promising advancements in FL-based privacy-preserving frameworks, several challenges remain. Chief among these is the inherent trade-off between privacy and utility in FL settings. While PPFL schemes strive to protect patient privacy, they must also ensure that the resulting models retain sufficient accuracy and generalizability for clinical use. Balancing these competing objectives remains a complex and ongoing research endeavor, requiring innovative solutions at the intersection of ML, cryptography, and healthcare domain knowledge.

Another critical consideration is the diversity of healthcare stakeholders and the varying levels of trust among participants. Building secure and resilient PPFL systems requires the establishment of robust governance structures, transparent communication channels, and mechanisms to verify the integrity of the participants.

Moreover, blockchain-enabled privacy-preserving FL presents several challenges such as latency, energy consumption, interoperability, and data storage costs. In fact,

the consensus mechanisms introduced by blockchain such as Proof of Work and Practical Byzantine Fault Tolerance can cause delays in large-scale FL–SHSs frameworks. This situation can significantly affect the efficiency of SHSs which require real-time blockchain protocols that are also known as high-energy consumers, which may not satisfy the SHSs' sustainability goals. Data storage is another challenge for blockchain-enabled PPFL, as the implementation of blockchain needs huge storage capacity to store models and gradients. It can be more challenging in SHSs with the management of high-dimensional healthcare data. Finally, the integration of blockchain into PPFL within SHSs requires seamless interoperability, which remains an ongoing challenge.

Joint efforts between researchers, healthcare providers, policymakers, and technology providers are required to foster trust and cooperation in FL-based smart healthcare ecosystems.

6.2. Future Works

This survey explored FL, PETs, and blockchain as well as their integration into SHSs, highlighting their potential to address the critical challenge of privacy protection and their combined capability to significantly enhance privacy and security in data handling. Each technology contributes uniquely to PPFL by training models on decentralized data [160], PETs by securing data at rest and in transit [106], and blockchain by ensuring data integrity and traceability [62]. As demonstrated, while each technology has its merits, their combined application can significantly enhance the privacy and security standards of data processing in the healthcare sector.

While FL enhances model utility without compromising data privacy [84], PETs add an additional layer of data protection, and blockchain provides a secure, immutable ledger for transparent and traceable transactions [90]. Our work highlights several critical findings and implications that can motivate future advancements in this domain. Given the heavy computational demands of blockchain-based frameworks and the resources constraints nature of smart healthcare devices, further research could focus on lightweight blockchain solutions, enabling efficient and secure computing for various SHS applications.

In addition, the scalability and efficiency of PPFL frameworks need further investigation. As healthcare datasets continuously grow in size and complexity, the computational and communication overhead associated with FL presents significant challenges. Efforts to optimize and streamline PPFL protocols, while maintaining robust privacy guarantees, are imperative to reap the full benefit of FL in healthcare. Despite the promising synergies identified, integrating these technologies into existing healthcare infrastructures presents notable challenges, including technical complexities and scalability concerns [25]. To address these challenges, a shift in regulatory frameworks and ongoing technological refinement are necessary to support innovative solutions.

Future research should therefore focus on advancing these technologies' seamless integration, developing methods that balance privacy with utility, privacy with computational demands, and crafting adaptive frameworks that respond to the dynamic nature of healthcare data and privacy standards. By continuing to innovate and rigorously evaluate PETs, the field of smart healthcare progresses toward a future where data-driven insights and patient privacy are not at odds but are instead facets of a harmonious and highly effective healthcare system.

7. Conclusions

This survey addresses a critical challenge of privacy protection in FL-based smart healthcare systems, highlighting the high potential of blockchain to be combined with PETs for the strongest privacy-preserving schemes. Specifically, this survey comprehensively

reviewed the latest advancements on the integration of PETs and blockchain into FL-based SHSs with a focus on four main applications of SHSs such as health data management, remote healthcare monitoring, medical imaging, and health finance management. To better explain the integration of blockchain in FL-based SHSs, this survey focuses on three technical dimensions, including model storage, gradients upload, and aggregation. Among the key findings of this survey, it is worth noting the potential of combining blockchain with PETs in mitigating privacy threats in FL-based SHSs. Despite significant progress in this field, challenges remain, including computational overhead, communication inefficiencies, latency, and the need for better regulatory alignment. By bridging the gaps identified, this work aims to inspire continued innovation toward robust and privacy-preserving SHSs, ultimately contributing to a trustworthy and more efficient healthcare ecosystem.

Author Contributions: Investigation, Z.N.L.; conceptualization, analysis and methodology Z.N.L. and K.G.; original draft preparation, Z.N.L.; writing—review and editing, J.Y. and K.G.; theoretical framework and project administration, K.G.; work synthesis, supervision and review, J.Y.; proofreading, J.Y., K.G. and Z.N.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Beijing Municipal Science and Technology Commission Project (Z241100009124008).

Data Availability Statement: Data are contained within the article.

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

References

1. Ashton, K. That 'internet of things' thing. *RFID J.* **2009**, *22*, 97–114.
2. Ibarra-Esquer, J.E.; González-Navarro, F.F.; Flores-Rios, B.L.; Burtseva, L.; Astorga-Vargas, M.A. Tracking the evolution of the internet of things concept across different application domains. *Sensors* **2017**, *17*, 1379. [CrossRef] [PubMed]
3. Kala, M.K.; Priya, M. A Comprehensive Survey on the IoT-Based Electronic Healthcare Records Security, Privacy Issues, and Countermeasures Using Blockchain Technology. In Proceedings of the 2023 International Conference on Innovations in Engineering and Technology (ICIET), Muvattupuzha, India, 13–14 July 2023 ; IEEE: New York, NY, USA, 2023; pp. 1–8.
4. Sinha, S. State of IoT 2023: Number of Connected IoT Devices Growing 16% to 16.7 Billion Globally. 2023. Available online: https://iot-analytics.com/number-connected-iot-devices/ (accessed on 14 January 2024).
5. Vailshery, L.S. IoT Connected Devices Worldwide 2030. 2023. Available online: https://www.statista.com/statistics/802690/worldwide-connecteddevices-by-access-technology (accessed on 5 February 2024).
6. Abaoud, M.; Almuqrin, M.; Khan, M.F. Advancing Federated Learning Through Novel Mechanism for Privacy Preservation in Healthcare Applications. *IEEE Access* **2023**, *11*, 83562–83579. [CrossRef]
7. Patel, V.A.; Bhattacharya, P.; Tanwar, S.; Gupta, R.; Sharma, G.; Bokoro, P.N.; Sharma, R. Adoption of federated learning for healthcare informatics: Emerging applications and future directions. *IEEE Access* **2022**, *10*, 90792–90826. [CrossRef]
8. Yang, Q.; Liu, Y.; Cheng, Y.; Kang, Y.; Chen, T.; Yu, H. *Federated Learning*; Morgan & Claypool Publishers: Kentfield, CA, USA, 2019.
9. Annas, G.J. HIPAA regulations: A new era of medical-record privacy? *N. Engl. J. Med.* **2003**, *348*, 1486. [CrossRef]
10. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; Arcas, B.A. Communication-efficient learning of deep networks from decentralized data. In Proceedings of the Artificial Intelligence and Statistics, PMLR, Fort Lauderdale, FL, USA, 20–22 April 2017; pp. 1273–1282.
11. Wibawa, F.; Catak, F.O.; Kuzlu, M.; Sarp, S.; Cali, U. Homomorphic encryption and federated learning based privacy-preserving cnn training: Covid-19 detection use-case. In Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference, Stavanger, Norway, 14–15 June 2022; pp. 85–90.
12. Hiwale, M.; Walambe, R.; Potdar, V.; Kotecha, K. A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine. *Healthc. Anal.* **2023**, *3*, 100192. [CrossRef]
13. Wei, Q.; Rao, G. EPFL-DAC: Enhancing Privacy in Federated Learning with Dynamic Aggregation and Clipping. *Comput. Secur.* **2024**, *143*, 103911. [CrossRef]
14. Nasr, M.; Shokri, R.; Houmansadr, A. Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; IEEE: New York, NY, USA, 2019; pp. 739–753.

15. Liu, L.; Wang, Y.; Liu, G.; Peng, K.; Wang, C. Membership inference attacks against machine learning models via prediction sensitivity. *IEEE Trans. Dependable Secur. Comput.* **2022**, *20*, 2341–2347. [CrossRef]
16. Hitaj, B.; Ateniese, G.; Perez-Cruz, F. Deep models under the GAN: Information leakage from collaborative deep learning. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 603–618.
17. Zhang, Y.; Jia, R.; Pei, H.; Wang, W.; Li, B.; Song, D. The secret revealer: Generative model-inversion attacks against deep neural networks. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Seattle, WA, USA, 13–19 June 2020; pp. 253–261.
18. Ali, M.; Naeem, F.; Tariq, M.; Kaddoum, G. Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. *IEEE J. Biomed. Health Inform.* **2022**, *27*, 778–789. [CrossRef]
19. Blanco-Justicia, A.; Domingo-Ferrer, J.; Martínez, S.; Sánchez, D.; Flanagan, A.; Tan, K.E. Achieving security and privacy in federated learning systems: Survey, research challenges and future directions. *Eng. Appl. Artif. Intell.* **2021**, *106*, 104468. [CrossRef]
20. Rehman, A.; Razzak, I.; Xu, G. Federated learning for privacy preservation of healthcare data from smartphone-based side-channel attacks. *IEEE J. Biomed. Health Inform.* **2022**, *27*, 684–690. [CrossRef] [PubMed]
21. Zhu, L.; Gai, K.; Li, M.; Zhu, L.; Gai, K.; Li, M. Security and Privacy Issues in Internet of things. In *Blockchain Technology in Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 29–40.
22. Gai, K.; Tang, H.; Li, G.; Xie, T.; Wang, S.; Zhu, L.; Choo, K.K.R. Blockchain-based privacy-preserving positioning data sharing for IoT-enabled maritime transportation systems. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 2344–2358. [CrossRef]
23. Gai, K.; She, Y.; Zhu, L.; Choo, K.K.R.; Wan, Z. A blockchain-based access control scheme for zero trust cross-organizational data sharing. *ACM Trans. Internet Technol.* **2023**, *23*, 1–25. [CrossRef]
24. Zhang, H.; Li, G.; Zhang, Y.; Gai, K.; Qiu, M. Blockchain-based privacy-preserving medical data sharing scheme using federated learning. In Proceedings of the Knowledge Science, Engineering and Management: 14th International Conference, KSEM 2021, Tokyo, Japan, 14–16 August 2021; Proceedings, Part III 14; Springer: Berlin/Heidelberg, Germany, 2021; pp. 634–646.
25. Gu, C.; Cui, X.; Zhu, X.; Hu, D. FL2DP: Privacy-Preserving Federated Learning Via Differential Privacy for Artificial IoT. *IEEE Trans. Ind. Inform.* **2023**, *20*, 5100–5111. [CrossRef]
26. Moon, S.; Lee, W.H. Privacy-Preserving Federated Learning in Healthcare. In Proceedings of the 2023 International Conference on Electronics, Information, and Communication (ICEIC), Singapore, 5–8 February 2023; IEEE: New York, NY, USA, 2023; pp. 1–4.
27. Briggs, C.; Fan, Z.; Andras, P. A review of privacy-preserving federated learning for the Internet-of-Things. In *Federated Learning Systems: Towards Next-Generation AI*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 21–50.
28. Yin, X.; Zhu, Y.; Hu, J. A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–36. [CrossRef]
29. Nguyen, D.C.; Pham, Q.V.; Pathirana, P.N.; Ding, M.; Seneviratne, A.; Lin, Z.; Dobre, O.; Hwang, W.J. Federated learning for smart healthcare: A survey. *ACM Comput. Surv. (CSUR)* **2022**, *55*, 1–37. [CrossRef]
30. Mansour, R.F.; El Amraoui, A.; Nouaouri, I.; Díaz, V.G.; Gupta, D.; Kumar, S. Artificial intelligence and internet of things enabled disease diagnosis model for smart healthcare systems. *IEEE Access* **2021**, *9*, 45137–45146. [CrossRef]
31. Sahinbas, K.; Catak, F.O. Secure multi-party computation-based privacy-preserving data analysis in healthcare IoT systems. In *Interpretable Cognitive Internet of Things for Healthcare*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 57–72.
32. Sethi, P.; Sarangi, S.R. Internet of things: Architectures, protocols, and applications. *J. Electr. Comput. Eng.* **2017**, *2017*, 324035. [CrossRef]
33. Lombardi, M.; Pascale, F.; Santaniello, D. Internet of things: A general overview between architectures, protocols and applications. *Information* **2021**, *12*, 87. [CrossRef]
34. Jiang, F.; Chen, Z.; Liu, L.; Wang, J. Federated Learning-Based Privacy Protection for IoT-based Smart Healthcare Systems. In Proceedings of the 2023 IEEE/CIC International Conference on Communications in China (ICCC Workshops), Dalian, China, 10–12 August 2023; IEEE: New York, NY, USA, 2023; pp. 1–6.
35. Schoder, D. Introduction to the Internet of Things. In *Internet of Things A to Z: Technologies and Applications*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2018; pp. 1–50.
36. Tian, S.; Yang, W.; Le Grange, J.M.; Wang, P.; Huang, W.; Ye, Z. Smart healthcare: Making medical care more intelligent. *Glob. Health J.* **2019**, *3*, 62–65. [CrossRef]
37. AbdulRaheem, M.; Oladipo, I.D.; González-Briones, A.; Awotunde, J.B.; Tomori, A.R.; Jimoh, R.G. An efficient lightweight speck technique for edge-IoT-based smart healthcare systems. In *5G IoT and Edge Computing for Smart Healthcare*; Elsevier: Amsterdam, The Netherlands, 2022; pp. 139–162.
38. Yadav, A.; Ahmad, N.; Khan, I.R.; Agarwal, P.; Kaur, H. Role of AI, Big data in Smart Healthcare System. In Proceedings of the 2023 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 3–4 March 2023; IEEE: New York, NY, USA, 2023; pp. 1–8.

39. Puthal, D.; Malik, N.; Mohanty, S.P.; Kougianos, E.; Yang, C. The blockchain as a decentralized security framework [future directions]. *IEEE Consum. Electron. Mag.* **2018**, *7*, 18–21. [CrossRef]
40. Saba Raoof, S.; Durai, M. A comprehensive review on smart health care: Applications, paradigms, and challenges with case studies. *Contrast Media Mol. Imaging* **2022**, *2022*, 822235. [CrossRef] [PubMed]
41. Jourdan, T.; Boutet, A.; Bahi, A.; Frindel, C. Privacy-Preserving IoT framework for activity recognition in personal healthcare monitoring. *ACM Trans. Comput. Healthc.* **2020**, *2*, 1–22. [CrossRef]
42. Warren, S.D.; Brandeis, L.D. The Right to Privacy. *Harv. Law Rev.* **1890**, *4*, 193–220. [CrossRef]
43. Kalaiarasy, C.; Sreenath, N.; Amuthan, A. Location privacy preservation in VANET using mix zones—A survey. In Proceedings of the 2019 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 23–25 January 2019; IEEE: New York, NY, USA, 2019; pp. 1–5.
44. Barker, E.; Smid, M.; Branstad, D.; Chokhani, S. A framework for designing cryptographic key management systems. *NIST Spec. Publ.* **2013**, *800*, 1–112.
45. Sagirlar, G. Enhancing Data Privacy and Security in Internet of Things Through Decentralized Models and Services. Ph.D. Thesis, Università degli Studi dell'Insubria, Busto Arsizio, Italy, 2018.
46. Majeed, A.; Lee, S. Anonymization techniques for privacy preserving data publishing: A comprehensive survey. *IEEE Access* **2020**, *9*, 8512–8545. [CrossRef]
47. Singh, S.; Rathore, S.; Alfarraj, O.; Tolba, A.; Yoon, B. A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Gener. Comput. Syst.* **2022**, *129*, 380–388. [CrossRef]
48. Jagarlamudi, G.K.; Yazdinejad, A.; Parizi, R.M.; Pouriyeh, S. Exploring privacy measurement in federated learning. *J. Supercomput.* **2023**, *80*, 10511–10551. [CrossRef]
49. Ding, D.; Conti, M.; Solanas, A. A smart health application and its related privacy issues. In Proceedings of the 2016 Smart City Security and Privacy Workshop (SCSP-W), Vienna, Austria, 11 April 2016; IEEE: New York, NY, USA, 2016; pp. 1–5.
50. Chen, W.; Wu, H.; Chen, X.; Chen, J. A Review of Research on Privacy Protection of Internet of Vehicles Based on Blockchain. *J. Sens. Actuator Netw.* **2022**, *11*, 86. [CrossRef]
51. Wang, W.; Li, X.; Qiu, X.; Zhang, X.; Brusic, V.; Zhao, J. A privacy preserving framework for federated learning in smart healthcare systems. *Inf. Process. Manag.* **2023**, *60*, 103167. [CrossRef]
52. Hassan, A. *Federated Learning and AI for Healthcare 5.0*; IGI Global: Hershey, PA, USA, 2024.
53. Stojkov, M.; Sladić, G.; Milosavljević, B.; Zarić, M.; Simić, M. Privacy concerns in IoT smart healthcare system. In Proceedings of the International Conference on Information Science and Technology (ICIST), Kopaonik, Serbia, 10–13 March 2019; pp. 62–65.
54. Ranjith, J.; Mahantesh, K. Privacy and security issues in smart health care. In Proceedings of the 2019 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT), Mysuru, India, 13–14 December 2019; IEEE: New York, NY, USA, 2019; pp. 378–383.
55. Javeed, D.; Gao, T.; Saeed, M.S.; Kumar, P.; Kumar, R.; Jolfaei, A. A softwarized intrusion detection system for iot-enabled smart healthcare system. *ACM Trans. Internet Technol.* **2023**. [CrossRef]
56. Newaz, A.I.; Sikder, A.K.; Rahman, M.A.; Uluagac, A.S. A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. *ACM Trans. Comput. Healthc.* **2021**, *2*, 1–44. [CrossRef]
57. Green, M.L.; Dozier, P. Understanding Human Factors of Cybersecurity: Drivers of Insider Threats. In Proceedings of the 2023 IEEE International Conference on Cyber Security and Resilience (CSR), Venice, Italy, 31 July–2 August 2023; IEEE: New York, NY, USA, 2023; pp. 111–116.
58. Ansbach, J.; Sharton, B. Preventing insider threats to cybersecurity. *Risk Manag.* **2020**, *67*, 12–13.
59. Reuben, N.; Irawan, R.; Jovann, R.N.; Achmad, S.; Junior, F.A.; Nadia. Raising Cyber Security Awareness to Reduce Social Engineering Through Social Media in Indonesia. In Proceedings of the 2023 3rd International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS), Yogyakarta, Indonesia, 9–10 August 2023; IEEE: New York, NY, USA, 2023; pp. 138–141.
60. Jin, J.; Lee, I. A Study on the Considerations for Establishing a Security Model for Non-face-to-face Telehealth. In Proceedings of the 2022 13th International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 19–21 October 2022; IEEE: New York, NY, USA, 2022; pp. 1806–1810.
61. Qin, Z.; Li, G.Y.; Ye, H. Federated learning and wireless communications. *IEEE Wirel. Commun.* **2021**, *28*, 134–140. [CrossRef]
62. Kairouz, P.; McMahan, H.B.; Avent, B.; Bellet, A.; Bennis, M.; Bhagoji, A.N.; Bonawitz, K.; Charles, Z.; Cormode, G.; Cummings, R.; et al. Advances and open problems in federated learning. *Found. Trends Mach. Learn.* **2021**, *14*, 1–210. [CrossRef]
63. Zhang, X.; Fu, A.; Wang, H.; Zhou, C.; Chen, Z. A privacy-preserving and verifiable federated learning scheme. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; IEEE: New York, NY, USA, 2020; pp. 1–6.

64. Thapa, C.; Arachchige, P.C.M.; Camtepe, S.; Sun, L. Splitfed: When federated learning meets split learning. In Proceedings of the AAAI Conference on Artificial Intelligence, Pittsburgh, PA, USA, 22 February–1 March 2022; Volume 36, pp. 8485–8493.
65. Hao, M.; Li, H.; Luo, X.; Xu, G.; Yang, H.; Liu, S. Efficient and privacy-enhanced federated learning for industrial artificial intelligence. *IEEE Trans. Ind. Inform.* **2019**, *16*, 6532–6542. [CrossRef]
66. Mammen, P.M. Federated learning: Opportunities and challenges. *arXiv* **2021**, arXiv:2101.05428.
67. Fang, L.; Yin, C.; Zhu, J.; Ge, C.; Tanveer, M.; Jolfaei, A.; Cao, Z. Privacy protection for medical data sharing in smart healthcare. *ACM Trans. Multimed. Comput. Commun. Appl. (TOMM)* **2020**, *16*, 1–18. [CrossRef]
68. Gai, K.; Qiu, M.; Li, Y.; Liu, X.Y. Advanced fully homomorphic encryption scheme over real numbers. In Proceedings of the 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, USA, 26–28 June 2017; IEEE: New York, NY, USA, 2017; pp. 64–69.
69. Liu, Z.; Guo, J.; Yang, W.; Fan, J.; Lam, K.Y.; Zhao, J. Privacy-preserving aggregation in federated learning: A survey. In *IEEE Transactions on Big Data*; IEEE: New York, NY, USA, 2022.
70. Kumar, R.; Kumar, J.; Khan, A.A.; Ali, H.; Bernard, C.M.; Khan, R.U.; Zeng, S. Blockchain and homomorphic encryption based privacy-preserving model aggregation for medical images. *Comput. Med. Imaging Graph.* **2022**, *102*, 102139. [CrossRef]
71. Liu, J.; Huang, J.; Zhou, Y.; Li, X.; Ji, S.; Xiong, H.; Dou, D. From distributed machine learning to federated learning: A survey. *Knowl. Inf. Syst.* **2022**, *64*, 885–917. [CrossRef]
72. Zhang, D.; Chen, X.; Wang, D.; Shi, J. A survey on collaborative deep learning and privacy-preserving. In Proceedings of the 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), Guangzhou, China, 18–21 June 2018; IEEE: New York, NY, USA, 2018; pp. 652–658.
73. Algarni, A. A survey and classification of security and privacy research in smart healthcare systems. *IEEE Access* **2019**, *7*, 101879–101894. [CrossRef]
74. Rivest, R.L. Chapter 13—Cryptography. In *Algorithms and Complexity*; van Leeuwen, J., Ed.; Handbook of Theoretical Computer Science; Elsevier: Amsterdam, The Netherland, 1990; pp. 717–755. [CrossRef]
75. Park, J.; Lim, H. Privacy-preserving federated learning using homomorphic encryption. *Appl. Sci.* **2022**, *12*, 734. [CrossRef]
76. Shi, Z.; Yang, Z.; Hassan, A.; Li, F.; Ding, X. A privacy preserving federated learning scheme using homomorphic encryption and secret sharing. *Telecommun. Syst.* **2023**, *82*, 419–433. [CrossRef]
77. Wang, B.; Li, H.; Guo, Y.; Wang, J. PPFLHE: A privacy-preserving federated learning scheme with homomorphic encryption for healthcare data. *Appl. Soft Comput.* **2023**, *146*, 110677. [CrossRef]
78. Kanagavelu, R.; Li, Z.; Samsudin, J.; Yang, Y.; Yang, F.; Goh, R.S.M.; Cheah, M.; Wiwatphonthana, P.; Akkarajitsakul, K.; Wang, S. Two-phase multi-party computation enabled privacy-preserving federated learning. In Proceedings of the 2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID), Melbourne, VIC, Australia, 11–14 May 2020; IEEE: New York, NY, USA, 2020; pp. 410–419.
79. Tran, A.T.; Luong, T.D.; Pham, X.S. A Novel Privacy-Preserving Federated Learning Model Based on Secure Multi-party Computation. In Proceedings of the International Symposium on Integrated Uncertainty in Knowledge Modelling and Decision Making, Kanazawa, Japan, 2–4 November 2023; Springer: Berlin/Heidelberg, Germany, 2023; pp. 321–333.
80. Dey, J.; Bhowmik, A.; Karforma, S. Neural perceptron & strict lossless secret sharing oriented cryptographic science: Fostering patients' security in the "new normal" COVID-19 E-Health. *Multimed. Tools Appl.* **2022**, *81*, 17747–17778.
81. Bonawitz, K.; Ivanov, V.; Kreuter, B.; Marcedone, A.; McMahan, H.B.; Patel, S.; Ramage, D.; Segal, A.; Seth, K. Practical secure aggregation for privacy-preserving machine learning. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 1175–1191.
82. Anand, A.; Singh, A.K. Secret sharing based watermarking for copy-protection and ownership control of medical Image. In Proceedings of the 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 6–8 July 2021; pp. 1–7.
83. Zheng, H.; Hu, H.; Han, Z. Preserving user privacy for machine learning: Local differential privacy or federated machine learning? *IEEE Intell. Syst.* **2020**, *35*, 5–14. [CrossRef]
84. Li, J.; Meng, Y.; Ma, L.; Du, S.; Zhu, H.; Pei, Q.; Shen, X. A federated learning based privacy-preserving smart healthcare system. *IEEE Trans. Ind. Inform.* **2021**, *18*, 2021–2031. [CrossRef]
85. Wei, K.; Li, J.; Ding, M.; Ma, C.; Su, H.; Zhang, B.; Poor, H.V. User-Level Privacy-Preserving Federated Learning: Analysis and Performance Optimization. *IEEE Trans. Mob. Comput.* **2022**, *21*, 3388–3401. [CrossRef]
86. Choudhury, O.; Gkoulalas-Divanis, A.; Salonidis, T.; Sylla, I.; Park, Y.; Hsu, G.; Das, A. Anonymizing data for privacy-preserving federated learning. *arXiv* **2020**, arXiv:2002.09096.
87. Sweeney, L. k-anonymity: A model for protecting privacy. *Int. J. Uncertain. Fuzziness-Knowl.-Based Syst.* **2002**, *10*, 557–570. [CrossRef]
88. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. 2008.

89. Yang, Z.; Shi, Y.; Zhou, Y.; Wang, Z.; Yang, K. Trustworthy federated learning via blockchain. *IEEE Internet Things J.* **2022**, *10*, 92–109. [CrossRef]
90. Moulahi, W.; Jdey, I.; Moulahi, T.; Alawida, M.; Alabdulatif, A. A blockchain-based federated learning mechanism for privacy preservation of healthcare IoT data. *Comput. Biol. Med.* **2023**, *167*, 107630. [CrossRef] [PubMed]
91. Alsamhi, S.H.; Myrzashova, R.; Hawbani, A.; Kumar, S.; Srivastava, S.; Zhao, L.; Wei, X.; Guizan, M.; Curry, E. Federated Learning Meets Blockchain in Decentralized Data-Sharing: Healthcare Use Case. *IEEE Internet Things J.* **2024**, *11*, 19602–19615. [CrossRef]
92. Kasyap, H.; Tripathy, S. Privacy-preserving decentralized learning framework for healthcare system. *ACM Trans. Multimed. Comput. Commun. Appl. (TOMM)* **2021**, *17*, 1–24. [CrossRef]
93. Rahman, M.A.; Hossain, M.S.; Islam, M.S.; Alrajeh, N.A.; Muhammad, G. Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach. *IEEE Access* **2020**, *8*, 205071–205087. [CrossRef]
94. Passerat-Palmbach, J.; Farnan, T.; McCoy, M.; Harris, J.D.; Manion, S.T.; Flannery, H.L.; Gleim, B. Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data. In Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2–6 November 2020; IEEE: New York, NY, USA, 2020; pp. 550–555.
95. Gai, K.; Wu, Y.; Zhu, L.; Zhang, Z.; Qiu, M. Differential privacy-based blockchain for industrial internet-of-things. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4156–4165. [CrossRef]
96. Ngan Van, L.; Hoang Tuan, A.; Phan The, D.; Vo, T.K.; Pham, V.H. A Privacy-Preserving Approach For Building Learning Models in Smart Healthcare using Blockchain and Federated Learning. In Proceedings of the 11th International Symposium on Information and Communication Technology, Wuhan, China, 4–6 February 2022; pp. 435–441.
97. Abou El Houda, Z.; Hafid, A.S.; Khoukhi, L.; Brik, B. When collaborative federated learning meets blockchain to preserve privacy in healthcare. *IEEE Trans. Netw. Sci. Eng.* **2022**, *10*, 2455–2465. [CrossRef]
98. Singh, M.B.; Singh, H.; Pratap, A. Energy-Efficient and Privacy-Preserving Blockchain Based Federated Learning for Smart Healthcare System. *IEEE Trans. Serv. Comput.* **2023**, *17*, 2392–2403. [CrossRef]
99. Shen, G.; Fu, Z.; Gui, Y.; Susilo, W.; Zhang, M. Efficient and privacy-preserving online diagnosis scheme based on federated learning in e-healthcare system. *Inf. Sci.* **2023**, *647*, 119261. [CrossRef]
100. Dwork, C.; McSherry, F.; Nissim, K.; Smith, A. Calibrating noise to sensitivity in private data analysis. In Proceedings of the Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, 4–7 March 2006; Proceedings 3; Springer: Berlin/Heidelberg, Germany, 2006; pp. 265–284.
101. Weng, S.; Zhang, L.; Feng, D.; Feng, C.; Wang, R.; Klaine, P.V.; Imran, M.A. Privacy-Preserving Federated Learning based on Differential Privacy and Momentum Gradient Descent. In Proceedings of the 2022 International Joint Conference on Neural Networks (IJCNN), Padua, Italy, 18–23 July 2022; IEEE: New York, NY, USA, 2022; pp. 1–6.
102. Abadi, M.; Chu, A.; Goodfellow, I.; McMahan, H.B.; Mironov, I.; Talwar, K.; Zhang, L. Deep learning with differential privacy. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 308–318.
103. Yang, G.; Wang, S.; Wang, H. Federated learning with personalized local differential privacy. In Proceedings of the 2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS), Chengdu, China, 23–26 April 2021; IEEE: New York, NY, USA, 2021; pp. 484–489.
104. Li, Z. A Personalized Privacy-Preserving Scheme for Federated Learning. In Proceedings of the 2022 IEEE International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA), Changchun, China, 25–27 February 2022; IEEE: New York, NY, USA, 2022; pp. 1352–1356.
105. Khanna, A.; Schaffer, V.; Gürsoy, G.; Gerstein, M. Privacy-preserving model training for disease prediction using federated learning with differential privacy. In Proceedings of the 2022 44th Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), Glasgow, UK, 11–15 July 2022; IEEE: New York, NY, USA, 2022; pp. 1358–1361.
106. Iqbal, M.; Tariq, A.; Adnan, M.; Ud Din, I.; Qayyum, T. FL-ODP: An Optimized Differential Privacy Enabled Privacy Preserving Federated Learning. *IEEE Access* **2023**, *11*, 116674–116683. [CrossRef]
107. Acar, A.; Aksu, H.; Uluagac, A.S.; Conti, M. A survey on homomorphic encryption schemes: Theory and implementation. *ACM Comput. Surv. (Csur)* **2018**, *51*, 1–35. [CrossRef]
108. Gai, K.; Wu, Y.; Zhu, L.; Qiu, M. Privacy-preserving data synchronization using tensor-based fully homomorphic encryption. In Proceedings of the 2018 17th IEEE International Conference On Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; IEEE: New York, NY, USA, 2018; pp. 1149–1156.
109. Jain, N.; Cherukuri, A.K.A.; Kamalov, F. Revisiting Fully Homomorphic Encryption Schemes for Privacy-Preserving Computing. In *Emerging Technologies and Security in Cloud Computing*; IGI Global: Hershey, PA, USA, 2024; pp. 276–294.
110. Gentry, C. A Fully Homomorphic Encryption Scheme. Ph.D. Thesis, Stanford University, Palo Alto, CA, USA, 2009.

111. Kim, A.; Polyakov, Y.; Zucca, V. Revisiting homomorphic encryption schemes for finite fields. In Proceedings of the Advances in Cryptology—ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, 6–10 December 2021; Proceedings, Part III 27; Springer: Berlin/Heidelberg, Germany, 2021; pp. 608–639.
112. Lee, J.W.; Kang, H.; Lee, Y.; Choi, W.; Eom, J.; Deryabin, M.; Lee, E.; Lee, J.; Yoo, D.; Kim, Y.S.; et al. Privacy-preserving machine learning with fully homomorphic encryption for deep neural network. *IEEE Access* **2022**, *10*, 30039–30054. [CrossRef]
113. Walskaar, I.; Tran, M.C.; Catak, F.O. A Practical Implementation of Medical Privacy-Preserving Federated Learning Using Multi-Key Homomorphic Encryption and Flower Framework. *Cryptography* **2023**, *7*, 48. [CrossRef]
114. Zhang, L.; Xu, J.; Vijayakumar, P.; Sharma, P.K.; Ghosh, U. Homomorphic encryption-based privacy-preserving federated learning in iot-enabled healthcare system. *IEEE Trans. Netw. Sci. Eng.* **2022**, *10*, 2864–2880. [CrossRef]
115. Liu, W.; Zhou, T.; Chen, L.; Yang, H.; Han, J.; Yang, X. Round efficient privacy-preserving federated learning based on MKFHE. *Comput. Stand. Interfaces* **2024**, *87*, 103773. [CrossRef]
116. Hijazi, N.M.; Aloqaily, M.; Guizani, M.; Ouni, B.; Karray, F. Secure federated learning with fully homomorphic encryption for iot communications. *IEEE Internet Things J.* **2023**, *11*, 4289–4300. [CrossRef]
117. Yang, X.; Wang, T.; Ren, X.; Yu, W. Survey on Improving Data Utility in Differentially Private Sequential Data Publishing. *IEEE Trans. Big Data* **2021**, *7*, 729–749. [CrossRef]
118. Stephanie, V.; Khalil, I.; Atiquzzaman, M.; Yi, X. Trustworthy privacy-preserving hierarchical ensemble and federated learning in healthcare 4.0 with blockchain. *IEEE Trans. Ind. Inform.* **2022**, *19*, 7936–7945. [CrossRef]
119. Wang, X.; Hu, J.; Lin, H.; Liu, W.; Moon, H.; Piran, M.J. Federated learning-empowered disease diagnosis mechanism in the internet of medical things: From the privacy-preservation perspective. *IEEE Trans. Ind. Inform.* **2022**, *19*, 7905–7913. [CrossRef]
120. Sachin, D.; Annappa, B.; Ambesenge, S. Fedrh: Federated learning based remote healthcare. In Proceedings of the 2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), New Raipur, India, 6–8 October 2023; IEEE: New York, NY, USA, 2023; pp. 1–7.
121. Ahmed, R.; Maddikunta, P.K.R.; Gadekallu, T.R.; Alshammari, N.K.; Hendaoui, F.A. Efficient differential privacy enabled federated learning model for detecting COVID-19 disease using chest X-ray images. *Front. Med.* **2024**, *11*, 1409314.
122. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Zomaya, A.Y. Federated learning for COVID-19 detection with generative adversarial networks in edge cloud computing. *IEEE Internet Things J.* **2021**, *9*, 10257–10271. [CrossRef]
123. Grech, A.; Balaji, V.; Miao, F. *Education and Blockchain*; Technical Report; UNESCO: Paris, France, 2022. [CrossRef]
124. Premkumar, R.; Sathya, P.S. A Blockchain based Framework for IoT Security. In Proceedings of the 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 8–10 April 2021; IEEE: New York, NY, USA, 2021; pp. 409–413.
125. Jiang, S.; Li, Y.; Wang, S.; Zhao, L. Blockchain competition: The tradeoff between platform stability and efficiency. *Eur. J. Oper. Res.* **2022**, *296*, 1084–1097. [CrossRef]
126. Zhonghua, C.; Goyal, S. Block chain Technology to Handle Security and Privacy for IoT Systems: Analytical Review. *Int. J. Electr. Electron. Res.* **2022**, *10*, 74–79. [CrossRef]
127. Yu, Y.; Li, Y.; Tian, J.; Liu, J. Blockchain-based solutions to security and privacy issues in the internet of things. *IEEE Wirel. Commun.* **2018**, *25*, 12–18. [CrossRef]
128. Wang, Y.; Su, Z.; Ni, J.; Zhang, N.; Shen, X. Blockchain-empowered space-air-ground integrated networks: Opportunities, challenges, and solutions. *IEEE Commun. Surv. Tutor.* **2021**, *24*, 160–209. [CrossRef]
129. Tian, H.; Ge, X.; Wang, J.; Li, C.; Pan, H. Research on distributed blockchain-based privacy-preserving and data security framework in IoT. *IET Commun.* **2020**, *14*, 2038–2047. [CrossRef]
130. Adhikari, N.; Ramkumar, M. IoT and Blockchain Integration: Applications, Opportunities, and Challenges. *Network* **2023**, *3*, 115–141. [CrossRef]
131. Ye, T.; Luo, M.; Yang, Y.; Choo, K.K.R.; He, D. A Survey on Redactable Blockchain: Challenges and Opportunities. *IEEE Trans. Netw. Sci. Eng.* **2023**, *10*, 1669–1683. [CrossRef]
132. Qu, Y.; Uddin, M.P.; Gan, C.; Xiang, Y.; Gao, L.; Yearwood, J. Blockchain-enabled federated learning: A survey. *ACM Comput. Surv.* **2022**, *55*, 1–35. [CrossRef]
133. Gai, K.; Wang, S.; Zhao, H.; She, Y.; Zhang, Z.; Zhu, L. Blockchain-based multisignature lock for uac in metaverse. *IEEE Trans. Comput. Soc. Syst.* **2022**, *10*, 2201–2213. [CrossRef]
134. Gai, K.; Wu, Y.; Zhu, L.; Choo, K.K.R.; Xiao, B. Blockchain-enabled trustworthy group communications in UAV networks. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 4118–4130. [CrossRef]
135. Egala, B.S.; Pradhan, A.K.; Dey, P.; Badarla, V.; Mohanty, S.P. Fortified-chain 2.0: Intelligent blockchain for decentralized smart healthcare system. *IEEE Internet Things J.* **2023**, *10*, 12308–12321. [CrossRef]

136. Begum, K.; Rashid, M.M.; Mozumder, M.A.I.; Kim, H.C. Leveraging the Power of Blockchain for Secure Healthcare Data Management System. In Proceedings of the 2023 26th International Conference on Computer and Information Technology (ICCIT), Cox's Bazar, Bangladesh, 13–15 December 2023; IEEE: New York, NY, USA, 2023; pp. 1–6.
137. Lei, Z.; Gai, K.; Yu, J.; Wang, S.; Zhu, L.; Choo, K.K.R. Efficiency-enhanced Blockchain-based Client Selection in Heterogeneous Federated Learning. In Proceedings of the 2023 IEEE International Conference on Blockchain (Blockchain), Danzhou, China, 17–21 December 2023; IEEE: New York, NY, USA, 2023; pp. 289–296.
138. Wang, S.; Gai, K.; Yu, J.; Zhu, L. BDVFL: Blockchain-based Decentralized Vertical Federated Learning. In Proceedings of the 2023 IEEE International Conference on Data Mining (ICDM), Shanghai, China, 1–4 December 2023; IEEE: New York, NY, USA, 2023; pp. 628–637.
139. Shu, Z.; Zhao, H.; Xu, B.; Xun, W.; Xu, B. Privacy-Preserving Federated Learning Framework via Blockchain and Committee Mechanism. In Proceedings of the 2023 IEEE 23rd International Conference on Communication Technology (ICCT), Wuxi, China, 20–22 October 2023; IEEE: New York, NY, USA, 2023; pp. 1269–1274.
140. Xu, C.; Qu, Y.; Eklund, P.W.; Xiang, Y.; Gao, L. Bafl: An efficient blockchain-based asynchronous federated learning framework. In Proceedings of the 2021 IEEE Symposium on Computers and Communications (ISCC), Athens, Greece, 5–8 September 2021; IEEE: New York, NY, USA, 2021; pp. 1–6.
141. Zhao, Y.; Zhao, J.; Jiang, L.; Tan, R.; Niyato, D.; Li, Z.; Lyu, L.; Liu, Y. Privacy-preserving blockchain-based federated learning for IoT devices. *IEEE Internet Things J.* **2020**, *8*, 1817–1829. [CrossRef]
142. Yang, X.; Xing, C. Federated Medical Learning Framework Based on Blockchain and Homomorphic Encryption. *Wirel. Commun. Mob. Comput.* **2024**, *2024*, 8138644. [CrossRef]
143. Mazzocca, C.; Romandini, N.; Colajanni, M.; Montanari, R. FRAMH: A federated learning risk-based authorization middleware for healthcare. *IEEE Trans. Comput. Soc. Syst.* **2022**, *10*, 1679–1690. [CrossRef]
144. Lin, H.; Chen, K.; Jiang, D.; Shou, L.; Chen, G. Refiner: A reliable and efficient incentive-driven federated learning system powered by blockchain. *VLDB J.* **2024**, *33*, 807–831. [CrossRef]
145. Awan, S.; Li, F.; Luo, B.; Liu, M. Poster: A reliable and accountable privacy-preserving federated learning framework using the blockchain. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; pp. 2561–2563.
146. Guduri, M.; Chakraborty, C.; Maheswari, U.; Margala, M. Blockchain-based federated learning technique for privacy preservation and security of smart electronic health records. *IEEE Trans. Consum. Electron.* **2023**, *70*, 2608–2617. [CrossRef]
147. Aich, S.; Sinai, N.K.; Kumar, S.; Ali, M.; Choi, Y.R.; Joo, M.I.; Kim, H.C. Protecting personal healthcare record using blockchain & federated learning technologies. In Proceedings of the 2022 24th International Conference on Advanced Communication Technology (ICACT), PyeongChang, Republic of Korea, 13–16 February 2022; IEEE: New York, NY, USA, 2022; pp. 109–112.
148. Samuel, O.; Omojo, A.B.; Onuja, A.M.; Sunday, Y.; Tiwari, P.; Gupta, D.; Hafeez, G.; Yahaya, A.S.; Fatoba, O.J.; Shamshirband, S. IoMT: A COVID-19 Healthcare System Driven by Federated Learning and Blockchain. *IEEE J. Biomed. Health Inform.* **2023**, *27*, 823–834. [CrossRef]
149. Wang, Z.; Cai, L.; Zhang, X.; Choi, C.; Su, X. A COVID-19 Auxiliary Diagnosis Based on Federated Learning and Blockchain. *Comput. Math. Methods Med.* **2022**, *2022*, 7078764. [CrossRef]
150. Kumar, R.; Khan, A.A.; Kumar, J.; Zakria; Golilarz, N.A.; Zhang, S.; Ting, Y.; Zheng, C.; Wang, W. Blockchain-Federated-Learning and Deep Learning Models for COVID-19 Detection Using CT Imaging. *IEEE Sens. J.* **2021**, *21*, 16301–16314. [CrossRef]
151. Kumar, R.; Bernard, C.M.; Ullah, A.; Khan, R.U.; Kumar, J.; Kulevome, D.K.; Yunbo, R.; Zeng, S. Privacy-preserving blockchain-based federated learning for brain tumor segmentation. *Comput. Biol. Med.* **2024**, *177*, 108646. [CrossRef] [PubMed]
152. Mu, J.; Kadoch, M.; Yuan, T.; Lv, W.; Liu, Q.; Li, B. Explainable federated medical image analysis through causal learning and blockchain. *IEEE J. Biomed. Health Inform.* **2024**, *28*, 3206–3218. [CrossRef] [PubMed]
153. Durga, R.; Poovammal, E. Fled-block: Federated learning ensembled deep learning blockchain model for COVID-19 prediction. *Front. Public Health* **2022**, *10*, 892499. [CrossRef] [PubMed]
154. Riahi, A.; Mohamed, A.; Erbad, A. BC-FL Location-Based Disease Detection in Healthcare IoT. In Proceedings of the 2023 International Wireless Communications and Mobile Computing (IWCMC), Marrakesh, Morocco, 19–23 June 2023; IEEE: New York, NY, USA, 2023; pp. 1684–1689.
155. Khan, M.F.; AbaOud, M. Blockchain-Integrated Security for real-time patient monitoring in the Internet of Medical Things using Federated Learning. *IEEE Access* **2023**, *11*, 117826–117850. [CrossRef]
156. Farooq, K.; Syed, H.J.; Alqahtani, S.O.; Nagmeldin, W.; Ibrahim, A.O.; Gani, A. Blockchain federated learning for in-home health monitoring. *Electronics* **2022**, *12*, 136. [CrossRef]
157. Jabarulla, M.Y.; Lee, H.N. A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the COVID-19 pandemic: Opportunities and applications. *Healthcare* **2021**, *9*, 1019. [CrossRef]
158. Gai, K.; Guo, J.; Zhu, L.; Yu, S. Blockchain meets cloud computing: A survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2009–2030. [CrossRef]

159. Andrew, J.; Isravel, D.P.; Sagayam, K.M.; Bhushan, B.; Sei, Y.; Eunice, J. Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. *J. Netw. Comput. Appl.* **2023**, *215*, 103633.
160. Truex, S.; Liu, L.; Chow, K.H.; Gursoy, M.E.; Wei, W. LDP-Fed: Federated learning with local differential privacy. In Proceedings of the Third ACM International Workshop on Edge Systems, Analytics and Networking, Heraklion, Greece, 27 April 2020; pp. 61–66.