electronics

MDPI

Article

Privacy-Enhancing Technologies in Federated Learning for the Internet of Healthcare Things: A Survey

Fatemeh Mosaiyebzadeh [1,*], Seyedamin Pouriyeh [2], Reza M. Parizi [3], Quan Z. Sheng [4], Meng Han [5], Liang Zhao [2], Giovanna Sannino [6], Caetano Mazzoni Ranieri [7], Jó Ueyama [7] and Daniel Macêdo Batista [1]

[1] Department of Computer Science, University of São Paulo, São Paulo 05508-090, SP, Brazil; batista@ime.usp.br
[2] Department of Information and Technology, Kennesaw State University, Marietta, GA 30152, USA; spouriye@kennesaw.edu (S.P.); lzhao10@kennesaw.edu (L.Z.)
[3] Decentralized Science Lab, Kennesaw State University, Marietta, GA 30144, USA; rparizi1@kennesaw.edu
[4] School of Computing, Macquarie University, Sydney, NSW 2109, Australia; michael.sheng@mq.edu.au
[5] Binjiang Institute, Zhejiang University, Hangzhou 310027, China; mhan@zju.edu.cn
[6] Institute of High Performance Computing and Networking (ICAR), National Research Council (CNR), 80131 Naples, Italy; giovanna.sannino@icar.cnr.it
[7] Institute of Mathematical and Computer Sciences, University of São Paulo, São Carlos 13566-590, SP, Brazil; cmranieri@usp.br (C.M.R.); joueyama@icmc.usp.br (J.U.)
* Correspondence: fatemehm@ime.usp.br

Abstract: Advancements in wearable medical devices using the IoT technology are shaping the modern healthcare system. With the emergence of the Internet of Healthcare Things (IoHT), efficient healthcare services can be provided to patients. Healthcare professionals have effectively used AI-based models to analyze the data collected from IoHT devices to treat various diseases. Data must be processed and analyzed while avoiding privacy breaches, in compliance with legal rules and regulations, such as the HIPAA and GDPR. Federated learning (FL) is a machine learning-based approach allowing multiple entities to train an ML model collaboratively without sharing their data. It is particularly beneficial in healthcare, where data privacy and security are substantial concerns. Even though FL addresses some privacy concerns, there is still no formal proof of privacy guarantees for IoHT data. Privacy-enhancing technologies (PETs) are tools and techniques designed to enhance the privacy and security of online communications and data sharing. PETs provide a range of features that help protect users' personal information and sensitive data from unauthorized access and tracking. This paper comprehensively reviews PETs concerning FL in the IoHT scenario and identifies several key challenges for future research.

Keywords: privacy-enhancing technologies; Internet of Healthcare Things; federated learning; security; privacy

check for updates

Citation: Mosaiyebzadeh, F.; Pouriyeh, S.; Parizi, R.M.; Sheng, Q.Z.; Han, M.; Zhao, L.; Sannino, G.; Ranieri, C.M.; Ueyama, J.; Batista, D.M. Privacy-Enhancing Technologies in Federated Learning for the Internet of Healthcare Things: A Survey. *Electronics* **2023**, *12*, 2703. https://doi.org/10.3390/electronics12122703

Academic Editor: Antoni Morell

Received: 31 March 2023
Revised: 26 May 2023
Accepted: 9 June 2023
Published: 16 June 2023

1. Introduction

Advances in communication technology have substantially increased the presence of Internet of Things (IoT) devices in domains such as healthcare [1], smart transportation [2], smart buildings [3], and smart cities [4]. In healthcare, IoT technology has shown its capabilities and applications in collecting patient data. It enables healthcare professionals to analyze the data for better and more efficient treatment of diseases. These devices are designed to collect, send, receive, and store data automatically over the network for the proactive management of patients' diagnoses or treatment in and out of the healthcare systems.

The IoHT is a branch of the IoT oriented to e-health that combines devices such as smart watches, wearable trackers, and other smart connected devices to record physiological variables, such as heart rate, body temperature, and blood pressure [5]. The considerable amount of information collected from IoHT devices and applications may be employed in data analytics. Users are then empowered with artificial intelligence (AI) and machine learning (ML) models to mine such information and improve healthcare decision making.

Traditionally, healthcare organizations use centralized ML-based models in clouds or data centers to train the data generated by IoHT devices, aiming to make reliable decisions in the healthcare domain. However, such models usually suffer from performance issues as a result of insufficient data being available on the centralized server for training due to direct access restrictions and regulations (HIPAA and GDPR). Consequently, the resulting models can become biased and untrustworthy [6,7]. Additionally, even with sufficient data, the training procedure in a centralized server is resource-demanding, increasing the costs and discouraging deployment in most hospitals and research centers [8].

The federated learning (FL) approach has been proposed as a promising way for eHealth systems to overcome data privacy concerns relating to the IoHT [9]. FL is a distributed ML-based approach that keeps patients' data restricted to their devices while training ML models collaboratively on multiple clients' health data from hospitals or IoHT devices in a decentralized network [10,11]. However, under certain conditions, FL alone cannot guarantee proper preservation of privacy [12].

Privacy-enhancing technologies (PETs) are tools and techniques designed to enhance the privacy and security of online communications and data sharing. PETs provide a range of features that help protect users' personal information and sensitive data from unauthorized access and tracking. The development of PETs can offer a reliable pathway toward data-driven technologies, such as ML-based models, while preserving privacy. PETs are a group of methods, procedures, and techniques used to extract value from data and simultaneously reduce the privacy and security risks for private information [13]. PETs are crucial, especially in some areas such as unmanned aerial vehicles (UAVs) [14] and the healthcare domain, where sensitive data are extensively collected and used. In healthcare, the gathered patient data allow researchers and healthcare professionals to distinguish diseases, assist drug development, and improve public health. For instance, vaccine development research during the COVID-19 pandemic illustrated the importance of data for public health [15].

Various PETs can be utilized to improve privacy in FL. Secure multi-party computation (SMPC) [16]; syntactic anonymization, such as k-anonymity [17]; homomorphic encryption [18]; zero-knowledge proofs [19]; differential privacy [20]; and blockchain techniques [21] are some of the techniques that are aligned with the FL framework and are discussed in this paper.

To the best of our knowledge, this is the first research paper to provide a comprehensive survey of FL for the IoHT from a PET perspective. In addition, it is the first work that reviews the integration of FL and blockchain techniques alongside other technologies that enhance privacy; thus, it is an important contribution. We comprehensively review PET and FL integration in smart healthcare environments, addressing privacy and FL in smart healthcare systems. Initially, we review the privacy requirements and the causes of privacy leakages and violations in FL. Then, we review the PET approach in terms of four PETs that have been applied to FL. Finally, we summarize the PETs that have been applied to FL and present some open issues.

The remainder of this paper is organized as follows. Section 2 summarizes the surveys related to ours while highlighting the differences. Section 3 presents IoHT devices and various security vulnerabilities. Section 4 provides the general principles of FL and the different versions of this technique used in smart healthcare environments. Section 5 provides the motivations for using privacy-preserving FL in smart healthcare. Section 6 is dedicated to a complete literature review of work pertaining to PETs. Section 7 presents PETs' application to FL in the smart healthcare environment. Section 8 presents open issues related to PETs in FL. Section 9 provides the concluding remarks. Figure 1 depicts a systematic outline of this survey paper.

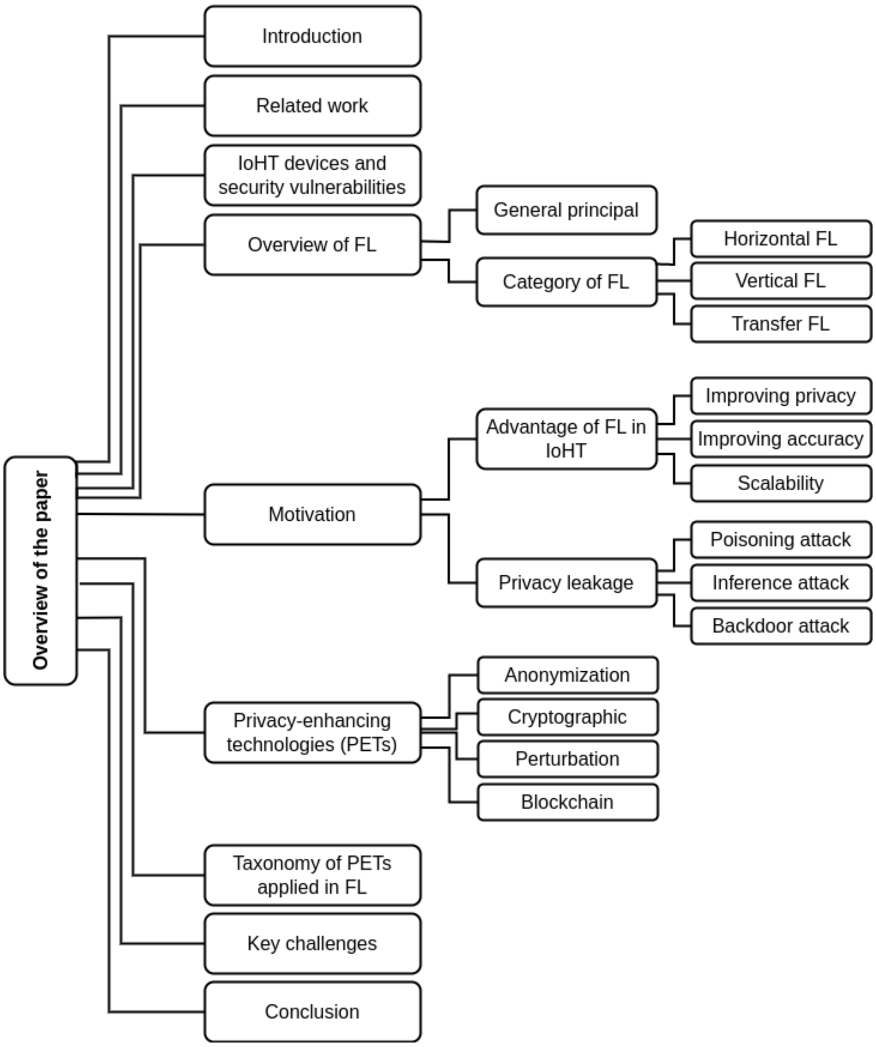

Figure 1. Outline of the paper.

2. Related Work

This section discusses the most recent work related to our survey. Other review papers cover security and privacy challenges in FL environments. However, these papers are either dedicated to other domains or cover security and privacy issues at the general level.

Aledhari et al. [22] provide an overview of FL, highlighting protocols, platforms, algorithms, market implications, and real-life use cases in terms of software and hardware. Privacy-related advantages brought by FL are presented, although this is not the paper's primary focus. Some use cases related to health applications are also discussed. Nonetheless, there are no discussions of the IoHT. Indeed, the authors state that IoT technologies are outside the scope of their paper.

Zhang et al. [23] provide a formal definition of FL and review previous papers. These papers are evaluated in terms of different aspects, and privacy mechanisms are one of them. Three mechanisms are considered: *model aggregation*, *homomorphic encryption*, and *differential privacy*. In our survey, we focus on privacy and consider a different approach, classifying four techniques: *anonymization*, *cryptography*, the *perturbation method*, and *blockchain*. Similarly to Aledhari et al., Zhang et al. [23] address use cases related to health applications. However, there are no comments about the IoHT.

Mothukuri et al. [24] review the FL paradigm specifically regarding security and privacy. Different implementations are evaluated. Some FL security and privacy threats are similar to those in our paper. Some of the applications are oriented to the IoT but they authors do not address the IoHT specifically.

Nguyen et al. [25] focus on the IoT domain only. Similarly to Zhang et al. [23], a formal definition of FL is presented. Although healthcare applications are considered, the comparison and analysis of the work do not specify which privacy attacks are tackled nor the datasets used by them.

Novikova et al. [26] assess several privacy-preserving mechanisms adopted for FL frameworks and their application to vehicle activity recognition. In this study, the authors examine the open-source FL frameworks FATE and PFL. They discover that the FATE framework uses homomorphic encryption to secure computations and input data. In contrast, PFL uses SMPC and differential privacy to protect the processing of vertically partitioned data and train neural networks for horizontally partitioned data. Similarly to Aledhari et al. [22], Zhang et al. [23], and Mothukuri et al. [24], there are no comments about the IoHT.

In another study, Nguyen et al. [27] provide a summary of FL in the Internet of Medical Things (IoMT). This study discusses a federated EHR management system, a federated remote monitoring system, a federated COVID-19 detection system, and a federated medical imaging system. Innovative FL designs for IoMT are investigated, including secure FL, resource-aware FL, and incentive-aware FL. Furthermore, the authors explore privacy-enhanced FL to enhance security, although this is not the paper's primary focus. Similarly to Novikova et al. [26], a differential privacy method is considered among the privacy-enhancing mechanisms. In contrast, our survey examines four different technologies that enhance privacy.

To the best of our knowledge, this work is the first survey specifically focused on reviewing FL applications in the IoHT from the perspective of PETs. A side-by-side comparison of the work is presented in Table 1.

Table 1. Comparison to the related work (A "✓" means that the aspect in the column is considered by the work in the line. A "×" means that the aspect in the column is not considered by the work in the line. This same nomenclature is adopted in the next tables).

References	IoHT Environment	Healthcare Domain	Privacy Mechanisms			
			Anonymization	Cryptography	Perturbation	Blockchain
Aledhari et al. [22]	×	✓	×	×	×	×
Zhang et al. [23]	×	×	×	✓	✓	×
Mothukuri et al. [24]	×	×	×	✓	✓	✓
Nguyen et al. [25]	✓	✓	×	×	✓	✓
Novikova et al. [26]	×	×	×	✓	✓	×
Nguyen et al. [27]	✓	✓	×	×	✓	×
Our work	✓	✓	✓	✓	✓	✓

3. IoHT Devices and Security Vulnerabilities

In the healthcare industry, the IoHT is playing a significant role by expanding the number of smart devices, which facilitate efficient interactions between patients and doctors. One of the best examples of the beneficial role of IoHT devices can be seen in telemedicine and online real-time monitoring. For instance, implantable IoHT devices are medical devices that can be implanted into a patient's body. Pacemakers, insulin pumps, glucose monitoring systems, and blood pressure monitoring systems are some of the most common devices in this category [28].

3.1. Glucose Monitoring System

A glucose monitoring system helps people with diabetes disease. Blood glucose (sugar) levels grow gradually with diabetes. Modern lifestyles make it difficult for patients to undergo blood glucose testing in labs or hospitals. This problem inspired scientists to develop an IoHT device that can track a person's blood glucose level and then assist the patient in obtaining the proper diet and medicine [29].

3.2. Smart Insulin Pumps

Insulin pumps are helpful for highly diabetic patients who require insulin to control their diabetes levels. This is an expensive task and requires additional nursing support to give the correct insulin dose. These challenges motivated researchers to develop smart IoHT devices that help patients take appropriate amounts of insulin [30].

3.3. Pacemaker

Pacemakers are implanted IoHT devices that support patients with heart rhythm disorders. A pacemaker powered by an internal battery is implanted in the patient's chest in order to assist the heart in beating at a normal rate and rhythm. It is well-known that people who suffer from heart rhythm disorders have a higher risk of developing depression than people who do not suffer from heart rhythm disorders. These challenges motivated researchers and organizations to develop smart pacemakers that help patients maintain a normal heartbeat [31].

3.4. Monitoring of Oxygen Levels

One of the key responsibilities of intelligent healthcare services is the monitoring of oxygen levels. Therefore, it is necessary to use intelligent monitoring tools or software to keep track of individuals' oxygen levels. For instance, it was essential to routinely check patients' oxygen levels during the COVID-19 pandemic. These difficulties drove researchers and organizations to create intelligent IoHT devices that continuously track patients' oxygen levels [32].

3.5. Security Vulnerabilities in the IoHT

Several security vulnerabilities are known in existing implementations of the IoHT, such as network and system vulnerabilities, as well as vulnerabilities associated with communication protocol implementations.

3.5.1. IoHT Device Operating System Vulnerability

Due to the specialized requirements of IoHT devices, as well as the limitations of the existing operating systems, it was necessary to create specialized operating systems to service these devices. However, complex encryption and authentication techniques cannot be implemented on these devices because of their limited computational capacity, memory, and power, which may result in increasing resource consumption and add extensive latency. As a result, these devices are susceptible to network and system attacks [33].

3.5.2. Communication Protocol Vulnerability

In IoHT devices, there are fewer safety checks, and it is their firmware that has the security vulnerabilities that make them vulnerable, such as hardcoded keys. Furthermore, because of the urgency of preparing the IoHT platform and limited experience, it is challenging to provide a common security protocol for the diverse and heterogeneous IoHT devices, which creates issues concerning how to quickly identify and fix security vulnerabilities in IoHT devices [34].

3.6. Data Leakage in IoHT Devices

IoHT devices store data in their memory. In many of these devices, the configuration of the security is weak because data are stored in an unencrypted format, so an attacker can exploit these vulnerabilities to access the data and steal them.

The majority of IoHT devices used by medical staff to monitor and process patient data are portable. Attacks that take advantage of memory leaks can affect these devices. This group of devices, such as laptops and mobile phones, are designed to monitor medical data. The fact that these devices communicate directly with IoHT data servers makes them extremely susceptible to various security assaults. Due to the communication between various devices, the impact from one compromised device can spread to different layers.

Furthermore, in IoHT implementations, information is transported from devices to servers using a variety of networking tools and protocols. IoHT devices are generally battery-focused and lightweight and have low computation capacities, and for these reasons, they use low-range protocols with weak security. Additionally, intermediate devices, such as mobile phones connected to wearable devices, collect data from end devices using a specific protocol to convert them into a different format that can be understood by the next device. These intermediate devices communicate with the IoHT and monitoring devices via a variety of protocols that have security issues and can cause data leakage [35].

3.7. Summary

The IoHT is significantly contributing to the growth of smart devices in the healthcare sector and enables effective communication between medical staff and patients. The healthcare industry has been significantly changed by the use of IoHT devices in telemedicine and online real-time monitoring. For instance, a glucose monitoring system can track a diabetic patient's blood glucose levels, and if the patient requires insulin, a smart insulin pump can inject the appropriate dosage; glucose monitoring systems can also assist the patient in creating an adequate diet. Pacemakers help patients maintain a healthy heart rhythm. Oxygen-level monitoring systems check the blood's oxygen level and take appropriate action if necessary. These IoHT devices, however, can be the targets of several security attacks, including those relating to operating system and communication protocol vulnerabilities. Furthermore, IoHT devices use weak security configurations and store data in non-encrypted forms. Additionally, security weaknesses in communication protocols can cause data leakage because IoHT devices communicate with other devices using intermediate devices that transform data using protocols that have security issues.

4. Federated Learning for Healthcare

This section discusses the overall principle of FL and the many types of FL in the e-healthcare context.

4.1. Principles of FL for Smart Healthcare

Privacy breaches have become a major concern in users' data management. Governments have established policies to prevent privacy leakages and preserve users' data privacy. The need to comply with these policies led to the development of FL in 2016 [36,37]. FL, or collaborative learning, consists of training a global ML model without explicitly exchanging data from multiple parties. In contrast, local ML models are trained on local datasets in the clients' devices. Instead of sharing data to train a model in a centralized server, parameters such as gradients or model weights from these local models are exchanged to produce a global model. In general, the FL process for IoHT consists of the following steps:

- **Initialization**. The aggregation server selects data generated by IoHT devices, such as blood sample readers or human motion detection devices, to perform a prediction or classification task. Furthermore, the central server chooses a group of participants to participate in the FL process;
- **Local model training**. The server sends an initial model to the devices for distributed training after choosing the IoHT devices for feeding the model. Each device computes its updated model by training a local model with its own dataset that is stored locally. Finally, each device sends its updated model to the central server, which is responsible for aggregating all the updated models;
- **Model aggregation**. After receiving the parameters from each IoHT device in the FL process, the aggregation step combines all parameters to generate a global learning model. The federated averaging (FedAvg) algorithm [36] is an averaging model that can be used to calculate the global model and send it to all IoHT devices to update the local models.

4.2. FL Types for Smart Healthcare

FL methods can be categorized into horizontal FL, vertical FL, and federated transfer learning.

In horizontal FL, or sample-based FL, the datasets of different healthcare clients have the same feature space but different sample spaces. Since the local data are in the same feature space, local healthcare participants can train the local model using their local data with the same AI model, such as the neural network model. Afterward, the global model can be updated by combining all the local models transmitted from local healthcare organizations or institutions [38]. An example of horizontal FL in smart healthcare would be multiple implanted medical devices with different hospitals as clients that collect very similar data but have little to no overlap in patients [39].

In vertical FL, the datasets of different healthcare organizations have similar sample spaces and different feature spaces. This method can be used to address overlapping samples with distributed clients. Vertical FL usually utilizes entity alignment techniques to collect the overlapping samples from the hospitals. Then, the overlapping data can be applied to the local training model integrated with encryption techniques [40]. An example of vertical FL in IoHT applications would be a learning model shared between hospitals and cardiologists. Both hospitals and cardiologists, two groups that have patients with similar sample spaces and various data features, can use vertical FL to train an AI model by utilizing their respective historical medical records and data for smart healthcare decisions [41].

Federated transfer learning integrates transfer learning into FL to handle datasets with various sample and feature spaces. Transfer learning is a way to transfer knowledge from one particular problem to another to decrease the distribution divergence between different domains [42]. An example of federated transfer learning in healthcare organizations would be disease diagnosis by collaborating countries through numerous hospitals with various patients and therapeutic programs [27].

4.3. Summary

Privacy violations have grown to be a serious concern in user data management. In order to stop privacy leaks and protect user data privacy, governments have adopted policies and regulations. In 2016, FL was created as a result of the requirement to comply with these regulations and policies. FL is a distributed learning model that trains a global ML model without sharing raw data with multiple organizations. There are three types of FL in the healthcare industry: horizontal FL, vertical FL, and federated transfer learning. In fact, FL uses local datasets that are stored on IoHT devices to train the local ML models. In general, the central server selects the IoHT devices to participate in the FL process and then the server sends an initial model to the devices to train the model using local data. Each device sends its updated local model to the server with the corresponding parameters and weights. Finally, the central server uses the FedAvg algorithm to aggregate all parameters, calculate the global model, and distribute it to all IoHT devices.

5. Motivation for Using Privacy-Preserving FL in Smart Healthcare

For IoHT devices, privacy requirements are more stringent than for typical IoT infrastructures. IoHT healthcare systems have various privacy requirements, such as data privacy protection [43]. Data privacy protection is a way to protect personal data from unauthorized use and manipulation. While collecting and storing patient data, we must continually consider ethical privacy regulations throughout the entire data lifecycle. For instance, privacy policies such as the GDRP and HIPAA are laws for preserving privacy at the data level [44]. According to privacy policies, only authorized individuals can access patient health data.

Thus, to protect the privacy of patient data, the IoHT system should be designed to guarantee the following principles [45]:

- Preserving the privacy of patients and the confidentiality of patient healthcare data (i.e., preventing unauthorized access to health information);

- Ensuring the integrity of healthcare data (i.e., preventing unauthorized data manipulation);
- Granting access to health data to authorized people.

The next two sections summarize the benefits and potential threats of using FL in smart healthcare.

5.1. Benefits of FL in IoHT

Various characteristics of FL, such as collaborative learning in a distributed data environment, bring many advantages to the IoHT domain, which are discussed briefly in the following sections.

5.1.1. Improving the Privacy of User Data

With the increasing numbers of IoHT devices and publicly available medical datasets generated by IoHT devices, privacy concerns are also growing regarding e-healthcare systems. According to data privacy protection legislation, private patient data are the most sensitive and restricted by government laws. Data collected from IoHT devices, such as heartbeat, blood pressure, and glucose level, are more sensitive than other data types. To address data privacy challenges in the e-healthcare domain, FL offers a decentralized training mechanism where each client or institution can control private data and define a privacy-preservation policy [46]. In the FL framework, the raw health data are stored in a medical device or at a local site and do not leave the IoHT devices during the federated data training process. During model training, only the local updates, such as model gradients, need to be sent to the central server, which reduces the risk of sensitive and personal data leakage, thus ensuring the privacy of patient data [47].

5.1.2. Less Biased Model

As a centralized model can only be trained using limited data from a single hospital, the result may be biased in the predictions. Therefore, mitigation bias has recently gained much attention in relation to modern ML techniques for e-healthcare [48]. More data must be used for models to be more generalizable, which can be achieved through data sharing between organizations. However, exchanging patients' electronic health data between hospitals raises security and privacy issues because healthcare data are sensitive [49]. Under these circumstances, FL has emerged as an option for building collaborative learning models for healthcare data. The trained models are less biased and smarter as different datasets from various sources are integrated into the learning process [50].

5.1.3. Improving Scalability

In a centralized paradigm, uploading all healthcare data to the centralized server wastes computing resources and violates privacy. It puts more pressure on the wireless communication network, reducing its scalability. FL's distributed nature improves the scalability of IoHT networks that rely on ML [51]. FL can use the computational resources located in multiple IoHT devices across different hospitals localized in distinct geographic regions in a parallel manner. When new hospitals or healthcare institutions participate, they add more computational resources to the federated learning process. Therefore, these greater computational resources allow FL to enhance performance. Moreover, the FL architecture avoids sending massive amounts of gathered IoHT data to the cloud, which can save significant network bandwidth and drastically reduce communication costs [52,53].

5.2. Privacy Leakage and Threats in FL

Although FL provides a privacy-aware framework to train global models without sharing data and allows clients to use the framework with their local datasets, recent work has shown that FL can still face privacy breaches and information leakage.

The FL frameworks restrict the sharing of data on local devices with third-party or central servers. Nonetheless, it is possible to obtain sensitive information through the back-tracing of gradients and the analysis of the updates to the communication models through the training process [54,55]. Previous studies have shown how sharing the gradients can easily leak private training data. For example, Zhu et al. [56] introduced deep leakage from gradients (DLG), which demonstrated that malicious attackers can steal the training data in a few iterations. Similarly, Aono et al. [57] reported that accessing a small portion of the original gradients may cause leakage of the local training data. Although FL models with decentralized data sources have shown promising results concerning preserving data privacy, they are still vulnerable to several types of attacks, such as poisoning attacks [58], inference attacks [59], and backdoor attacks [60].

In a poisoning attack, which occurs during the training time, an attacker tries to manipulate the training data sample by injecting designed samples to compromise the whole learning process [61]. In poisoning attacks, including data poisoning attacks [62] and model poisoning attacks [63], the ultimate goal of the attackers is to change the behavior of the target model. A data poisoning attack aims to mislead the global model by manipulating the local training data. The attacker flips the training data labels and adds noise in order to degrade the quality of the models [64]. Figure 2 shows how an attacker can change a trained model by flipping the data labels. In the model poisoning attack, the attacker attempts to manipulate local model updates before sending the models to the server. This method includes various techniques to manipulate the FL local training procedure, such as direct gradient manipulation and changing the learning rule [65].

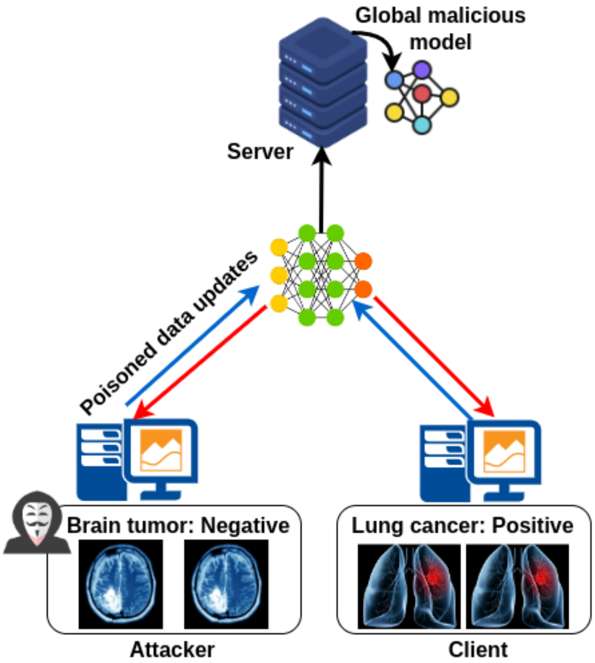

Figure 2. An illustration of poisoning attacks against FL.

In an inference attack, the attacker aims to exchange gradients during the FL training process, which can result in serious leakage of information about clients' training data features. Inference attacks include inferring class representatives [66], inferring membership [67], inferring data properties [68], and inferring samples/labels [69]. In the inference of class representatives, the adversary creates samples that are not in the original training dataset. Attackers use these false samples to learn sensitive information about the training dataset [70]. The inference of memberships tries to determine whether a given data sample has been used for model training [71]. In the property inference attack, the attacker aims to infer the property information for the training dataset [72]. In the inferring samples, the attacker recreates labels from the gradients and recovers the original training samples used during training [73]. Figure 3 shows an example of inference attacks.

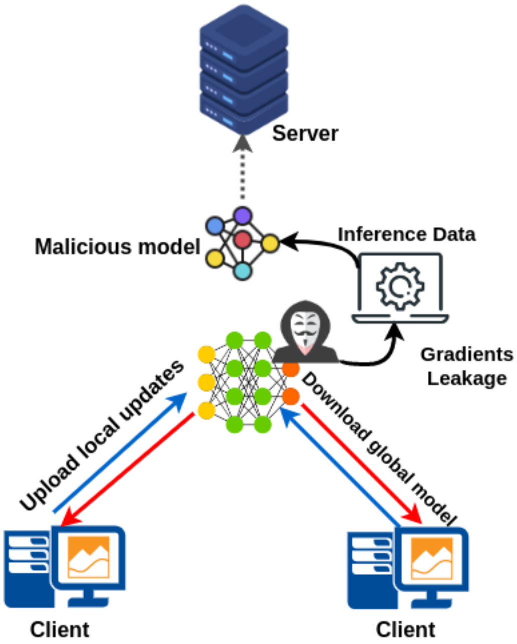

Figure 3. An illustration of inference attacks against FL.

In a backdoor attack, the attacker's goal is to destroy the global FL model and replace the actual global FL model with the attacker's model [74]. This attack can also be classified as a model poisoning attack but it is more harmful than poisoning attacks [60]. The attacker compromises the devices of one or several participants, trains a model using backdoor data, and submits the resulting model. After federated averaging, the global model is replaced with the backdoored model, as shown in Figure 4. In a backdoor attack, the adversary can be hidden and have no impact on the performance metrics of the global model with the validation dataset. Consequently, it is not easy to distinguish a backdoor attack [75,76].

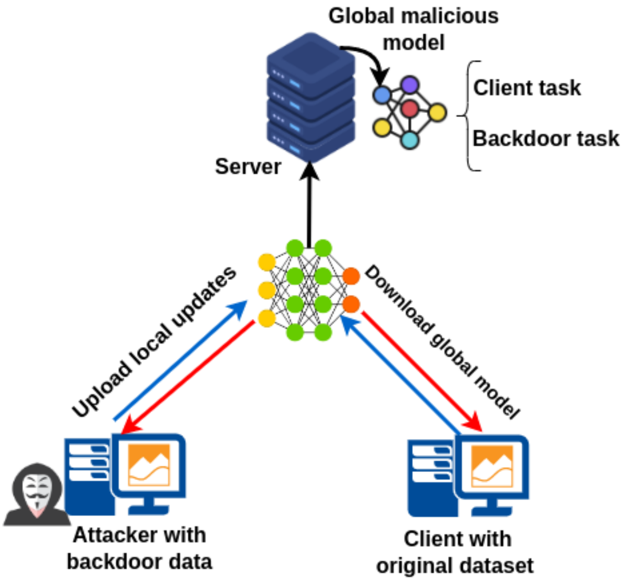

Figure 4. An illustration of backdoor attacks against FL.

5.3. Summary

In terms of AI, FL offers several advantages, including the preservation of privacy, a less biased model, and scalability. However, FL has not gained much popularity in industries such as healthcare, primarily because of privacy and security deficiencies. Although FL offers more privacy protection than traditional machine learning methods by not transmitting data directly to the central server, there are still some insecure issues in particular real-world applications that require more research and solutions. There are several different attack types that can affect FL, and various attack classification criteria have been used in previous studies. Several studies have shown that certain private information can be inferred from the transfer of data. Moreover, using the trained model, the member inference attack can determine whether a sample is a part of the relevant training set. For instance, in some circumstances, disease classification models in the medical industry can reveal private information. In poisoning attacks, including data poisoning and model poisoning attacks, an attacker changes the parameters of the target model directly, leading to errors in the global model. Backdoor attacks are even more harmful than poisoning attacks as they add malicious data to the training set instead of modifying it, training a model using this data and then replacing the actual global FL model with the backdoor one.

6. Privacy-Enhancing Technologies

PETs are tools and techniques that protect individuals' privacy. PETs are designed to enable companies to embed privacy-by-design principles into their data governance practices to minimize the amount of personal data they collect, use, and share while maximizing data security and privacy. In this context, we aim to explore how PETs can enhance privacy preservation in FL to improve patient data privacy in relation to IoHT devices and e-healthcare. Four broad categories of PETs are used to improve privacy protection: (i) anonymization techniques [77]; (ii) cryptographic techniques [78]; (iii) perturbation techniques [79]; (iv) blockchain techniques [80].

6.1. Anonymization Techniques

Anonymization techniques are broadly used for privacy enhancement and involve changing the state of a dataset and removing any subject identifiers while preserving the dataset's usability [81]. Anonymity technology can better avoid leaking sensitive patient data and provide a more secure environment for smart healthcare systems. Various anonymization technologies are appropriate for big medical data, and they are based on three categories of widely used anonymity protection techniques: *k-anonymity*, *l-diversity*, and *t-closeness* models [82].

The idea of k-anonymity is to anonymize the quasi-identifier in the dataset that attackers can use to identify sensitive information about individuals. After selecting the quasi-identifiers, k-anonymity is applied to each sample in the dataset, which can guarantee that each sample cannot be re-identified from at least $k - 1$ samples [83]. l-diversity is an extension of the k-anonymity mechanism to enhance privacy against homogeneity attacks and background knowledge attacks on k-anonymity [84]. l-diversity ensures at least l "well-performing" values for the sensitive attributes and protects against attribute disclosure [85]. Finally, t-closeness has been proposed to reduce attacks against k-anonymity and l-diversity approaches and solve the attribute disclosure problem [86].

6.2. Cryptographic Techniques

Cryptographic techniques have been used to avoid the disclosure of individuals' private data in FL [87]. These methods consist of *homomorphic encryption*, *secure multi-party computation*, and *zero-knowledge proofs*.

Homomorphic encryption is a form of encryption for enhancing privacy in FL that prevents information leakage during the the parameter-exchanging process among clients. This method encodes parameters before adding or multiplying operations [88]. There are two widely used homomorphic encryption types: fully homomorphic and partially homomorphic. Fully homomorphic encryption supports both additive and multiplicative operations on ciphertext, while partially homomorphic encryption only supports either additive or multiplicative operations on the ciphertext. Compared to partially homomorphic encryption, fully homomorphic encryption provides more robust encryption, and both can be applied to horizontal and vertical FL [89].

Secure multi-party computation (SMPC) [90] is a sub-field of cryptographic schemes for the protection of private information. SMPC can address the problem of collaborative computing between parties such that no party learns anything about other participants' data [91]. The application of SMPC allows multiple participants to concentrate on safely calculating a function for various participants without the requirement for trusted third parties or the need to reveal inputs. However, due to the additional encryption and decryption operations, SMPC suffers from the need for computational overhead [92].

Zero-knowledge proofs (ZKPs) [93] are cryptographic systems designed to achieve input privacy and verifiability, which are essential features in FL [94]. A ZKP involves a prover and a verifier that distinguishes the validity of a given statement. ZKP can be an appropriate method for the verification of sensitive healthcare data among collaborators because it allows sharing data securely and privately between multiple participants [95].

6.3. Perturbation Techniques

A perturbation method protects private data and models by adding random noise to the original data. By adding noise to the model parameters or data, the data can be made differentially private [96,97], and the parties cannot determine whether an individual record participates in the learning process or not. The differential privacy technique is a widely used perturbation method implemented in the FL frameworks in medical applications. It is one of the PET methods that guarantees privacy [98] by using statistical probability models to mask sensitive private data in a dataset [99] and protect healthcare data against inference attacks on FL frameworks.

Differential privacy techniques may be classified as *global differential* or *local differential*. In the global differential privacy (GDP) setting, a trusted curator applies careful random noise to the real values returned for a particular query [100]. Unlike GDP, a local differential privacy (LDP) technique does not need a trusted third party. LDP allows users to perturb the input data locally. It often produces overly noisy data, as noise is applied to achieve individual record privacy [101]. As an advantage, the differential privacy technique makes datasets more secure because attackers cannot distinguish what information is valid. Therefore, the amount and quality of noise added to the sensitive data directly relate to how complex it is for an attacker to recognize correct information about individuals in the dataset [102].

6.4. Blockchain Techniques

Blockchain technology benefits many non-financial industries, such as healthcare, due to its cryptographic security, immutability, and accountability [103]. Researchers have recently started implementing blockchain technology to decentralize traditional data management systems. For instance, blockchain-based data management prevents security breaches and assures GDPR compliance [104]. Therefore, blockchain-based PET solutions can be used in the IoHT to safeguard individuals' rights over their data [105]. Additionally, blockchain technology is a promising technique to improve the security and scalability of the FL system.

An improved level of security may be achieved in healthcare by integrating blockchain technology into FL to maintain the trained parameters [106]. The blockchain-based system is adequate for decentralized FL training without any central server, which can mitigate the risks of single-point failures [107]. To provide IoHT data provenance, blockchain technology also provides permission control for the participants, enhancing the security and privacy of parameters in FL.

Blockchain technology has gained popularity for ensuring the trustworthiness and provenance of trustworthy federated nodes and their datasets, as well as the models' accuracy and the immutability of the global model [108]. A blockchain method includes public (permissionless), private, and consortium (permissioned) aspects. A public blockchain system allows any client to participate in the decentralized process without authorized permission. Only a client with authorized permission can be involved in private and consortium systems' block validation and confirmation process.

6.5. Summary

The techniques and tools that protect individual privacy are known as PETs. The purpose of PETs is to give companies the ability to integrate privacy techniques with their data in order to increase data security and privacy. Anonymization techniques, cryptography techniques, perturbation techniques, and blockchain techniques are the four main kinds of PETs that are utilized to increase privacy protection in the FL framework. Anonymization techniques improve privacy by altering a dataset's state and removing any subject identities while maintaining the dataset's usability. Furthermore, numerous cryptography methods are widely used as PETs in FL frameworks for healthcare applications, including homomorphic encryption, secure multi-party computation (SMC), and zero-knowledge proofs. In cryptography approaches, each client encrypts the data before sending them to the cloud server and then decrypts the updates to generate a new global model. A third method, known as perturbation, adds random noise to the original data to protect sensitive information or model parameters. By including noise, it is possible to prevent the parties from knowing if a given record actively contributes to the learning phase. The differential privacy approach, which can be categorized as global differential or local differential, is a commonly used perturbation technique in FL frameworks for medical applications. Blockchain technology is a novel technology with several benefits, such as immutability, accountability, and cryptographic security, that has been used in numerous non-financial industries, especially in the healthcare domain.

7. Applying PETs in FL

This section discusses the security and privacy issues in FL from the perspective of PETs. The PETs used in FL can be classified into the following categories, described in the next sections: anonymization, cryptographic, perturbation, and blockchain.

7.1. Anonymization Methods

Much research has been published that integrates anonymization techniques and FL [109–111]. Some of these studies attempt to evaluate the incorporation of FL and anonymization methods in a smart healthcare environment [112].

Choudhury et al. [113] proposed a syntactic anonymity approach to guarantee data privacy in FL that complies with legal regulations. The authors used anonymization based on a (k, k^n) algorithm. This approach comprised two steps. In the first step, the anonymization method was applied to the original private data, which included relational and transactional attributes at the local site. These anonymized data were fed to a global model. The second step was a global anonymization mapping process, which could be used for the prediction process in the FL global model. The authors took into consideration the two key tasks of predicting patient mortality and drug reactions. For patients admitted to the intensive care unit (ICU), in particular, accurate and timely prediction of these outcomes can greatly enhance the standard of care. The authors evaluated the proposed method using the Medical Information Mart for Intensive Care (MIMIC III) (https://registry.opendata.aws/mimiciii/ (accessed on 1 June 2023)) dataset for mortality prediction and the Limited MarketScan Explorys Claims—EMR Data (LCED) dataset for adverse drug prediction, which was gathered from 3.7 million patients. The results demonstrated high model performance and a high level of de-identification that could be defended under current privacy regulations compared to the differential privacy method for FL.

Similarly, Grama et al. [114] presented an adaptive privacy-preserving FL method for healthcare data. In order to enhance privacy, they used the k-anonymity method and differential privacy on top of the FL, which could protect data through anonymization. Although anonymization based on this data protection method can cause information loss, the proposed k-anonymity method from this paper decreased data loss. Similarly to Choudhury et al. [113], the authors evaluated the performance of the proposed approach with two health datasets related to predicting diabetes mellitus onset (https://www.kaggle.com/datasets/uciml/pima-indians-diabetes-database (accessed on 1 June 2023)) and heart failure diseases (https://archive.ics.uci.edu/ml/datasets/heart+disease (accessed on 1 June 2023)). Compared to differential privacy, their results showed that the k-anonymity method using $k = 4$ demonstrated a lower error rate, and it could improve the robustness of aggregation and provide more healthcare data protection if applied to a large dataset.

Alsulaimawi [115] presented a federated PF-NMF framework. This FL framework contained multiple local privacy filters (PFs), which were used to remove sensitive data to minimize the risk of private data leakage. In the training phase, the PF acted as an encoder. The framework included a decoder in the testing phase and fed the test data into the autoencoder. The author evaluated the proposed approach with the MNIST (https://www.tensorflow.org/datasets/catalog/mnist (accessed on 1 June 2023)) and HARUS (human static and dynamic activities gathered by wearable devices) (http://archive.ics.uci.edu/ml/datasets/Human+Activity+Recognition+Using+Smartphones (accessed on 1 June 2023)) datasets. The results showed that federated learning with two PF-NMF frameworks achieved better accuracy and enhanced the privacy protection of sensitive data compared to a single PF-NMF model.

Cui et al. [116] proposed a new method called federated machine learning with anonymous random hybridization (FeARH) to mitigate privacy issues in an untrustworthy central analyzer. A more detailed explanation is that the suggested approach was designed to be used against active adversaries, where the main unreliable party may violate the protocol and maliciously alter model parameters in order to obtain private training data. Therefore, the hybridization algorithm added randomization into the parameter sets shared with other parties. With the hybrid algorithm, the medical data replaced by randomized parameters did not need to be shared with other institutions. The authors evaluated the proposed approach with the eICU dataset (https://eicu-crd.mit.edu/ (accessed on 1 June 2023)), which includes the medicine taken by each patient and the mortality of each patient. The results showed that FeARH achieved similar performance compared to FL and centralized the ML method. Similarly to Alsulaimawi [115], the authors used anonymized data in the training phase.

Table 2 summarizes the representative work on anonymization techniques applied for FL in smart healthcare.

Table 2. Summary of anonymization techniques applied in FL for the smart healthcare environment.

Ref.	Aim	Dataset	Dataset Available	Open-Source	Privacy Attack	Privacy-Enhancing Method
Choudhury et al. [113]	Maximize data utility and model performance	MIMIC III and LCED	✓	×	Inference attack	Syntactic anonymization
Grama et al. [114]	Applying data privacy engineering without reducing the accuracy	Pima Indians diabetes and Cleveland heart disease	✓	×	Poisoning attack	k-anonymity
Alsulaimawi [115]	Preserving private data with high accuracy	MNIST and HARUS	✓	×	-	Non-negative matrix factorization
Cui et al. [116]	Avoiding an attack from an untrustworthy central analyzer in FL, obtaining similar performance compared to a centralized model	eICU	✓	×	Inference attack	Anonymous random hybridization

7.2. Cryptographic Methods

Cryptographic methods are widely used in several FL methods to preserve data privacy when exchanging intermediate parameters during the FL training process [117–119]. Similarly to Cui et al. [116], whose work falls into the smart healthcare domain, Zhang et al. [120] presented an FL mechanism for the IoHT. They applied a cryptographic masking scheme based on homomorphic encryption and SMPC to protect private medical data against reconstruction or model inversion attacks. In this masking scheme, the standard weight calculation method based on the quantity of data was replaced with a weighted average algorithm based on the data quality. Additionally, the authors used Diffie–Hellman key exchange and the Shamir secret-sharing algorithm to provide a dropout-tolerable and participant collusion-resistant solution for the proposed scheme. To evaluate the efficiency of the proposed FL model and the validity of the privacy-enhancing masking scheme, the authors used real skin cancer datasets (https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/DBW86T (accessed on 1 June 2023)). The results showed that the proposed model improved the privacy protection for medical data and achieved reliable accuracy in skin cancer detection.

Ma et al. [121] proposed a novel privacy-enhancing FL-based environment in a smart healthcare scenario for detection of falls among the elderly. The authors used the UP-FALL Detection dataset (http://sites.google.com/up.edu.mx/har-up/ (accessed on 1 June 2023)). Similarly to Zhang et al. [120], they applied a homomorphic encryption scheme to prevent privacy leakage and achieve secure encryption and decryption in the FL system. The proposed xMK-CKKS multi-key homomorphic encryption scheme utilizes an aggregated public key to encrypt the model updates before sharing them with a server for aggregation. They proposed an aggregated public key that would, in particular, be used to encrypt the sum of all individual public keys. The model's secure decryption occurs after clients shared information about their secret keys. During the secure decryption, devices calculate the decryption share, which consists of information about the aggregated ciphertexts and individual secret keys. As a result, the xMK-CKKS scheme provides robust security and prevents more interactive decryption mechanisms. The results showed that the proposed FL scheme using multi-key homomorphic encryption was effective in terms of communication, computational cost, and energy consumption while ensuring the implementation of secure FL on IoHT devices.

Stripelis et al. [122] combined FL and fully homomorphic encryption (FHE) to develop a novel, secure FL framework for biomedical data analysis. They used the CKKS homomorphic encryption scheme based on ciphertext packing and rescaling, similarly to Ma et al. [121]. Three crucial steps (encryption, encrypted aggregation, and decryption) are included in the proposed environment. Participants encrypt the locally trained models with an HE scheme using the public keys and send the encrypted models to the controller. The controller uses encrypted weighted aggregation to obtain the new encrypted model without decrypting any of the participant models. Finally, the controller distributes the new encrypted model to the participants. The participants then decrypt it using the private key and train the decrypted model with their local data. The authors evaluated the performance of the proposed FL model using a large-scale 3D brain MRI dataset (https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/2RKAQP (accessed on 1 June 2023)), aiming to predict brain age in a secure environment. The results showed that integrating an FL framework and encryption scheme did not reduce the efficiency of FL, although it improved the privacy of the patients' private data.

Rachakonda et al. [123] provided a secure and scalable FL framework to implement AI across hospital sites, collaborators, and edge devices. Similarly to Zhang et al. [120], they integrated the proposed FL framework with an SMPC algorithm to address privacy challenges and avoid reverse engineering data leakage attacks via model updates. Each client's weight is encrypted using SMPC before being transmitted to the server. Using encrypted weights prevents the original weights from being retrieved, which can prevent reverse engineering of model updates and reduce communication and computation costs. They evaluated the performance of the SMPC method in FL using the Philips ICU dataset. The results demonstrated that the developed FL framework with an SMPC algorithm could be used in a large ecosystem consisting of the IoHT and healthcare hospital sites. Moreover, the proposed framework could effectively protect medical data privacy.

Heiss et al. [124] proposed a model for blockchain-based FL that leverages verifiable off-chain computations (VOCs) using ZKPs. The architecture enables the computational correctness of local learning processes verifiable on the blockchain and provides globally verifiable management of global learning parameters. The proposed system has a unique characteristic. Smart contracts are used to manage the global model, which is stored on the blockchain. This feature uses the system guarantees of the underlying blockchain to enable public verifiability. The authors evaluated the architecture's performance through an in-home health monitoring system where sensitive data were used as inputs to the FL system. They used the Daily and Sports Activities dataset (https://archive.ics.uci.edu/ml/datasets/daily+and+sports+activities (accessed on 1 June 2023)). The results showed that VOC using ZKPs enhanced privacy in decentralized applications. Similarly to Zhang et al. [120] and Rachakonda et al. [123], the authors integrated ZKPs with FL in order to enhance privacy in the IoHT ecosystem.

Table 3 summarizes the cryptographic methods applied for FL in smart healthcare.

Table 3. Summary of cryptographic algorithms applied in FL for the smart healthcare environment.

Ref.	Aim	Dataset	Dataset Available	Open-Source	Privacy Attack	Privacy-Enhancing Method
Zhang et al. [120]	Preserving privacy in skin cancer detection while ensuring reliable accuracy	HAM10000	✓	×	Inference attack	Homomorphic encryption and secure multi-party computation
Ma et al. [121]	Securing the FL environment with IoHT devices	UP-FALL	✓	×	Inference attack	xMK-CKKS multi-key homomorphic encryption
Stripelis et al. [122]	Enhancing patients' data privacy	3D brain MRI	✓	×	Membership inference attack	Fully homomorphic encryption (FHE)
Rachakonda et al. [123]	Protecting medical data privacy with IoHT devices	eICU	✓	×	Reverse engineering attack	Secure multi-party computation
Heiss et al. [124]	Privacy-enhanced decentralized applications	Daily and Sports Activities	✓	×	Global aggregation and poisoning attack	Zero-knowledge proofs

7.3. Perturbation Methods

Next, we discuss the perturbation methods. Similarly to Ma et al. [121], Kerkouche et al. [125] proposed a bandwidth-efficient FL framework for the IoHT environment. The framework ensures privacy for the FL using differential privacy (DP). The authors acknowledged that exchanging the model updates from many IoHT devices requires significant bandwidth. Therefore, they proposed the FL-SIGN-DP scheme to reduce communication costs and enhance privacy. Participants in the FL-SIGN-DP scheme only transmit the updated models' signs to the aggregation server. The authors proposed a model that guarantees differential privacy with practical utility, even in the case of highly imbalanced training datasets. The FL-SIGN-DP technique ensures that the patient data utilized by hospitals cannot be stolen by any internal or external adversary who has access to the final model, intermediate updates, or the messages exchanged during the training process. They used the electronic health records (https://www.premierinc.com/newsroom/education/premier-healthcare-database-whitepaper (accessed on 1 June 2023)) of roughly a million patients to assess the performance of the proposed scheme in terms of the in-hospital mortality rate. The proposed scheme was compared with centralized learning, FL-SIGN without standard FL, DP, and DP with standard FL. The results showed that the FL-SIGN-DP consumed less bandwidth and could guarantee privacy protection.

Islam et al. [126] proposed an FL model to analyze patients' genomic data and identify the risk of heart failure. To enhance the privacy preservation of patients' private data while sharing them among collaborating healthcare organizations in the FL framework, the authors applied DP mechanisms by using feature selection based on statistical methods to increase scalability and accuracy in federated settings where data are vertically partitioned. The authors utilize the highest correlation value technique to select the features of the dataset. Then, they apply the differential privacy method to add noise to the selected data. The noisy data are sent to the central aggregator server. Finally, a trustworthy central aggregator server creates the final global model using the received noisy data to predict heart failure possibilities. The authors evaluated the performance of the proposed FL framework using the IQVIA and BC-TCGA datasets (https://data.mendeley.com/datasets/v3cc2p38hb/1 (accessed on 1 June 2023)). The IQVIA dataset was used to predict the causes of inevitable heart failures, and the BC-TCGA dataset addressed cancer prediction. The results demonstrated that the proposed model could obtain better accuracy with the highest privacy for the IQVIA and BC-TCGA datasets in a federated training setting.

Zhao et al. [127] proposed federated adversarial learning (FAL) with biomedical named entity recognition (BioNER). The DP technology was also used to ensure data security and privacy by adding Gaussian noise during the local training and model aggregation process. Only the noised parameters with DP are transferred between the server and the client. Therefore, the data leakage possibility decreases on the local client's side. A dataset collected from five departments of a tumor hospital was employed to examine the performance of the proposed scheme. The results showed that the training impact of the federated learning technology was comparable to centralized training when it came to unbalanced data from the five hospital departments. This demonstrates how the federated learning approach suggested in this work can successfully overcome data islands and the ethical issues brought about by data exchange between departments of a medical institution.

Similarly to Kerkouche et al. [125], Li et al. [128] proposed a cost-effective and privacy-preserving FL framework for an IoHT Alzheimer's disease detection scheme. They presented an FL-based privacy-preserving smart healthcare system named ADDetector for the detection of Alzheimer's disease. Moreover, they implemented a DP mechanism for the user data to avoid patient data leakage while transferring data to the client and enhance the privacy level against attackers. The proposed FL-based framework and the DP-based mechanism employ audio from smart devices to detect Alzheimer's disease. They system has three layers: the cloud layer, the detecting client layer, and the user layer. The data collection module requests the user prepare voice samples for AD detection in the user layer, and the feature extraction module extracts features from both linguistic and auditory characteristics. At the user level, the FL framework enables the preservation of raw data, while DP is used to protect communication between the user layer and the detecting client layer. Finally, in order to ensure the confidentiality and integrity of communication between the cloud layer and the detecting client layer, an asynchronous privacy-preserving aggregation module is implemented. The ADReSS Challenge dataset from INTERSPEECH 2020 (https://luzs.gitlab.io/adress/ (accessed on 1 June 2023)) was used to evaluate the performance of the ADDetector FL-based scheme. The experimental results showed that the ADDetector FL-based framework achieved better accuracy and a low average time overhead with strong privacy and security protection.

Nguyen et al. [129] proposed an FL framework called FedGAN to facilitate COVID-19 detection by enhancing privacy among medical institutions in edge cloud computing.

The framework aims to create realistic COVID-19 X-ray data and detect the disease automatically without sharing COVID-19 images with parties. Additionally, the authors integrated DP at each hospital site to increase and guarantee data privacy in the federated COVID-19 data training. They used differentially private stochastic gradient descent and a gradient perturbation technique to apply DP. They also added Gaussian noise to the gradient during the training. Additionally, they used the FedGAN blockchain-based system for safe COVID-19 data analysis. To evaluate the performance of the proposed FedGAN model, they used two popular COVID-19 X-ray datasets for simulations: the DarkCOVID (https://github.com/ieee8023/COVID-chestxray-dataset (accessed on 1 June 2023)) and the ChestCOVID (https://github.com/ieee8023/covid-chestxray-dataset (accessed on 1 June 2023)) datasets. The results demonstrated that the FedGAN framework enhanced the performance of COVID-19 detection and provided a high level of privacy.

Table 4 summarizes the perturbation methods for FL in smart healthcare.

Table 4. Summary of perturbation methods applied in FL for the smart healthcare environment.

Ref.	Aim	Dataset	Dataset Available	Open-Source	Privacy Attack	Privacy-Enhancing Method
Kerkouche et al. [125]	Enhancing privacy and bandwidth efficiency	Two real-world electronic health records	✓	✓	Inference attack	Differential privacy
Islam et al. [126]	Preserving privacy and predicting risk of heart failure	BC-TCGA	✓	×	-	Differential privacy
Zhao et al. [127]	Avoiding medical data leakage during data exchange	Dataset from a tumor hospitals	×	×	Adversarial attack	Differential privacy
Li et al. [128]	Privacy-preserving IoHT and Alzheimer's disease detection	ADReSS	✓	×	Man-in-the-middle attack	Differential privacy
Nguyen et al. [129]	Preserving privacy and improving COVID-19 detection	DarkCOVID and ChestCOVID	✓	×	-	Differential privacy

7.4. Blockchain Methods

Blockchain methods have been widely used in many FL frameworks to provide privacy and security in the IoHT and smart healthcare systems.

For smart healthcare systems, Samuel et al. [130] proposed an infrastructure called FedMedChain based on secure FL and blockchain technology to predict COVID-19 for IoMT scenarios, similarly to Nguyen et al. [129], who proposed a privacy-preserving FL-based scheme for the analysis of COVID-19 data in a secure environment. An FL system was suggested for this model to address the issues of data privacy and ineffective COVID-19 prediction. The blockchain is used to assure data immutability, availability, and security, as well as trust between entities. For the proposed model, a new consensus protocol for the blockchain system was developed based on the idea of a reinforcing addition game. Block genesis and miner selection both take place using the suggested consensus process. The proposed system could improve public communication and address the challenges of giant data silos and data security. Furthermore, information security and privacy analyses showed that the proposed infrastructure was robust against privacy breaches and could improve information security.

Similarly to Samuel et al. [130], Aich et al. [131] presented a model based on FL and blockchain technology to address privacy concerns. The model was used to predict COVID-19 symptoms and how the disease spreads, speeding up the use of the medical data in research and treatment. In addition, the combination of FL and blockchain technology could be helpful for real-time environments and organizations that do not want to share sensitive data with third parties because of privacy concerns. In the proposed blockchain service, users register on the platform and request access to a certain resource, and the smart contract determines whether the resource is available in the ledger. The smart contract notifies the user and reserves the requested data if they are available, and the user then signs the contract. After validation, the user receives a usage token. After analyzing the combination of blockchain and FL solutions, the authors concluded that the proposed solution securely protected data access and could help to build a robust model.

In the same context, Lakhan et al. [132] proposed a privacy-preserving FL framework for an IoMT system. It includes an FL-BETS model—an FL-based, privacy-enhancing, malware-detection, and blockchain-enabled IoMT system—for different healthcare workloads. This study aimed to preserve data privacy and protect against fraud in the local fog nodes and remote cloud network with minimum energy consumption and delay. The proposed model contains different layers, such as an application layer including ECG heartbeat, E-hospital, and blood pressure data, that share data for processing in the network. To prevent any attack on the storage in between different transactions, the local fog-node layer includes several federated and fraud blockchain fog nodes in order to train the models at different nodes. The top layer, known as the fog-cloud agent (FCA) layer, is responsible for scheduling all task requests to the global federated learning model using shared models. Compared to other ML and blockchain methods in malware analysis, the FL-BETS framework showed the best performance in terms of fraud analysis, data validation, energy efficiency, and delay constraints for healthcare applications. The model decreased energy consumption by 41% and delay by 28%.

Similarly to Samuel et al. [130] and Lakhan et al. [132], Singh et al. [133] proposed a model integrating blockchain and FL-enabled approaches to provide a secure architecture for privacy preservation in smart healthcare systems. In this model, blockchain-based IoT cloud apps enhance security and privacy by combining FL and blockchain technologies. In the proposed architecture, the blockchain technology records the data usage behavior and ensures authenticity for data aggregation. When a data user utilizes a target set of data, the system handles it, processes it, and then returns the results to the data user. By separating data ownership and permissions, the blockchain makes the data rotation process safe and secure. Therefore, the proposed model can provide secure data sharing for the IoHT environment with privacy preservation. Organizations can use a federated learning-based blockchain cloud architecture without sharing sensitive and private healthcare system data in the cloud.

Kumar et al. [134] developed an FL blockchain-based approach to train a global model for COVID-19 detection based on computed tomography (CT) slices while preserving the privacy of patients' private data and that of the organization. There are two important parts of the proposed model: the local model and the federated learning based on blockchain technology. Using blockchain-based federated learning, the proposed framework aggregates the weights received from the different local models while maintaining the privacy of the hospitals' data. In the case that a new hospital provides the data, a transaction is stored in the block to verify that the hospital owns the data. In fact, the blockchain stores two types of transactions in the blockchain ledger: data-sharing transactions and data retrieval transactions. The authors use a permissioned blockchain for the management of data accessibility in order to ensure data privacy. One of the key advantages of a permissioned blockchain is that it creates a record of all transactions, allowing the data to be retrieved from a global model. The proposed model was used to evaluate real-life COVID-19 patients' data (https://paperswithcode.com/dataset/cc-19 (accessed on 1 June 2023)) collected from various hospitals with different types of CT scanners and made publicly available to the research community. The results showed that the blockchain-based FL detected COVID-19 with good performance using CT scans from various hospitals while preserving sensitive data privacy.

Table 5 summarizes the blockchain methods applied for FL in smart healthcare.

Table 5. Summary of blockchain methods applied in FL for the smart healthcare environment.

Ref.	Aim	Dataset	Dataset Available	Open-Source	Privacy Attack	Privacy-Enhancing Method
Samuel et al. [130]	IoMT privacy preservation and prediction of COVID-19	-	×	×	Backdoor and inference attacks	Blockchain
Aich et al. [131]	Preserving data privacy and predicting COVID-19	-	×	×	-	Blockchain
Lakhan et al. [132]	Fraud detection for the IoHT	ECG heartbeat E-heart videos Blood pressure	×	×	Fraud attack	Blockchain
Singh et al. [133]	Privacy preservation for the IoHT in clouds	Healthcare data	×	×	Replay attack	Blockchain
Kumar et al. [134]	Preserving patients' privacy and detecting COVID-19 from CT scans	CC-19	✓	✓	-	Blockchain

7.5. Summary

There are four types of PETs used in FL, which can be classified into the following categories: anonymization, cryptography, perturbation, and blockchain. Anonymization methods and FL have been integrated in various studies published in the literature; moreover, there are some studies that have combined FL and anonymization techniques in smart healthcare systems. In [113], the author proposed a syntactic anonymity approach for FL for predicting patient mortality and drug reactions and ensuring data privacy. Grama et al. [114] presented a k-anonymity method for FL to implement data privacy engineering without reducing accuracy. In [115], the authors presented a federated PF-NMF framework to minimize the risk of private data leakage. In the training phase, the PF acts as an encoder. The framework includes a decoder in the testing phase and feeds the test data into the autoencoder. Cui et al. [116] proposed a new method called federated machine learning with anonymous random hybridization (FeARH) to mitigate privacy issues in an untrustworthy central analyzer and obtained similar performance compared to a centralized model.

Several FL methods use cryptographic methods for protecting data privacy when exchanging intermediate parameters. Zhang et al. [120] presented a cryptographic masking scheme based on homomorphic encryption and SMPC to protect private medical data during skin cancer detection with reliable accuracy. Ma et al. [121] applied an xMK-CKKS multi-key homomorphic encryption scheme to achieve secure encryption and decryption in the FL system and prevent privacy leakage with IoHT devices. In [122], the authors combined FL and the CKKS homomorphic encryption scheme based on ciphertext packing and rescaling to define a novel, secure FL framework for biomedical data analysis. Rachakonda et al. [123] combined a proposed FL framework for the protection of privacy in IoHT devices with an SMPC algorithm to avoid reverse engineering data leakage attacks via model updates. In [124], the authors proposed a model for blockchain-based FL that leverages verifiable off-chain computations (VOCs) using ZKPs to enhance privacy in decentralized applications.

Perturbation methods are widely used in FL to protect data privacy in the IoHT environment. Kerkouche et al. [125] proposed the FL-SIGN-DP framework to enhance privacy and bandwidth efficiency in the IoHT environment. The framework ensures privacy for FL using differential privacy (DP). In [126], the authors applied DP mechanisms through feature selection based on the statistical methods in the FL model to enhance privacy, analyze patients' genomic data, and identify the risk of heart failure. Zhao et al. [127] applied the DP technology in FL to ensure data security and privacy by adding Gaussian noise during the local training and model aggregation process. Li et al. [128] developed a cost-effective and privacy-preserving FL framework by implementing the DP method for an IoHT Alzheimer's disease detection scheme. In [129], the authors proposed an FL framework called FedGAN to facilitate COVID-19 detection and enhance privacy using differentially private stochastic gradient descent.

A wide range of FL methods use blockchain technology to provide privacy and security in the IoHT and smart healthcare applications. For smart healthcare systems, Samuel et al. [130] proposed an infrastructure called FedMedChain based on secure FL and blockchain technology to predict COVID-19 in IoMT scenarios. Aich et al. [131] presented a model based on FL and blockchain technology to address privacy concerns. The model was used to predict COVID-19 symptoms and how the disease spreads, speeding up the use of the medical data in research and treatment. Lakhan et al. [132] proposed a privacy-preserving FL framework for an IoMT system. It is an FL-BETS model—an FL-based, privacy-enhancing, malware-detection, and blockchain-enabled IoMT system—that can be used for different healthcare workloads. Singh et al. [133] proposed a model integrating blockchain and FL-enabled approaches to provide a secure architecture to enhance privacy for the IoHT in the cloud. In [134], the authors developed an FL blockchain-based approach to train the global model for COVID-19 detection based on computed tomography (CT) slices while preserving the privacy of patients' private data.

8. Key Challenges for Future Research

While PETs in FL have yielded promising results, some challenges can be highlighted. This section discusses the most prominent of these challenges.

8.1. Computation Costs

One of the main challenges in FL is represented by privacy enhancements to prevent data leakage. As shown by Rachakonda et al. [123], SMPC is one way to protect data privacy in FL. FL needs multiple iterations to develop the final global model. Therefore, the number of training iterations directly increases the cost of the training model. Performing experiments with a different number of workers does not impact the computation cost. However, increasing the number of training rounds significantly increases the computation cost. Therefore, the trade-off between privacy risk and computation time is a good topic for future research.

8.2. Privacy and Security

In Section 7.4, several studies were described that show that integration of the blockchain method and FL is another way to enhance privacy in the IoHT. However, there is an open issue that may lead to privacy leakage. In FL, only the central server has information about the sources of the local model updates, and the addresses of the clients are private. However, addresses in the blockchain are public, and using blockchain technology in FL allows other clients to communicate with each other and obtain the training model based on the public information from the blockchain. Therefore, the risk of data leakage among clients cannot be ignored.

8.3. Linkage Attacks

The k-anonymity technique is a way to preserve the anonymity of individuals. The main idea is to modify the attributes of the dataset in such a way that each instance has at least $k-1$ other entities with identical quasi-identifiers. Therefore, an identifiable record would link to multiple records in the anonymous dataset. However, k-anonymity cannot avoid privacy leakage resulting from linkage attacks where a sensitive attribute is shared among individuals with the same quasi-identifier.

8.4. Storage Cost

Local model updates in a traditional FL model are stored in the aggregator, whereas local model updates in a blockchain-based FL model are stored in the blockchain. With blockchain technology, each client is also able to store a local copy of the blockchain and update it regularly, which can increase storage costs. As a result, devices with limited storage capacity may not be able to continue with the training as the amount of data stored in the blockchain rises.

8.5. Energy Consumption

It is critical to remember that the majority of IoHT devices have constrained battery life, which makes it challenging to implement training effectively and continually. One of the major issues with homomorphic encryption is the resources needed to develop and implement it. Typically, encrypted data are substantially larger than unencrypted data, so processing encrypted data takes longer than processing unencrypted data. Therefore, significant amounts of processing time and energy are required not only to encrypt, store, and decrypt data while they are at rest and in transit but also when they are actually being used.

8.6. Communication Latency

In order to implement FL with blockchain technology, it is important to meet stringent latency requirements, especially when it comes to real-time healthcare analytics. However, FL and blockchain technology demonstrate communication latency, which limits the advancement of these two technologies. In FL, communication latency can be reduced without the need to offload raw data due to optimized training. However, the use of blockchain technology imposes additional latency due to block mining, which presents a new challenge for the FL system since it forces clients to wait for the mining process to be completed before they receive an updated model and perform their next training iterations.

8.7. Summary

It is clear that PETs have succeeded in FL, but there are some challenges that cannot be ignored despite the positive results. There are several ways to protect data privacy in FL, including using SMPC. However, federated learning requires multiple iterations to reach the final global model, which significantly increases the computation cost. Furthermore, there are several open issues related to the integration of blockchain technology and FL that can lead to privacy breaches, storage costs, and communication latency. One of the major issues with the combination of FL and homomorphic encryption is the increasing energy consumption because processing encrypted data requires more time and energy. A linkage attack can also cause privacy leaks with the k-anonymity technique as a result of the fact that a sensitive property may be shared by multiple people using the same quasi-identifiers.

9. Conclusions

This survey reviewed representative work that has applied FL in the IoHT domain in terms of privacy, including attacks and PETs. We demonstrated three potential privacy leakages and threats in FL and presented four types of PETs: anonymization, cryptography, perturbation, and blockchain technologies. Then, we investigated and summarized the currently available papers based on these four privacy-enhancing technologies. The datasets used by these studies were also summarized, which will be helpful for researchers aiming to reproduce the results. Although PETs are promising technologies that meet data privacy requirements and have made rapid advancements in recent years, some open research issues still exist, such as the trade-off between privacy risk and computational time, the risk of data leakage among colluding clients, and the sharing of sensitive attributes. The cost of storage, for instance, may increase with the integration of FL and blockchain technology because the majority of IoHT devices have a finite amount of storage. Additionally, the combination of FL and homomorphic encryption is a significant challenge for IoHT devices due to their battery limitations, as it increases the processing time and consumes more battery power during data encryption and decryption. Therefore, researchers need to find a way to address this challenge. Along with the current research efforts, we encourage more work addressing the problems in this area and the open research issues identified in this paper.

Author Contributions: Conceptualization, F.M., S.P. and D.M.B.; methodology, F.M., S.P., R.M.P., Q.Z.S., M.H., L.Z., G.S., C.M.R., J.U. and D.M.B.; investigation, F.M.; writing—original draft preparation, F.M.; writing—review and editing, F.M., S.P., R.M.P., Q.Z.S., M.H., L.Z., G.S., C.M.R., J.U. and D.M.B.; supervision, S.P. and D.M.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research is part of the INCT of the Future Internet for Smart Cities funded by CNPq proc. 465446/2014-0, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior—Brasil (CAPES)—Finance Code 001, FAPESP proc. 14/50937-1 and proc. 15/24485-9. This work was also partly funded by the São Paulo Research Foundation (FAPESP), grants 2021/10921-2 and 2013/07375-0.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

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

References

1. Mani, N.; Singh, A.; Nimmagadda, S.L. An IoT guided healthcare monitoring system for managing real-time notifications by fog computing services. *Procedia Comput. Sci.* **2020**, *167*, 850–859. [CrossRef]
2. Cheng, J.; Wu, W.; Cao, J.; Li, K. Fuzzy group-based intersection control via vehicular networks for smart transportations. *IEEE Trans. Ind. Inform.* **2016**, *13*, 751–758. [CrossRef]
3. Stojkoska, B.L.R.; Trivodaliev, K.V. A review of Internet of Things for smart home: Challenges and solutions. *J. Clean. Prod.* **2017**, *140*, 1454–1464. [CrossRef]
4. Chen, Z.; Sivaparthipan, C.; Muthu, B. IoT based smart and intelligent smart city energy optimization. *Sustain. Energy Technol. Assess.* **2022**, *49*, 101724. [CrossRef]
5. Aceto, G.; Persico, V.; Pescapé, A. Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0. *J. Ind. Inf. Integr.* **2020**, *18*, 100129. [CrossRef]
6. Rajotte, J.F.; Mukherjee, S.; Robinson, C.; Ortiz, A.; West, C.; Ferres, J.M.L.; Ng, R.T. Reducing bias and increasing utility by federated generative modeling of medical images using a centralized adversary. In Proceedings of the Conference on Information Technology for Social Good, Roma, Italy, 9–11 September 2021; pp. 79–84.
7. Vayena, E.; Blasimme, A.; Cohen, I.G. Machine learning in medicine: Addressing ethical challenges. *PLoS Med.* **2018**, *15*, e1002689. [CrossRef] [PubMed]
8. Joshi, M.; Pal, A.; Sankarasubbu, M. Federated Learning for Healthcare Domain-Pipeline, Applications and Challenges. *ACM Trans. Comput. Healthc.* **2022**, *3*, 1–36. [CrossRef]
9. Aouedi, O.; Sacco, A.; Piamrat, K.; Marchetto, G. Handling Privacy-Sensitive Medical Data with Federated Learning: Challenges and Future Directions. *IEEE J. Biomed. Health Inform.* **2022**, *27*, 790–803. [CrossRef]
10. Yang, Q.; Liu, Y.; Chen, T.; Tong, Y. Federated machine learning: Concept and applications. *ACM Trans. Intell. Syst. Technol.* **2019**, *10*, 1–19. [CrossRef]
11. Antunes, R.S.; André da Costa, C.; Küderle, A.; Yari, I.A.; Eskofier, B. Federated Learning for Healthcare: Systematic Review and Architecture Proposal. *ACM Trans. Intell. Syst. Technol.* **2022**, *13*, 1–23. [CrossRef]
12. Asad, M.; Moustafa, A.; Yu, C. A critical evaluation of privacy and security threats in federated learning. *Sensors* **2020**, *20*, 7182. [CrossRef] [PubMed]
13. Danezis, G. An Introduction to Privacy Enhancing Technologies. In Proceedings of the Internet Society Geneva's Monthly Conferences Cycle, Barcelona, Spain, 10–14 May 2004.
14. Islam, A.; Al Amin, A.; Shin, S.Y. FBI: A federated learning-based blockchain-embedded data accumulation scheme using drones for Internet of Things. *IEEE Wirel. Commun. Lett.* **2022**, *11*, 972–976. [CrossRef]
15. Bagabir, S.; Ibrahim, N.K.; Bagabir, H.; Ateeq, R. COVID-19 and Artificial Intelligence: Genome sequencing, drug development and vaccine discovery. *J. Infect. Public Health* **2022**, *15*, 289–296. [CrossRef]
16. Abou El Houda, Z.; Hafid, A.S.; Khoukhi, L. MiTFed: A Privacy Preserving Collaborative Network Attack Mitigation Framework Based on Federated Learning using SDN and Blockchain. *IEEE Trans. Netw. Sci. Eng.* **2023**. [CrossRef]
17. Yu, B.; Mao, W.; Lv, Y.; Zhang, C.; Xie, Y. A survey on federated learning in data mining. *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.* **2022**, *12*, e1443. [CrossRef]

18. Xue, Z.; Zhou, P.; Xu, Z.; Wang, X.; Xie, Y.; Ding, X.; Wen, S. A resource-constrained and privacy-preserving edge-computing-enabled clinical decision system: A federated reinforcement learning approach. *IEEE Internet Things J.* **2021**, *8*, 9122–9138. [CrossRef]
19. Hao, M.; Ye, D.; Wang, S.; Tan, B.; Yu, R. URLLC resource slicing and scheduling for trustworthy 6G vehicular services: A federated reinforcement learning approach. *Phys. Commun.* **2021**, *49*, 101470. [CrossRef]
20. Zhang, L.; Shen, B.; Barnawi, A.; Xi, S.; Kumar, N.; Wu, Y. FedDPGAN: Federated differentially private generative adversarial networks framework for the detection of COVID-19 pneumonia. *Inf. Syst. Front.* **2021**, *23*, 1403–1415. [CrossRef] [PubMed]
21. Garrido, G.M.; Sedlmeir, J.; Uludağ, Ö.; Alaoui, I.S.; Luckow, A.; Matthes, F. Revealing the landscape of privacy-enhancing technologies in the context of data markets for the IoT: A systematic literature review. *J. Netw. Comput. Appl.* **2022**, *207*, 103465. [CrossRef]
22. Aledhari, M.; Razzak, R.; Parizi, R.M.; Saeed, F. Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Access* **2020**, *8*, 140699–140725. [CrossRef]
23. Zhang, C.; Xie, Y.; Bai, H.; Yu, B.; Li, W.; Gao, Y. A survey on federated learning. *Knowl.-Based Syst.* **2021**, *216*, 106775. [CrossRef]
24. Mothukuri, V.; Parizi, R.M.; Pouriyeh, S.; Huang, Y.; Dehghantanha, A.; Srivastava, G. A Survey on Security and Privacy of Federated Learning. *Future Gener. Comput. Syst.* **2021**, *115*, 619–640. [CrossRef]
25. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Li, J.; Vincent Poor, H. Federated Learning for Internet of Things: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1622–1658. [CrossRef]
26. Novikova, E.; Fomichov, D.; Kholod, I.; Filippov, E. Analysis of privacy-enhancing technologies in open-source federated learning frameworks for driver activity recognition. *Sensors* **2022**, *22*, 2983. [CrossRef]
27. 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.* **2022**, *55*, 1–37. [CrossRef]
28. Yuehong, Y.; Zeng, Y.; Chen, X.; Fan, Y. The internet of things in healthcare: An overview. *J. Ind. Inf. Integr.* **2016**, *1*, 3–13.
29. Joy, A.; Hafsiya, T.; King, G. A Review on Glucose Monitoring Using Enabling Technologies of Internet of Things. In Proceedings of the 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 19–20 March 2021; Volume 1, pp. 270–273.
30. Ketu, S.; Mishra, P.K. Internet of Healthcare Things: A contemporary survey. *J. Netw. Comput. Appl.* **2021**, *192*, 103179. [CrossRef]
31. Lin, Y.; Cai, H.; Liu, H.H.; Su, X.J.; Zhou, C.Y.; Li, J.; Tang, Y.L.; Jackson, T.; Xiang, Y.T. Prevalence of depression and its association with quality of life in patients after pacemaker implantation during the COVID-19 pandemic: A network analysis. *Front. Psychiatry* **2023**, *14*, 1084792. [CrossRef] [PubMed]
32. Dang, V.A.; Vu Khanh, Q.; Nguyen, V.H.; Nguyen, T.; Nguyen, D.C. Intelligent Healthcare: Integration of Emerging Technologies and Internet of Things for Humanity. *Sensors* **2023**, *23*, 4200. [CrossRef] [PubMed]
33. Nyakina, J.N.; Taher, B.H. A survey of healthcare sector digitization strategies: Vulnerabilities, countermeasures and opportunities. *World J. Adv. Eng. Technol. Sci.* **2023**, *8*, 282–301. [CrossRef]
34. Shahid, J.; Ahmad, R.; Kiani, A.K.; Ahmad, T.; Saeed, S.; Almuhaideb, A.M. Data protection and privacy of the internet of healthcare things (IoHTs). *Appl. Sci.* **2022**, *12*, 1927. [CrossRef]
35. Aghili, S.F.; Mala, H.; Shojafar, M.; Peris-Lopez, P. LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT. *Future Gener. Comput. Syst.* **2019**, *96*, 410–424. [CrossRef]
36. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; y Arcas, B.A. Communication-efficient learning of deep networks from decentralized data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (PMLR), Lauderdale, FL, USA, 20–22 April 2017; pp. 1273–1282.
37. Konečnỳ, J.; McMahan, H.B.; Yu, F.X.; Richtárik, P.; Suresh, A.T.; Bacon, D. Federated learning: Strategies for improving communication efficiency. *arXiv* **2016**, arXiv:1610.05492.
38. Mammen, P.M. Federated learning: Opportunities and challenges. *arXiv* **2021**, arXiv:2101.05428.
39. Pfitzner, B.; Steckhan, N.; Arnrich, B. Federated learning in a medical context: A systematic literature review. *ACM Trans. Internet Technol.* **2021**, *21*, 1–31. [CrossRef]
40. Zhang, T.; Mao, S. An introduction to the federated learning standard. *GetMobile Mob. Comput. Commun.* **2022**, *25*, 18–22. [CrossRef]
41. Shyu, C.R.; Putra, K.T.; Chen, H.C.; Tsai, Y.Y.; Hossain, K.T.; Jiang, W.; Shae, Z.Y. A systematic review of federated learning in the healthcare area: From the perspective of data properties and applications. *Appl. Sci.* **2021**, *11*, 11191.
42. Chen, Y.; Qin, X.; Wang, J.; Yu, C.; Gao, W. Fedhealth: A federated transfer learning framework for wearable healthcare. *IEEE Intell. Syst.* **2020**, *35*, 83–93. [CrossRef]
43. Huang, H.; Zhou, J.; Li, W.; Zhang, J.; Zhang, X.; Hou, G. Wearable indoor localisation approach in Internet of Things. *IET Netw.* **2016**, *5*, 122–126. [CrossRef]
44. Mooney, G. Is HIPAA Compliant with the GDPR? 2018. Available online: https://www.ipswitch.com/blog/is-hipaa-compliant-with-the-gdpr (accessed on 3 May 2018).
45. Barrows, R.C., Jr.; Clayton, P.D. Privacy, confidentiality, and electronic medical records. *J. Am. Med. Inform. Assoc.* **1996**, *3*, 139–148. [CrossRef]
46. Ng, D.; Lan, X.; Yao, M.M.S.; Chan, W.P.; Feng, M. Federated learning: A collaborative effort to achieve better medical imaging models for individual sites that have small labelled datasets. *Quant. Imaging Med. Surg.* **2021**, *11*, 852. [CrossRef] [PubMed]

47. 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]
48. Wahab, O.A.; Mourad, A.; Otrok, H.; Taleb, T. Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1342–1397. [CrossRef]
49. Sheller, M.J.; Edwards, B.; Reina, G.A.; Martin, J.; Pati, S.; Kotrotsou, A.; Milchenko, M.; Xu, W.; Marcus, D.; Colen, R.R.; et al. Federated learning in medicine: Facilitating multi-institutional collaborations without sharing patient data. *Sci. Rep.* **2020**, *10*, 12598. [CrossRef] [PubMed]
50. Rieke, N.; Hancox, J.; Li, W.; Milletari, F.; Roth, H.R.; Albarqouni, S.; Bakas, S.; Galtier, M.N.; Landman, B.A.; Maier-Hein, K.; et al. The future of digital health with federated learning. *NPJ Digit. Med.* **2020**, *3*, 119. [CrossRef] [PubMed]
51. Lim, W.Y.B.; Luong, N.C.; Hoang, D.T.; Jiao, Y.; Liang, Y.C.; Yang, Q.; Niyato, D.; Miao, C. Federated learning in mobile edge networks: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2031–2063. [CrossRef]
52. Khan, L.U.; Saad, W.; Han, Z.; Hossain, E.; Hong, C.S. Federated learning for internet of things: Recent advances, taxonomy, and open challenges. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1759–1799. [CrossRef]
53. Khan, L.U.; Pandey, S.R.; Tran, N.H.; Saad, W.; Han, Z.; Nguyen, M.N.; Hong, C.S. Federated learning for edge networks: Resource optimization and incentive mechanism. *IEEE Commun. Mag.* **2020**, *58*, 88–93. [CrossRef]
54. Melis, L.; Song, C.; De Cristofaro, E.; Shmatikov, V. Exploiting unintended feature leakage in collaborative learning. In Proceedings of the IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 20–22 May 2019; pp. 691–706.
55. Bhowmick, A.; Duchi, J.; Freudiger, J.; Kapoor, G.; Rogers, R. Protection against reconstruction and its applications in private federated learning. *arXiv* **2018**, arXiv:1812.00984.
56. Zhu, L.; Liu, Z.; Han, S. Deep leakage from gradients. *Adv. Neural Inf. Process. Syst.* **2019**, *32*, 14774–14784.
57. Aono, Y.; Hayashi, T.; Wang, L.; Moriai, S. Privacy-preserving deep learning via additively homomorphic encryption. *IEEE Trans. Inf. Forensics Secur.* **2017**, *13*, 1333–1345.
58. Bhagoji, A.N.; Chakraborty, S.; Mittal, P.; Calo, S. Analyzing federated learning through an adversarial lens. In Proceedings of the International Conference on Machine Learning (PMLR), Long Beach, CA, USA, 9–15 June 2019; pp. 634–643.
59. Ying, Z.; Zhang, Y.; Liu, X. Privacy-preserving in defending against membership inference attacks. In Proceedings of the 2020 Workshop on Privacy-Preserving Machine Learning in Practice, Virtual Event, 9 November 2020; pp. 61–63.
60. Bagdasaryan, E.; Veit, A.; Hua, Y.; Estrin, D.; Shmatikov, V. How to backdoor federated learning. In Proceedings of the International Conference on Artificial Intelligence and Statistics (PMLR), Online Event, Palermo, Italy, 26–28 August 2020; pp. 2938–2948.
61. Zhou, X.; Xu, M.; Wu, Y.; Zheng, N. Deep model poisoning attack on federated learning. *Future Internet* **2021**, *13*, 73. [CrossRef]
62. Tolpegin, V.; Truex, S.; Gursoy, M.E.; Liu, L. Data poisoning attacks against federated learning systems. In Proceedings of the European Symposium on Research in Computer Security, Guildford, UK, 14–18 September 2020; Springer: Guildford, UK 2020; pp. 480–501.
63. Cao, D.; Chang, S.; Lin, Z.; Liu, G.; Sun, D. Understanding distributed poisoning attack in federated learning. In Proceedings of the IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS), Tianjin, China, 4–6 December 2019; pp. 233–239.
64. Lyu, L.; Yu, H.; Yang, Q. Threats to federated learning: A survey. *arXiv* **2020**, arXiv:2003.02133.
65. Jere, M.S.; Farnan, T.; Koushanfar, F. A taxonomy of attacks on federated learning. *IEEE Secur. Priv.* **2020**, *19*, 20–28. [CrossRef]
66. Sun, J.; Li, A.; Wang, B.; Yang, H.; Li, H.; Chen, Y. Soteria: Provable defense against privacy leakage in federated learning from representation perspective. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Nashville, TN, USA, 20–25 June 2021; pp. 9311–9319.
67. Zhang, J.; Zhang, J.; Chen, J.; Yu, S. Gan enhanced membership inference: A passive local attack in federated learning. In Proceedings of the ICC 2020-2020 IEEE International Conference on Communications (ICC), Virtual Conference, 7–11 June 2020; pp. 1–6.
68. Wang, Z.; Huang, Y.; Song, M.; Wu, L.; Xue, F.; Ren, K. Poisoning-assisted property inference attack against federated learning. *IEEE Trans. Dependable Secur. Comput.* **2022**. [CrossRef]
69. Duan, Q.; Hu, S.; Deng, R.; Lu, Z. Combined federated and split learning in edge computing for ubiquitous intelligence in internet of things: State-of-the-art and future directions. *Sensors* **2022**, *22*, 5983. [CrossRef] [PubMed]
70. 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.
71. Wang, Z.; Song, M.; Zhang, Z.; Song, Y.; Wang, Q.; Qi, H. Beyond inferring class representatives: User-level privacy leakage from federated learning. In Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications, Paris, France, 29 April–2 May 2019; pp. 2512–2520.
72. Shen, M.; Wang, H.; Zhang, B.; Zhu, L.; Xu, K.; Li, Q.; Du, X. Exploiting unintended property leakage in blockchain-assisted federated learning for intelligent edge computing. *IEEE Internet Things J.* **2020**, *8*, 2265–2275. [CrossRef]
73. Wei, W.; Liu, L.; Loper, M.; Chow, K.H.; Gursoy, M.E.; Truex, S.; Wu, Y. A framework for evaluating client privacy leakages in federated learning. In Proceedings of the European Symposium on Research in Computer Security, Guildford, UK, 14–18 September 2020; Springer: Guildford, UK, 2020; pp. 545–566.

74. Zeng, H.; Zhou, T.; Wu, X.; Cai, Z. Never Too Late: Tracing and Mitigating Backdoor Attacks in Federated Learning. In Proceedings of the 2022 41st International Symposium on Reliable Distributed Systems (SRDS), Vienna, Austria, 19–22 September 2022; pp. 69–81.
75. Yin, Z.; Yuan, Y.; Guo, P.; Zhou, P. Backdoor attacks on federated learning with lottery ticket hypothesis. *arXiv* **2021**, arXiv:2109.10512.
76. Sun, Z.; Kairouz, P.; Suresh, A.T.; McMahan, H.B. Can you really backdoor federated learning? *arXiv* **2019**, arXiv:1911.07963.
77. Fischer-Hübner, S. *IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms*; Springer: Berlin/Heidelberg, Germany, 2001.
78. Abbas, A.; Khan, S.U. A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. *IEEE J. Biomed. Health Inform.* **2014**, *18*, 1431–1441. [CrossRef]
79. Parra-Arnau, J.; Rebollo-Monedero, D.; Forné, J. Privacy-enhancing technologies and metrics in personalized information systems. In *Advanced Research in Data Privacy*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 423–442.
80. Liu, H.; Crespo, R.G.; Martínez, O.S. Enhancing privacy and data security across healthcare applications using blockchain and distributed ledger concepts. *Healthcare* **2020**, *8*, 243. [CrossRef] [PubMed]
81. Dhiman, G.; Juneja, S.; Mohafez, H.; El-Bayoumy, I.; Sharma, L.K.; Hadizadeh, M.; Islam, M.A.; Viriyasitavat, W.; Khandaker, M.U. Federated learning approach to protect healthcare data over big data scenario. *Sustainability* **2022**, *14*, 2500. [CrossRef]
82. Samarati, P.; Sweeney, L. *Protecting Privacy When Disclosing Information: K-Anonymity and Its Enforcement through Generalization and Suppression*; Technical Report; SRI International: Menlo Park, CA, USA, 1998.
83. 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.
84. Machanavajjhala, A.; Kifer, D.; Gehrke, J.; Venkitasubramaniam, M. l-diversity: Privacy beyond k-anonymity. *ACM Trans. Knowl. Discov. Data* **2007**, *1*, 3-es. [CrossRef]
85. Sei, Y.; Okumura, H.; Takenouchi, T.; Ohsuga, A. Anonymization of sensitive quasi-identifiers for l-diversity and t-closeness. *IEEE Trans. Dependable Secur. Comput.* **2017**, *16*, 580–593. [CrossRef]
86. Domingo-Ferrer, J.; Soria-Comas, J. From t-closeness to differential privacy and vice versa in data anonymization. *Knowl.-Based Syst.* **2015**, *74*, 151–158. [CrossRef]
87. 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]
88. Li, L.; Fan, Y.; Tse, M.; Lin, K.Y. A review of applications in federated learning. *Comput. Ind. Eng.* **2020**, *149*, 106854. [CrossRef]
89. 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]
90. Yao, A.C. Protocols for secure computations. In Proceedings of the 23rd Annual Symposium on Foundations of Computer Science, Chicago, IL, USA, 3–5 November 1982; pp. 160–164.
91. 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]
92. Ma, X.; Liao, L.; Li, Z.; Lai, R.X.; Zhang, M. Applying Federated Learning in Software-Defined Networks: A Survey. *Symmetry* **2022**, *14*, 195. [CrossRef]
93. Goldwasser, S.; Micali, S.; Rackoff, C. The knowledge complexity of interactive proof systems. *SIAM J. Comput.* **1989**, *18*, 186–208. [CrossRef]
94. Guo, X.; Liu, Z.; Li, J.; Gao, J.; Hou, B.; Dong, C.; Baker, T. Verifl: Communication-efficient and fast verifiable aggregation for federated learning. *IEEE Trans. Inf. Forensics Secur.* **2020**, *16*, 1736–1751. [CrossRef]
95. Liu, W.; Wang, X.; Peng, W. Secure remote multi-factor authentication scheme based on chaotic map zero-knowledge proof for crowdsourcing internet of things. *IEEE Access* **2019**, *8*, 8754–8767. [CrossRef]
96. Xiao, X.; Wang, G.; Gehrke, J. Differential privacy via wavelet transforms. *IEEE Trans. Knowl. Data Eng.* **2010**, *23*, 1200–1214. [CrossRef]
97. Song, S.; Chaudhuri, K.; Sarwate, A.D. Stochastic gradient descent with differentially private updates. In Proceedings of the IEEE Global Conference on Signal and Information Processing, Austin, TX, USA, 3–5 December 2013; pp. 245–248.
98. Li, Q.; Wu, Z.; Wen, Z.; He, B. Privacy-preserving gradient boosting decision trees. In Proceedings of the AAAI Conference on Artificial Intelligence, New York, NY, USA, 7–12 February 2020; Volume 34, pp. 784–791.
99. Jordan, S.; Fontaine, C.; Hendricks-Sturrup, R. Selecting Privacy-Enhancing Technologies for Managing Health Data Use. *Front. Public Health* **2022**, *10*, 814163. [CrossRef] [PubMed]
100. Chan, T.H.H.; Li, M.; Shi, E.; Xu, W. Differentially private continual monitoring of heavy hitters from distributed streams. In Proceedings of the 12th International Symposium on Privacy Enhancing Technologies Symposium, Vigo, Spain, 11–13 July 2012; Springer: Berlin/Heidelberg, Germany, 2012; pp. 140–159.
101. Cormode, G.; Jha, S.; Kulkarni, T.; Li, N.; Srivastava, D.; Wang, T. Privacy at scale: Local differential privacy in practice. In Proceedings of the 2018 International Conference on Management of Data, Houston, TX, USA, 10–15 June 2018; pp. 1655–1658.
102. Kaaniche, N.; Laurent, M.; Belguith, S. Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey. *J. Netw. Comput. Appl.* **2020**, *171*, 102807. [CrossRef]

103. Javed, I.T.; Alharbi, F.; Margaria, T.; Crespi, N.; Qureshi, K.N. PETchain: A blockchain-based privacy enhancing technology. *IEEE Access* **2021**, *9*, 41129–41143. [CrossRef]
104. Truong, N.B.; Sun, K.; Lee, G.M.; Guo, Y. Gdpr-compliant personal data management: A blockchain-based solution. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 1746–1761. [CrossRef]
105. Alamri, B.; Javed, I.T.; Margaria, T. Preserving patients' privacy in medical IoT using blockchain. In Proceedings of the Edge Computing–EDGE 2020: 4th International Conference, Held as Part of the Services Conference Federation (SCF 2020), Honolulu, HI, USA, 18–20 September 2020; Springer: Honolulu, HI, USA, 2020; pp. 103–110.
106. Lu, Y.; Huang, X.; Zhang, K.; Maharjan, S.; Zhang, Y. Blockchain and federated learning for 5G beyond. *IEEE Netw.* **2020**, *35*, 219–225. [CrossRef]
107. Nguyen, D.C.; Ding, M.; Pham, Q.V.; Pathirana, P.N.; Le, L.B.; Seneviratne, A.; Li, J.; Niyato, D.; Poor, H.V. Federated learning meets blockchain in edge computing: Opportunities and challenges. *IEEE Internet Things J.* **2021**, *8*, 12806–12825. [CrossRef]
108. Hu, R.; Yan, Z.; Ding, W.; Yang, L.T. A survey on data provenance in IoT. *World Wide Web* **2020**, *23*, 1441–1463. [CrossRef]
109. Orekondy, T.; Oh, S.J.; Zhang, Y.; Schiele, B.; Fritz, M. Gradient-leaks: Understanding and controlling deanonymization in federated learning. *arXiv* **2018**, arXiv:1805.05838.
110. Hao, W.; Mehta, N.; Liang, K.J.; Cheng, P.; El-Khamy, M.; Carin, L. Waffle: Weight anonymized factorization for federated learning. *IEEE Access* **2022**, *10*, 49207–49218. [CrossRef]
111. Song, M.; Wang, Z.; Zhang, Z.; Song, Y.; Wang, Q.; Ren, J.; Qi, H. Analyzing user-level privacy attack against federated learning. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 2430–2444. [CrossRef]
112. Marulli, F.; Verde, L.; Marrone, S.; Barone, R.; De Biase, M.S. Evaluating Efficiency and Effectiveness of Federated Learning Approaches in Knowledge Extraction Tasks. In Proceedings of the International Joint Conference on Neural Networks (IJCNN), Virtual Event, 18–22 July 2021; pp. 1–6.
113. Choudhury, O.; Gkoulalas-Divanis, A.; Salonidis, T.; Sylla, I.; Park, Y.; Hsu, G.; Das, A. A syntactic approach for privacy-preserving federated learning. In *ECAI 2020*; IOS Press: Amsterdam, The Netherlands, 2020; pp. 1762–1769.
114. Grama, M.; Musat, M.; Muñoz-González, L.; Passerat-Palmbach, J.; Rueckert, D.; Alansary, A. Robust aggregation for adaptive privacy preserving federated learning in healthcare. *arXiv* **2020**, arXiv:2009.08294.
115. Alsulaimawi, Z. A non-negative matrix factorization framework for privacy-preserving and federated learning. In Proceedings of the IEEE 22nd International Workshop on Multimedia Signal Processing (MMSP), Tampere, Finland, 21–24 September 2020; pp. 1–6.
116. Cui, J.; Zhu, H.; Deng, H.; Chen, Z.; Liu, D. FeARH: Federated machine learning with anonymous random hybridization on electronic medical records. *J. Biomed. Inform.* **2021**, *117*, 103735. [CrossRef]
117. 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, Barcelona, Spain, 15–16 June 2022; pp. 85–90.
118. Bai, Y.; Fan, M. A Method to Improve the Privacy and Security for Federated Learning. In Proceedings of the IEEE 6th International Conference on Computer and Communication Systems (ICCCS), Chengdu, China, 23–26 April 2021; pp. 704–708.
119. Wibawa, F.; Catak, F.O.; Sarp, S.; Kuzlu, M. BFV-Based Homomorphic Encryption for Privacy-Preserving CNN Models. *Cryptography* **2022**, *6*, 34. [CrossRef]
120. 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**. [CrossRef]
121. Ma, J.; Naas, S.A.; Sigg, S.; Lyu, X. Privacy-preserving federated learning based on multi-key homomorphic encryption. *Int. J. Intell. Syst.* **2022**, *37*, 5880–5901. [CrossRef]
122. Stripelis, D.; Saleem, H.; Ghai, T.; Dhinagar, N.; Gupta, U.; Anastasiou, C.; Ver Steeg, G.; Ravi, S.; Naveed, M.; Thompson, P.M.; et al. Secure neuroimaging analysis using federated learning with homomorphic encryption. In Proceedings of the 17th International Symposium on Medical Information Processing and Analysis (SPIE), Campinas, Brazil, 17–19 November 2021; Volume 12088, pp. 351–359.
123. Rachakonda, A.S.; Moorthy, B.S.; Jain, C.A.; Bukharev, D.A.; Bucur, E.A.; Manni, F.F.; Quiterio, G.T.M.; Joosten, H.L.; Mendez, I.N.I. Privacy enhancing and scalable federated learning to accelerate AI implementation in cross-silo and IoMT environments. *IEEE J. Biomed. Health Inform.* **2022**, *27*, 744–755. [CrossRef] [PubMed]
124. Heiss, J.; Grünewald, E.; Haimerl, N.; Schulte, S.; Tai, S. Advancing Blockchain-based Federated Learning through Verifiable Off-chain Computations. *arXiv* **2022**, arXiv:2206.11641.
125. Kerkouche, R.; Acs, G.; Castelluccia, C.; Genevès, P. Privacy-preserving and bandwidth-efficient federated learning: An application to in-hospital mortality prediction. In Proceedings of the Conference on Health, Inference, and Learning, New York, NY, USA, 8–10 April 2021; pp. 25–35.
126. Islam, T.U.; Ghasemi, R.; Mohammed, N. Privacy-Preserving Federated Learning Model for Healthcare Data. In Proceedings of the IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 26–29 January 2022; pp. 0281–0287.
127. Zhao, H.; Yuan, S.; Xie, N.; Leng, J.; Wang, G. A Federated Adversarial Learning Method for Biomedical Named Entity Recognition. In Proceedings of the IEEE International Conference on Bioinformatics and Biomedicine (BIBM), Houston, TX, USA, 9–12 December 2021; pp. 2962–2969.

128. 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]
129. 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]
130. Samuel, O.; Omojo, A.; Onuja, A.; Sunday, Y.; Tiwari, P.; Gupta, D.; Hafeez, G.; Yahaya, A.; Fatoba, O.; Shamshirband, S. IoMT: A COVID-19 Healthcare System driven by Federated Learning and Blockchain. *IEEE J. Biomed. Health Inform.* **2022**, *27*, 823–834. [CrossRef]
131. 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 24th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Republic of Korea, 13–16 February 2022; pp. 109–112.
132. Lakhan, A.; Mohammed, M.A.; Nedoma, J.; Martinek, R.; Tiwari, P.; Vidyarthi, A.; Alkhayyat, A.; Wang, W. Federated-Learning Based Privacy Preservation and Fraud-Enabled Blockchain IoMT System for Healthcare. *IEEE J. Biomed. Health Inform.* **2022**, *27*, 664–672. [CrossRef]
133. 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]
134. Kumar, R.; Khan, A.A.; Kumar, J.; 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]

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