information

Review

A Review on Federated Learning and Machine Learning Approaches: Categorization, Application Areas, and Blockchain Technology

Roseline Oluwaseun Ogundokun [1], Sanjay Misra [2,*], Rytis Maskeliunas [1] and Robertas Damasevicius [3]

[1] Department of Multimedia Engineering, Kaunas University of Technology, 51368 Kaunas, Lithuania; rosogu@ktu.lt (R.O.O.); rytis.maskeliunas@ktu.lt (R.M.)
[2] Department of Computer Science and Communication, Østfold University College, 1757 Halden, Norway
[3] Department of Applied Informatics, Vytautas Magnus University, 44404 Kaunas, Lithuania; robertas.damasevicius@vdu.lt
* Correspondence: ssopam@gmail.com

Abstract: Federated learning (FL) is a scheme in which several consumers work collectively to unravel machine learning (ML) problems, with a dominant collector synchronizing the procedure. This decision correspondingly enables the training data to be distributed, guaranteeing that the individual device's data are secluded. The paper systematically reviewed the available literature using the Preferred Reporting Items for Systematic Review and Meta-analysis (PRISMA) guiding principle. The study presents a systematic review of appliable ML approaches for FL, reviews the categorization of FL, discusses the FL application areas, presents the relationship between FL and Blockchain Technology (BT), and discusses some existing literature that has used FL and ML approaches. The study also examined applicable machine learning models for federated learning. The inclusion measures were (i) published between 2017 and 2021, (ii) written in English, (iii) published in a peer-reviewed scientific journal, and (iv) Preprint published papers. Unpublished studies, thesis and dissertation studies, (ii) conference papers, (iii) not in English, and (iv) did not use artificial intelligence models and blockchain technology were all removed from the review. In total, 84 eligible papers were finally examined in this study. Finally, in recent years, the amount of research on ML using FL has increased. Accuracy equivalent to standard feature-based techniques has been attained, and ensembles of many algorithms may yield even better results. We discovered that the best results were obtained from the hybrid design of an ML ensemble employing expert features. However, some additional difficulties and issues need to be overcome, such as efficiency, complexity, and smaller datasets. In addition, novel FL applications should be investigated from the standpoint of the datasets and methodologies.

Keywords: federated learning; machine learning; PRISMA; blockchain technology; systematic review

Citation: Ogundokun, R.O.; Misra, S.; Maskeliunas, R.; Damasevicius, R. A Review on Federated Learning and Machine Learning Approaches: Categorization, Application Areas, and Blockchain Technology. *Information* **2022**, *13*, 263. https://doi.org/10.3390/info13050263

Academic Editor: Willy Susilo

Received: 26 March 2022
Accepted: 18 May 2022
Published: 23 May 2022

1. Introduction

The volume of data is no longer the focus of our consideration, because of the emergence of big data [1]. Data privacy and security are pressing issues that must be addressed. Data leakage is never a minor issue, and the public has recently been more concerned about data security [2–4]. Individuals, collectives, and society are all working to improve data security and privacy protection. The GDPR [5] strives to safeguard consumers' privacy and data security, as shown by the European Union's execution of the Wide-ranging Data Fortification Guidelines on 25 May 2018. This requires operators to properly state user agreements and prohibits operators from deceiving or inducing users to waive their privacy rights. Operators were also forbidden from training the model without the handler's authorization. It also enables users to remove their personal information. Similarly, since 2017, China's Cyber Security Law of the People's Republic of China (PPC) [6] and the

Wide-ranging Values of the Civil Law of the PPC [7] have stated that network handlers must not reveal, tamper with, or delete the individual statistics that they gather. Minute data transactions are accomplished with a third party, ensuring that the projected contract properly defines the extent of the data to be transferred as well as the data fortification requirements. The enactment of these rules and protocols has posed additional difficulties to the typical data processing mode of AI to varying degrees.

Data are the cornerstone of artificial intelligence; therefore, model training is impossible without it. Data, on the other hand, is often found in the form of data islands. Processing data in a centralized manner is a straightforward answer to data islands. Centralized data gathering, uniform processing, cleansing, and modeling are common data processing methods. Most of the time, data seeps through the collection and conversion procedures. Users' personal information is more safeguarded as rules improve, but collecting data to train algorithms is becoming increasingly difficult. The question of how to handle the issue of data islands has sparked the bulk of discussions and artificial intelligence (AI) speculation. Established data statistics approaches are presently strained in the face of different restrictions to address the challenge of data silos. The issue of data islands has become the focus of federated learning studies. Traditional machine learning mostly employs centralized methods of training the ML method, which requires the training data to be stored on the same server. Indeed, owing to data privacy rules and regulations, centralized training methods that may seep data and infringe on the confidentiality of the data possessor are becoming increasingly difficult to adopt. If mobile phone users (MPU) wish to train ML methods using their data in centralized training settings, the quantity of data they have is insufficient. As a result, before using FL, the MPU must transfer its particular phone data to a dominant server, which may then train ML methods using the data. In contrast with federal training, FL, which is a circulated training technique, tolerates distinct handlers in dissimilar spatial positions to team up with additional handlers to study ML methods, and the entire individual data, as well as delicate personal information, can be deposited on the device. Distinct handlers may profit from a well-trained ML method without having to upload their privately delicate individual data to a dominant server via FL [3].

FL introduces new avenues for AI research. FL is a revolutionary training strategy for developing tailored models that do not compromise user privacy. The computational resources of client gadgets have become increasingly powerful with the introduction of AI chipsets. Likewise, the training of AI models moves away from the central server and toward the terminal devices. FL is a confidential-protection method that successfully uses terminal instrument processing competencies to train the model, preventing private data from being visible through data transmission. Since there are many mobile devices and devices in various domains, there are plenty of exceptional dataset resources, that FL can completely exploit.

The key aspect of federated learning is that it protects users' privacy, although it differs significantly from typical large data privacy protection methods such as differential privacy and k-order inconspicuousness. FL primarily safeguards handler confidentiality by communicating encoded administered constraints, with invaders unable to access basic data. This ensures that FL will not compromise handler confidentiality at the data level and that GDPR and other laws will not be broken. According to the data distribution, FL may be classified as horizontal FL, vertical FL, or federated transfer learning (FTL). Horizontal FL is appropriate when the user characteristics of the two datasets intersect significantly but the handlers do not. When the user characteristics of the two datasets intersect slightly but the operators intersect significantly, vertical FL is an option. Transfer learning can be applied to overcome the paucity of data or tags when the operators and user characteristics of the two datasets seldom coincide. Multi-party computing and distributed ML are examples of federated learning. There are several different types of distributed ML, such as distributed model result posting, distributed training data storage, and distributed computing activities. One of the methods for accelerating the training pace of ML models is the parameter server in distributed ML. To obtain the concluding training model effectively

it saves data on multiple working nodes in a distributed manner and distributes resources via a trustworthy central server. Compared to dispersed ML, each worker node in federated learning is the single owner of its data and a model training participant.

Users have total sovereignty over local data, which stresses the confidentiality fortification of data owners. This is the fundamental quintessence of FL to ensure confidentiality. In a federated learning environment, there are two types of privacy protection systems. Encryption methods such as homomorphic encryption and safe aggregation are often used. Adding the noise of variance confidentiality to the method constraints is another common method. To maintain privacy, Google's planned federated learning [8] uses a combination of secure convergence and differential confidentiality. Other research [9] relies only on homomorphic encoding fortification settings to accomplish confidentiality fortification. The following five research questions (RQ) were formulated to accomplish the aim and objective of the systematic review conducted.

RQ1: What are the applicable machine learning methods for FL?

RQ2: What is the categorization of federated learning?

RQ3: What are the FL application areas?

RQ4: What is the relationship between FL and BT concerning data sharing in distributed systems?

RQ5: What are the ML algorithms implemented with FL?

Therefore, the foremost contribution of this study is as follows:

1. Review the appliable ML approach for FL.
2. Review the categorization of federated learning.
3. Discuss the FL application areas.
4. Presents the relationship between FL and BT.
5. Discussed some existing literature that has used FL and ML approaches.

The remainder of this article is arranged as follows: Section 2 discusses the interrelated pieces of literature on FL. Section 3 presents the materials and methods used in this investigation. Here the search strategy, suitability measures, information source and search, the study selected, data collection processes, and data extraction with analysis were similarly discussed. The results, including the search strategy yield, study characteristics, and study limitations, are discussed in Section 4. The remainder of this paper is concluded in Section 5.

2. Related Works

A lot of reviews have been conducted on FL, BT, and ML. Few of them are presented in this section and a summary of their study is summarized and shown in Table 1.

Yang et al. [10] focused on the concept and application of Federated ML, and Kairouz et al. [11] presented the present advanced and open problems in FL. Many of the researchers focused on the problems encountered in FL, Li et al. [12] performed a survey on FL system components in terms of privacy and protection. Nguyen et al. [13] did an overview of the concepts and opportunities of the FL chain in mobile-edge computing (MEC). Mothukuri et al. [14] presented a comprehensive review on FL security and privacy that can assist in bridging the gaps between the present state of federated AI (FAI). Ali, Karinmipour and Tariq [15] discussed the integration of BT and FL for IoT in terms of the privacy issue and preservative measures. Antunes et al. [16] conducted an SLR o FL for healthcare and they focused on recent studies on FL in HER for healthcare applications. Lee and Kim [17] focused on the trends in BT and FL for data sharing in disturbed platforms such as industrial vehicles and healthcare applications. Khan et al. [18] presented the recent advances of FL towards enabling FL-powered IoT applications. Li, Yan and Lin [19] conducted a reviewed related studies of FL based on the baseline of a universal definition to give guidance for future works.

In summary, most of the reviews conducted by the researchers were focused on FL privacy and protection [10,12,14,15], and others were on problems and challenges in

FL [11,15,18,20]. Most of all the few pieces of literature reviewed focused on just review and only one of the studies did a systematic literature review (SLR).

The motivation for this SLR is that it was noticed that there haven't existed many studies on SLR in the area of federated learning. It was also noticed that there hasn't been an SLR conducted on the integration of FL and ML with BT. We, therefore, decided to conduct an SLR on the recent advances in FL and ML application, as well as on the integration of BL and FL which we think does not exist even from the review of related works as shown in Table 1. We also discussed the FL application areas as researchers have not looked in that area recently.

Table 1. Summary of the state-of-the-art related works reviews.

Authors	Topic	Objective
Yang et al. [10]	Federated ML: Concept and Application	The authors proposed secure federated learning by introducing a comprehensive secured FL-framework
Kairouz et al. [11]	Advances and Open problems in FL	The authors discussed the recent advances and extensive collection of open problems and challenges
Li et al. [12]	A survey on FL systems: Vision, Hype, and Reality for Data Privacy and Protection	They conducted a comprehensive review of FL systems. They analyzed the FL system components in terms of privacy and protection.
Nguyen et al. [13]	FL meets BT in edge computing: Opportunities and Challenges	The authors presented an overview of the fundamental concepts and explore the opportunities for FL chain in MEC
Mothukuri et al. [14]	A survey on security and privacy of federated learning	The authors provided a comprehensive study on FL security and privacy that can assist to bridge the gap between the present state of FAI.
Ali, Karinmipour & Tariq [15]	Integration of BT and FL for IoT: Recent advances and future challenges	The authors presented the notion of BT and its application in IoT systems. They discussed the privacy issues and preservation techniques in FL
Antunes et al. [16]	FL for Healthcare: Systematic review and architecture proposal	The authors presented a systematic literature review on the recent study about FL in the context of electronic health records for healthcare applications.
Lee & Kim [17]	Trends in BT and FL for data sharing in distributed platforms	They reviewed FL and BT mechanisms and then described a survey on the integration of BT and FL for data sharing in industrial vehicles and healthcare applications.
Khan et al. [18]	FL for IoT: Recent advances, taxonomy, and open challenges.	The authors presented the recent advances of FL towards enabling FL-powered IoT applications.
Li, Yan & Lin [19]	A survey on FL	The authors reviewed related studies of FL based on the baseline of a universal definition to give guidance for future works.

3. Method

This section, the search strategy, eligibility criteria, information source and search, study selection, data collection processes, data extraction, and analysis.

3.1. Study Selected and Data Gathering Procedures

After the first literature exploration, each article's title, keywords, and abstract were examined, and possibly pertinent articles were further retrieved and tested for suitability

using full-text articles. The PRISMA flow diagram contains detailed information regarding the research selection process (Figure 1). Figure 1 depicts the entire procedure of the literature search and selection. Identification, screening, eligibility, and inclusion were the four stages of this procedure. In the identification stage, 4893 papers were gathered (IEEE Xplore = 1785, Taylor and Francis = 830, Sage = 492, SpringerLink = 274, WoS = 167). The total number of papers was 3424 after duplicates were removed. Following that, two independent reviewers undertook a coarse-to-fine evaluation of manuscript eligibility, with one screening title, keywords, and abstracts and the other reading complete texts. Unpublished thesis and dissertation studies, conference papers, not published in a peer-reviewed journal, not in English, and not applying artificial intelligence models were all exclusion criteria. As a result, screening eliminated 3145 articles and full-text evaluation eliminated 101 papers. 84 papers were from the original 3548 papers. Eighty-four studies were selected for the eligibility phase. Following these steps, 84 publications were found suitable for inclusion in this study.

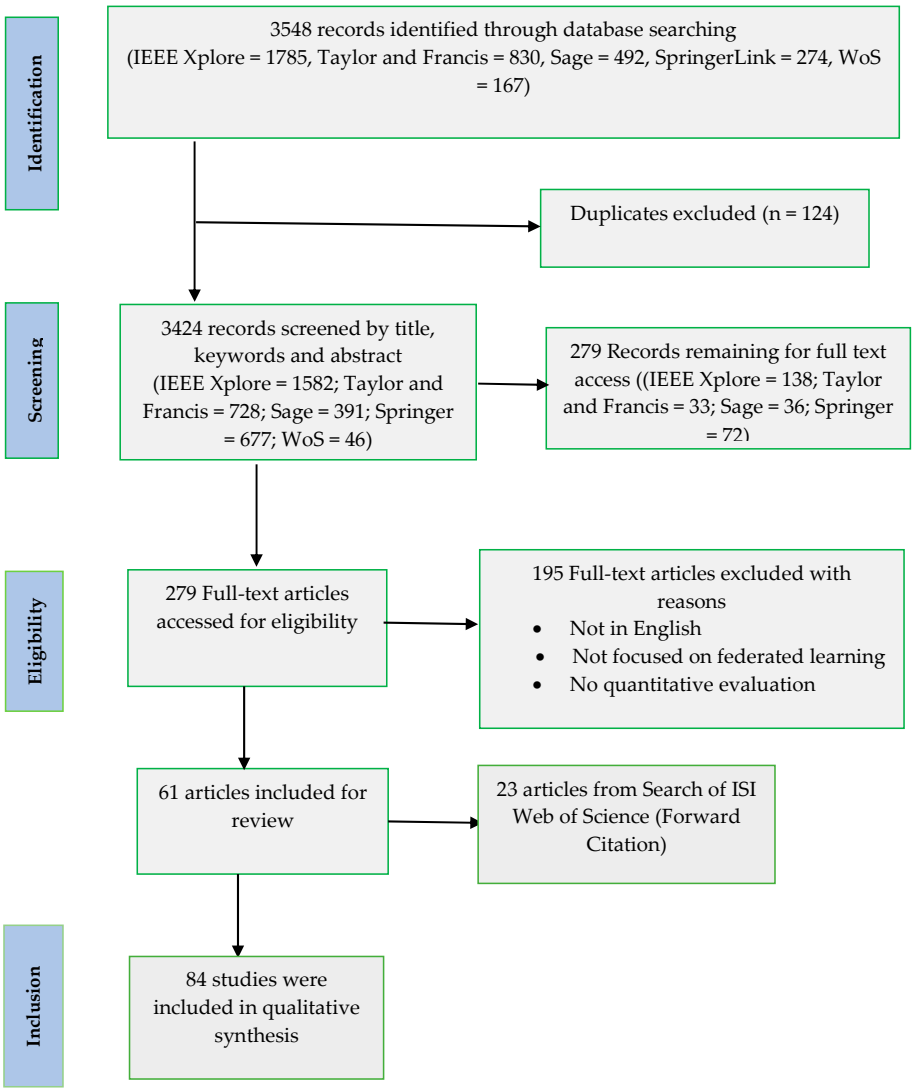

Figure 1. PRISMA flow diagram of paper selection employed in this review study.

3.2. Search Strategy

The authors performed an electronic search using five publishing databases: IEEE Xplore, Taylor and Francis, Sage, Springer, and WoS. The language of the search was restricted to the English language. The publishing date was set as the time of the search (November 2021), with a lower limit of January 2017. Table 2 lists the terms used in the

search. The AND was used as a logical operator. A targeted search was performed to supplement the computerized search. This comprised a Google Scholar online search and a manual examination of the cited references of relevant publications found using the search approach. The relevant papers were then placed on the ISI Web of Science (on 2 December 2021) to determine whether any additional publications cited them (forward citation search).

Table 2. Databases and Keywords used for Study Search.

Database	Search Keywords
IEEE Xplore	Federated learning AND Distributed environment AND Machine learning Model OR Blockchain
SpringerLink	'Federated learning AND Distributed environment AND Machine learning Model OR Blockchain' within Computer Science Remove this filter Article Remove this filter 2017–2021
Talyor and Francis	[All: federated] AND [All: learning] AND [All: distributed] AND [All: environment] AND [All: machine] AND [All: learning] AND [[All: model] OR [All: blockchain]] AND [Publication Date: (01/01/2017 TO 12/31/2021)]
Sage	[All federated] AND [All learning] AND [All distributed] AND [All environment] AND [All machine] AND [All learning] AND [[All model] OR [All blockchain]]within2017–2021
Web of Science	Federated learning AND Distributed environment AND Machine learning Model OR Blockchain

3.3. Eligibility Criteria

All papers that examined Federated Learning in a Distributed Environment and their applications were considered. The admission criteria were (i) published between 2017 and 2021, (ii) written in English, (iii) published in a peer-reviewed scientific journal, and (iv) Preprint published papers. Studies that were unpublished thesis and dissertation studies, (ii) conference papers, (iii) not in English, and (iv) did not use artificial intelligence models and blockchain technology were all removed from the review.

3.4. Information Source and Search

Literature exploration was achieved via IEEE Xplore, Taylor, Francis, Sage, Springer, and Web of Science (WoS). Numerous explorations in the stated e-databases were accomplished during December 2021 using the following search terms: (Federated learning AND Distributed environment AND Machine learning Model OR Blockchain; 'Federated learning AND Distributed environment AND Machine learning Model OR Blockchain' within Computer Science Remove this filter Article Remove this filter 2017–2021; [All: federated] AND [All: learning] AND [All: distributed] AND [All: environment] AND [All: machine] AND [All: learning] AND [[All: model] OR [All: blockchain]] AND [Publication Date: (01/01/2017 TO 12/31/2021)]; [All federated] AND [All learning] AND [All distributed] AND [All environment] AND [All machine] AND [All learning] AND [[All model] OR [All blockchain]]within2017–2021 OR Federated learning AND Distributed environment AND Machine learning Model OR Blockchain) The keywords used in the database searching is shown in Table 3 and distribution per publication source types is shown in Figure 2. Figures 2–4 show the outcomes of these processes. In the next section, the mentioned headings are used to summarize the recognized studies and their distribution in research.

Table 3. Keywords and search string.

Keywords	Search String
Federated learning, Distributed environment, Machine learning Model, Blockchain technology	Federated learning AND Distributed environment AND Machine learning Model OR Blockchain OR 'Federated learning AND Distributed environment AND Machine learning Model OR Blockchain' within Computer Science Remove this filter Article Remove this filter 2017–2021 OR [All: federated] AND [All: learning] AND [All: distributed] AND [All: environment] AND [All: machine] AND [All: learning] AND [[All: model] OR [All: blockchain]] AND [Publication Date: (01/01/2017 TO 12/31/2021)] OR [All federated] AND [All learning] AND [All distributed] AND [All environment] AND [All machine] AND [All learning] AND [[All model] OR [All blockchain]]within2017–2021

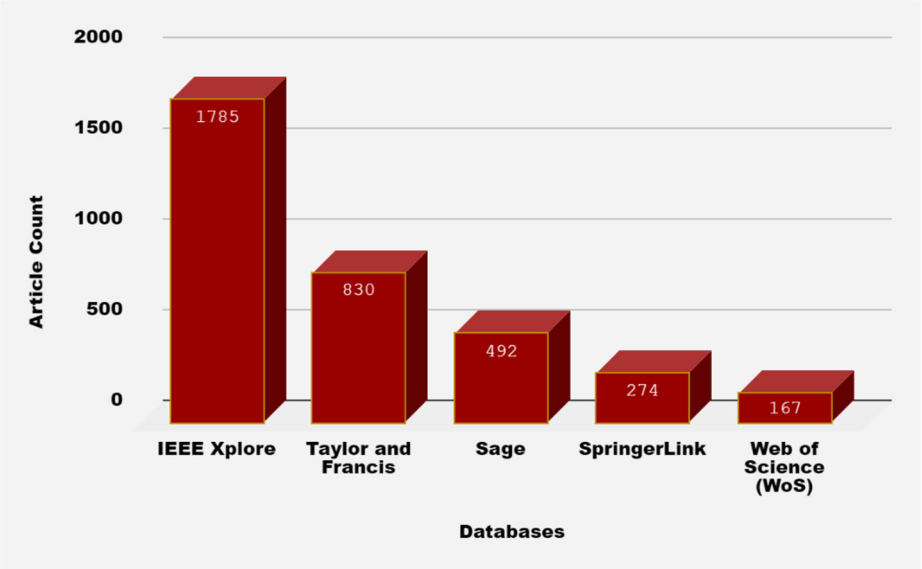

Figure 2. Distribution per publication source types.

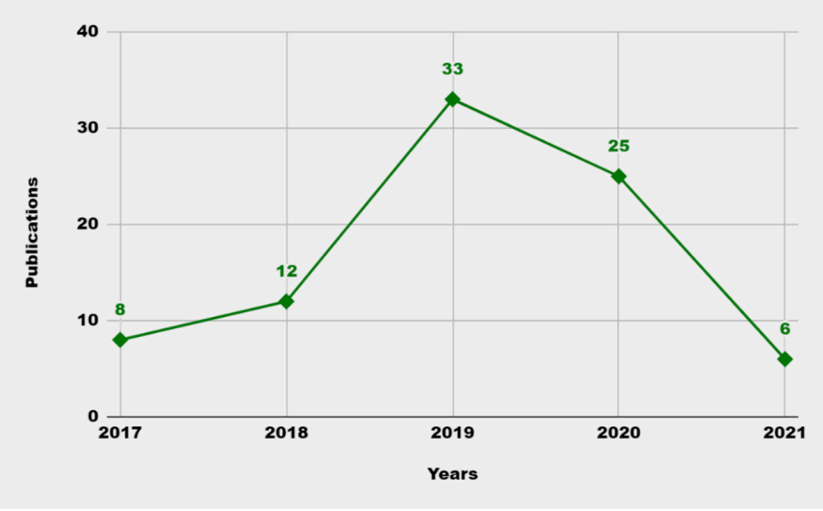

Figure 3. Number of publications per year.

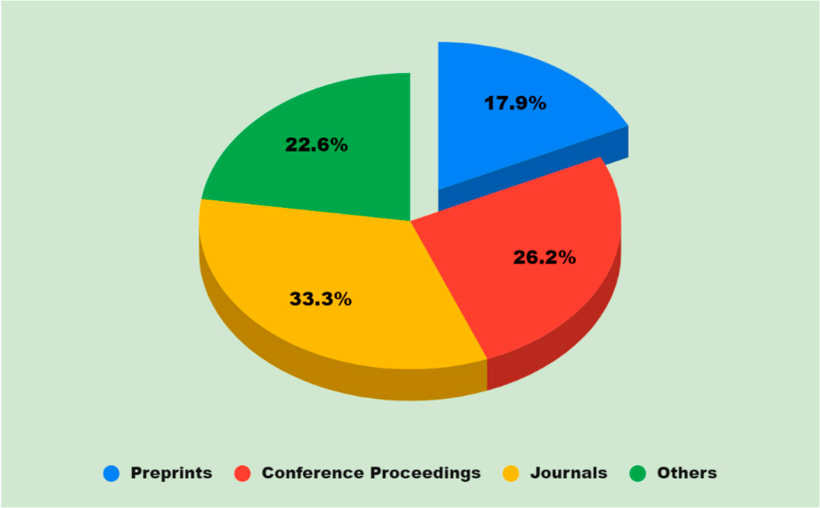

Figure 4. Articles that are pertinent to the study which was reviewed.

3.5. Selection Execution

The goal of the search was to compile a preliminary list of research that will be evaluated further. The papers were then examined to determine whether they were appropriate and could be utilized to answer the research questions formulated, which had a time frame of five years between 2017 and 2021 (Figures 1–5). Tables 4–10 summarize some of the studies chosen based on the formulated research questions.

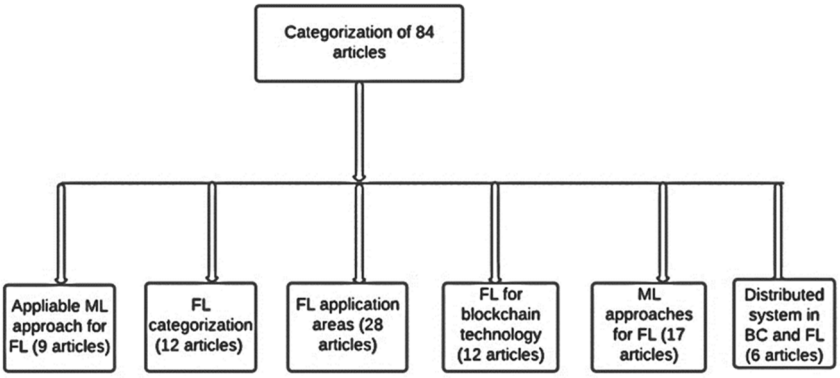

Figure 5. Categorization of primary articles based on a present review on FL.

Table 4. Summary of some selected studies and number of articles reviewed.

Application Areas	Number of Articles
ML methods applicable for FL	9
Categorization of FL	12
FL application areas	28
FL for Blockchain technology	12
Implementation of ML algorithms for FL	17
Distributed system in BC and FL	6
Total	84

Table 5. Summary of Applicable Machine learning Methods.

ML Models	Advantages	Applications
Linear Models	• LM is in a concise form • It is easy to model	• Linear regression • Ridge regression
Tree Models	• TM is accurate • It is a stable model • The model can map non-linear relationships	• Classification tree • Regression tree
Neural Network Model	• NNM has learning capabilities • It is a highly robust system • It tolerates faults	• Pattern recognition • Intelligent control

Table 6. Summary of FL categorization.

Categories of FL	Advantages	Applications
Horizontal FL	• It increases the operator sample size	• Android phone model • Logistic regression
Vertical FL	• It increases feature dimensions	• DT • NN
FTL	• It increases the operator sample size • It also increases feature dimension	• Transfer learning

Table 7. Summary of FL application in mobile devices.

Authors	Applicable Domain	Objective	Contribution	Limitation
Chen et al. [21]	Smartphone keyboard (SPK)	Learn out-of-vocabulary words	Increasing a keyboard's repertoire without exporting sensitive data	Has a strong reliance on a probabilistic model that has been taught.
Leroy et al. [22]	Smartphone voice assistant	Learn how to use the built-in wake word detector.	Instead of employing a typical weighted model averaging technique, an adaptive averaging strategy was used.	Do not demonstrate resilience in the face of background noise.
Hard et al. [23]	SPK	Prediction of the next word on a computer-generated keyboard	Improve recall by training an RNN model from scratch in the server and federation contexts.	Communication costs are still expensive.
Yang et al. [24]	SPK	increase the quality of virtual keyboard search suggestions	Given the convexity of the error function, the LR model is readily trainable.	Model training with a high number of parameters is impracticable
Ramaswamy et al. [25]	SPK	Emoji may be predicted from text written on a keyboard.	Yield better results than a model that has been trained on a server	Because client cache contents vary, measurements from multiple tests cannot be compared.

Table 7. *Cont.*

Authors	Applicable Domain	Objective	Contribution	Limitation
Wang et al. [26]	Mobile edge computing (MEC)	MEC, caching, and communication all were optimized.	The possibility of combining Deep Reinforcement Learning and the FL framework with the mobile edge system was discussed.	The question of how to disperse the massive compute burden among heterogeneous situations remains unsolved.
Qian et al. [27]	MEC	Placement of privacy-conscious services for mobile edge computing	To suit users' service expectations, suggest a privacy-aware service placement (PSP) method.	It can't be utilized for many edge clouds.
Feng et al. [28]	Mobile devices' motion sensors	Predicting Human Mobility While Maintaining Privacy	Reduce performance deterioration by using a group optimization technique.	Consider simply the fundamental mobility model for the sake of simplicity
Sozinov et al. [29]	Smart devices' motion sensors	Recognizing Human Motion	Erroneous customers are identified and rejected.	When compared to centralized models, producing models with somewhat lower accuracy.
Aivodji et al. [30]	Smart home IoT	Create a secure federated smart home environment.	FL is combined with safe data aggregation in this system.	Implementing a pretty sophisticated architecture
Yu et al. [31]	Smart home IoT	Discover the patterns of consumers' activity	Identify physical dangers efficiently	For a variety of deployments, the mapping process isn't flexible enough.
Liu et al. [32]	Robot System	Consider learning from robots	Boosts the effectiveness of local robots' simulated learning in cloud robotic schemes	There is much more work to be done on the fusion process's convergence rationale.

Table 8. Summary of FL application in industrial engineering.

Authors	Applicable Domain	Objective	Contribution	Limitation
Hu et al. [33]	Environmental Preservation	Founded on federated region learning, an environmental monitoring framework was developed.	To increase inference accuracy incorporates geographical factors while distributing training data.	Rather than two-layer structures, multi-layer structures should be used.
Han et al. [34]	Image recognition	Providing manufacturers with automated fault inspection services	Fix the issue of not having enough faulty samples to discover flaws	To service a variety of sectors, a rapid model deployment is required.
Mowla et al. [35]	Aerial Vehicles that are unmanned	Detection of harmful attempts in UAV communication systems	Using the Dempster–Shafer theory, improve the model using a client group prioritizing strategy.	In this design, there is a need to increase the dependability of global updates.
Saputra et al. [36]	Electronic vehicles	Energy demand forecasting in a federated manner	To further increase forecast accuracy, the clustering-based energy demand learning approach was used.	More stability and flexibility are required.

Table 8. *Cont.*

Authors	Applicable Domain	Objective	Contribution	Limitation
Yang et al. [37]	Financial field	Credit card theft is detected	The test AUC is 10% higher on average than the previous approach.	To preserve the privacy of individuals, more accurate measures should be taken into consideration.
Wang et al. [38]	Mining of text	Filtering spam and analyzing user sentiment	Using Random Response with Priori (RRP) assures both data privacy and model correctness theoretically.	The noise generated by our perturbing approach will have little impact on overall performance.

Table 9. Summary of FL application in healthcare.

Authors	Applicable Domain	Objective	Contribution	Limitation
Brisimi et al. [39]	Predict the number of times a patient will be admitted to the hospital in the future.	Algorithm for Cluster Primal-Dual Splitting	Yield classifiers with a small number of features	For convergence, additional iterations are required.
Silva et al. [40]	MRI examination	Establish a federated analytic framework that is compatible with ENIGMA's standard pipelines.	Effortlessly deal with a variety of high-dimensional features.	Only a small dataset was used for testing.
Liu et al. [41]	Clinical notes are extracted.	Federated NLP approach with two stages.	To increase accuracy, a pre-processing step has been included.	Small, suspect instances are not suited.
Gao et al. [42]	Classification of EEG	Make a horizontal FL framework that is hierarchical and diverse.	Over heterogeneous EEG data, the first EEG classifier was developed.	Work on just three separate datasets at a time.
Li et al. [43]	Calculate the likelihood of death and the length of time spent in the hospital.	Introduce community-based FL and assess its effectiveness on non-iid icu EMRs.	In comparison to the baseline FL model, the model was able to achieve greater prediction accuracy in fewer communication cycles.	Extra communication overhead will result from community model settings.
Pfohl et al. [44]	Medical Forecasting	Determine the effectiveness of FL in comparison to centralized and local learning.	Perform FL in a way that is both distinct and private.	The cost of privacy is undervalued.
Huang et al. [45]	Predicting mortality based on drug use data	Method of adaptive boosting	Introduce data-sharing technologies to alleviate non-iid.	Using iid data for training iid data outperforms non-iid data
Kim et al. [46]	Computer phenotypes are studied.	Computational phenotyping using federated tensor factorization for privacy.	The patient data is not revealed since the information is summarized.	Only accurate when the data is tiny or skewed distributed.
Lee et al. [47]	Similar patient matching	Framework for patient hashing that is federated	Reverse engineering is a security threat that should be avoided.	Computed complexity is unavoidable.

Table 10. Summary of research on the current state of data sharing in distributed systems in BC and FL.

Authors	Applicable Domain	Objective	Contribution	Limitation
Salah, Rehman, Nizamuddin & Al-Fuqaha [48]	Blockchain and AI	Survey on blockchain applications for AI	The review pieces of literature on emerging blockchain applications, platforms, and protocol	Privacy, smart contract security, trusted oracles, scalability, consensus protocols, standardization, interoperability, quantum computing resiliency and governance were not considered in their study
Zheng, Xie, Dai, Chen & Wang [49]	Blockchain Technology	A comprehensive review of BC	Over BC, BC architecture and core characteristics of BC were discussed in this study	In-depth investigations on blockchain-based applications were not conducted
Li, Chen, Liu, Huang, Zheng & Yan [50]	BC-built decentralized FL framework	A BC-built FL context with committee consensus, i.e., a distributed FL architecture founded on BC (BFLC)	A novel committee consensus technique has been presented that may effectively minimize the amount of consensus computation while also reducing malicious assaults.	Time complexity was not considered
Lu, Huang, Dai, Maharjan, & Zhang [51]	BC and FL for confidentiality-conserved data allocation in IoT industries	Create a safe data sharing architecture for dispersed multiple parties using blockchain technology.	FL was incorporated into the permissioned BC consensus process by the authors, allowing the consensus computing effort to be utilized for federated training as well.	The study used inadequate resources of devices.
Kang, Yu, Huang, Wu, Maharjan, Xie & Zhang [52]	BC in vehicular edge computing	In-vehicle computing and systems, a safe peer-to-peer data exchange scheme was suggested.	The suggested TWSL method outperforms standard reputation schemes in terms of enhancing the detection rate of anomalous cars and ensuring data security during data exchange, according to numerical findings.	Dataset used in this study is limited
Rahman, Hossain, Islam, Alrajeh & Muhammad [53]	A Blockchain-based Federated Learning Methodology	FL and discrepancy confidentiality (DC) were suggested to preserve the confidentiality and safety of IoHT data, allowing secluded IoHT data to be educated at the holder's location.	The authors tackled the issue of incorporating lightweight security and privacy solution into the FL ecosystem.	The accuracy and loss metrics values are very low and this can be improved in the future

As presented in Table 4, the systematic review of the literature summarized the number of related articles reviewed.

4. Results and Discussion

In this section, data extraction and analysis, a summary of the reviews, the search strategy yielded during the study and, the limitations of the review study are presented.

4.1. Data Extraction and Analysis

The outcomes of each study topic are discussed in the following parts, as well as an appraisal of the existing works' strengths and limitations.

RQ1: What are the applicable ML methods for FL?

FL is slowly entering the prevalent ML paradigm, intending to ensure privacy and efficiency in FL systems. We focus on three classes of methods that federated learning can support: linear models, decision trees, and neural networks (Table 5).

i. Linear methods

There are three types of linear models: linear regression, ridge regression, and lasso regression. Du et al [54] suggested using a federated environment to train a linear model, which addresses the security concern of entity analysis and accomplishes the equivalent accuracy as the non-private alternative. Nikolaenko et al [55] created the highest performing ridge regression system using homomorphic encoding, and Lindell and Pinkas [56]. The linear method is straightforward to apply in comparison to other models, and it is a good model for adopting FL.

ii. Tree models

Single or many decision trees (DT), for instance, gradient boosting decision trees and random forests (RF), may be trained via federated learning. The Gradient Boosting Decision Tree (GBDT) method has attracted a lot of consideration lately, owing to its excellent performance in a variety of classification and regression applications. For the first time, Zhao et al. [57] used the GBDT confidentiality fortification system in regression and binary classification responsibilities. To avoid the leak of user data privacy, the system securely combines regression trees learned by multiple data owners into a group. Cheng et al. [58] presented the SecureBoost framework, which allows users to create an FL system by training the gradient lifting DT model for horizontal and vertical partition data.

iii. Neural network (NN) models

The NN model is a prominent ML method right now, and it seeks to train neural networks to do complicated tasks. Deep neural network research is becoming further prevalent in the federal context. Drones may help with a wide range of tasks, including trajectory planning, target identification, and target localization. The UAV (Unmanned Aerial Vehicle) group typically trains the model through DL to provide more efficient services, but owing to the absence of an unceasing linking between the UAV group and the ground base station, the federal training technique cannot produce the UAV's real-time performance. Zeng et al. [59] were the foremost to apply a distributed FL approach to a UAV group, improve federated learning convergence speed, and perform joint power allocation and scheduling. The principal UAV recaps the local flight method taught by the other UAVs to develop the comprehensive flight method, which is then delivered to the other UAVs over the intra-group network. Bonawitz et al. [60] used TensorFlow to create a scalable FL system for mobile devices that can train a great quantity of distributed data models. To accomplish priority applications incorporating data, Yang et al. [10] put up a federated DL system built on data division. In addition to corporate data applications, traffic flow data in government affairs big data regularly includes a significant amount of user confidentiality. Liu et al. [61] recommend a clustering FedGRU technique that incorporates the ideal comprehensive method and captures the Spatio-temporal correlation of traffic flow data more precisely by combining GRU (Gated Recurrent Unit) NN for traffic flow forecasting with FL. Experiments on actual data sets reveal that it outperforms non-federated learning approaches significantly.

RQ2: What is the categorization of federated learning?

Here we converse on how to classify FL based on the distribution characteristics of the data. According to Yang et al. [10], FL may be divided into three categories: horizontal FL, vertical FL, and FTL. Data deposited in separate nodes or institutions are generally in the form of a feature matrix. In most cases, data comprises numerous occurrences, with the horizontal axis of the sheet representing the client and the vertical axis representing the customer's qualities. Then, depending on the data partition mode, we may split FL (Table 6).

i. Horizontal FL

There is some intersection between the features of data dispersed over multiple nodes in horizontal FL, even though the data are fairly diverse in sample space. At the moment, current FL algorithms are largely intended for use in smart devices or internet of things devices (IoT). Horizontal FL is the most common kind of FL in these settings. Since data may vary greatly in model space while having a comparable feature space at the same time. Since the data has the same feature dimension (FD), the federated model solution for the Android mobile phone update proposed by Google [62] is often a horizontal FL. In addition, Gao et al. [42] proposed a hierarchical heterogeneous horizontal FL frame to address the problem of limited labeled entities. The problem of a lack of label may be handled by adapting heterogeneous domain adaption numerous times, each time utilizing each partaker as the aimed domain. This would help to compensate for the absence of data annotation in EEG classification. Data collecting is inextricably linked to a great amount of effort in real-world applications such as medical care. It is almost hard for any institution to create a data pool for sharing when it comes to cross-regional collaboration. To strengthen the joint model, FL might build a federal network for cross-regional hospitals with comparable healthcare information.

ii. Vertical FL

Vertical FL is appropriate for scenarios in which data is segregated vertically based on FD. The entire parties have homogenous data, which indicates that they have some sample ID overlap but vary in feature space. For instance, there was a healthcare facility that aimed to forecast disorders such as diabetes mellitus. According to studies, those with high blood pressure (HBP) and obesity are more likely to acquire type 2 diabetes [63]. As a result, it may be assessed based on certain general measurements, for instance, the age and weight of the patients, including their health history. If a young guy does not have obesity or HBP but consumes extra calories and does not engage in physical exercise. He is also at risk for diabetes, but owing to a lack of knowledge, it cannot be anticipated or tailored. With the development of FL, it will be possible to collaborate with firms that have data sets from smartphone applications such as step counters or dietary structures. Furthermore, they may work together without requiring raw data transfer. Scholars often approach this topic by removing similar entities with different qualities to receive joint training. Due to entity resolution, it is a more difficult task than horizontal FL. Not nearly as straightforward as in horizontal FL, pooling all the datasets on a shared server to acquire from the worldwide model does not work on vertical FL since the communication among various proprietors remains a pressing issue. To preprocess vertical segregated data, Nock et al. [64] have developed an improved token-built entity resolution technique. To defend honest-but-curious opponents for vertical FL, Hardy et al. [65] proposed an end-to-end technique based on a linear classifier and applied improver homomorphic encoding. Existing applications for parties with similar illustration space, such as traffic desecration evaluation and trivial business credit risk investigation, are said to be founded on FATE, which was established by the Webank team. Furthermore, Cheng et al. [58] developed SecureBoost, a safe context for vertically partitioned data sets. The approaches outlined above, on the other hand, could only be used in basic ML methods such as logistic regression. As a result, vertical FL still has a lot of potential for development when it comes to applying it to more complex machine learning methodologies.

iii. Federated Transfer Learning (FTL)

In most circumstances, in contrast with the scenarios in horizontal and vertical FLs, data does not share model or feature space. As a result, the key issue in this scenario is an absence of data markers and deprived data value. Transfer learning (TL) allows you to transfer information from one domain (the source domain) to another domain (the target domain) to improve your learning outcomes, which is ideal in this case [66]. In this fashion, Liu et al. [9] devised FTL as a technique to take a broad view of FL for use with shared parties with minor intersections. This is the first FL stack that includes training, assessment, and cross-validation and is based on transfer learning. Furthermore, the neural networks in this frame with additive homomorphic encryption technology may not solitarily avoid confidentiality seepage but similarly, give equivalent accuracy to non-confidentiality-conserving methods. Nevertheless, communication proficiency continues to be a problem. As a result, Sharma et al. [67] labor diligently to enhance FTL. Instead of using HE, they used secret sharing technology to cut overhead while maintaining accuracy. It might also be expanded to block rogue servers. They presume that the model is semi-honest in the earlier work. For a real-world application, Chen et al. [13] built a FedHealth system that uses FL to collect data from many organizations and then uses transfer learning to provide individualized healthcare services. Certain illness diagnostic and treatment data from one infirmary might be moved to an additional infirmary to aid in the analysis of other diseases using FTL. FTL research is still in its early stages, therefore there is a lot of possibility for enhancement to make it further versatile with various data structures. Data isles and confidentiality concerns are two major difficulties that have arisen as a result of the present large-scale industrialization of ML. FTL, on the other hand, is a viable technique to safeguard both data safety and user confidentiality while breaking down data island boundaries.

RQ3: What are the FL application areas?

With the establishment of a collaborative model free of legal worry, FL becomes a popular strategy. Despite the restrictions and considerable problems outlined above, early participants saw significant prospects in FL and began a series of associated research and efforts to implement FL in actual life. Numerous applications connected to industrial engineering or computer science are discussed in this section.

i. Application for mobile devices

Since Google originally proposed the notion of FL to forecast users' input via Gboard on Android gadgets, academics have been paying close attention to it. Chen et al. [12]; Leroy et al. [21]; Hard et al. [23], and Yang et al. [24] have all made improvements to keyboard prediction. Emoji prediction is also a center for study [25]. A possible application is to apply the FL method to smart equipment to forecast human trajectory [28] or human behavior [29].

Although mobile device storage space and computational power are rapidly increasing. Due to transmission capacity constraints, it is challenging to meet the increased quality demand from mobile users. To avoid network congestion, most comprehensive providers choose to provide a service environment at the cellular network's edge, near to the client, rather than integrating cloud computing and cloud storage into the main network. Mobile edge computing (MEC) is the name given to this technology; however, it comes with a higher danger of data leakage. The combination of FL and MEC is one potential approach. Wang et al. [26] develop an 'In-Edge AI' framework that combines FL founded on deep reinforcement learning with a MEC system to additionally enhance resource apportionment issues. Furthermore, Qian et al. [27] focused on the application of FL to MEC. They created a confidentiality-consciousness service placement technique that allows them to deliver high-quality service by secreting needed services on edge servers near to customers.

In this scenario, mobile devices don't only relate to regular phones; they also refer to IoT devices. One of the most essential IoT applications is smart homes. Devices in smart home design will upload certain associated data to a cloud server to better understand customers' preferences, which might lead to a data breach. As a result, Aïvodji et al. [30]

describe a safe federated architecture that can be used to develop joint models. Yu et al. [31] create a federated multi-task learning framework for smart home IoT to robotically study users' activity patterns and identify physical dangers. In addition, Liu et al. [32] suggested a data fusion strategy for robots' artificial learning in automaton networking based on FL. This technology might be used to develop guidance models and predict different crises in self-driving automobiles. The research on FL applications in mobile devices discussed earlier is summarized in Table 7.

ii. Application in industrial engineering

As a result of FL's success in data confidentiality fortification, it's only natural for industrial engineering (IE) to follow suit with FL applications. Due to legal and regulatory restrictions, data in certain sectors is not readily accessible. However, we can only take advantage of these dispersed datasets to acquire limitless benefits if FL is applied to these locations.

To the best of our knowledge, FL might have widespread adoption and application possibilities in data-sensitive domains for IE as a result of its ascent and development. In the context of environmental protection, Hu et al. [33] devised a new conservational monitoring framework based on federated region learning (FRL) to compensate for the difficult interchangeability of observing data. Thus, observing data scattered from many sensors might be used to improve the collaborative model's performance. FL is also used to do visual inspections [34]. It could not solitarily assist us to overcome the issue of insufficient faulty illustrations for detecting flaws in production jobs, nonetheless, it could similarly provide manufacturers with privacy assurances. Liu et al. [32] use FL to collect diversiform illustrations from federated tasks for improved grounding applications in picture fields. FL has suited for malicious attack detection in communication systems constituted of Unmanned Aerial Vehicles (UAVs) in addition to picture recognition and representation [35]. Since UAV characteristics such as imbalanced data distribution and poor communication situations are extremely similar to FL difficulties. With the increased popularity of electric cars, Saputra et al. [36] developed a federated energy demand forecast approach for diverse charging stations to avoid energy congestion in the communication procedure. Furthermore, Yang et al. [37] used FL to transactions held by multiple banks to easily identify credit card swindles, which is a major addition to the financial area. Wang et al. [38] use a federated architecture based on Latent Dirichlet Allocation to do text mining. It passed the spam filtering and sentiment analysis tests on actual data.

To conclude, FL allows data owners to increase the scope of their data applications and enhance model performance by iterating across multiple entities. FL technology will help more sectors become smarter in the future. The combination of FL and AI will create a federal ecology free of data privacy concerns. The research on FL applications in industrial engineering discussed earlier is summarized in Table 8.

iii. Application in HealthCare

FL has a bright future in health care as a disruptive technique of conserving data confidentiality. Although each medical facility may have a huge volume of patient data, this may not be sufficient to train their prediction methods [68]. One of the effective options for breaking down the boundaries of analysis across various hospitals is to combine FL with illness prediction.

EMRs (electronic medical records) provide a wealth of clinical information. Kim et al., 2017 attempted to employ tensor factorization models for phenotyping examination to extract information from health annals without revealing patient-level data. It might be considered the first FL application in the medical field. In a federated setup, Pfohl et al. [44] investigated differentially secluded learning for EMR. They also showed that the results are equivalent to training in a unified environment. Huang et al. [45] utilize EMRs from several hospitals to estimate the death rate of heart disease patients. There is no data or parameter communication across hospital databases throughout the training phase. Aside from that, data collected from various distant clients into a dominant server is encoded ahead of time,

and the decipherer is turned off after the training. Brisimi et al. [39] also utilize EMRs to determine if a patient with heart disease will be admitted to the hospital using an FL method known as cluster Primal-Dual Splitting (cPDS). This forecasting work may be carried out on health managing gadgets or in hospitals that save medical data without leaking information. Lee et al. [47] suggested a federated patient hashing architecture based on health data to find similar patients in multiple institutions without exchanging patient-level information. This kind of patient matching might assist physicians in determining a patient's overall personality and directing them to a patient with greater experience. Huang et al. [45] used the Loss-based adaptive boosting Federated Averaging method on medication consumption retrieved from the MIMIC-III database to forecast patient death rates. This study looked at computing complexity, communication costs, and accuracy for each client, and found that they outperformed baselines.

Studies have also shown that FL can be used to assess genuine data from health records in the realm of natural language processing (NLP). The necessity for unstructured data processing of clinical notes is highlighted by Liu et al. [41]. It was the first time NLP was used in conjunction with FL. They used a two-stage federated training model that included pre-processing to forecast a representation model for each patient and phenotyping training to investigate each kind of sickness. FL has recently been popular in the field of biological-image analysis. Silva et al. [40] proposed federated principal components analysis (fPCA) to extract characteristics from magnetic resonance imaging (MRI) from several medical facilities. In addition, Gao et al. [42] developed a hierarchical heterogeneous horizontal FL (HHHFL) framework for EEG classification to tackle the difficulty of limited labeled cases as well as the privacy limitation.

To the best of our knowledge, FL might have a broad range of popularization and application possibilities in data-sensitive industries in addition to the aforementioned domains as a result of its ascent and maturity. In 2019, the use of FL has increased by leaps and bounds. As a result, it is expected that FL will have a lot of potential in the future. FL now contributes mostly to horizontally collaborative training for landing applications, implying that the feature dimensions of each data are identical. Medical data at hospitals might be shared with other institutions in the future, such as insurance agents, to acquire more affordable pricing. As a result, vertical FL is a viable path to pursue. Furthermore, one issue is that current government training is focused on a limited number of organizations and is unable to scale to include collaborative training for a large number of devices or institutions. As a result, better analysis of mobile device data based on FL should be pursued to provide more useful data. The research on FL applications in healthcare discussed earlier is summarized in Table 9.

RQ4: What is the relationship between FL and BT concerning data sharing in distributed systems?

Blockchain (BC) is a relatively new technology that is rapidly gaining traction in other countries. In a nutshell, BC is a distributed ledger inspired by Bitcoin [69–73], categorized by decentralization, immutableness, traceability, communal conservation, frankness, and transparency. Quality investigation of 3D-printed articles [74], utilization observation and confidentiality-conserving energy trading for shrewd grids [75], and emergency healthcare facilities for pre-hospital maintenance are just a few of the BC-aided structures for industrial data allotment that have been projected [76]. Existing BC research is mostly focused on developing innovative medical information allocation systems [77], but collaborative training to optimize data use has yet to be applied. BC can drastically modify several challenges in Florida, according to a new study. FL and BC are complementary technologies. BC is a natural fit for FL since it is a distributed technology that is inherently safe. Since the BC architecture is forgiving of rogue nodes, it will continue to function correctly as long as bad nodes do not account for more than 51% of total nodes.

Majeed and Hong [78] imagined a strong FL chain that could validate local model updates by injecting blockchain technology (BCT) into the language. Although BCT may ensure the security of a complete architecture, it has nothing to do with privacy. Individual

node allusion does not pose a threat to privacy. If a malevolent clinic or hospital participates in the collaborative training, it may go to great lengths to pry into the personal information of other participants. Hence Ilias and Georgios [79] employed a BC smart convention to coordinate all clients and homomorphic encryption to provide further anonymity. Awan et al. [80] integrated a variant of the Paillier cryptosystem into their BC-based privacy-preserving FL architecture as a precautionary step to prevent privacy leaking. Furthermore, by using BC, each party's contribution to optimizing the global model can be tracked, allowing for an incentive system to be implemented. The BC-based FL frames stated above did not provide a special incentive for clients to participate in training. A dynamic weighing mechanism was presented to increase the performance of FL [81]. To inspire high-quality clients to partake in the training, it used learning accuracy and participation frequency as training weights. In addition, Kim et al. [46] introduced Block-FL, which rewards clients that store a large number of samples and thereby minimizes convergence time. To summarize, combining BC with FL is advantageous since blockchain is a decentralized technology that eliminates the need for a dominant server to anticipate worldwide models. As a result, it may be able to overcome FL's bandwidth limitations. In addition, it could not solitarily exchange updates while verifying accuracy to improve safety, but it could also use some kind of activation mechanism to advance FL service. When it comes to sharing learning models, however, incorporating blockchain may create extra delay. A BC-built FL with minimal dormancy would be preferable.

Blockchain is a networked peer-to-peer distributed, open-source, unchangeable public digital register. A blockchain is a ledger that is made up of a chain of blocks with agreement methods and encoding. This register keeps track of all transactions and interactions between users of the dispersed and distributed BC scheme [48]. This network setup is resistant to malicious attacks since it only has negotiated blocks between users. Consensus techniques, for instance, proof-of-steak (PoS) and proof-of-work (PoW) are used to obtain an agreement in a dispersed setting. Fiscal facilities, smart contracts, IoT, and safety services are all possible applications of blockchain technology.

Blockchain may be used to attract clients for businesses that demand a high level of dependability and honesty. It is also spread, which eliminates the peril of a sole point of failure [49]. The combination of AI and BCT has prepared the method for several robust structures that enable the collaboration of numerous gadgets while maintaining secrecy, verification, and veracity [48]. The decentralized nature of BC [50] potentially replaces the central server in the BC-built FL (BCFL) system. Instead of a centralized server, smart contracts (SC) may perform the same operations and be triggered by blockchain transactions. In other words, the FL is carried out by the participating nodes using BC, which keeps track of global models and local modifications. BC storage, a group consensus device, and a method training component make up the method. The BCFL training material is stored on a BC scheme, which solitary approved gadgets may have access. Limited trustworthy nodes form a committee that verifies changes and provides a score to them in the committee consensus method. Only the most up-to-date changes will be stored on the blockchain. A new committee is constituted at the beginning of each cycle. Other than committees, nodes undertake local training for the model training every cycle. The researchers of Lu et al. [51] present a technique for distributing manifold clients in IIoT applications that combines federated learning into permissioned blockchain and integrates FL into authorized BCT. Kang et al. [52] propose a distributed vehicle strategy to alleviate the communication burden and meet provider confidentiality issues. The integration of FL with BCT, according to Rahman et al. [53] offers increasing value to the healthcare industry. Table 10 shows the summary of articles reviewed on the current state of data sharing in distributed systems in BC and FL.

RQ5: What are the ML algorithms implemented with FL?

Some studies have employed ML and Deep learning (DL) with FL, and some of these are shown in Table 11. The methods, datasets, performance metrics, and limitations of the study were listed.

Table 11. Summary of ML algorithms implemented with FL.

Authors	Approaches	Dataset	Assessment Metrics	Limitations
Luo et al. [82]	YOLO, Faster R-CNN	900 images engendered from 26 street cameras and 7 object	Interaction Over Union (IOU), Mean Average Precision (mAP)	Limited to just one benchmark on the datasets used in their study
Li et al. [50]	LR, CNN, and RNN	FEMNIST, MNIST, Sentiment140	F1-score	More advanced ML models were not used
Gao et al. [42]	CNN	MindBigData dataset (Electroencephalography (EEG))	Accuracy	protected multi-party computation and differential confidentiality was not used in this study
Wang et al. [38]	FedMA (Deep CNN and LSTM)	Shakespeare dataset over	Accuracy, Epoch	Lesser deep learning building blocks were used in this study. FedMA fault tolerance and fewer datasets were not considered in this study.
Lee & Shin [63]	FedAVG	MNIST dataset, MIMIC-III dataset	AUROC, F1-score, Precision recall	Real-life medical data with multiple institutions were not considered
Hamer et al. [83]	FedBoost, AFLBoost	Synthetic dataset	-	The study proposed performance algorithm was not evaluated
Yang et al. [84]	SVM	MNIST dataset	AoU	Only one ML algorithm was considered in this study. The proposed system has low complexity
Sheller et al. [85]	U-net of DCNN	BraTS 2017	Precision	Low datasets were used in this study
Ahmadi et al. [86]	Deep-Q-Reinforcement Learning Ensemble based on Spectral Clustering called DQRE-SCnet	MNIST, Fashion MNIST, and CIFAR-10	Accuracy, AUC, Recall, Kappa, Run time	The study had high computation time and high complexity for any dataset
Elbir & Coleri [87]	CNN	channel data	Accuracy, complexity order	Compression techniques and scheduling time was not considered in the study
Elbir & Coleri [88]	CNN	local datasets	RMSE, NMSE	Compression-centered approaches for both training data and the approach constraints to additionally decrease the communication overhead was not considered
Pokhrel & Choi [89]	Local policy, global policy, learning idea	TCP CUBIC streams	Loss comparison, throughput,	Time complexity was not considered in this study
Hard et al. [23]	FederatedAveraging (Federated CIFG)	7.5 billion sentences	Recall	The time complexity and accuracy were not considered

Table 11. *Cont.*

Authors	Approaches	Dataset	Assessment Metrics	Limitations
Bhagoji et al. [90]	CNN	Fashion MNIST	Accuracy, weight values, time	The system was not robust enough to prevention from attackers
Lalitha et al. [91]	DNN	-	Mean square error (MSE)	An empirical study was not conducted to evaluate the proposed system
Chen et al. [92]	Echo state networks (ESN)	Real pedestrian mobility patterns from BUPT and actual content transmission data	Time, Throughput, Number of UAV	The limited dataset used for the study implementation
McMahan et al. [62]	CNN, LSTM	MNIST, Shakespeare	Accuracy	Hybridization of differential privacy and secure multi-party computation was not considered

4.2. Summary of the Review

The review study included 22 articles in our systematic review and examined them founded on the aspects of ML approaches, categorization and application areas. A summary of our investigation is obtainable in Figure 2. This investigation reviews several fascinating and valuable articles regarding the state-of-the-art in FL. This article is organized based on ML approaches, categorization, and application areas. Figure 2 shows the PRISMA flow diagram of how the systematic review was conducted. Table 1 shows the summary of the related pieces of literature reviewed and finally, Table 2 shows the databases and keywords used for the study search.

4.3. Search Strategy Yield

Figure 2 shows a full summary of the search strategy yield. The database search yielded sixty-one published publications, with an additional twenty-three items discovered using a focused Google Scholar search and the reference lists of pertinent articles. Two reviewers (ROO and SM) looked through the publications and used inclusion criteria to find the relevant ones. Figure 2 depicts the technique. Despite satisfying all of the inclusion requirements, one hundred and twenty-four articles were rejected for being duplicates, one hundred and twelve for being irrelevant, ten for being book chapters, and twenty-six for being beyond the topic of the article. At this point, sixty-one papers were selected, and these sixty-one articles were placed into the ISI Web of Science database for a forward citation search. This search resulted in the discovery of eight new articles. A total of eighty-four publications were found to be suitable for inclusion in this systematic review.

4.4. Comparative Analysis

The study was compared with existing related works (literature reviews) and it was discussed that our study drove more into the relationship between blockchain, ML, and federated learning as seen in Table 12. Ali, Karimipour and Tariq [15] discussed the present progress and incoming challenges in blockchain and federated learning for IoTs. Nguyen et al. [20] presented the opportunities and challenges experienced in FL meeting BT in edge computing. Li et al. [19] discussed the application areas of federated learning alone. Passerat-Palmbach et al. [93] presented a study on Blockchain-orchestrated ML for confidentiality preserving FL in automated medical data. Zeng et al. [94] presented an all-inclusive review of the incentive mechanism for FL. In Hou et al. [95] architectures, applications, and issues encountered in blockchain-built FL were systematically reviewed

in this research. Preuveneers et al. [96] examined an intrusion detection case study that is a chained anomaly detection model for FL. Lee and Kim [17] discussed the inclinations in BT and FL for data allocation in disseminated platforms.

Table 12. Summary of some related review.

Authors	Year	Objectives
Ali, Karimipour & Tariq [15]	2021	The study discussed the present progress and incoming challenges in blockchain and federated learning for IoTs.
Nguyen et al. [20]	2021	The authors presented the opportunities and challenges experienced in FL meeting BT in edge computing.
Li et al. [19]	2020	The study discussed the application areas of federated learning alone.
Passerat-Palmbach et al. [93]	2020	The authors presented a study on Blockchain-orchestrated ML for confidentiality preserving FL in automated medical data.
Zeng et al. [94]	2021	The authors presented an all-inclusive review of the incentive mechanism for FL.
Hou et al. [95]	2021	The architectures, applications, and issues encountered in blockchain-built FL were systematically reviewed in this research.
Preuveneers et al. [96]	2018	The authors examined an intrusion detection case study that is a chained anomaly detection model for FL.
Lee & Kim [17]	2021	The authors discussed the inclinations in BT and FL for data allocation in disseminated platforms.

The closest studies to this present review are surveys by Nguyen et al. [13], Li et al. [19], Zeng et al. [94], Hou et al. [95], and Lee and Kim [17], but the difference is that PRISMA systematic review method was not used and then their studies are limited to only one aspect of blockchain and FL. ML was not also included in their studies. Hence, we contributed to knowledge by conducting a systematic review using the PRISMA method on federated learning and machine learning methods categorization, application areas, and blockchain technology.

4.5. Limitation

Due to the inclusion of only studies published in English, chosen search keywords, and database constraints, some relevant publications may be missing despite the exhaustive search across databases. Important data may also be found in non-peer-reviewed research, as well as unpublished thesis and dissertation studies.

5. Conclusions and Future Work

FL is a jointly decentralized privacy-preserving system that addresses data silos and data sensitivity issues. We looked at existing machine learning models for FL in this work. For FL modeling, it was argued that hybrid ML and DL models can typically outperform classic ML. However, there are several hurdles and issues with these ML approaches that have yet to be overcome. There are two aspects to this research that it contributes. To begin, we've included a comprehensive overview of several machine learning (ML) methodologies that may be used in FL applications. Secondly, we discussed some future research possibilities. Federated learning is expected to offer safe and shared security services for more applications soon, promoting the steady growth of artificial intelligence. The study acknowledges certain unsolved difficulties in its analysis based on existing

studies, including Extreme communication schemes, communication reduction, the Pareto frontier, heterogeneity diagnostics, and granular privacy constraints, beyond supervised learning and productionizing FL and benchmarks.

A future study might advance the understanding of FL by providing (i) findings on hybrid deep learning classification methods for FL and (ii) findings on using larger datasets for FL implementations. Similarly, the unsolved difficulties can also be considered for solutions in the future. It is also suggested that FL solutions exist for different data partition cases and for what application domains can be surveyed in the future.

Author Contributions: Conceptualization, R.O.O. and S.M.; methodology, R.O.O. and S.M.; resources, R.M. and R.D.; writing—original draft preparation, R.O.O.; writing—review and editing, S.M.; visualization, R.M., and R.D.; supervision, R.O.O. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

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

References

1. Awotunde, J.B.; Jimoh, R.G.; Ogundokun, R.O.; Misra, S.; Abikoye, O.C. Big Data Analytics of IoT-Based Cloud System Framework: Smart Healthcare Monitoring Systems. In *Artificial Intelligence for Cloud and Edge Computing*; Misra, S., Kumar Tyagi, A., Piuri, V., Garg, L., Eds.; Springer: Cham, Switzerland, 2022; pp. 181–208. [CrossRef]
2. Zhang, C.; Hu, X.; Xie, Y.; Gong, M.; Yu, B. A privacy-preserving multi-task learning framework for face de-tection, landmark localization, pose estimation, and gender recognition. *Front. Neurorobotics* **2020**, *13*, 112. [CrossRef] [PubMed]
3. Gong, M.; Xie, Y.; Pan, K.; Feng, K.; Qin, A. A Survey on Differentially Private Machine Learning. *IEEE Comput. Intell. Mag.* **2020**, *15*, 49–64. [CrossRef]
4. Xie, Y.; Wang, H.; Yu, B.; Zhang, C. Secure collaborative few-shot learning. *Knowl.-Based Syst.* **2020**, *203*, 106157. [CrossRef]
5. Albrecht, J.P. How the GDPR Will Change the World. *Eur. Data Prot. Law Rev.* **2016**, *2*, 287–289. [CrossRef]
6. Parasol, M. The impact of China's 2016 Cyber Security Law on foreign technology firms, and on China's big data and Smart City dreams. *Comput. Law Secur. Rev.* **2018**, *34*, 67–98. [CrossRef]
7. Gray, W.; Zheng, H.R. General principles of civil law of the People's Republic of China. *Am. J. Comp. Law* **1986**, *34*, 715–743. [CrossRef]
8. Bonawitz, K.; Ivanov, V.; Kreuter, B.; Marcedone, A.; McMahan, H.B.; Patel, S.; Ramage, D.; Segal, A.; Seth, K. Practical secure aggregation for privacy-preserving machine learning. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 1175–1191.
9. Liu, Y.; Kang, Y.; Xing, C.; Chen, T.; Yang, Q. A Secure Federated Transfer Learning Framework. *IEEE Intell. Syst.* **2020**, *35*, 70–82. [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. Kairouz, P.; McMahan, H.B.; Avent, B.; Bellet, A.; Bennis, M.; Bhagoji, A.N.; Bonawitz, K.; Charles, Z.; Cormode, G.; Cummings, R.; et al. Advances and Open Problems in Federated Learning. *arXiv* **2021**, arXiv:1912.04977.
12. Li, Q.; Wen, Z.; Wu, Z.; Hu, S.; Wang, N.; Li, Y.; Liu, X.; He, B. A survey on federated learning systems: Vision, hype and reality for data privacy and protection. *IEEE Trans. Knowl. Data Eng.* **2021**, 1–20. [CrossRef]
13. 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]
14. Mothukuri, V.; Parizi, R.M.; Pouriyeh, S.; Huang, Y.; Dehghantanha, A.; Srivastava, G. A survey on security and privacy of federated learning. *Futur. Gener. Comput. Syst.* **2020**, *115*, 619–640. [CrossRef]
15. Ali, M.; Karimipour, H.; Tariq, M. Integration of blockchain and federated learning for Internet of Things: Re-cent advances and future challenges. *Comput. Secur.* **2021**, *108*, 102355. [CrossRef]
16. Antunes, R.S.; da Costa, C.A.; 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]
17. Lee, H.; Kim, J. Trends in blockchain and federated learning for data sharing in distributed platforms. In Proceedings of the 2021 Twelfth International Conference on Ubiquitous and Future Networks (ICUFN), Barcelona, Spain, 17–20 August 2021; pp. 430–433.
18. 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]
19. Li, L.; Fan, Y.; Lin, K.Y. A survey on federated learning. In Proceedings of the 2020 IEEE 16th International Conference on Control & Automation (ICCA), Hokkaido, Japan, 6–9 October 2020; pp. 791–796.

20. Yu, S.; Chen, X.; Zhou, Z.; Gong, X.; Wu, D. When deep reinforcement learning meets federated learning: Intelligent multitimescale resource management for multiaccess edge computing in 5G ultradense network. *IEEE Internet Things J.* **2020**, *8*, 2238–2251. [CrossRef]
21. Chen, M.; Mathews, R.; Ouyang, T.; Beaufays, F. Federated learning of out-of-vocabulary words. *arXiv* **2019**, arXiv:1903.10635.
22. Leroy, D.; Coucke, A.; Lavril, T.; Gisselbrecht, T.; Dureau, J. Federated learning for keyword spotting. In Proceedings of the ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, UK, 12–17 May 2019; pp. 6341–6345.
23. Hard, A.; Rao, K.; Mathews, R.; Ramaswamy, S.; Beaufays, F.; Augenstein, S.; Eichner, H.; Kiddon, C.; Ramage, D. Federated learn-ing for mobile keyboard prediction. *arXiv* **2018**, arXiv:1811.03604.
24. Yang, T.; Andrew, G.; Eichner, H.; Sun, H.; Li, W.; Kong, N.; Ramage, D.; Beaufays, F. Applied federated learning: Improving google keyboard query suggestions. *arXiv* **2018**, arXiv:1812.02903.
25. Ramaswamy, S.; Mathews, R.; Rao, K.; Beaufays, F. Federated learning for emoji prediction in a mobile key-board. *arXiv* **2019**, arXiv:1906.04329.
26. Wang, X.; Han, Y.; Wang, C.; Zhao, Q.; Chen, X.; Chen, M. In-Edge AI: Intelligentizing Mobile Edge Computing, Caching and Communication by Federated Learning. *IEEE Netw.* **2019**, *33*, 156–165. [CrossRef]
27. Qian, Y.; Hu, L.; Chen, J.; Guan, X.; Hassan, M.M.; Alelaiwi, A. Privacy-aware service placement for mobile edge computing via federated learning. *Inf. Sci.* **2019**, *505*, 562–570. [CrossRef]
28. Feng, J.; Rong, C.; Sun, F.; Guo, D.; Li, Y. PMF: A privacy-preserving human mobility prediction framework via federated learning. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2020**, *4*, 1–21. [CrossRef]
29. Sozinov, K.; Vlassov, V.; Girdzijauskas, S. Human activity recognition using federated learning. In Proceedings of the 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom), Melbourne, VIC, Australia, 11–13 December 2018; pp. 1103–1111.
30. Aïvodji, U.M.; Gambs, S.; Martin, A. IOTFLA: A secured and privacy-preserving smart home architec-ture implementing federated learning. In Proceedings of the 2019 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 19–23 May 2019; pp. 175–180.
31. Yu, T.; Li, T.; Sun, Y.; Nanda, S.; Smith, V.; Sekar, V.; Seshan, S. Learning context-aware policies from multiple smart homes via federated multi-task learning. In Proceedings of the 2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI), Sydney, Australia, 21–24 April 2020; pp. 104–115.
32. Liu, B.; Wang, L.; Liu, M.; Xu, C.-Z. Federated Imitation Learning: A Novel Framework for Cloud Robotic Systems With Heterogeneous Sensor Data. *IEEE Robot. Autom. Lett.* **2020**, *5*, 3509–3516. [CrossRef]
33. Hu, B.; Gao, Y.; Liu, L.; Ma, H. Federated Region-Learning: An Edge Computing Based Framework for Urban Environment Sensing. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–7. [CrossRef]
34. Han, X.; Yu, H.; Gu, H. Visual Inspection with Federated Learning. In *International Conference on Image Analysis and Recognition*; Springer: Cham, Switzerland, 2019; pp. 52–64.
35. Mowla, N.I.; Tran, N.H.; Doh, I.; Chae, K. Federated Learning-Based Cognitive Detection of Jamming Attack in Flying Ad-Hoc Network. *IEEE Access* **2019**, *8*, 4338–4350. [CrossRef]
36. Saputra, Y.M.; Hoang, D.T.; Nguyen, D.N.; Dutkiewicz, E.; Mueck, M.D.; Srikanteswara, S. Energy demand prediction with federated learning for electric vehicle networks. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.
37. Yang, W.; Zhang, Y.; Ye, K.; Li, L.; Xu, C.Z. FFD: A Federated Learning Based Method for Credit Card Fraud Detection. In *Big Data–BigData 2019*; Lecture Notes in Computer Science; Chen, K., Seshadri, S., Zhang, L.J., Eds.; Springer: Cham, Switzerland, 2019; Volume 11514, pp. 18–32. [CrossRef]
38. Wang, H.; Yurochkin, M.; Sun, Y.; Papailiopoulos, D.; Khazaeni, Y. Federated learning with matched averaging. In Proceedings of the International Conference on Learning Representations (ICLR), Addis Ababa, Ethiopia, 26–30 April 2020.
39. Brisimi, T.S.; Chen, R.; Mela, T.; Olshevsky, A.; Paschalidis, I.C.; Shi, W. Federated learning of predictive models from federated Electronic Health Records. *Int. J. Med. Inform.* **2018**, *112*, 59–67. [CrossRef]
40. Silva, S.; Gutman, B.A.; Romero, E.; Thompson, P.M.; Altmann, A.; Lorenzi, M. Federated Learning in Distributed Medical Databases: Meta-Analysis of Large-Scale Subcortical Brain Data. In Proceedings of the 2019 IEEE 16th International Symposium on Biomedical Imaging (ISBI 2019), Venice, Italy, 8–11 April 2019; pp. 270–274. [CrossRef]
41. Liu, D.; Dligach, D.; Miller, T. Two-stage Federated Phenotyping and Patient Representation Learning. *Proc. Conf. Assoc. Comput. Linguist. Meet.* **2019**, *2019*, 283–291. [CrossRef]
42. Gao, D.; Ju, C.; Wei, X.; Liu, Y.; Chen, T.; Yang, Q. Hhhfl: Hierarchical heterogeneous horizontal federated learning for electroencephalography. *arXiv* **2019**, arXiv:1909.05784.
43. Li, X.; Huang, K.; Yang, W.; Wang, S.; Zhang, Z. On the convergence of fedavg on non-iid data. *arXiv* **2019**, arXiv:1907.02189.
44. Pfohl, S.R.; Dai, A.M.; Heller, K. Federated and differentially private learning for electronic health records. *arXiv* **2019**, arXiv:1911.05861.

45. Huang, L.; Yin, Y.; Fu, Z.; Zhang, S.; Deng, H.; Liu, D. LoAdaBoost: Loss-based AdaBoost federated machine learning with reduced computational complexity on IID and non-IID intensive care data. *PLoS ONE* **2020**, *15*, e0230706. [CrossRef]
46. Kim, Y.; Sun, J.; Yu, H.; Jiang, X. Federated tensor factorization for computational phenotyping. In Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Halifax, NS, Canada, 13–17 August 2017; pp. 887–895.
47. Lee, J.; Sun, J.; Wang, F.; Wang, S.; Jun, C.H.; Jiang, X. Privacy-preserving patient similarity learning in a federated environment: Development and analysis. *JMIR Med. Inform.* **2018**, *6*, e7744. [CrossRef] [PubMed]
48. Salah, K.; Rehman, M.H.U.; Nizamuddin, N.; Al-Fuqaha, A. Blockchain for AI: Review and Open Research Challenges. *IEEE Access* **2019**, *7*, 10127–10149. [CrossRef]
49. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
50. Li, Y.; Chen, C.; Liu, N.; Huang, H.; Zheng, Z.; Yan, Q. A Blockchain-Based Decentralized Federated Learning Framework with Committee Consensus. *IEEE Netw.* **2020**, *35*, 234–241. [CrossRef]
51. Lu, Y.; Huang, X.; Dai, Y.; Maharjan, S.; Zhang, Y. Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4177–4186. [CrossRef]
52. Kang, J.; Yu, R.; Huang, X.; Wu, M.; Maharjan, S.; Xie, S.; Zhang, Y. Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks. *IEEE Internet Things J.* **2018**, *6*, 4660–4670. [CrossRef]
53. Rahman, M.A.; Hossain, M.S.; Islam, M.S.; Alrajeh, N.A.; Muhammad, G. Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach. *IEEE Access* **2020**, *8*, 205071–205087. [CrossRef]
54. Du, W.; Han, Y.S.; Chen, S. Privacy-Preserving Multivariate Statistical Analysis: Linear Regression and Classification. In Proceedings of the 2004 SIAM International Conference on Data Mining (SDM), Lake Buena Vista, FL, USA, 22–24 April 2004. [CrossRef]
55. Nikolaenko, V.; Weinsberg, U.; Ioannidis, S.; Joye, M.; Boneh, D.; Taft, N. Privacy-preserving ridge re-gression on hundreds of millions of records. In Proceedings of the 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 19–22 May 2013; pp. 334–348.
56. Lindell, Y.; Pinkas, B. A Proof of Security of Yao's Protocol for Two-Party Computation. *J. Cryptol.* **2008**, *22*, 161–188. [CrossRef]
57. Zhao, L.; Ni, L.; Hu, S.; Chen, Y.; Zhou, P.; Xiao, F.; Wu, L. Inprivate digging: Enabling tree-based dis-tributed data mining with differential privacy. In Proceedings of the IEEE INFOCOM 2018-IEEE Conference on Computer Communications, Honolulu, HI, USA, 16–19 April 2018; pp. 2087–2095.
58. Cheng, K.; Fan, T.; Jin, Y.; Liu, Y.; Chen, T.; Papadopoulos, D.; Yang, Q. SecureBoost: A Lossless Federated Learning Framework. *IEEE Intell. Syst.* **2021**, *36*, 87–98. [CrossRef]
59. Zeng, T.; Semiari, O.; Mozaffari, M.; Chen, M.; Saad, W.; Bennis, M. Federated Learning in the Sky: Joint Power Allocation and Scheduling with UAV Swarms. In Proceedings of the ICC 2020-2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6. [CrossRef]
60. Bonawitz, K.; Eichner, H.; Grieskamp, W.; Huba, D.; Ingerman, A.; Ivanov, V.; Kiddon, C.; Konečný, J.; Mazzocchi, S.; McMahan, B.; et al. Towards federated learning at scale: System design. *arXiv* **2019**, arXiv:1902.01046.
61. Liu, Y.; James, J.Q.; Kang, J.; Niyato, D.; Zhang, S. Privacy-preserving traffic flow prediction: A federated learning approach. *IEEE Internet Things J.* **2020**, *7*, 7751–7763. [CrossRef]
62. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; Arcas, B.A.Y. Communication-efficient learning of deep networks from decentralized data. In *Artificial Intelligence and Statistics, Fort Lauderale*; JMLR: Wesley Chapel, FL, USA, 2017; pp. 1273–1282.
63. Lee, G.H.; Shin, S.-Y. Federated Learning on Clinical Benchmark Data: Performance Assessment. *J. Med. Internet Res.* **2020**, *22*, e20891. [CrossRef] [PubMed]
64. Nock, R.; Hardy, S.; Henecka, W.; Ivey-Law, H.; Patrini, G.; Smith, G.; Thorne, B. Entity resolution and federated learning get a federated resolution. *arXiv* **2018**, arXiv:1803.04035.
65. Hardy, S.; Henecka, W.; Ivey-Law, H.; Nock, R.; Patrini, G.; Smith, G.; Thorne, B. Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption. *arXiv* **2017**, arXiv:1711.10677.
66. Pan, S.J.; Ni, X.; Sun, J.T.; Yang, Q.; Chen, Z. Cross-domain sentiment classification via spectral feature alignment. In Proceedings of the 19th International Conference on World Wide Web, Raleigh, CA, USA, 26–30 April 2010; pp. 751–760.
67. Sharma, S.; Xing, C.; Liu, Y.; Kang, Y. Secure and efficient federated transfer learning. In Proceedings of the 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 9–12 December 2019; pp. 2569–2576.
68. Szegedi, G.; Kiss, P.; Horváth, T. Evolutionary Federated Learning on EEG-data. *ITAT*. 2019, pp. 71–78. Available online: http://ceur-ws.org/Vol-2473/paper14.pdf (accessed on 17 May 2022).
69. Ryznar, M. The Future of Bitcoin Futures. *Hous. L Rev.* **2018**, *56*, 539. [CrossRef]
70. Awotunde, J.B.; Ogundokun, R.O.; Misra, S.; Adeniyi, E.A.; Sharma, M.M. Blockchain-Based Framework for Se-cure Transaction in Mobile Banking Platform. In *International Conference on Hybrid Intelligent Systems*; Springer: Cham, Switzerland, 2021; pp. 525–534.
71. Nofer, M.; Gomber, P.; Hinz, O.; Schiereck, D. Blockchain. *Bus. Inf. Syst. Eng.* **2017**, *59*, 183–187. [CrossRef]
72. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain technology overview. *arXiv* **2019**, arXiv:1906.11078.

73. Awotunde, J.B.; Adeniyi, E.A.; Ogundokun, R.O.; Ayo, F.E. Application of Big Data with Fintech in Financial Ser-vices. In *Fintech with Artificial Intelligence, Big Data, and Blockchain*; Springer: Singapore, 2021; Volume 107, pp. 107–132.
74. Kennedy, Z.C.; Stephenson, D.E.; Christ, J.F.; Pope, T.R.; Arey, B.W.; Barrett, C.A.; Warner, M.G. En-hanced anti-counterfeiting measures for additive manufacturing: Coupling lanthanide nanomaterial chemical signatures with blockchain technology. *J. Mater. Chem. C* **2017**, *5*, 9570–9578. [CrossRef]
75. Aitzhan, N.Z.; Svetinovic, D. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. *IEEE Trans. Dependable Secur. Comput.* **2016**, *15*, 840–852. [CrossRef]
76. Hasavari, S.; Song, Y.T. A Secure and Scalable Data Source for Emergency Medical Care using Blockchain Technology. In Proceedings of the 2019 IEEE 17th International Conference on Software Engineering Research, Management and Applications (SERA), Honolulu, HI, USA, 29–31 May 2019; pp. 71–75. [CrossRef]
77. Gill, S.S.; Tuli, S.; Xu, M.; Singh, I.; Singh, K.V.; Lindsay, D.; Tuli, S.; Smirnova, D.; Singh, M.; Jain, U.; et al. Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges. *Internet Things* **2019**, *8*, 100118. [CrossRef]
78. Majeed, U.; Hong, C.S. FLchain: Federated learning via MEC-enabled blockchain network. In Proceedings of the 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), Matsue, Japan, 18–20 September 2019; pp. 1–4.
79. Ilias, C.; Georgios, S. Machine Learning for All: A More Robust Federated Learning Framework. In Proceedings of the 5th International Conference on Information Systems Security and Privacy-ICISSP, Prague, Czech Republic, 23–25 February 2019; pp. 544–551. [CrossRef]
80. Awan, S.; Li, F.; Luo, B.; Liu, M. Poster: A reliable and accountable privacy-preserving federated learning framework using the blockchain. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; pp. 2561–2563.
81. Kim, Y.J.; Hong, C.S. Blockchain-based Node-aware Dynamic Weighting Methods for Improving Federated Learning Performance. In Proceedings of the 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), Matsue, Japan, 18–20 September 2019. [CrossRef]
82. Luo, J.; Wu, X.; Luo, Y.; Huang, A.; Huang, Y.; Liu, Y.; Yang, Q. Real-world image datasets for federated learning. *arXiv* **2019**, arXiv:1910.11089.
83. Hamer, J.; Mohri, M.; Suresh, A.T. Fedboost: A communication-efficient algorithm for federated learning. In Proceedings of the 37th International Conference on Machine Learning, online, 13–18 July 2020; pp. 3973–3983.
84. Yang, H.H.; Arafa, A.; Quek, T.Q.S.; Poor, H.V. Age-Based Scheduling Policy for Federated Learning in Mobile Edge Networks. In Proceedings of the ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Barcelona, Spain, 4–8 May 2020; pp. 8743–8747. [CrossRef]
85. 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]
86. Ahmadi, M.; Taghavirashidizadeh, A.; Javaheri, D.; Masoumian, A.; Ghoushchi, S.J.; Pourasad, Y. DQRE-SCnet: A novel hybrid approach for selecting users in Federated Learning with Deep-Q-Reinforcement Learning based on Spectral Clustering. *J. King Saud Univ. Comput. Inf. Sci.* **2021**. [CrossRef]
87. Elbir, A.M.; Coleri, S. Federated Learning for Hybrid Beamforming in mm-Wave Massive MIMO. *IEEE Commun. Lett.* **2020**, *24*, 2795–2799. [CrossRef]
88. Elbir, A.M.; Coleri, S. Federated Learning for Channel Estimation in Conventional and RIS-Assisted Massive MIMO. *IEEE Trans. Wirel. Commun.* **2021**. [CrossRef]
89. Pokhrel, S.R.; Choi, J. Improving TCP Performance over WiFi for Internet of Vehicles: A Federated Learning Approach. *IEEE Trans. Veh. Technol.* **2020**, *69*, 6798–6802. [CrossRef]
90. Bhagoji, A.N.; Chakraborty, S.; Mittal, P.; Calo, S. Analyzing federated learning through an adversarial lens. In *International Conference on Machine Learning*; PMLR: Long Beach, CA, USA, 2019; pp. 634–643.
91. Lalitha, A.; Shekhar, S.; Javidi, T.; Koushanfar, F. Fully decentralized federated learning. In Proceedings of the Third workshop on Bayesian Deep Learning (NeurIPS), Montreal, QC, Canada, 7 December 2018.
92. Chen, M.; Mozaffari, M.; Saad, W.; Yin, C.; Debbah, M.; Hong, C.S. Caching in the Sky: Proactive Deployment of Cache-Enabled Unmanned Aerial Vehicles for Optimized Quality-of-Experience. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 1046–1061. [CrossRef]
93. Passerat-Palmbach, J.; Farnan, T.; McCoy, M.; Harris, J.D.; Manion, S.T.; Flannery, H.L.; Gleim, B. Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data. In Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2–6 November 2020; pp. 550–555. [CrossRef]
94. Zeng, R.; Zeng, C.; Wang, X.; Li, B.; Chu, X. A Comprehensive Survey of Incentive Mechanism for Federated Learning. *arXiv* **2021**, arXiv:2106.15406.
95. Hou, D.; Zhang, J.; Man, K.L.; Ma, J.; Peng, Z. A Systematic Literature Review of Blockchain-based Fed-erated Learning: Architectures, Applications and Issues. In Proceedings of the 2021 2nd Information Communication Technologies Confer-ence (ICTC), Nanjing, China, 7–9 May 2021; pp. 302–307.
96. Preuveneers, D.; Rimmer, V.; Tsingenopoulos, I.; Spooren, J.; Joosen, W.; Ilie-Zudor, E. Chained anomaly de-tection models for federated learning: An intrusion detection case study. *Appl. Sci.* **2018**, *8*, 2663. [CrossRef]