IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 28 May 2024, accepted 6 June 2024, date of publication 12 June 2024, date of current version 21 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3413069

SURVEY

A Multifaceted Survey on Federated Learning: Fundamentals, Paradigm Shifts, Practical Issues, Recent Developments, Partnerships, Trade-Offs, Trustworthiness, and Ways Forward

ABDUL MAJEED AND SEONG OUN HWANG, (Senior Member, IEEE)
Department of Computer Engineering, Gachon University, Seongnam 13120, South Korea

Corresponding authors: Seong Oun Hwang (sohwang@gachon.ac.kr) and Abdul Majeed (ab09@gachon.ac.kr)

This work was supported by the National Research Foundation of Korea (NRF) Grant funded by Korea Government (Ministry of Science and ICT) under Grant RS-2024-00340882.

ABSTRACT Federated learning (FL) is considered a de facto standard for privacy preservation in AI environments because it does not require data to be aggregated in some central place to train an AI model. Preserving data on the client side and sharing only the model's parameters with a central server preserves privacy while training an AI model of higher generalizability. Unfortunately, sharing the model's parameters with the server can create privacy leaks, and therefore, FL is unable to meet privacy requirements in many situations. Furthermore, FL is prone to other technical issues, such as data poisoning, model poisoning, fairness, client dropout, and convergence issues, to name just a few. In this work, we provide a multifaceted survey on FL, including its fundamentals, paradigm shifts, technical issues, recent developments, and future prospects. First, we discuss the fundamental concepts of FL (workflow, categorization, the differences between centralized learning and FL, and applications of FL in diverse fields), and we then discuss the paradigm shifts brought on by FL from a broader perspective (e.g., data use, AI model development, resource sharing, etc.). Later, we pinpoint ten practical issues currently hindering the viability of the FL landscape, and we discuss developments made under each issue by summarizing state-of-the-art (SOTA) literature. We highlight FL partnerships with two or more technologies that either improve practical aspects/issues in FL or extend its adoption to new areas/domains. We pinpoint various trade-offs that exist in an FL ecosystem, and the corresponding SOTA developments to mitigate them. We also discuss the latest studies that have been proposed to make FL trustworthy and beneficial for the community. Lastly, we suggest valuable research directions towards enhancing technical efficacy by guiding researchers to less explored topics in FL.

INDEX TERMS Federated learning, AI models, poisoning attacks, privacy preservation, training data.

I. INTRODUCTION

Before 2016, centralized learning (CL) was one of the promising solutions for training AI models. CL usually requires some centralized environment for aggregating data, and AI models are subsequently trained on them. However, most data owners like hospitals, banks, and insurance companies are reluctant to transfer their data to a centralized architecture owing to the risks of privacy breaches and personal data misuse. In the traditional CL approach, data owners collect measurements, readings, sounds, etc., from record owners or the industry, apply basic pre-processing, and transfer the data to a centralized environment, which subsequently performs computationally expensive tasks (e.g., training AI models). Such a setting/approach, however, places significant computing overhead on the server, since the training of complex AI models usually requires significantly large blocks of data, and places a heavy computing burden on a single server [1]. Apart from performance bottlenecks,

The associate editor coordinating the review of this manuscript and approving it for publication was Mostafa M. Fouda.

privacy preservation is a big obstacle in CL, creating the need for distributed/federated learning. The concept of federated learning (FL) was coined by Google in 2016 [2] and has attracted the attention of researchers worldwide. In FL, data transfer to a central server is not needed, and AI models can still be trained with distributed data. Only the parameters of the AI/learning model are sent to the server instead of the data; training is delegated to the client, and the (local) data are protected from third-party/server access. In FL, AI models are transferred periodically over the network, in contrast to transferring the raw data in the CL setting. FL has been deployed in many domains, such as object detection in a vehicle [3], the predictive keyboards of Google, and healthcare with distributed data [4].

FL is a promising candidate for producing AI models that exhibit better generalization than CL, and privacy problems are inherently solved because the data do not move from clients to a centralized environment [5]. Furthermore, FL is a modern-day paradigm with higher privacy guarantees and robust AI model development [22], [23]. Without FL, the privacy of clients' data cannot be preserved, and the AI model cannot achieve higher generalizability [24], [25], [26]. FL can assist in developing data-driven products and AI applications that benefit the community. Since its inception, researchers have explored FL use in almost all fields, including medical practices [27], [28], dealing with COVID-19 [29], [30], [31], finance [32], robotics [33], the automotive industry [34], mobile robotics [35], autonomous driving [36], [37], traffic prediction [38], and IoT-based applications [39].

Motivation: FL has become a ground-breaking invention of AI, and this topic is gaining the compelling interest of researchers around the globe. Due to a variety of upsides (e.g., higher generalizability, privacy protection of training data, DIP solution, etc.) and drawbacks (e.g., data aggregation, privacy leakage, byzantine client behavior, poor network design, and poisoning attacks [40], [41].) of FL, a lot of experiential and theoretical studies have been recently published. Therefore, a unified and systematic classification of most works is imperative to guide researchers/practitioners in designing next-generation FL systems. Although many surveys focusing on FL have been recently published, broad aspects were not adequately discussed, and coverage was limited to only a few well-known aspects (e.g., privacy, poisoning, etc.). Table 1 lists previous surveys and their coverage in order to visualize the research gaps. Referring to Table 1, most surveys covered limited aspects of FL; practical issues of diverse types were not discussed along with the state-of-the-art (SOTA) literature. Various trade-offs and corresponding studies were not reported. Furthermore, trustworthy aspects and FL partnerships with other technologies (two or more) were not covered in them, which could be highly beneficial for researchers and practitioners in navigating the potential harms of FL systems and making the FL systems more robust/dependable. To fill this research gap, we offer a multifaceted survey on FL with broader coverage of most concepts and aspects with the support of recently published SOTA studies and their methodological contributions. We aim to provide deeper insight into FL developments/concepts that either remained unexplored or partially covered in the previous surveys to provide a solid foundation for future studies in this line of work.

In Table 1, we choose factors such as paradigm shift, trustworthy aspects, trade-offs, and partnerships to highlight the recent trends in the FL topic, and these factors have not been mentioned or thoroughly researched in other survey articles. For instance, there exist many surveys on FL applications, privacy preservation, poisoning attacks, etc., but surveys centering on the above factors are very limited in the literature. Recently, most of the research works have focused on the optimization of FL and navigating the potential harms in FL (e.g., making FL trustworthy), and therefore, we chose these factors to highlight developments in them with the help of SOTA studies. The comparison given in Table 1 depicts the coverage of existing surveys, highlights the limitations of existing surveys, and underscores research gaps to be filled by this survey. This comparison also highlights the different sub-topics which are being researched under the umbrella of FL, but yet not explicitly reported through survey articles. Our major contributions are listed below.

- **A multifaceted and comprehensive coverage:** This survey provides a multifaceted and in-depth analysis of different topics associated with FL, including fundamentals, paradigm shifts, practical issues, partnerships, optimizations, trustworthy aspects, and prospects.
- **Delving into paradigm shifts of FL:** We delve deeper into the paradigm shifts brought on by FL in the AI field, and we present examples to systematically demonstrate this paradigm shift through ten different aspects.
- **Taxonomy of FL practical issues:**We provide a taxonomy of practical issues with FL which can either lead to poor performance or make FL the target of various adversarial attacks. We identify and discuss 10 practical issues along with relevant studies to pinpoint recent developments that have not been thoroughly reported in the literature. The presented analysis can assist researchers in quickly grasping the challenges associated with FL without enduring a difficult learning process.
- **Different optimizations in FL landscape:** We highlight various kinds of optimizations in the FL landscape which are due to either integrating FL with other technologies or solving different types of trade-offs. Specifically, we discuss the partnerships of FL with two or more different technologies that were made to either improve the practical aspects/issues in FL or extend its adoption/use to new unexplored areas/domains. We illuminate various trade-offs that exist in the FL and the corresponding SOTA developments to mitigate them.
- **Trustworthy aspects of FL:** We identify and discuss the latest studies that have proposed ways to make FL

TABLE 1. Analysis of recently published SOTA surveys centered on FL (from year 2020 onward).

Ref.	Year	Coverage of the survey/review	Fundamental concepts	Paradigm shifts	# of practical issues	Trustworthy aspects	Trade-offs	Partnerships
Zhang et al. [5]	2021	Report on five aspects[1] related to FL	Limited	×	2	×	×	×
Li et al. [6]	2021	Basic categorization of FL components	Limited	×	2	×	×	×
Yu et al. [7]	2022	Novel FL taxonomies and applications in data mining	Limited	×	2	×	×	×
Banabilah et al. [8]	2022	Basic applications of FL in diverse fields	Detailed	×	0	×	×	×
El Ouadrhiri et al. [9]	2022	Privacy issues and solutions in FL	Limited	×	1	×	×	×
Caruccio et al. [10]	2023	Applications of FL in data mining	Detailed	×	3	×	×	×
Ye et al. [11]	2023	New settings of FL (e.g., HFL) and analysis of related studies	Detailed	×	4	×	×	×
Rodríguez et al. [12]	2023	Taxonomies of adversarial attacks and defenses	Limited	×	1	×	×	×
Beltr et al. [13]	2023	Differentiating DFL and CFL; optimization	Detailed	×	4	×	×	×
Zhang et al. [14]	2023	Security, robustness, and privacy in FL	Detailed	×	3	✓	×	×
Rafi et al. [15]	2024	Brief analysis of the privacy/fairness trade-off in FL	Detailed	×	2	×	×	×
Xiao et al. [16]	2024	Introducing over-the-air FL concepts and related studies	Limited	×	3	×	×	×
Wan et al. [17]	2024	Model and data poisoning, backdoor attacks, and defenses	Detailed	×	1	×	×	×
Xie et al. [18]	2024	Threat models to the FL learning process	Limited	×	1	×	×	×
Chaddad et al. [19]	2024	FL applications in healthcare; use cases	Detailed	×	1	×	×	×
Nguyen et al. [20]	2024	Backdoor attacks, and defense methods	Limited	×	1	×	×	×
Pei et al. [21]	2024	Device, data, and model heterogeneity	Limited	×	1	×	×	×
This study	2024	Broader coverage of FC, PS, PIs, TOs, P, and TA of FL	Detailed	✓	10	✓	✓	✓

Abbreviations: FC: fundamental concepts, PS: paradigm shifts, PIs: practical issues, TOs: trade-offs, P= partnerships, TA: trustworthy aspects. **Aspects[1]:** privacy mechanism, data partitioning, systems heterogeneity, communication architecture, and machine learning models. **Symbols:** ×: not covered/discussed, ✓: covered/discussed

trustworthy and beneficial. Specifically, we summarize SOTA literature centering on FL trustworthy aspects (e.g., six dimensions of trustworthy AI/FL).

- **Prospects of FL:** We suggest various research tracks and potential topics for future work in the FL ecosystem. The presented analysis offers a valuable resource for researchers/practitioners who aim to tackle one or more of the issues in FL or design next-generation FL systems.

The rest of this paper is structured as follows. Section II presents the fundamentals of FL, including its major types and entities, a detailed comparison between CL and FL, and practical applications. Section III provides the methodology used in this survey. Section IV discusses the paradigm shifts in FL with examples. Section V presents practical issues w.r.t. performance and adversarial attacks, as well as corresponding SOTA developments. The partnership of FL with two or more technologies is discussed in Section VI. Trade-offs of diverse types and the associated SOTA literature to mitigate them are in Section VII. Recent developments making FL trustworthy are discussed in Section VIII. Lessons learned and potential topics for future research are listed in Section IX. We conclude this paper in Section X. For ease of reference, we list all the acronyms used in this survey article in Table 2.

II. FUNDAMENTALS OF FL

In this section, we provide the fundamentals of FL from four different aspects (i.e., FL workflow, major categorizations, comparisons between CL and FL, and FL applications in diverse fields).

A. WORKFLOW

FL is a decentralized technology in which N clients collaboratively train an AI model with their local data, and only the parameters of local models are shared with a centralized server. By not sharing local data with the central server, FL is a mainstream privacy-preserving technology. In typical FL, n rounds are performed to accomplish the training and eventual convergence. In each round, the server shares the global model with each client, and each client trains the local model and shares its local model with the server. This process is repeated until accuracy reaches a specific threshold or a specified number of rounds are completed. In some cases, convergence is accomplished when there is no change in accuracy/loss for a certain number of rounds.

1) SERVER AND CLIENT ACTIVITIES

In this subsection, we discuss the key activities performed by the server and client under the traditional FL setting. The server usually performs three key activities: (i) chooses a set of clients, (ii) aggregates their local models, and (iii) curates a global model. However, a few additional steps are performed by the server to detect malicious clients/models. In some cases, the noise is added/removed to secure the local/global models from the adversaries. Clients usually perform three key activities: (i) acquire a global model, (ii) train a local model with local data, and (iii) forward the local training results to the server. Clients can offload some computations when they do not have sufficient resources [42], [43]. Figure 1 presents the typical FL workflow including the main activities of clients and servers in medical scenario.

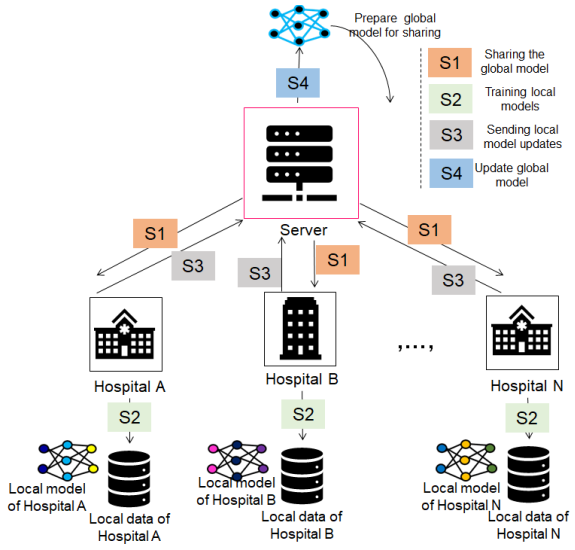

FIGURE 1. Illustration of workflow of the traditional FL. The main activities of the clients and server are marked with S1∼S4 (adapted from [89]).

TABLE 2. Acronym used in this survey article.

Acronym	Definition	Acronym	Definition	Acronym	Definition	Acronym	Definition
FL	federated learning	CL	centralized learning	NLP	natural language processing	CV	computer vision
VFL	vertical federated learning	HFL	horizontal federated learning	SFL	synchronous federated learning	FHE	fully homomorphic encryption
DIP	data island problem	PP	privacy-preserving	PbD	privacy-by design	MA	micro-aggregation
SVM	support vector machine	RF	random forest	CNN	convolutional neural networks	LSTM	long short term memory
RNN	Recurrent neural network	PPFL	privacy preserving federated learning	PPMs	privacy preserving methods	CD	cross-device
CS	cross silo	QoS	quality of service	FLA	federated learning architechtures	IIoT	industrial internet of things
BC	blockchain	AV	autonomous vehicles	RA	resource allocation	6G	sixth generation
IT	inference threats	SMC	secure multi-party computation	DP	differential privacy	LAT	loss and accuracy trade-off
AD	autonomous driving	GM	global model	PCAT	privacy convergance and accuracy trade-off	ANP	alternating noise permutation
ADP	adaptive differential privacy	LM	local model	HDP	heterogeneous differential privacy	IoMT	internet of medical things
GLA	gradient leakage attacks	DP-GANs	differential private GANs	PI	pseudo-identity	FLI-PSS	FL incentivizer payoff-sharing scheme
AFT	accuracy-fairness trade-off	DMG	double momentum gradient	CS	client selection	SV	shapley value
CC-MAB	Contextual combinatorial multi-armed bandit	WDP	winner determination problem	CSMAB	copeland score and multi-arm bandits	CEPD	cumulative effective participation data
VFL	volatile federated learning	LFA	label flipping attack	LFS	latent feature space	GT	game theory
IST	irrelevance sampling technique	QSR	quality scoring rules	DCM	data-centric methods	RS	regularization strategies
MCE	mutual cross-entropy	QE	quality enhancement	AI	artificial intelligence	CP	clients profiling
k-NNG	k-nearest neighbor graph	AP	accuracy-based predictions	AG	auto group	IC	infleunce computation
PA	poisoning attacks	TC	trusted coordinates	GAE	graph autoencoder	SGD	sub-gradient descent
GoMORE	G l o bal MO del RE use strategy	FedAdp	Fed erated Ad a p tive Weighting	FedPNS	P robabilistic N ode S election framework	CT	contact theory
OIMAF	online incentive mechanism for AFL	AFL	asynchronous FL	ACN	aerial computing networks	KLD	Kullback-Leibler divergence
MA	mobile apps	ZMS	zone merge and split	ZGD	zone gradient diffusion	MN	mobile network
OB	open banking	HEco	healthcare ecosystem	DEco	digital ecosystem	TWA	temporally weighted aggregation
SLD	skin lesion diagnosis	MI	medical images	SCP	skin cancer prediction	CT	classification threshold
LE	lightweight encryption	DL	discrete logarithm	Cr	cryptography	I4.0	industry 4.0
PoC	proof of concept	IRT	image recognition task	GE	gradient encryption	STE	spatio temporal entropy
CC	confidential computing	ATZ	arm trust zone	CFL	clustered federated learning	RM	randomization and mixture
IR	image representation	DAM	domain adaptation methods	WT	wavelet transform	EI	edge intelligence
BANet	brain-region attention network	PP-FDL	privacy protection-based federated deep learning	F-IoT	fog-assisted internet of things	GANs	generative adversarial networks
Anon.	anonymity	Enc.	encryption	CC	cloud compuring	UKG	user and context-based knowledge graph
RD	real dataset	SD	synthetic dataset	i.i.d.	independent and identically distributed	IoT	internet of things
PR	pattern recognition	NMF	non-negative matrix factorization	ALS	alternating least squares	SS	secret sharing
FDI	false data injection	GT	game theory	SCS	symmetric cryptosystem	DDPG	deep deterministic policy gradient
PCS	pallier crypto system	GC	gradient compression	KD	knowledge distillation	FE	feature engineering
RI	real identity	GI	gradient indistinguishability	KA	k-anonymity	LS^{2}DNN	linear sigmoid singleton DNN
PBKA	pearson and brownian motion induced KA	Facor.	factorization	LDP	local differential privacy	NN	neural networks
HE	homomorphic encryption	PUT	privacy-utility trade-off	DT	decision tree	SDL	shallow deep layers
QC	quantum computing	LMU	lattice-based multi-use	NAS	neural architecture search	PET	parameter efficient fine-tuning
EC	edge computing	DNN	deep neural network	CEDDLA	cost-effective dynamic distributed learning algorithms	non-i.i.d.	non independent and identically distributed

In Figure 1, N hospitals are jointly training a global model by training their own local models on their local data. The quantity and quality of the data can be different at each site/hospital, and the local data of each hospital is not shared with either the server or other hospitals. It is worth noting that the parties can be either the same (e.g., only hospitals) or different (hospital, bank, clinic, etc.) depending on the scenario. The training process is repeated over several iterations until convergence. In some cases, clients and servers share additional information about the underlying data to speed up the convergence process or to eliminate the risks of attack. Similarly, some additional algorithms or evaluations are applied to judge the quality of local models and to prune malicious-looking local models. After convergence, a global model is curated, which exhibits better generalization and robustness. This model can be deployed in some real-world environments (e.g., hospitals) for prediction or classification tasks.

B. MAJOR CATEGORIZATIONS

There are multiple FL categories w.r.t. training architectures: centralized, decentralized, and hybrid. Communication between clients and servers can be either direct or via edge/fog computing. There are FL categories based on the privacy mechanism used in them, either syntactic (k-anonymization) or semantic (differential privacy). Similarly, there are FL categories w.r.t. defense mechanisms used to ensure security [44]. FL systems have been categorized based on data heterogeneity (e.g., non-i.i.d. and i.i.d.). Li et al. [6] discussed six FL categories (data partitioning, AI models, privacy methods, communication procedures, federation scale, and motivation for federation). Liu et al. [45] discussed the differences among three FL categories w.r.t. data. In this work, we present major FL categories w.r.t. data, resources, response sharing with clients, and network topologies that are relevant to the context of this paper.

1) DATA

Based on the data, FL can be categorized into three main types: vertical FL (VFL), horizontal FL (HFL), and hybrid(a.k.a. federated transfer learning (FTL)). Figure 2 illustrates all three types of FL categorized w.r.t. data. In Figure 2, the x-axis is the feature space, and the y-axis is the sample space. In HFL, the data are different in the sample space, but the same in the feature space. In contrast, VFL has different data in the feature space, similar in

sample space. However, hybrid FL settings have different data in both spaces. All these types of FL enable identical or distinct clients to collaboratively train an AI model of higher generalizability.

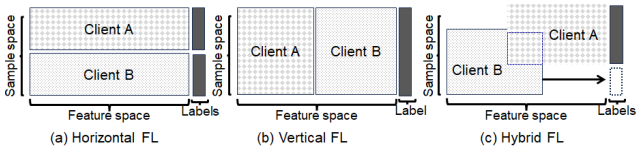

FIGURE 2. Major categories of FL w.r.t. data (adapted from [6]).

2) RESOURCES

Based on resources, FL can be categorized into two main types: cross-device (CD) and cross-silo (CS) [46]. Table 3 compares these categories, and each has challenges and benefits. In the literature, CD FL has been widely investigated compared to CS. However, most of the recent studies were focused on CS FL [47]. In CD FL, there are many devices, and therefore, client management is challenging. In contrast, CS FL has fewer clients, but data sizes are very large, which can lead to higher computing and communications costs. Recently, a new category of FL named intra-domain was introduced to accelerate convergence in heterogeneous data centers [48]. This new type of FL can overcome the effect of stragglers without losing guarantees of accuracy and efficiency while training AI models.

TABLE 3. Comparison between CD and CS settings of FL.

Parameter/Criteria	CD setting	CS setting
Clients	Mobile devices	Organizations/companies
Number of clients	$\sim$ 1 million	$\sim$ 100

3) RESPONSE

Based on the response interval from the server to the clients, FL is categorized into two types: synchronous FL (SFL) and asynchronous FL (AFL) [49]. In SFL, the server begins aggregation of the global model only after the local models of all participating clients are retrieved. In AFL, the global model is updated as soon as a local model is uploaded by a client without waiting for the local models of all participating clients. AFL is preferable for faster convergence, particularly if clients intentionally hold on to their local models to delay the convergence. In some cases, clients have fewer resources, and their updates do not arrive at the central server in a reasonable time. SFL and AFL workflows are illustrated in Figure 3.

In Figure 3, some clients can be idle in SFL, but client updates are immediately aggregated in AFL, so clients are never idle. Recently, semi-synchronous FL was introduced in which clients are not idle, but keep doing some additional training to contribute to faster convergence [50]. In the literature, SFL has been widely investigated, but not AFL and semi-synchronous FL. These categorizations pave the way to

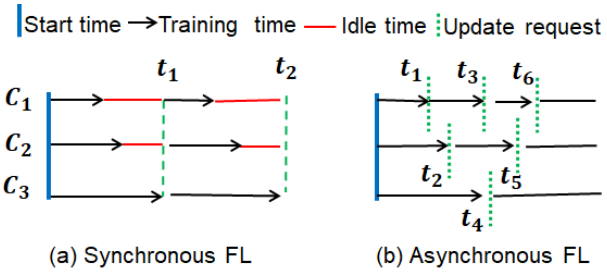

FIGURE 3. Major categories of FL w.r.t. response.

choosing the appropriate FL type by considering the available data and computing resources.

4) TOPOLOGY

Based on the arrangement of clients and the server, FL can be categorized into three network topologies: star, ring, and hybrid [10]. Figure 4 illustrates the structure of each one. The star topology is widely used, where each client is linked to the server via one-to-one communications but does not communicate with other clients. In the ring topology, each client connects to two clients, constituting the ring. In this topology, there is no server; instead, clients curate the global model through different rounds of training, and the global model is distributed to all. Wang et al. [51] devised a ring-topology FL mechanism for healthcare systems by protecting the privacy of medical data while reducing bandwidth and communications overheads. The hybrid topology combines the features of both star and ring topologies. Specifically, clients are arranged into different groups, and only some clients from each group communicate with the server. Training is usually done in ring fashion within each group, and results are communicated to

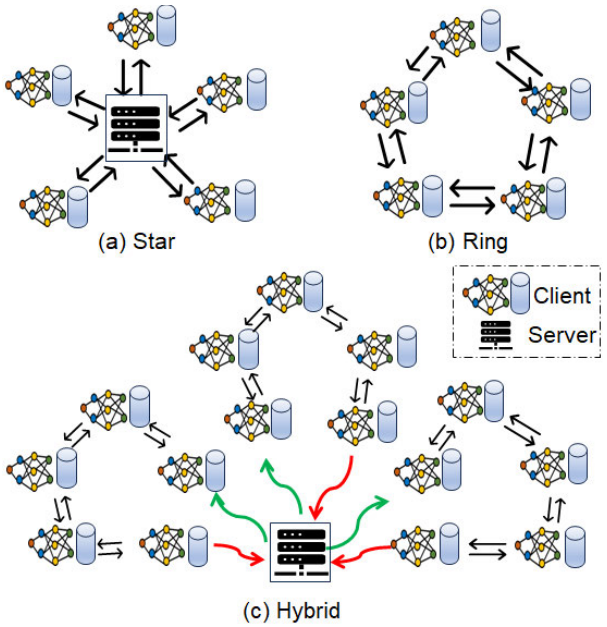

FIGURE 4. Major categories of FL w.r.t. network toplogies.

the central server (akin to the star topology) by at least two clients from each group.

Hosseinalipour et al. [52] proposed a hybrid topology for FL systems by extending the star topology and designing the network in a multi-level, cluster-based structure. Some hybrid topology FL systems have been proposed to overcome the issues of data heterogeneity by placing clients with similar resources into the same clusters. For each client group, training of the local model is performed by using a ring topology, which then forwards results to a central server to curate the global model. All these topologies have benefits and challenges, and the choice depends on performance objectives, client nature, convergence criteria, and target domains.

C. COMPARISON BETWEEN CL AND FL

In this section, we provide a comparative analysis of CL and FL, which are two mainstream methods for training AI models. Before the advent of FL, CL was mostly used in general as well as in client/server scenarios. Service scenarios for the CL and FL are visualized in Figure 5. As seen in Figure 5, FL omits data sharing from the client's environments to the server and therefore is a privacy-preserving paradigm of modern times. In contrast, CL always gathers data from clients at centralized servers first, and AI models are then trained on the data. However, most clients are reluctant to share their data with centralized servers to avoid data manipulation risks. Furthermore, a server in CL works in a black-box manner, which can put subjects' privacy at risk [53]. FL resolves the above-cited issues because data are no longer forwarded to a server, and AI models can be trained from the data of different clients.

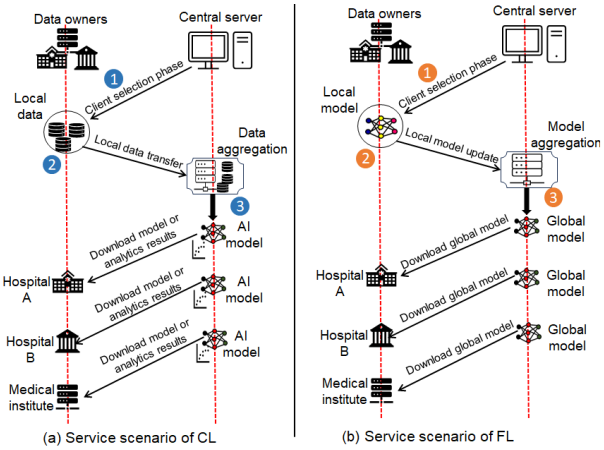

FIGURE 5. Illustration of service scenarios of CL and FL.

In CL, clients are selected and asked to share their data with the server. Afterward, the AI model is trained in a black-box manner [54], and the model or analytics results are subsequently sent back. While CL is handy, it often dilates privacy issues, because there is a risk that personal information will be sold to third parties without proper consent from data providers. Moreover, the data can be used for purposes other than those intended upon collection. CL-based AI applications have demonstrated effectiveness in solving many real-world problems and in making AI developments more trustworthy [55]. However, the lack of transparency in data processing, and aggregating all the data in a central place, makes CL-based AI less adoptable in real-world settings.

In FL, clients are selected, and a global model from the server is shared with them. Later, each client trains a local model using its local data and forwards the local model to the server. The server collects all the local models and generates a new global model that is shared with all clients. This process keeps repeating until the desired accuracy is achieved or the specified number of iterations is met [56]. Not acquiring data transfer to a server, and working only with parameters (local models), made this technology famous in both academia and industry [57]. Additionally, there has been significant investment in this technology, and its use in most sectors is expanding at an astonishing speed. In the future, sophisticated developments are expected, and more promising applications will emerge in diverse sectors [58]. FL resolves CL technical issues and is preferred in most cases, particularly when privacy requirements are strict. Table 4 provides a detailed comparison between CL and FL based on 30 different parameters.

TABLE 4. Detailed comparison between CL and FL.

Parameters	CL setting	FL setting
Working nature	Centralized	Distributed
Data transfer	Copied to server	Not copied
Privacy risks	Very high	Relatively low
Data size	Small & fixed	Large & dynamic
AI model quality	Low	High
Clients role	Data provision	Local training
Communication overhead	Low	Very high
Data quality	High	Low
Data diversity	Low	High
AI model	Single	Multiple
Convergence	Faster	Slower
Computing cost	Low	High
Data corruptions	Low	High
Computations	Local only	Local and global
Reliability of models	Low	High
GDPR application	Required	Not required
Straggler effect	Does not exist	Exist
Model complexity	Medium	Very high
Non-i.i.d. data	Less prevalent	Mostly prevalent
Client selection	Less challenging	Very challenging
Scalability	Low	High
Manageability cost	High	Low
Possible poisoning attacks	Few types	Many types
Results aggregation	Not required	Required
Resource skew	Does not exist	Might exist
Model type	Shared	Shared/personalized
Sharing	Raw data	Local models
Training	Done together	Done separately
Number of iterations	One	N
Client dropout	None	Yes

Based on the comparisons between CL and FL, we can see that FL is better in terms of data management, privacy

guarantees, etc. Researchers are combining FL with other technologies such as blockchain, IoT, differential privacy, etc., to alleviate performance concerns [39], [59], [60], [61], [62], and efforts are underway to enhance the technical efficacy of FL [63]. In the future, most of the deficiencies in traditional FL can be resolved through these advancements.

D. FL APPLICATIONS IN DIVERSE FIELDS

In recent years, FL has been used in diverse fields, and many practical applications of FL exist in each sector. FL is highly suitable for scenarios involving sensitive data because it can overcome privacy issues and data manipulation risks. For example, it can be used in the medical sector to protect sensitive data while generating models of higher generalizability [64], [65]. Table 5 highlights applications of FL in diverse sectors by summarizing SOTA surveys. Referring to Table 5, it can be observed that FL has many practical applications in diverse fields. Soon, FL will have applications in most fields where data are sensitive and owners are reluctant to share them. The listing in Table 5 can pave the way to understanding the diversity of FL applications. In some cases, FL can be used to verify computations in cloud computing scenarios [90]. It can also be used to securely transfer data without leaking any private information [91]. In some cases, it enables knowledge discovery from encrypted data and preserves the integrity of the data, leading to higher privacy preservation for sensitive data [92]. Additionally, FL has been used in authentication scenarios such as biometric recognition [93]. FL has also been used in descriptive analytics of large-scale data, which can contribute to the development of new treatments and clinical assessments [94]. Based on the above analysis, we can conclude that FL has diverse applications and is one of the most beneficial technologies of recent times.

TABLE 5. Summary of FL applications in diverse fields.

Year	Reference	Major application area (s)
2020	Li et al. [66]	Industrial applications
2021	Rahman et al. [67]	NLP, healthcare, CV, transportation
2022	Zheng et al. [68]	Smart cities
2022	Dhiman et al. [69]	Smart healthcare
2022	Lim et al. [70]	Mobile edge networks
2022	Ma et al. [71]	Software-defined networks
2022	Khokhar et al. [72]	Image processing
2022	Lavaur et al. [73]	Intrusion detection
2023	Wang et al. [74]	Mobile health
2023	Issa et al. [75]	IoT data analytics
2023	Chen et al. [76]	Metaverse
2023	Chellapandi et al. [77]	Connected and automated vehicles
2023	Sirohi et al. [78]	Secure 6G communications
2024	Choi et al. [79]	Medical applications
2024	Liu et al. [80]	Multi-party computation
2024	Woisets et al. [81]	Foundation model training
2024	Bentaleb et al. [82]	Sustainable development
2024	Hafi et al. [83]	6G networks
2024	Rana et al. [84]	Predictive healthcare analytics
2024	Simić et al. [85]	Emotion recognition
2024	Yang et al. [86]	Diverse knowledge fusion
2024	Tan [87]	Energy services
2024	Guan et al. [88]	Medical image analysis
2024	Hwang et al. [89]	General medical and COVID-19

III. METHODOLOGY

In this paper, we performed a comprehensive review to identify and retrieve SOTA studies for accurate and complete conclusions. We applied a systematic approach to retrieve relevant studies from credible sources. We conducted this multifaceted and comprehensive survey by following the PRISMA method, which assists in identifying, assessing, and synthesizing highly relevant studies about some specific research questions/topics [95]. This survey focuses on five main research questions as listed below.

1) What kind of paradigm shift has been brought on by federated learning compared to the conventional centralized learning in the AI field?
2) What is the status of current developments in solving the various practical issues encountered by FL in real-world settings?
3) What are the different technologies with whom FL has been partnered, and what is the main purpose of these ever-increasing partnerships?
4) What are the primary trade-offs in FL, and what are the recent SOTA and effective solutions to mitigate them?
5) What are the dimensions of trustworthiness in the context of FL, and what developments have been made thus far to navigate its potential harms in realistic scenarios?

In this work, we aim to provide systematic and multi-faceted coverage of the FL and related topics that can assist researchers and developers to clearly understand the recent developments. To accomplish this key objective, we conduct an in-depth analysis of relevant studies that envision the upsides and downsides of FL and are published at credible venues.

Paper selection criteria: To transparently report the findings of previous studies, we select peer-reviewed journal papers, conferences, magazines, and some highly-cited arXiv papers. Although arXiv is not an explicit database, we chose some papers from it based on the relevance and analyzing the reference citations of the paper we chose in our primary databases. While selecting the papers, we ensure that most papers are written in English, and their full text (or metadata) is easily accessible. Through this method, we ensure that highly relevant, high-quality, SOTA, and recent literature is selected for inclusion in this survey paper.

Scientific databases consulted: The studies reported in this survey paper were obtained from different scientific databases. The mainstream scientific databases consulted in this survey are, IEEE Explore, Science Direct, ACM Digital library, Springer, PubMed, Web of Science, Scopus, etc. The main reason to consult these scientific databases was their higher credibility in terms of academic integrity and availability of different articles related to the scope of this survey.

Query approach: We queried relevant literature for this survey paper from Google Scholar and dedicated search

functions available in the above-cited scientific databases. We also applied language, years, and full-text-related filters to query relevant papers. We performed forward and backward searches of citations of some highly cited papers to identify the relevant literature for our work. We used different keywords as a search item to find related studies from databases. Our search keywords are different for each topic. For example, the main search keywords for identifying studies related to developments in practical issues are, ''federated learning'', combined with (AND), ''potential threats/ practical issues/'' and (OR) ''vulnerabilities''. We also used practical issue names combined with federated learning to search relevant studies such as ((federated learning) AND (privacy disclosure OR poisoning attacks OR client dropout OR client selection OR fairness OR data quality problems OR global model issues OR ecosystem issues OR aggregation problems) AND (privacy protection OR defense against poisoning attacks OR client dropout prevention OR suitable client selection OR fairness/bias mitigation OR addressing data quality problems OR reliability enhancement of global model OR end-to-end approach for FL ecosystem OR secure/robust aggregation)). To find relevant literature for partnership, we used federated learning combined with the names of technologies with whom FL has been partnered. Similarly, we find relevant studies for trustworthy aspects by using the dimension's name combined with federated learning as the query. We also searched some papers by combining the words survey, review, or perspective with federated learning to cover deep knowledge about established concepts in the field. The systematic process employed in the selection of studies is given in Figure 6.

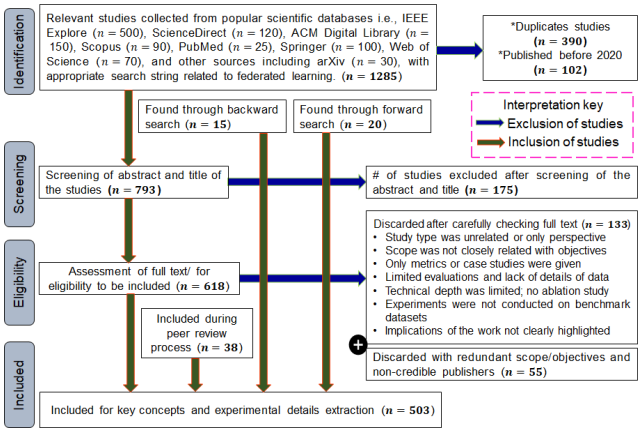

FIGURE 6. Overview of the systematic process employed in the selection of articles for multifaceted analysis on FL and its associated concepts.

Exclusion criteria: As shown in Figure 6, we systematically selected articles to be included in our paper and excluded those that were either redundant or lacked detailed methodological/experimental descriptions. In the preliminary assessment, we excluded papers that do not closely align with the objectives of this paper by carefully analyzing the abstracts and titles. We also removed non-English papers for ease of readability of included studies. In the detailed assessment, we excluded research papers that focus on narrow areas like vehicular networks or discuss a few well-known FL issues (e.g., privacy, poisoning, etc.) with slightly different methodologies. We discarded the papers for which metadata or full text was not available. We also excluded some papers that only discuss FL potentials without experiments.

Years considered in research: We included most papers that were published in the past five years (e.g., the year 2020 and onward).

Threats to validity: Two main threats related to the validity of our survey are, (i) search bias and (ii) quality assessment bias, which can destroy the reliability and robustness of our findings [96]. The former threat is related to an incomplete search or searching only some famous sources, leading to the exclusion of some studies that have been published in lower-tier venues. The latter threat is related to criteria employed in screening the studies for inclusion/exclusion, which can be unclear, biased, etc. In the context of the survey paper, if these threats are not addressed properly can affect the generalizability of findings and the conclusions can be incomplete/inaccurate. To address these threats, we included studies from diverse scientific databases and employed techniques like snowballing from the [96] to prevent search bias. To resolve the second threat, we evaluated each study's full text and examined the methodological and experimental contributions. We also adopted techniques from [96] to prevent bias related to quality assessment and to exclude low-quality or irrelevant papers. We analyzed the relevance of each study by carefully comparing each study with the scope/objectives of this paper. Based on the above analysis, it is conclusive that threats to the validity are restrained, and the findings/conclusions are complete and reliable.

IV. PARADIGM SHIFTS BROUGHT ON BY THE FL

Since the inception of FL, data governance and use have gotten a new life, which was not possible with CL. In addition, the collaborative training process and client behavioral analysis methods were devised and integrated with the FL ecosystem. Conclusively, FL has brought a kind of paradigm shift in the AI domain, and is one of the groundbreaking inventions of AI. The paradigm shift is defined as a sudden change in conventional approaches/methods leveraged to accomplish certain real-world tasks. For example, AI models have been widely used in the healthcare domain for the past thirty years. However, to accomplish certain real-world medical tasks at any hospital X with AI such as training the CNN model to classify the cancerous and non-cancerous cells always require data to be collected first from certain subjects or relevant hospitals. Let's say a similar task is to be performed at N different hospitals located in different regions of the country, it will follow the same conventional approach (e.g., collect data and subsequently train model) that can be time-consuming and slow. Furthermore, many subjects or hospitals will be reluctant to share their data in central settings, owing to privacy and security concerns. To this end, can we come up with a brand new solution/method

to bypass the conventional workflow by not collecting the data from subjects/hospitals, but still training the CNN model for better performance? If yes, then the respective solution/method/approach will be regarded as a paradigm shift because it completely/partially changed the way of approaching a similar problem in a completely different way. Moreover, if the newly devised solution/method/approach successfully outperforms the previous solution in many ways (specifically, privacy in our example), then it is regarded as a paradigm shift. In the case of FL, it has brought many unique aspects compared to CL in terms of AI model training without acquiring data from clients, privacy protection of training data, training AI models without moving data from data owner environments to public domains, engaging heterogeneous data sources (e.g., hospitals, banks, medical institutes, etc.) in the training process, extending AI benefits to clients/hospitals having insufficient resources to train complex AI models, utilizing interdisciplinary approaches to enhance the security of AI models, creating AI models which are more generalizable and dependable, linking multiple technologies to solve many complex real-world problems with AI, utilizing fragmented and complex datasets, to name a just few. Considering the above-cited sudden changes that have happened in quick succession after FL's emergence in the AI field, it is fair to say that FL has brought a kind of paradigm shift. We discuss and visualize the paradigm shifts brought by FL technology from 10 different aspects. To the best of our knowledge, that is the first work that comprehensively figures out paradigm shifts brought on by FL in the computing and AI field. A concise description of each aspect with examples is given below.

A. A SOLUTION TO THE DATA ISLAND PROBLEM

Before the emergence of FL, there was a serious lack of privacy-by-design approaches, and the data island problem (DIP) was very common. In the DIP, organizations (data owners) with poor AI model performance cannot acquire data from a neighboring organization due to privacy concerns, as shown in Figure 7.

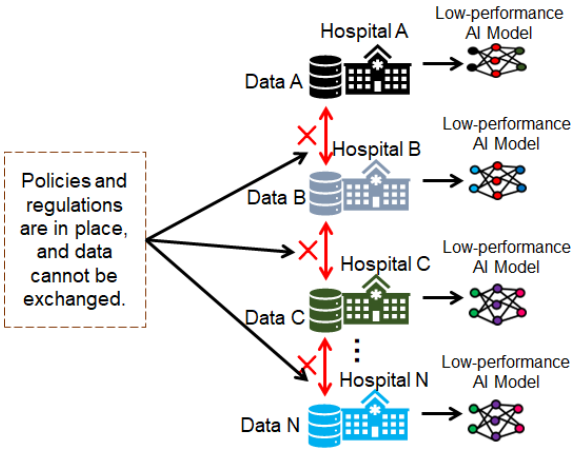

FIGURE 7. Overview of the data island problem.

In DIP, an organization having fewer data and deficient model performance cannot develop a generalizable AI model, and therefore, the potential benefits from the latest AI developments cannot be fully harnessed. However, FL resolves this issue, and data exchanges among organizations are no longer needed, but high-quality AI models can still be trained with diverse data. Hence, it is fair to say that FL is one of the promising candidates that can effectively resolve the longstanding DIP.

B. A FEASIBLE ALTERNATIVE TO CL

Before the emergence of FL, the only solution for training powerful AI models was to first aggregate data at some central place from relevant data owners/parties.

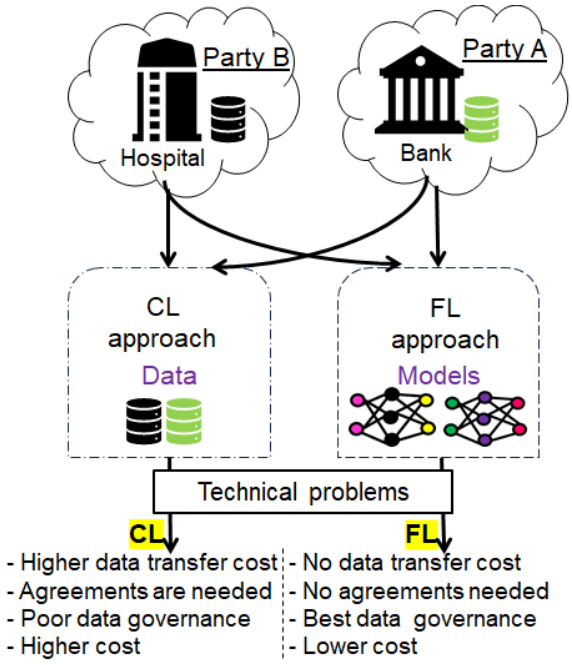

FIGURE 8. Technical problems in CL, and FL as solutions.

The CL setting is handy because it can reduce the computing burden on data owners, but most data owners are reluctant to transfer their data to outside environments, fearing privacy issues and the risk of data manipulation. Besides privacy, there are other technical problems, as depicted in Figure 8. It is worth noting that FL also works in a centralized fashion, but instead of the data, the models are shared with the server. By not aggregating data on the server, FL can ensure responsible governance of those data. Considering, these points, it is fair to say that FL is a feasible alternative to CL; it meets performance guarantees and attains data mining/analysis objectives.

C. PRIVACY BY DESIGN

Although many privacy-preserving (PP) approaches exist in the literature, FL is a promising privacy-by-design (PbD) approach. Other approaches to protecting privacy, such

as differential privacy (DP), anonymization, and micro-aggregation (MA), require access to the data in data owner environments (hospitals, banks, etc.). In contrast, access to data in FL is not required, making it a PbD approach because privacy is a default setting in the architecture. In some cases, data characteristics are shared with a central server, but that is general information that can still guarantee data privacy. In terms of service scenarios, we compare the conventional PP approaches and FL in Figure 9.

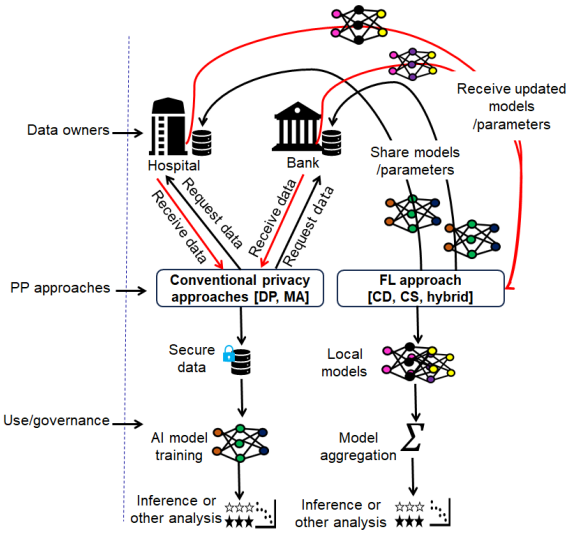

FIGURE 9. Comparison between conventional PP approaches and FL.

In Figure 9 we can see that FL is more PP than conventional approaches because it does not access local data held by data owners, but still allows knowledge extraction or inference.

D. TRAINING GENERALIZABLE AI MODELS

Data constitute the cornerstone of AI development; data quality and quantity can seriously impact AI models' performance/generalizability. AI models/products that are developed from too few, or bad-quality, data cannot generalize well from unseen data. Furthermore, AI models trained on bad-quality data yield more misclassifications in real-world settings, and different kinds of data drift can occur. To overcome these issues, retraining the AI model over regular intervals is required, which can be costly, depending on the scenario. To this end, FL is handy and can contribute to training AI models with higher generalizability by utilizing data from multiple parties. Since data do not move in FL, most parties can contribute to the training process. In contrast, the conventional setting (before FL) requires agreement/consent, and most parties choose to opt out of the training process because they do not want to expose their data to the outside world. We demonstrate a proof of concept in Figure 10 with 10 parties.

In the conventional scenario, an organization with good-quality data might refrain from participating in the training process, and the AI model cannot yield desirable

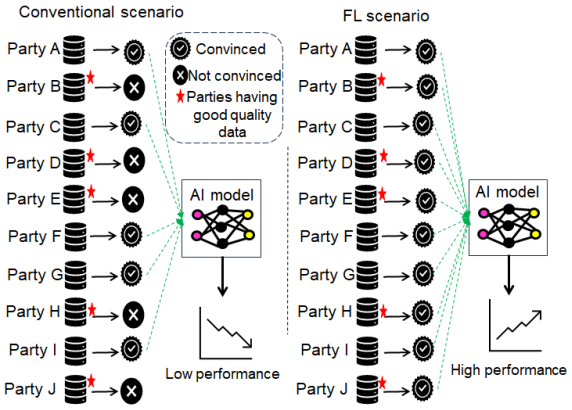

FIGURE 10. Training high-quality models due to higher participation of the diverse organization under FL scenario.

results. If all organizations with good data decide to not take part, the performance of AI models can easily be substandard. In contrast, it is relatively easy to convince different parties to take part in the training process in the FL setting; therefore, an AI model with higher generalizability can be trained. Also, strict laws and consent are not required in FL, and therefore, all parties can join the training process, leading to training AI models with greater inference accuracy. This situation was common in the recent pandemic where data disparities were very high across hospitals, and FL-like solutions to train AI models were in high demand.

E. KNOWLEDGE EXTRACTION W/O DATA MOBILITY

The knowledge extraction concept is somewhat identical in both CL and FL because both approaches extract patterns/trends from the data with the help of AI models. However, the key difference is that FL does not change the environment of the data during the knowledge extraction process. In contrast, CL changes the data locality before knowledge extraction. Therefore, CL needs to verify the security of the environment before data transfer, which can be hard in most cases. Fewer organizations will agree to donate data to untrusted environments, and knowledge extraction can be impacted. In contrast, FL moves AI models to the data, and knowledge extraction is relatively easy. Also, due to the inclusion of many diverse parties in the training process, knowledge extraction is more meaningful and can enhance real-world services. Figure 11 demonstrates a real-world scenario in which two hospitals want to extract knowledge from their data by using the services of a third party (e.g., an analytics company).

Now, if the hospitals are collaborating under the conventional setting, they need to transfer their data to a third party for knowledge extraction. In contrast, if they collaborate under FL, they do not need to transfer their data, but knowledge can still be extracted. This scenario demonstrates the supremacy of knowledge extraction by using FL instead of CL. We regard this as a paradigm shift because it was unknown before the advent of FL.

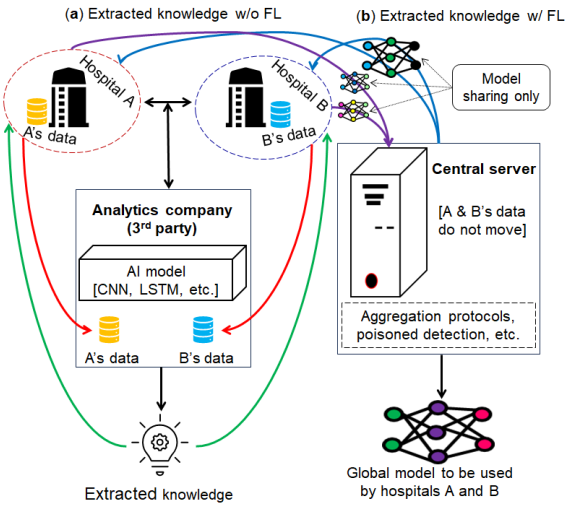

FIGURE 11. Knowledge extraction from data with and without FL.

F. TRANSFERRING ALGORITHMS

Before the advent of FL, data of diverse modalities (tables, images, text, multimedia, etc.) were always brought close to the AI models (SVM, RF, DT, CNN, LSTM, RNN, etc.). However, FL reversed this, and now algorithms are brought to the data. By doing so, data privacy is preserved, and models of high quality can be trained on them. In the conventional setting, it is hard to clear out all the data from all environments after use, and therefore, bringing data close to the algorithm can be manipulated for marketing purposes. Additionally, data can be transferred to other companies/organizations without the knowledge of true data owners. The fundamental relationship between algorithms and data is formally expressed in Eq. 1: CL brings data to algorithms, whereas FL sends algorithms to data.

$$Case(FL||CL) = \begin{cases} algorithms \rightarrow data, & \text{FL} \\ data \rightarrow algorithms, & \text{CL} \end{cases} \quad (1)$$

An example of CL is moving tabular data close to an RF classifier for classification/prediction. In contrast, FL sends a CNN model to image data for either image segmentation or feature extraction. We consider this change under the umbrella of paradigm shifts brought on by FL.

G. HARNESSING THE POTENTIAL OF EDGE/FOG COMPUTING

Cloud and fog computing technologies were mainly regarded as centralized settings before the advent of FL. However, limited resources at the network edge in the FL system necessitated a need to develop new solutions by leveraging hardware and software resources because existing solutions did not consider resource management for the edge, particularly under FL [97]. These computing architectures facilitated deployment, the discovery of resources, local model computing, load balancing, energy efficiency, and resource migration. We consider these technologies a paradigm shift because they cooperate with FL to resolve many technical problems [98]. Under these technologies, clients with fewer computing resources can offload some of the computations to edge/fog servers, which contributes to faster convergence in the global model. Additionally, these technologies are employed to enhance robustness and privacy preservation in FL [99]. Figure 12 illustrates the use of edge/fog computing in FL.

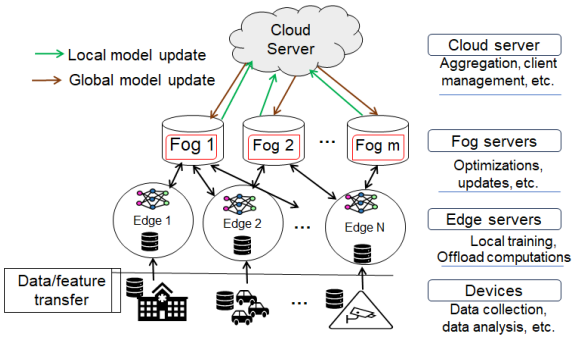

FIGURE 12. Use of edge/fog computing in FL.

Figure 12 shows that edge/fog computing methods decrease communications overhead and assist clients having the least computing power to train complex AI models [100]. In addition, these technologies can extend the application horizon of FL to time-sensitive applications. In some cases, these technologies help to achieve faster convergence in AI models under FL, which helps to reduce overall costs [101]. Considering these benefits, it is fair to say that FL fully harnesses the potential of edge/fog computing to improve technical deficiencies.

H. EXTENSIVE DIGITAL INNOVATION VIA FUSION OF DIVERSE TECHNOLOGIES

With the advent of FL, many technologies have been integrated into it to accomplish objectives such as data fusion, privacy protection, poisoned data detection, anomaly detection, client analysis, offloading computation, gradient protection, data quality assessment, shrinking hyper network parameters, addressing local model discrepancies, and data sanitization [102], [103], [104], [105], [106], [107], [108]. However, the application of FL and other technologies to any domain (e.g., healthcare) requires modifications to accomplish the desired goals, which we refer to as digital innovation. Since many technologies have now been linked with FL, more integrations are underway, therefore leading to extensive digital innovation. In some cases, FL is linked to established fields in order to optimize performance or address privacy issues. An example is FL integration into the IoT. In some cases, other technologies are linked with FL in order to improve its critical aspects. An example is linking fog/edge computing with FL to reduce communications overhead. In this regard, fusing multiple technologies under the umbrella of FL contributes to digital innovation worldwide. In Figure 13, we present five examples that pave the way to understanding the notion of digital innovation under FL.

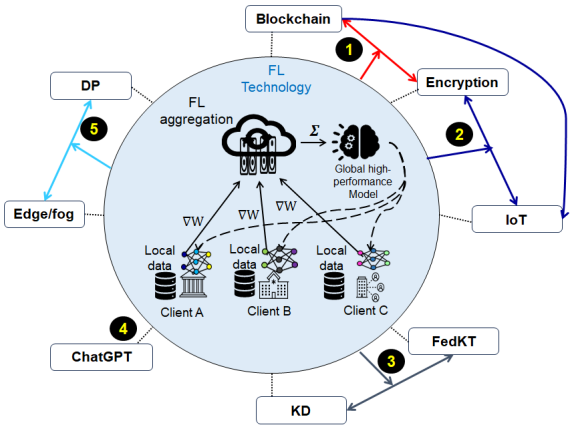

FIGURE 13. Digital innovation enhancement by fusing distinct solutions/concepts/software with FL. KD= knowledge distillation, FedKT= federated knowledge transfer, DP= differential privacy.

Recently, some critical components of FL have been enriched by adopting ChatGPT [109], which indicates ever-increasing digital innovation via the fusion of diverse technologies. Lastly, new dimensions of FL are emerging with each passing day, which requires new technologies, leading to digital innovation [110], [111], [112], [113]. For example, both ChatGPT and FL are new technologies, and exploring ways to complement each other can bring about digital innovation (new business models, use cases, or service delivery methods, etc.). It is worth noting that digital innovation in the FL context can be regarded as linking new technologies with FL or establishing cross-disciplinary approaches. In some cases, FL can help replace old technologies with new ones. For instance, FL and blockchain can alleviate the need for anonymization/DP in data-sharing scenarios [114]. With the emergence of FL, digital innovation is increasing at a rapid pace, and FL is on its way to becoming mainstream technology in diverse sectors.

I. UNPRECEDENTED USE OF STATISTICAL MEASURES/FORMULAS

Although FL is one of the mainstream solutions that ensure privacy and train AI models for higher generalizability, the decentralized nature of FL leads to many practical issues. For example, while sharing local updates/models with the server, some clients may send the wrong model, necessitating a detection mechanism at the server. To this end, most detection methods employ statistical or mathematical methods to filter out faulty local models [115]. Hence, a lot of statistical measures have been integrated with FL to either protect against diverse types of attacks or to accomplish other performance objectives. Wang et al. [116] employed the information entropy concept to protect FL from the byzantine attack. Shejwalkar and Houmansadr employed singular value decomposition to protect against model poisoning attacks [117]. They also discussed many statistical measures to protect against untargeted poisoning attacks. Panda et al. [118] used sparsification techniques to mitigate model poisoning threats in FL. Zhang and Hu [119] used variance reduction and the DP method to make FL byzantine-robust. Yang et al. [120] devised a vector norm-based approach to detecting model poisoning attacks in FL systems. Zhu et al. [121] employed the Hessian matrix to remove bursty adversarial patterns in both non-i.i.d. and i.i.d. data distributions. Yang et al. [122] utilized two concepts (dimensionality reduction and heterogeneity) against adaptive model poisoning attacks. Chang et al. [123] adopted conditional random sampling for FL communications efficiency and privacy preservation. Akai et al. [124] employed the concept of Gaussian and normal distributions in order to pinpoint and remove biased clients/nodes in an FL system. Based on these developments it is fair to say that FL's increased use of statistical measures of various kinds is unprecedented.

J. KNOWLEDGE DISCOVERY FROM SCATTERED AND DIVERSE DATASETS

By removing the privacy barrier, FL has significantly increased access to massive, diverse, and scattered datasets. Therefore, the scope and scale of knowledge discovery have significantly evolved, compared to the CL approach. In an FL system, multiple parties can participate where each one can have different data, and therefore, FL can make sense of the data and enhance the knowledge discovery process. In Figure 14, we illustrate the knowledge discovery process endorsed by FL from scattered and diverse datasets. In this

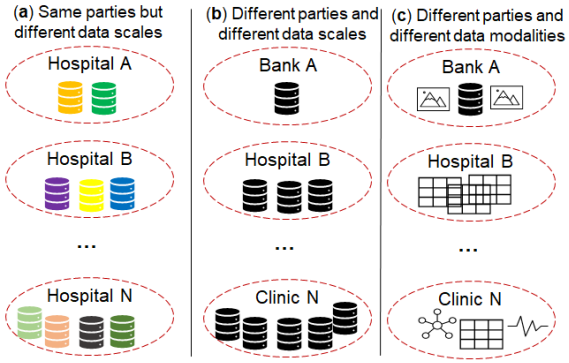

FIGURE 14. Knowledge discovery from scattered and diverse data.

example, we pinpoint three cases about data scales, data types, and the nature of the parties. However, there are many scattered datasets in real-world cases, and the knowledge discovery process can be significantly fastened down under the FL setting regardless of data locality [125]. These findings highlight the paradigm shift brought on by FL from the knowledge discovery standpoint with diversity in the data.

Based on the above analysis, we can conclude that FL has brought on radical paradigm shifts in the computing discipline. It is worth noting that FL has brought paradigm shifts to many other aspects, such as privacy-preserving AI, client characteristics, attack development, data-intensive computing, cost-reduction methods, energy minimization,

and enhanced reliability in trained AI models [126]. In recent years, FL has attracted widespread attention from researchers, and many unique advancements have been made in all aspects.

V. FL PRACTICAL ISSUES AND SOTA DEVELOPMENTS

Though FL has revolutionized the privacy arena, there are performance issues with the FL landscape that can limit its potential in many ways. In this work, we pinpoint 10 practical issues in FL systems to foster research. Figure 15 lists the 10 critical issues in the FL paradigm along with concise details. To the best of our knowledge, none of these issues have been jointly discussed in a single paper. The extended knowledge/taxonomy presented in this paper can pave the way to clearly understanding the technical deficiencies of FL, leading to more investigations of these issues.

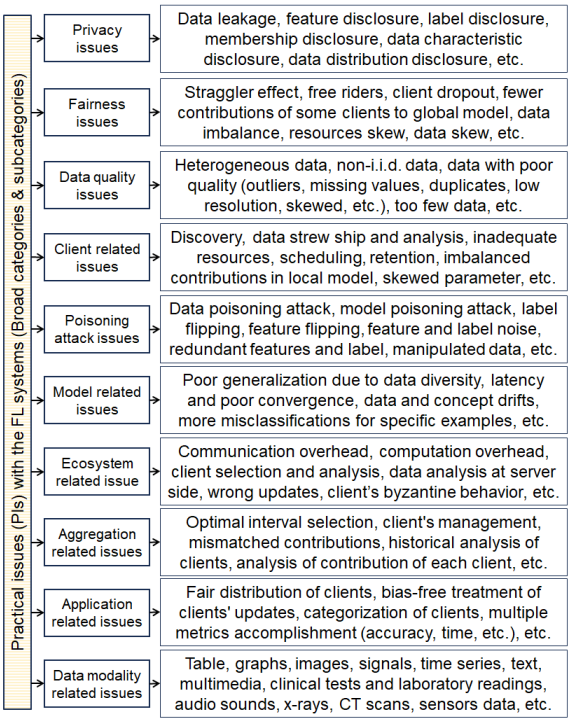

FIGURE 15. Different kinds of practical issues with FL.

A. PRIVACY

In FL systems, data do not leave the client devices, but private information about clients still leaks from sharing with a server the parameters or gradients of the local model [127], [128], [129]. Figure 16 demonstrates a scenario of individual privacy leakage from sharing gradients. An attacker can acquire local models uploaded by clients after intercepting the communication channel. Investigating the local model parameters shared by each client can reveal private information if clients do not implement/design strong privacy-preserving methods (PPMs). Thus, an attacker can leverage sensitive information to carry out illegal acts without the clients' knowledge [130].

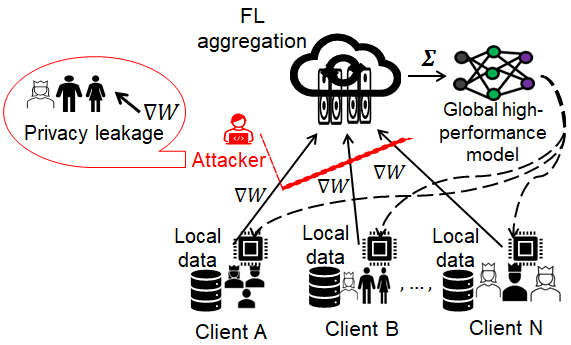

FIGURE 16. Privacy disclosures under FL during local model exchanges.

Considering the stringent privacy-preserving requirements in the FL framework, a more general practice is to alter or encrypt gradient parameters before uploading them to the server in order to protect them from attack. Adding noise or applying encryption can prevent attackers from gathering the data. Considering the communications overhead in FL, encryption may not be an ideal choice. Apart from encryption, DP, anonymization, secure multi-party computation, secret sharing, and hardware-based solutions have been suggested to address privacy problems [131], [132], [133], [134], [135], [136]. However, privacy-preserving FL (PPFL) is still a hot issue, and many SOTA studies centering on PPFL have been published.

B. FAIRNESS

FL can train AI models for higher generalizability by taking advantage of the benefits of large-scale and diverse datasets. However, ensuring fairness in local model updates at a central server is challenging [137], as shown in Figure 17. In this

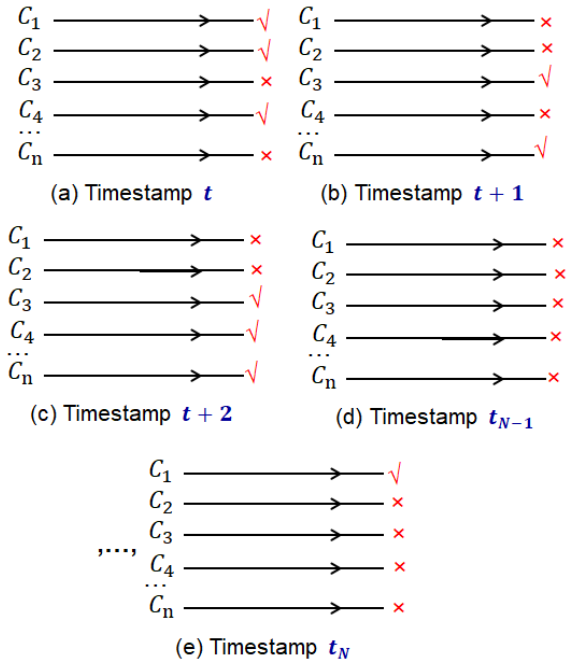

FIGURE 17. Illustration of fairness issue in the FL setting.

case, the behavior of five clients in four rounds is depicted. In each round, certain clients do not share their local model, and the global model can become biased if certain client updates are reflected only at the aggregation stage. For example, at timestamp t, only three clients (C_1, C_2, C_4) share updates with the server. At timestamp $t+1$, two clients (C_3, C_n) share updates. At timestamp $t+2$, three clients (C_3, C_4, C_n) share updates. At timestamp t_{N-1}, no client shares an update, but at timestamp t_N, one client (C_1) shares the update. Since clients do not participate equally in the training process, the global model cannot be equitable, because it might be biased towards clients making the most contributions. This issue has recently gained the attention of the researchers around the globe [138].

There are methods like equalized odds, group fairness, loss history-based analysis, statistical parity differences, equal opportunity differences, a discrimination index, and equal client selection [139], [140], [141], [142]. Despite these approaches, it is still challenging to ensure fairness from all aspects (e.g., client selection, local model updates, data size, data quantity).

C. CLIENT SELECTION

The strength of FL systems largely depends on activeness/reliability in the clients and on the local data held by each client. However, it is challenging to choose an appropriate set of clients as a part of the training process in FL, because there is greater skewness in data, resources, and AI models [143], [144], [145]. Clients with good-quality data, adequate resources, plus computational and communications capabilities are vital to completing the training task under a distributed setting [146]. Meanwhile, it is challenging to identify and retain good clients throughout the FL training process. Figure 18 demonstrates the challenges with client selection in FL environments w.r.t. data characteristics, computing devices, and the nature of the AI models. From Figure 18 we can conclude that there are greater disparities among clients in the FL system, which can lead to performance deficiencies.

Recently, some reinforcement learning (RL) methods have been proposed that model client selection as a Markov decision process in order to choose the optimal set of clients [147]. The proposed model tries to reduce training delay and energy consumption to encourage an increase in the number of clients that participate in training and model updates. Some methods assist in client selection by jointly considering the quality of both learning and the channel [148]. In the literature, some approaches have been proposed to select clients based on characteristics in their data [149]. In addition, some multi-criteria client selection methods have been proposed that consider channel gain, data information, and computing power while selecting the optimal number of clients [150]. Fan et al. developed the MiniPFL framework to select highly similar clients for clustering and aggregation [151]. The proposed approach can

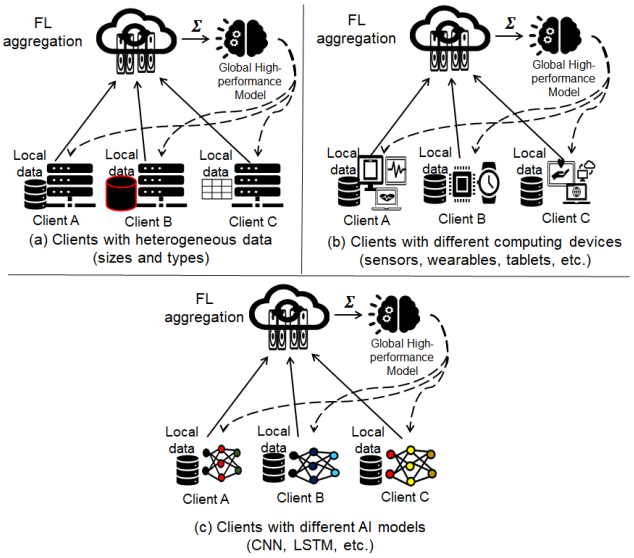

FIGURE 18. Challenges with client selection in FL environments.

achieve faster convergence and reduce the number of rounds by up to 30%. Despite these efforts, it is still very challenging to select suitable clients in different FL environments.

D. DATA-RELATED ISSUES

Data are considered the cornerstone for AI development, and they can seriously upgrade/downgrade the performance of any AI model. In FL, data often sit in silos (i.e., with owners), and there is no way to gauge and evaluate them. Therefore, the performance or contribution of each client to the server side is hard to evaluate, particularly from the perspective of content. For example, a benign client can be regarded as a poor performer if the accuracy is low. However, low accuracy can be due to data-related problems (e.g., non-i.i.d. data) [11], [152], [153], [154], [155]. Figure 19 shows common data-related challenges in FL environments that result in poor convergence guarantees or desirable accuracy not being easily accomplished.

Figure 19 (a) shows label distributions that are different across clients, which is common in practical scenarios where either data annotation or data collection is inconsistent. The unbalanced data problem is also common in real-life FL applications, as shown in Figure 19 (b). In this case, the number of data points or images is imbalanced across participating subjects/clients. Due to the imbalanced data, accuracy from data with an inadequate number of samples will be low, impacting the accuracy of the global model. Due to data imbalance, the number of iterations can be high, and performance bottlenecks can occur.

Figure 19 (c) illustrates differing data characteristics across clients. For example, some clients have all labeled data, and performance is high; some clients have only unlabeled data and accuracy might be low, but some clients have mixed data (e.g., labeled and unlabeled). Due to the deviations in characteristics, the FL system cannot yield consistent

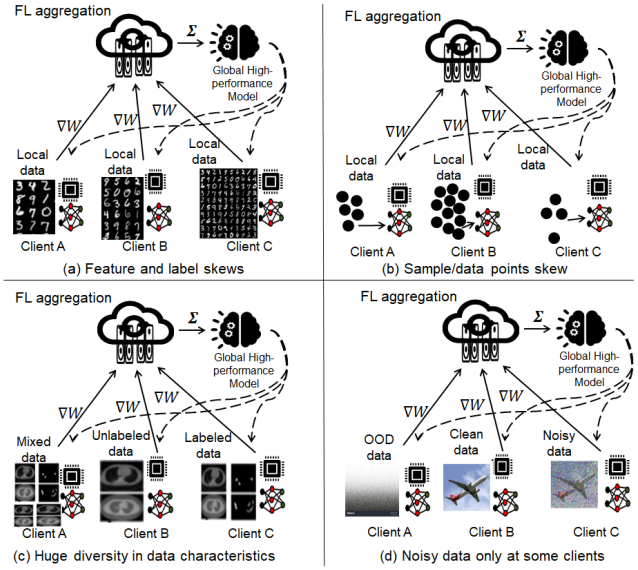

FIGURE 19. Data-quality challenges in FL environments.

performance in most cases. Lastly, some clients have noisy data, as shown in Figure 19 (d), and training may not contribute anything to the global model's accuracy. Apart from these challenges, data corruption, cross-correlations, data resolution skews, etc., seriously impact the quality of FL models [156], [157], [158], [159]. In some cases, new data that are more novel than the existing data are injected into the training data, which can significantly prolong the convergence time [160]. In the future, robust and practical solutions to address these data-quality challenges are required to unlock the potential of the FL technology [161], [162]. Lastly, addressing these data-related issues in both CD and CS settings is very challenging.

E. POISONING ISSUES

Due to the distributed nature of clients and data silos in FL, some clients behave benignly which, in effect, can be malicious. For example, some clients can train the local model with data that are erroneous, and the resulting local model causes a performance drift when aggregated with other models [163]. There are two main kinds of poisoning attacks in FL: (1) data poisoning, and (2) model poisoning. Both are defined below.

- *Data poisoning:* This relates to the local data held by each client. Since FL allows clients to not share their data, a dangerous vulnerability is introduced: *How can AI models that are trained under FL be trusted as accurate predictors?* Consider a real-world situation with a set/subset of clients that are either malicious by default or have been compromised. In this situation, clients can have poisoned or mislabeled local data. In FL, there is no central authority to validate each client's data, and therefore, those data can poison the global model. For example, consider Microsoft's AI chatbot Tay, which was installed on the underlying NLP model of Twitter (now called X) to interact with clients and learn from them. Due to malicious users, Tay was suddenly learning racist and offensive language [164]. Data integrity is compromised by a data poisoning attack, which manipulates/diverts global model performance, as shown in Figure 20.

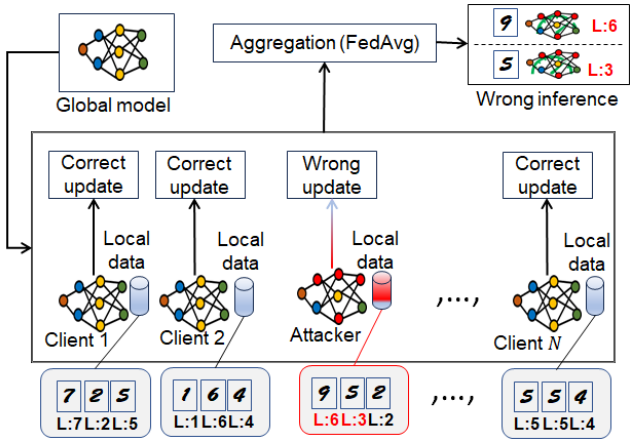

FIGURE 20. Overview of data poisoning attack in FL.

- *Model poisoning:* This relates to local models uploaded by each client to the central server. Unlike data poisoning, model poisoning corrupts the local models, compromising the FL training procedure, as shown in Figure 21. Specifically, the aim is to corrupt (or significantly modify) local model updates before they are forwarded to the central server. A variety of methods can be used to manipulate training on the client side (e.g., direct gradient manipulation). Unlike CL, FL is highly susceptible to model poisoning because the global model is shared with all clients during training and can easily be captured/intercepted during transmission [165]. In practice, model poisoning is much more severe because even a single non-colluding client can cause the global model to misclassify specific input. In conclusion, model poisoning can severely downgrade the reliability of the global model.

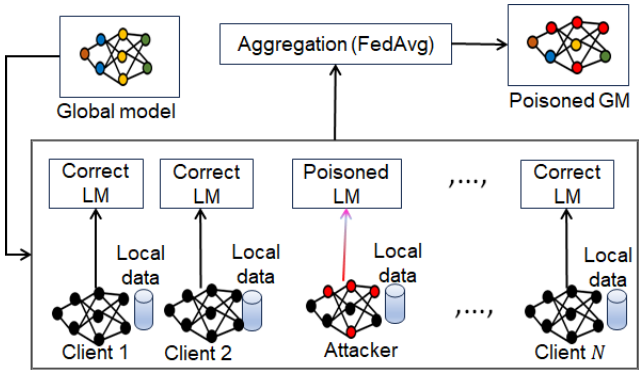

FIGURE 21. Overview of model poisoning attack in FL. LM= local model, GM= global model.

Further details about poisoning attacks are in Liu et al. [166]. Both attacks can severely degrade the FL's reliability. The use

of a poisoned model in some safety-critical applications can be dangerous and/or lead to financial loss. In the literature, many methods have been developed to undermine both attacks in order to make FL trustworthy and robust [167], [168], [169], [170]. Other types of attack, such as property inference, backdoor [171], gradient inversion [172], and targeted/untargeted attacks can also degrade the reliability of FL systems. Hence, it is vital to develop more security methods to thwart them and enhance public trust in this decentralized technology.

F. GLOBAL MODEL ISSUES

Although AI models trained under FL are more generalizable and dependable than training under CL, certain factors can still degrade their performance in realistic scenarios. For instance, a neural network (NN) has millions of parameters, and training NN with FL yields many performance bottlenecks. Training local models with highly redundant data does not contribute additional local/global features to the global model, leading to poor inference/generalization [173]. Furthermore, transmitting global models over a network often incurs high computing costs. In some settings, many free riders just acquire the trained global model but do not share local models in return. As cited above, poisoning attacks decrease the reliability of the global model, and convergence cannot be accomplished in a reasonable time. Non-i.i.d. data (e.g., skewed data points, labels, and features) can lead to poor performance from the global model, which is also prone to concept/data drift if information from the datasets is not reflected in it.

Furthermore, the global model can leak information at inference time, which can provoke privacy concerns. In some applications, the model can reveal data properties that can lead to data reconstruction attacks [174]. Additionally, both poisoned data and poisoned local models can corrupt the global model. There are very high structural differences (computing power, data possessed, communication volume, etc.) between clients, and therefore, directly integrating local models is challenging, posing threats to unified global model curation.

In the literature, many methods have been developed to address global model issues to enhance the FL efficacy [175]. Chen et al. [176] developed an in-cluster method to enhance communications efficiency (i.e., reduce uplink communications) to enhance the accuracy of the global model in non-i.i.d. scenarios. Li et al. [177] developed a novel method to address clients' uncertainties about FL in order to lessen any negative impact on global model performance. Nguyen et al. [178] developed a high-compression FL method to reduce training overhead by reducing the amount of data without losing guarantees on performance. Jiang et al. [179] developed the PruneFL method to fasten down the training process without losing guarantees of accuracy. Zhu and Jin [180] developed a multi-objective evolutionary method to compress network parameters and reduce network costs without degrading performance from the global model. Apart from these methods, some others have been developed to optimize the trade-off between accuracy loss and communications overhead. However, it is vital to develop more practical methods to prevent performance bottlenecks in the global model.

G. FL ECOSYSTEM ISSUES

The distributed nature of FL makes it vulnerable to attacks such as sniffing, spoofing, interception, privacy leakage, data and model theft, client dropout, and aggregation manipulation [181], [182]. The main reason to discuss this separately is to show how failure in one module affects the entire FL system. For example, the effect of poisoned data is not only related to clients but can affect the global model and its accuracy. Similarly, a malicious local model can pose challenges to integration and harmonization on the server side. High client dropout can leave an FL system waiting for updates [183], [184]. In addition, malicious action by one entity in the FL ecosystem can affect other entities, which can lead to deficient performance from the entire system. Similarly, the use of some statistical measures cannot capture all sorts of vulnerabilities, which can make the FL system costly [185]. Furthermore, poor design can lead to higher energy consumption and other issues [186]. Sometimes, the aggregation server might stop responding to clients due to physical damage or a security attack [187]. The FL ecosystem can make biased and unfair decisions, which can lead to social problems [188]. Lastly, anomaly/poisoning-attack detection on the server side can waste the computing resources of clients from longer latency and slow responses.

In the literature, many methods have been developed to address FL ecosystem issues to enhance quality of service (QoS). Yan et al. [189] discussed a practical method to align local and global models to extend the application of the FL ecosystem to heterogeneous settings. Cho et al. [190] discussed a method to select a subset of clients that receive incentives to prevent client dropout. The proposed method can help achieve faster convergence by enhancing contributions from good clients. Ma et al. [191] discussed SOTA studies that solved low-accuracy and convergence issues caused by non-i.i.d. data. Li et al. [192] proposed hard feature-matching data synthesis to reduce the complexity of FL systems while enhancing accuracy and privacy. Yan et al. [193] proposed a method to efficiently detect a poisoning attack and reduce server malfunctions. The authors aimed to minimize failures, reduce redundancy, and improve the quality of the FL ecosystem. Apart from these, other methods have been developed to prevent failures and make FL ecosystems resilient.

H. AGGREGATION PROTOCOL ISSUES

In FL, the aggregation algorithm/protocol plays a central role in the training process, being responsible for merging information from all participating clients by combining local

models to train a global model [194]. Twelve types of aggregation strategy are discussed in Moshawrab et al. [194]. Despite significant developments, it is still challenging to aggregate all local model results and transform them into one unified global model. For example, it is difficult to decide on the time window for responses from all clients. Similarly, it is hard to decide the optimal number of clients to reflect sufficient results in the global model. It is challenging to maintain a history of each client and their corresponding local model. Assessment of the quality in each local model, discarding malicious ones, also poses challenges for aggregation protocols/algorithms, particularly for non-i.i.d. data. Skewed resources can slow the aggregation process, particularly when many clients do not have powerful enough computing resources. Additionally, local models can be forged in order to launch security attacks or violate privacy. Therefore, the challenge is to ensure appropriate aggregation in FL to curate a global model that is fair, highly accurate, and robust.

Of late, many efforts have been devoted to resolving aggregation-related issues in FL [195]. Guo et al. [196] developed a method to ensure fast and secure aggregation of local models when a substantial number of clients drop out during training. Pillutla et al. [197] developed a robust aggregation approach with greater robustness for FL, particularly when local models are corrupted. So et al. [198] developed a secure aggregation protocol for FL when a large number of clients drop out. The authors showed the applicability of their method to AFL settings, which is the latest development in the field. Nguyen et al. [199] developed a privacy-preserved aggregation protocol for both synchronous and asynchronous FL, which can work with any type of optimizer. Shi et al. [200] developed a generic aggregation protocol that requires updates only from some clients, rather than all of them, to reduce communications overhead, only marginally losing performance. Apart from these SOTA methods, others have been developed to correctly aggregate local models into a global one [201]. However, more practical methods are needed to ensure secure and correct aggregation in different FL settings.

I. FL APPLICATION ISSUES

The naive use of FL in any area is challenging for multiple reasons: client selection, client strength, data modality, convergence requirements, aggregation methodology, and communications infrastructure. For example, FL use in anomaly detection and the medical domain is quite different due to the nature of the data as well as the objectives (accuracy, correctness of classification/prediction, fairness, etc.). Furthermore, in some cases, global model requirements vary from application to application, and it can be challenging to accomplish all the desired goals in each application. Furthermore, FL for some sensitive applications may require a stronger privacy mechanism, while less-sensitive applications may need only basic security. Similarly, the decision to employ cloud/fog computing with FL in each application requires in-depth analysis. Considering these issues, it is fair to say that FL use in diverse application scenarios is challenging. Lastly, training a robust global model is challenging when using centralized, decentralized, or hybrid FL architectures; different network topologies (star, ring, and hybrid); small, big, or complex datasets; either ML or DL models, or to meet differing application requirements (e.g., time-sensitive, safety-critical, elderly care, etc.) [202].

Of late, many efforts have been devoted to resolving application-related issues in FL environments by achieving multiple objectives simultaneously and opening the FL source code. Yu et al. [203] developed a framework named IronForge that can contribute to making FL secure, open, and fair. The proposed framework can work in open networks without requiring rigorous security controls. Hasan et al. [204] extended the application of FL to vehicular networks (6G-V2X) while ensuring crucial objectives such as privacy protection for sensitive data and/or models, lowering the communication costs, and shortening the training process. Liu et al. [205] discussed ways to reduce the cost of FL training in non-i.i.d. settings by curating and distributing personalized models with each client. Fu et al. [206] discussed strategies for selecting a portion of clients to train global models by considering the application requirements. Xu et al. [207] discussed ways to resolve device heterogeneity in diverse applications in the asynchronous FL setting. Zellinger et al. [208] discussed ways to ensure the confidentiality of industrial data, particularly with FL in manufacturing. Apart from these SOTA methods, other methods have been developed to address application-related problems in conventional FL by using a personalized FL [209]. However, more practical methods are needed to ensure consistent performance and the governance of FL in diverse or unexplored application areas.

J. DIVERSE DATA MODALITY ISSUES

Although image data are among the most widely used modalities in the FL environment, other data modalities (tables, graphs, time series, audio) can be used depending on the application scenario. However, each modality can pose different challenges to FL settings depending on the scenario or application requirements. For example, AI models for images can use a CNN, whereas tabular data may require simple regression/perceptron. Similarly, the number of training rounds for image data can be relatively higher than tabular data. Similarly, bandwidth and latency issues can vary from modality to modality. Xiong et al. [287] solved modality discrepancy in conventional FL by proposing a unified framework. Their framework can extract handy global features from different data modalities to collaboratively train global models for all participating clients. Chen and Zhang [288] proposed a framework for achieving good performance in multi-task and multi-model FL. The proposed framework helps address data heterogeneity, particularly

TABLE 6. Recent SOTA developments in addressing practical issues in FL systems.

Issue #	Strength	Weakness	Method	Application area	Data	Ref.
1	Protects against IT & yields high accuracy	Higher complexity & low accuracy	SMC + DP	General	RD	Truex et al. [210]
	Resolves LAT with privacy protection	Extensive corruption in GM	BC + ZKP	AD	SD	Li et al. [37]
	Novel solution for PCAT	Adds more noise; 1.1% accuracy increase	ADP	General	RD	Wang et al. [211]
	Less noise in LM	Higher offset in GM	HDP	General	RD	Ling et al. [212]
	Strong privacy & verification	Slow when clients leave	Grad. masking	IoMT	RD	Wang et al. [213]
	Protects from inference and GLA	Same noise for all clients	LDP	VANETs	SD	Batool et al. [214]
	Strong protection of local data	Attacker can evade detection	DP-GANs	General	RD	Tran et al. [215]
	Safeguards model parameters	Latency issues and higher complexity	BC+HE+IP	General	RD	Xiong et al. [216]
	Works with both non-i.i.d. and i.i.d.	Same noise for all clients	ANP	General	RD	Li et al. [217]
	Strong protection against GLA	High storage cost and computing cost	Outpost	General	RD	Wang et al. [218]
	Client privacy and FL performance enhancement	Slow convergance in non-i.i.d. data cases	PBR & DAW	Smart homes	RD	Li et al. [219]
2	Fair analysis of clients' contributions	Difficulty in dividing budgets (e.g., ϵ)	FLI-PSS	General	SD	Yu et al. [220]
	Ensures group fairness in FL	Poor performance with non-i.i.d. data	FairFed	General	SD	Ezzeldin et al. [138]
	Solves AFT in generic FL	Poor training accuracy	DMG	General	RD	Huang et al. [221]
	Solves AFT in HFL	Limited to HFL scenario only	DMG	General	RD	Huang et al. [222]
	Fairness-aware CS for FL	Poor generalization of models	C^2-MAB	General	RD	Huang et al. [223]
	Works with unreliable clients	Extensive computing operations	SRA	IoT	RD	Li et al. [224]
	Fair ranking of clients based on updates	Slow when contributions are the same	SV	General	RD	Fan et al. [225]
3	Context-aware online CS	Limited to HFL scenario only	CC-MAB	General	RD	Qu et al. [226]
	Contribution-based CS	Prone to PA and data leaks	WDPs	General	RD	Pang et al. [227]
	Select a good pool of clients	Difficult to quantify noise	CS-MAB	General	RD	Yang et al. [228]
	Reduces the difficulty in CS process	Works with VFL setting only	CEPD	General	RD	Shi et al. [229]
	Analyzes client profiles in CS	Difficult to detect fake profiles	SCS	General	RD	Tan et al. [230]
	Best CS for imperfections in data	Requires heavy computation and is slow	IST	General	RD	Rai et al. [143]
	Needs-based CS in each training round	Hard to determine optimal number of clients	Docker	IoT	RD	Shenoy et al. [231]
	Effectively groups heterogeneous clients	Cannot resist backdoor and other attacks	FedSeq	General	RD	Silvi et al. [232]
4	Solid defense against LFA	Failure to detect other practical issues	LFS	General	RD	Jiang et al. [233]
	Incentivizes clients for best data	Heavier noise in data from some clients	GT	General	RD	Zhang et al. [234]
	Enhances ratio of correct labels	Does not fix other issues (e.g., skews)	QSR	General	RD	Pejó & Biczók [235]
	Curates high quality training samples	High cost for large and complex data	DCM	General	RD	Li et al. [236]
	Multi-level data quality analysis	High cost and latency issues	RS	General	RD	Zhang et al. [237]
	Enhances label quality	Ignores other quality issues (e.g., distribution)	MCE	General	RD	Chen et al. [238]
	Local data analysis for QE	Works well with i.i.d. data only	CEDDLA	General	SD	Zhao et al. [239]
	Evaluates data for accuracy increase	Biased toward some clients	CP	General	RD	Wu et al. [240]
	Efficient label-noise filtering	Extensive data conversion cost	k-NNG	General	RD	Duan et al. [241]
	Ensures global distribution is balanced	Does not analyze label/feature noise	AG	General	RD	He et al. [242]
	Filtration of corrupted local data	Relies on client updates only	IC + DP	General	RD	Rokvic et al. [243]
5	Correctly filters malicious clients	Sometime removes benign clients	FF	General	RD	Campos et al. [244]
	Solid defense against PA	Threshold misalignment	FlexibleFL	General	RD	Zhao et al. [245]
	Solves multiple trade-offs	Non-adaptive noise	DP	General	RD	Huang et al. [246]
	Restricts attack impacts	Low defense when clients leave	TC	General	RD	Kasyap et al. [247]
	Executes stealthy attack on FL	Easy detection and mitigation in some cases	GAE+ SGD	General	RD	Li et al. [248]
	Solid defense for PA in F-SVMs	Limited to one AI/ML model	AM	General	RD	Mouri et al. [249]
	Provides better security	High cost when # of clients is large	BC	General	RD	Xu et al. [250]
	Protects from model poisoning attacks	Cannot be used in generic cases	FedKC	Metaverse	RD	Sun et al. [251]
6	Reduces distribution discrepancy among clients	Slow when clients are large in number	FedFTG	General	RD	Zhang et al. [252]
	Filters erroneous local models in aggregation	Higher cost in terms of analysis	GoMORE	WFL	RD	Yao et al. [253]
	Prevents client dropout by GM appeal	Higher bias from ignoring some clients	MaxFL	General	RD	Cho et al. [254]
	Faster convergence of GM in i.i.d. cases	Performance issues in non-i.i.d. cases	FedAdp	General	RD	Wu et al. [255]
	Faster construction of GM via aggregation	Can drop legitimate clients in some cases	FedPNS	General	RD	Wu et al. [256]
	Reliability and quality enhancement of GM	Fewer incentives for clients with non-i.i.d. data	CT	General	RD	Li et al. [257]
	GM accuracy enhancement in AFL	Latency and high communications cost	OIMAF	General	RD	Li et al. [258]
	Faster convergence of GM with limited budget	Less robust when clients increase	CMAB	ACN	RD	Wang et al. [259]
	Accelerates GM convergence with high accuracy	Privacy issues from data sharing with server	KLD	General	RD	Li et al. [260]
	Uses multiple GM rather than one	Extensive computations and calculations	AP	General	RD	Bidgoly et al. [261]
	Accelerates GM convergence by 40 %	Difficult to detect poisoned model effect	LDP	General	RD	Weng et al. [262]
7	Supports diverse AI models	Poor scalability when diversity increases	FLSys	MA	RD,SD	Jiang et al. [263]
	Higher accuracy and stability in GM	Poor performance when data are skewed	ZMS+ ZGD	MN	RD,SD	Jiang et al. [264]
	Extends FL application to mobile devices	Straggler problem, CS issues	DP	OB	RD	Long et al. [265]
	Executes edge-enabled AI models	Limited accuracy enhancement (e.g., 3 %)	LEAF	HEco	RD	Patel et al. [266]
	Faster convergence of GM in HFL	Aggregation is hard when models are diverse	RF-HFL	DEco	RD	Zhang et al. [267]
	Reduced communication rounds in AFL	Works well with i.i.d. data only	TWA + SDL	SLD	RD	Yaqoob et al. [268]
	Effective segmentation and classification of MI	Difficult to chose optimal CT in some cases	TWA	SCP	RD	Ain et al. [269]
8	Faster aggregation in just 2 rounds	Poisoned local model can enter FL system	SAFELearn	General	RD	Ferei et al. [270]
	Aggregates obscure model updates	Privacy leakage through model updates	LE	General	RD	Zheng et al. [271]
	Prevents data re-construction attacks	Convergence will be slow when clients drop out	EPPDA	General	RD	Song et al. [272]
	Protocol for both cross-device and cross-silo FL	Data diversity issues are not resolved	DL	General	RD	Tang et al. [273]
	Safeguards against backdoor attacks	Might filter benign clients with non-i.i.d. data	Cr	I4.0	RD	Gao et al. [274]
	Enhances robustness of aggregation process	No defense against poisoned clients	RM	General	RD	Nabavi et al. [275]
9	FL use in operational environments	Vulnerable to poisoning attacks	PoC	IRT	SD	Kourtellis et al. [276]
	FL for resource-constrained devices	Susceptible to backdoor attacks	TEEs	General	RD	Mo et al. [277]
	Privacy preservation with less computation	Minimal accuracy enhancement	GE	AVs	RD	Parekh et al. [278]
	Privacy protection of clients' data	High computing costs when clients are large	CC	General	SD	Mo et al. [278]
	Reduction in FL training time	No protection for privacy and GLA	ATZ	General	SD	Mesaoud et al. [280]
10	Training with multi-modality data	Unsuitable for time-sensitive applications	CFL	COVID-19	RD,SD	Qayyum et al. [39]
	IR for various vision-related tasks	Works well with only image datasets	aimNet	VLG	RD	Liu et al. [281]
	Training with multi-institutional data	Limited application in non-i.i.d. settings	FedAvg	Medical	RD	Sheller et al. [282]
	Robust multi-site fMRI analysis	Less generalization to other types of data	DAM	Medical	RD	Li et al. [283]
	Learning with multi-sensor data	Higher signal/data alignment cost	WT	EI	RD	Saeed et al. [284]
	Trains AI models with unlabeled data	Poor scalability and high overheads	BANet	Medical	RD	Lei et al. [285]
	Privacy protection from GAN attacks	Limited to image classification tasks	PP-FDL	F-IoT	RD	Abdel et al. [286]

when clients have heterogeneous configurations of sensors, and their data encompass diverse combinations of modalities. Kang et al. [289] devised a framework to address different data quality issues (specifically, it aligns samples) in

diverse data modalities to ensure consistent learning in FL. Yan et al. [290] discussed using a CycleGAN architecture to address disparity among clients (the cross-client variation problem) in terms of the number of images. Xiao et al. [291] discussed an FL method to synthesize diverse features from the same data modality to recognize the activities of users. Zhang et al. [292] proposed a generic framework for diverse medical images. Their proposed framework is CNN-agnostic, achieving an accuracy of 96.2%. Despite these developments, it is still challenging to fuse diverse data modalities and extract the enclosed knowledge under FL.

K. DEVELOPMENTS IN ADDRESSING PRACTICAL ISSUES: A SOTA ANALYSIS

In this section, we discuss recent developments addressing practical issues in FL by analyzing SOTA literature. It is worth noting that there are lots of disparities in the above-cited solutions. For instance, many studies have addressed privacy issues but relatively few discuss FL applicability to diverse data modalities. Similarly, a lot of studies proposed poisoning attack mitigation but fewer studies were on data quality enhancement, particularly in cross-silo FL. Similarly, fairness issues have had relatively less attention from researchers compared to privacy and poisoning attacks. Table 6 presents SOTA papers published to resolve FL practical issues. In Table 6, we sequentially present recent developments in addressing each issue. In Table 6, Segment 1 presents developments in privacy issues, and Segment 6 presents developments for global models. We compared SOTA papers based on five criteria: strengths, weaknesses, method used, application area, and datasets (real dataset (RD) or synthetic dataset (SD)) used in the evaluation. The analysis in Table 6 paves the way to understanding recent developments in the 10 FL issues identified. To the best of our knowledge, this is the first paper that systematically summarizes recent developments in major issues of FL based on SOTA studies. The abbreviations used in Table 6 are listed in Table 2.

VI. PARTNERSHIP OF FL WITH TWO OR MORE TECHNOLOGIES

As discussed earlier, FL alone fails to meet its intended objectives/goals in many aspects, and therefore, FL has partnered with other technologies to address deficiencies. For example, privacy leakage through gradient sharing was a hot issue that was resolved by combining FL with DP [293]. Similarly, to resolve poisoning issues and detection of lazy clients, FL was integrated with blockchain [294], in some cases to ensure verifiability and auditability of clients' data or results [295], [296]. In recent years, FL partnerships with current technologies have been steadily increasing. Ji et al. [297] discussed the coupling of FL with many learning algorithms (e.g., meta-learning, transfer learning, adversarial learning, knowledge distillation, etc.) to resolve two crucial challenges: statistical heterogeneity and robust learning. The authors coined the term, Federated *X* Learning, in which FL is customized to fit different learning algorithms. In our previous work, we discussed the partnership of FL with just one technology [298]. In this work, we extend that to two or more technologies. The integration of two or more technologies with FL helps to enhance the robustness of FL from many perspectives. Table 7 discusses partnerships of FL with two or more technologies along with the purpose of partnerships by highlighting SOTA studies. The abbreviations used in Table 7 are given in Table 2.

TABLE 7. FL partnerships with other technologies (2+).

Ref.	Partnership with	Purpose of partnership
[299]	BC, DP	Privacy-preserved data sharing
[300]	BC, masking	Security and verifiablity
[301]	BC, NN (diverse)	Client selection
[302]	BC, Enc	Security enhancement
[303]	DRL, MDP	Trust enhancement
[304]	DP, HE, BC	Data protection at $\sum$ time
[305]	Crypto, BC	Privacy preservation
[306]	UKG, FSL, IoMT	Elderly healthcare
[307]	EC, CC	Reduction in delay time
[308]	SMC, BC	Privacy and trust enhancement
[30]	Normalization, BC	COVID-19 detection
[309]	Anon., Facor.	Statistical heterogeneity solution
[310]	EC, DP	Big data analysis with privacy
[311]	PR, Encryption, BC	Patient monitoring
[32]	DP, SMC	AI for financial applications
[312]	NMF, ALS	Customized data privacy
[313]	Enc., SS	Detection of FDI attacks
[314]	SCS, GT	Model training in P2P networks
[315]	PCS, DDPG	Higher accuracy & fast convergence
[316]	GC, KD	Reduction in communications cost
[317]	FE, SMC	Improve computational efficiency
[318]	GI, DP	Protection of RI for the client
[319]	KA, Enc.	Privacy protection of data
[320]	LS^{2}DNN, PBKA	Intrusion detection
[321]	LDP, HE	Enhance efficiency and accuracy
[322]	FE, Anon.	Optimize PUT in FL systems
[323]	DP, KA	Accuracy enhancement from FL
[324]	DT, RF	Accuracy increase (i.i.d. & non-i.i.d.)
[325]	DP, GT	Graphic element detection
[326]	DP, HE	Security and robustness in FL
[327]	SMC, SS	Protection against collusion attacks
[328]	STE, KLD, SMC	Making FL low-cost
[329]	FS, DP	LM's utility enhancement
[330]	BC, FHE, DP	Performance enhancement
[331]	DP, QC	Fast computation with privacy
[332]	SS, LMU	Protection against quantum attacks
[333]	Gen AI, SDM	Content generation
[334]	NAS, PET	Privacy enhancement by 81.5%
[335]	SL, AIoT	Robustness and scalability enhancement without compromising privacy
[336]	BC, HE, Reputation	Privacy and security enhancement

Table 7 shows that many technologies have partnerships with FL to either improve deficiencies or extend FL use into unexplored areas. For example, DP was combined with FL to improve privacy while BC was linked to enable patient monitoring in cloud environments. In most cases, an FL partnership enhanced a technical efficacy or optimized certain performance indicators. It is worth noting that FL has been adopted in diverse sectors to accomplish multiple objectives (e.g., privacy-preserved data analytics,

data sharing with privacy guarantees, privacy-preserved model sharing) [337]. Table 7 contributes to understanding the latest developments in FL in conjunction with other technologies. To the best of our knowledge, this has not been discussed in the literature, particularly FL and ChatGPT. This extended knowledge can help to clearly understand partnerships between FL and other technologies. The five key roles of this section are: (i) figure out the name of the latest technologies with whom FL has been integrated, (ii) explore the various purposes of FL integration with other emerging technologies, (iii) comprehensive list of SOTA papers which has proposed ways to successfully integrate FL with other technologies, (iv) offers a valuable resource for researchers/practitioners who aim to work on one or more of these FL integrations, and (v) depicting latest trends in augmenting the viability and practicality of FL through integration with latest/emerging technologies.

VII. TRADE-OFFS IN FL, CORRESPONDING SOLUTIONS

Though FL is one of the latest technologies to train high-quality AI models for many real-world applications, it is confronted by many trade-offs that require robust resolution. For example, to mitigate the poisoned data effect, one needs to explore client data that might violate data privacy, leading to a privacy-versus-poisoning trade-off. Clients that have non-i.i.d. data might degrade accuracy in the global model, which as a result may require more iterations until convergence, leading to an accuracy-versus-convergence trade-off. Early convergence in the global model might drop certain legitimate client updates, which leads to a fairness-versus-convergence trade-off. There is a trade-off between fairness and accuracy when clients have disparities in terms of data and computing resources. There is a trade-off between energy use and accuracy, particularly in the CS setting of FL. Similarly, there is a trade-off between client selection and convergence because the number of clients affects convergence time. It is worth noting that trade-offs can involve two or more performance metrics/objectives [338], and some solutions have been proposed recently to mitigate them.

The five key roles of this section are (i) insight into different types of trade-offs that exist in the FL landscape, (ii) explore the common and uncommon trade-offs in FL landscape, (iii) comprehensive list of SOTA research papers which has devised practical ways to successfully resolve trade-offs of two or more types in FL, (iv) provide a valuable resource for researchers/practitioners who aim to optimize trade-offs of different types in FL, and (v) showcasing one important research topic to further enhance the robustness of FL by optimizing existing trade-offs or resolving yet unexplored trade-offs. The effective solution of different types of trade-offs is vital to deploy FL in resource-constrained environments as well as to enhance the credibility of this distributed technology. Table 8 discusses different SOTA studies that resolved different types of trade-offs in an FL ecosystem.

TABLE 8. SOTA solutions for optimizing trade-offs in FL.

Ref.	Trade-off(s) resolved
[339]	Privacy, accuracy, and model fairness
[340]	Accuracy and test loss
[341]	Fairness and accuracy
[342]	Privacy and fairness
[137]	Fairness and global model performance
[343]	Local and global fairness
[344]	Accuracy and training time
[345]	Accuracy and communication cost
[346]	Privacy, utility, and fairness
[347]	Utility and fairness
[348]	Privacy protection and test accuracy
[349]	Fairness, integrity, and privacy
[350]	Communication efficiency, robustness, and fairness
[351]	Robustness and privacy
[352]	Privacy and latency
[353]	Utility and privacy
[354]	Model fairness and user privacy
[355]	Communications cost and training loss
[356]	Privacy and utility
[357]	Privacy and accuracy
[358]	Fairness and heterogeneity
[359]	Fairness and drifts
[360]	Computing time and prediction accuracy
[361]	Accuracy, worst node performance, and communications cost
[362]	Privacy and explainability
[363]	Privacy and efficiency
[364]	Accuracy and communication cost
[365]	Communications overhead and training time
[366]	Privacy, accuracy, and communication efficiency
[367]	Privacy and model poisoning
[368]	Privacy, accuracy, and energy use
[369]	Privacy, accuracy, and communications cost
[370]	Accurate learning and energy
[371]	Computing speed and accuracy
[372]	User/client dropout and efficiency
[373]	Accuracy, robustness, and flexibility
[374]	Privacy, accuracy, and adversarial attacks
[375]	Energy consumption and convergence

In Table 8, we can see that many studies have resolved two, three, or four different trade-offs in the FL ecosystem. In the literature, the privacy and accuracy/utility trade-offs have been widely investigated from diverse perspectives. However, the energy and privacy trade-off is relatively less investigated than others. It is worth noting that some studies in the literature have significantly improved one metric while keeping the other metric the same as in previous studies [376], [377]. Some studies have extended the application of FL to a completely new domain with results similar to previous work. The extended knowledge presented in Table 8 can pave the way to understanding the different kinds of trade-offs in the FL landscape and the corresponding SOTA solutions from a broader perspective.

VIII. RECENT DEVELOPMENTS TO MAKE FL TRUSTWORTHY

Over the past couple of years, AI experts have recognized that most AI systems lack trustworthiness. They are prone to adversarial attacks, and are biased toward certain demographics; they risk the privacy of users, lack robustness against poisoned data/model attacks, lack explanations concerning decisions/predictions made, and they work in a black-box

manner [378]. The use of AI without paying ample attention to trustworthiness is risky and can lead to various types of social problems and invisible harm [379], [380]. Considering the need for trustworthy AI systems, various suggestions have been made in diverse sectors to add trustworthiness. For example, El-Sappagh et al. [381] discussed SOTA papers concerning trustworthy AI in Alzheimer's disease scenarios. The authors stressed the need to make AI results more explainable/understandable, enhancing the trust in diverse entities in medicine (e.g., patients, regulators, and medical professionals). Qi et al. [382] devised a method to enhance the robustness of AI systems in intent detection. Mylrea and Robinson [383] discussed key pillars of trustworthiness in AI systems and devised a framework to measure trust in them. Badawy [384] discussed a data-driven framework to quantify risk from AI systems and the interplay among AI, digitization, and various environmental factors. Bonifazi et al. [385] proposed a framework to make ML classifiers explainable by employing network theory concepts. The proposed concepts can be useful in explaining the behavior of ML classifiers and the decisions made by them, which is a vital step toward making classifiers trustworthy. Lalor et al. [386] proposed a framework for quantifying fairness in AI models by using multiple protected attributes and the associated harm. The proposed framework is a pivotal step to making AI systems more reliable and trustworthy, and it can be used in many scenarios such as user modeling, information retrieval, and digital platforms to reduce bias in AI pipelines. A generic analysis of six dimensions for trustworthy AI and the associated developments is discussed by Liu et al. [387].

Considering these developments in general AI, FL is no exception, and many such developments have been made to make FL trustworthy and explainable. Sánchez et al. [388] discussed salient pillars, metrics, and notions to compute trustworthiness in FL. The authors suggested there are six pillars (robustness, privacy, explainability, fairness, accountability, and federation) to quantify trust in FL. They are akin to the generic concept of trustworthy AI depicted in Figure 22, which shows six key dimensions/pillars of trustworthy AI/FL.

Tariq et al. [389] comprehensively discussed the recent literature, metrics, notions, and criteria of trustworthy FL. The authors stressed the need to pinpoint trustworthiness metrics and pillars specific to FL, and to develop corresponding solutions. However, their survey was limited to three dimensions/pillars: security and privacy, interpretability, and fairness. Zhang et al. [390] presented a survey on the trustworthy aspects of FL by focusing on privacy, security, and robustness. Psaltis et al. [391] discussed ways to enhance trustworthiness in FL by adopting appropriate privacy-preserving mechanisms and aggregation algorithms. In the recent literature, some studies have focused on developing a framework to assess trustworthiness or to improve two or more dimensions of trustworthy FL. Rehman et al. [392] developed a blockchain-based framework to accomplish

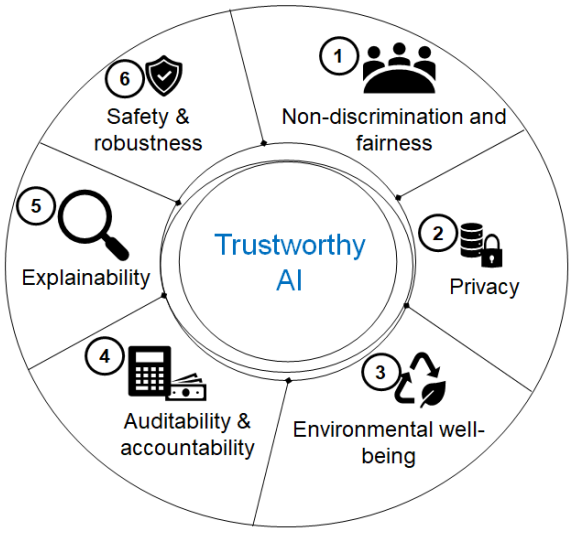

FIGURE 22. Six dimensions of trustworthy AI/FL.

trustworthy and fair FL learning in IIoT. Lo et al. [393] developed a BC-based architecture to make FL systems more accountable and fair while sustaining higher generalizability and accuracy. Wang et al. [394] proposed a scheme for decentralized FL that enhances both trustworthiness and privacy. Han et al. [395] discussed a GAN-based method to enhance performance consistency and algorithmic fairness in FL. Rjoub et al. [396] devised the DDQN-Trust solution to enhance the trustworthiness of FL in IoT. Yuan et al. [397] proposed a scheme to enhance FL trustworthiness in terms of accuracy and privacy while resisting a variety of adversarial attacks. Table 9 presents a summary of SOTA studies that have explored ways to make FL trustworthy. In Table 9, we analyze previous studies in terms of the number of dimensions concerning trustworthiness and the names of those dimensions.

TABLE 9. Analysis of SOTA studies related to trustworthy FL.

Ref.	# of dimen.	Name of dimensions
[398]	2	Privacy, safety
[399]	3	Accuracy, efficiency, scalability
[400]	2	Effectiveness, efficiency
[401]	2	Fairness, privacy
[402]	3	Robustness, fairness, privacy
[403]	2	Privacy, robustness
[404]	2	Privacy, robustness
[405]	3	Non-discrimination, privacy, safety
[406]	3	Accountability, robustness, privacy
[407]	2	Explainability, robustness
[408]	4	Well-being, privacy, robustness, explainability
[409]	3	Well-being, privacy, robustness
[410]	2	Privacy, robustness
[411]	2	Privacy, robustness
[412]	3	Fairness, privacy, robustness
[413]	3	Auditability, explainability, robustness
[414]	3	Robustness, governance, privacy
[415]	3	Accuracy, privacy, efficiency

From Table 9 we can see that most studies explored ways to make FL trustworthy by exploring two dimensions

only. To this end, more effort is needed to enhance the explainability of FL systems, leading to trustworthiness enhancements in FL systems. It is worth noting that most studies that discussed trustworthy aspects of FL from a broader perspective are theoretical, and therefore, implementation workflows/designs are imperative in order to make FL more trustworthy for real-world applications. Also, most studies mainly addressed one or two dimensions concerning trustworthiness [416], [417], [418], [419]. Some hardware-based solutions to accomplish trustworthiness in distributed AI systems like FL were discussed in a survey by Ağca et al. [420]. Since this is a niche area that lacks solid approaches, it therefore offers a lot of room for further research/developments in future endeavors.

The six key roles of this section are (i) highlight the need for trustworthy FL, (ii) demonstrate the six noteworthy dimensions of trustworthy FL, (iii) summarize SOTA research papers that have devised practical ways to make FL trustworthy, (iv) delving into the number as well as the name of dimensions tackled in SOTA research papers focusing on FL, (v) provide a valuable resource for researchers/practitioners who aim to work on trustworthy aspects of FL, and (vi) showcasing one important research topic/area that requires urgent attention of researchers/practitioners to lower harms of rapidly evolving technical landscape of AI. The analysis presented in this section contributes to understanding the existing works on trustworthy FL and navigating the potential harms of FL by designing next-generation FL systems that obey all six dimensions of trustworthiness.

IX. LESSONS LEARNED AND WAYS FORWARD

In this section, we highlight the important lessons learned throughout this survey and the ways forward. Specifically, we discuss past works, current issues and associated developments, and future prospects concerning FL.

A. PAST WORKS

Nowadays, large-scale data are generated in each industry, which can feed into AI models to get actionable insights. However, sensitive information in the data can hinder data sharing and subsequent knowledge discovery. The development of FL has relaxed this problem; data mobility is no longer needed. Though FL has resolved privacy, it is confronted with many other technical and social issues. For example, achieving convergence in FL in a reasonable time is challenging, particularly when data are non-i.i.d.. Similarly, the inclusion of a few highly responsive clients in global model aggregation can lead to biased global models. Sharing gradients can expose characteristics of the data, leading to privacy disclosure of various kinds. Last but not least, the characteristics of the data owned by each client can impact global model construction and convergence. In the literature, a lot of empirical and theoretical studies focusing on the upsides and downsides of FL have been published. The past research has mainly focused on advocating the bright sides of FL in terms of solving one of the crucial problems (e.g., privacy preservation). However, most of the past works have focused on implementing FL on different publicly available datasets, demonstrating FL potential in diverse tasks. In a short period, FL applications have expanded from simpler tasks such as image classification to more complex tasks (e.g., medical image analysis). As a result, many survey and research papers have been published on FL topics.

In the beginning, it was believed that FL had resolved one of the crucial problems of data privacy by not moving private data to central settings. However, after some time, researchers identified a variety of practical issues that privacy can still be leaked from FL even though the design is very secure, prompting the need to resolve this issue at a reasonable cost. Later, many different practical issues with entities (e.g., client and server) of the FL were observed, and FL became one of the most extensive research topics. The weakness of FL opened different research tracks: privacy breaching, privacy protection, poisoning attack detection, poisoning attack defenses, optimal client selection, client dropout prevention, incentivizing clients, securing client parameters, robust aggregation, and filtering wrong local models, to name just a few. Most of the past works addressed the above-cited research topics. It is worth noting that most past works implemented the FL on a few public datasets without rigorous evaluation due to the absence of a benchmark (or baseline scores) and real-world datasets. The implementation of FL on a few well-known datasets (e.g., MNIST, FashinMNIST, CIFAR10, CIFAR100, etc.) and limited evaluations hindered the wide-scale adoption of FL in different domains. It is worth noting that most of the past works assumed a reasonable # of clients of a similar nature and employed simple averaging algorithms that were not closely aligned to the real-world environments/settings. Lastly, most of the past works addressed only a limited aspect of FL, mainly privacy protection or privacy leakage. Lastly, some conventional defense methods such as DP, encryption, SMC, etc. were also integrated with FL to secure it from malicious adversaries. The main focus of most works was on privacy protection, convergence in a short time, and other optimization in FL ecosystems. The past works are discussed in the introduction, fundamentals, paradigm shift, and practical issues sections of this survey.

B. CURRENT ISSUES

Over the past few years, various new research avenues emerged under the umbrella of FL. The new research avenues are (1) introduction of two new FL types (e.g., vertical FL, hybrid FL) and settings (e.g., asynchronous FL), (2) data and model poisoning attacks in different settings of FL, (3) introduction of other security attacks (e.g., backdoor, spoofing, etc.) on FL systems, (4) changes in FL design from cross-device to cross silos, (5) new aggregation mechanisms for global model curation, and (6) working with multi-modality and non-i.i.d. data. Considering these avenues, the nature of FL research shifted to the next level,

meaning the methods/mechanisms proposed for fundamental FL (or i.i.d. data) were extended to these new avenues, bringing much-needed enhancements to the FL systems. Most of the current works focus on these avenues as opposed to the previous work which mainly focused on privacy protection or FL application in narrow domains. In recent years, the FL topic has gained a compelling interest from both academia and industry.

Recently, FL systems have been implemented not only in public datasets but also in private/customized datasets. However, we believe that most of the research topics that have been already studied for one type of FL have been investigated again for another type of FL. For example, past works have mainly focused on statistical heterogeneity in HFL, but recent works are extending the previous approaches to VFL and hybrid FL. The current issues in FL are mainly: poisoning attacks detection and mitigation, communication and computation overhead reduction, trade-off optimization, integrating FL with other technologies, robustness enhancement, data offloading, quantization of AI model, securing entire FL pipeline, reducing model size, bias reduction, preventing inference time vulnerabilities, etc. Since 2024 most researchers are mainly focusing on vertical FL [421], [422], verifiability in FL [296], [423], [424], [425], [426], edge-assisted FL [427], protecting data integrity [428], non-i.i.d. data handling [429], [430], transitioning from one server to two/more [431], drift handling [432], aggregation related optimization [433], [434], security enhancement with optimized solutions [435], [436], [437], poisoning attack prevention [438], [439], client participation enhancement [440], incentive mechanisms [441], game theory based optimizations/solutions [442], [443], copyright protection of final model [444], computation offloading [445], [446], [447], and optimizations in the related topics such as privacy preservation [448], [449], [450]. Some researchers are addressing the issues related to the trustworthiness and reliability aspects of FL. The current issues are mainly discussed in the trade-off optimization, partnership, trustworthy aspects, and practical issues section of this survey paper. However, there is still room for improvement to address these current issues at a reasonable cost.

C. FUTURE PROSPECTS

In this subsection, we pinpoint 10 hot topics for future research on FL systems. Some of the mentioned topics have been investigated in the literature, but we believe there is still room for improvement to optimize them or extend them to different settings of FL. In Figure 23, we pinpoint 10 topics for future research and development to enhance technical efficacy in FL systems. Below we concisely present the details of each topic.

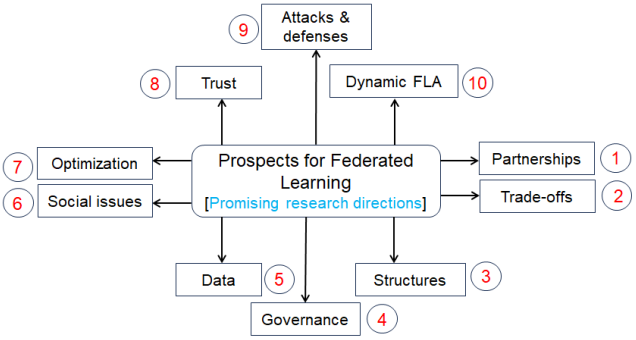

FIGURE 23. Overview of hot topics for future research on FL.

1) *Partnership with latest technologies:* FL has been integrated with many other technologies, such as DP, BC, SMC, the IoT, and cloud/edge/fog computing, to either extend applications or improve technical strengths. However, it has been minimally linked with emerging technologies like quantum computing [451], ChatGPT [452], subspace clustering, and 5G/6G technologies [453]. It is worth exploring FL partnerships with these emerging technologies to extend FL service scenarios and service delivery mechanisms.
2) *Trade-off optimization:* In FL systems, a variety of trade-offs need to be optimized, depending upon the scenario. For instance, an AI model with higher generalizability is usually required in high-stakes medical applications, but a poorly designed defense mechanism that keeps filtering out clients that have non-i.i.d. data can lead to a biased model. Using a biased model can provoke patient safety concerns in medical environments [454]. Thus, optimization of diverse trade-offs without compromising other performance indicators is a promising area for research. Some types of trade-offs, such as energy vs. privacy, energy vs. communication, and convergence vs. poisoning, have been relatively less explored. Therefore, exploring such trade-offs in diverse FL systems is a worthy research direction.
3) *Methods for diverse structures:* As stated earlier, there are diverse structures/types of FL, and the method proposed for one cannot be directly applied to another. For example, the aggregation mechanism proposed for SFL cannot be directly applied to AFL because of the difference in the arrival order of client updates [455]. Hence, it is worth studying developments in SFL, making them generic for diverse types of FL. Similarly, attacks and corresponding defense methods vary from type to type, and therefore, developing generic as well as FL-specific methods is a vibrant area of research.
4) *Data/model governance:* In FL, all clients jointly train an AI model, and therefore, there are issues related to ownership of the final model [456]. In some cases, data can be limited, and curating more data incurs additional costs for some clients [457]. However, there are few methods to pay dividends to clients whose contributions to the global model are comparatively high. Also, there is a mismatch between computing resources at each client, making it hard to properly govern AI systems. In some cases, the server shares

data or data properties with clients to ensure consistent training. However, protecting the integrity of those data or the global models is hard to guarantee. It is worth exploring methods/frameworks to ensure data/model governance in FL systems. There are some initiatives, like GPAI,[1] but more technical/regulatory solutions are needed to properly govern FL in diverse domains/sectors.

5) *Data-related problems:*Data are an indispensable component for AI development, and quality is imperative to building reliable AI systems under both CL and FL settings. In the literature, plenty of methods have been proposed to enable AI model training under FL by using both i.i.d. and non-i.i.d. data [458]. However, statistical changes in non-i.i.d. data make achieving convergence in a reasonable time challenging. Furthermore, in cross-silo FL, data are massive, unstructured, and noisy, requiring robust techniques for quality enhancement. To this end, exploring the recently developed data-centric AI [459] concept is a promising area of research. In addition, exploring and resolving data skew and heterogeneity issues in different types of FL is an attractive area for research. Lastly, detecting poisoned data upon sharing updates is a complex problem, and multidisciplinary approaches are required to detect/remove poisoned data to make FL reliable.
6) *Social issues:* As discussed earlier, in FL ecosystems, there are higher heterogeneities in clients from the perspectives of local data size, local data quality, computing resources, network infrastructure, and bandwidth requirements, to name just a few. These huge differences/disparities among clients make an FL system unfair to certain clients, leading to discrimination and bias in the global model. The use of such a model in realistic scenarios can haunt the pursuit of diversity, inclusion, and equity. In some cases, algorithmic disparity can also affect the learned model [460]. In some cases, a global model trained with imbalanced/noisy data cannot make fair predictions/classifications, leading to social issues of various kinds [461]. Lastly, FL systems can make wrong predictions about certain underrepresented groups or special groups when inadequate data are used in training the federated model, which can lead to discrimination. In this regard, a lot of effort is required to overcome the social implications of AI, including FL [462]. In the future, more socially aware FL frameworks are needed to overcome the societal perils of FL for diverse societies/populations.
7) *Optimization:* FL systems have been optimized from the perspectives of communication rounds, global and local models, bandwidth allocations, trade-off solutions, model design, network topologies, update sharing and receiving, and convergence time [463], [464]. However, with the rapid proliferation and emergence of new concepts in FL, it is challenging to accomplish optimal performance in all cases. Therefore, there is room for optimization when it comes to diverse data modalities as well as application scenarios. In some cases, the FL system needs to meet diverse performance objectives, and optimization is a non-trivial task [465]. It is worth noting that different settings for FL have different optimization requirements, which require hybrid approaches. For instance, in a cross-device setting, the challenge is to correctly reflect in the global model the updates of a million devices [466]. In contrast, the cross-silo setting needs to utilize the mammoth amounts of data held by each site. Hence, both settings require different optimization methods and models [467]. Similarly, optimization objectives for non-i.i.d. and i.i.d. settings are quite different. In some cases, a certain optimization is required based on the application scenario, which complicates the process [468]. Lastly, FL is a versatile system, meaning it has many components (data, model, clients, aggregation, anomaly detection, the global model, local models, rounds of communication, data size, etc.), and there is room for improvement in each aspect [469], [470], [471], [472]. In this regard, developing optimized solutions to enhance robustness and performance in FL by optimizing conventional procedures/pipelines is an attractive area of research.
8) *Trust enhancement/estimation:* Trust has different shades in an FL system, and quantification/ enhancement is challenging, particularly in personalized and non-i.i.d. settings. In addition, the distributed nature of FL makes it vulnerable to nefarious actors, so trust in the AI model trained under FL can be low if detection methods are not robust [473]. Although some methods have been proposed to enhance trust in FL, they require data sharing, which may violate the privacy of clients' data [474]. Some reinforcement methods have been suggested to augment trust in FL, but hefty computations in client evaluations can prolong convergence. In addition, trust quantification requires multiple criteria to be considered in the calculations, which may increase the computing complexity in trust estimation [475]. In some cases, FL has partnered with BC to establish trust [476], but this synergy is costly given the fact that BC requires a lot of memory and computations. Lastly, trust enhancement requires more data and deep training of AI models, which can increase the overall cost of building AI models under FL. All these technical issues require robust solutions in the future AI-driven era.
9) *Attacks and defenses:* Since its inception, malicious actors have attacked FL systems, ranging from data reconstruction to backdoor attacks. The distributed

[1]https://gpai.ai/

nature of the technology and weaker control over clients make it prone to attack. Thus far, many have been executed, even in the presence of defenses. Yang et al. [367] launched a model poisoning attack even though the FL system was protected by a DP mechanism. Plenty of backdoor attacks with a boundary trigger set have been designed to navigate the true behaviors of a global model under FL [429]. A plethora of privacy attacks exist, such as property inference, label disclosure, sample disclosure, class disclosure, etc. Model poisoning and data poisoning degrade the reliability of FL in many real-world cases [477]. In some, parameter sharing with the server can expose private information in the data, leading to privacy attacks [478]. Although a lot of defense mechanisms (e.g., DP, SMC, secret sharing, anonymization, and micro-aggregation) have been developed for each attack [428], [479], [480], [481], [482], [483], [484], there is still a lot of room for research. Furthermore, some attacks have been recently developed which are specific to the FL type. Lou et al. [485] devised a feature inference attack tailoring to VFL, which undermines the credibility of VFL in protecting the prediction outputs from leakage. In the current era, most of the traditional mechanisms cannot withstand emerging threats, and this area is getting the attention of researchers around the globe [486]. To this end, it is worth designing new attacks on FL and finding the corresponding defenses to increase the reliability of FL systems in realistic scenarios.

10) *Dynamic/adaptive FL architectures:* Most of the existing FL architectures (FLAs) are static, which means they cannot adapt to changing conditions (e.g., data increase or decrease, client strength increases or decreases, more or fewer malicious clients). However, in this rapidly evolving landscape of data avenues and commodities, most of the data are non-i.i.d., which requires dynamic FLAs that can tackle changing characteristics in real time. Some developments make FL more adaptive/dynamic [487], [488], but more approaches are needed to tackle different kinds of practical issues. Adaptive FLAs can be more resilient to attack, can dynamically adjust the participation of clients, and can make FL systems more autonomous, privacy-preserving, and self-optimizing so they are capable of dealing with subtle differences, particularly when the data are non-i.i.d. To this end, exploring practical approaches such as knowledge distillation, RL, and meta-learning are vibrant areas of research.

Apart from the promising directions cited above, exploring robust statistical/formal measures that can assist in distinguishing benign and malicious clients is an active area of research. Additionally, designing unified frameworks to make FL trustworthy and resilient to attack requires the attention of researchers and developers. Devising methods to verify the activities of both server and client is a promising area of research [489], [490]. Additionally, due to the diverse goals (i.e., utility, privacy, efficiency, fairness, and system security) and interdisciplinary nature of FL, the evaluation of FL algorithms is very hard [491]. To this end, robust and reliable evaluation frameworks/metrics are required to gauge the efficacy of FL in diverse domains. Recently, the fusion of quantum FL (QFL) with IoT has opened a new research track with simultaneous optimization of privacy enhancement and computational improvements [492]. Hence, investigating the potential of QFL with other technologies is a vibrant area of research. Finally, developing low-cost, end-to-end solutions that can secure the entire FL system without degrading performance can contribute to unlocking the hidden potential of this emerging technology.

X. CONCLUSION AND FUTURE WORK

This paper presented a multifaceted analysis of federated learning (FL), including the fundamentals, paradigm shifts, practical issues, and corresponding developments. It explores the integration of FL with two or more technologies, the various kinds of trade-offs in FL and the corresponding SOTA studies, as well as research on the trustworthiness aspects of FL, and promising directions for future research. In the fundamentals section, we provide the workflow of FL, major FL categorization from four different perspectives (data, resources, response, topology), comprehensive comparisons between CL and FL, and FL applications in diverse fields. In the paradigm shift section, we define paradigm shift and discuss ten different aspects to support our assertion that FL has indeed brought a kind of paradigm shift in the AI field. In the practical issues section, we highlight ten issues that are currently hindering the viability/applicability of FL in different scenarios and introduce each issue with relevant examples and supportive studies. In this section, we summarize and tabulate the SOTA literature which has been proposed to resolve each issue. In the partnership section, we discuss the integration of FL with two or more other emerging technologies that have been recently made to accomplish two objectives: (i) to extend the horizons of FL applications, and (ii) to overcome technical deficiencies in FL. Furthermore, we identify and discuss relevant SOTA studies that have been published centering on FL integration along with the purpose of each integration. In the trade-off section, we pinpoint various kinds of trade-offs that exist in FL systems, and we highlight developments that have been made to resolve them. In the trustworthy section, we depict the dimensions of trustworthy AI/FL and highlight the developments that have been made thus far in each dimension. Specifically, we provide the number of dimensions along with their names which have been covered in recent SOTA papers. In the lessons learned and ways forward section, we discuss the transition of research in FL topics by summarizing past works, current issues, and prospects. Furthermore, we provide ten different avenues for future research, which can be handy for earlier researchers to work on. Through this work, we provide a holistic overview of recent developments

in FL along with supportive studies and examples, which can pave the way to clearly understanding the FL topic from basic to advanced levels. To the best of our knowledge, this is the first work that depicts the paradigm shifts and provides a broader coverage of the practical issues, trade-offs, partnerships of FL with other technologies, trustworthy aspects, and other related developments by summarizing SOTA literature. Our work is a timely contribution intended to demonstrate the developments in the most widely researched topics of FL, and it can provide a solid foundation for future studies. In future work, we intend to discuss the promises of quantum computing in the FL landscape from a broader perspective in order to highlight recent developments in that context.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

REFERENCES

[1] G. Drainakis, K. V. Katsaros, P. Pantazopoulos, V. Sourlas, and A. Amditis, "Federated vs. Centralized machine learning under privacy-elastic users: A comparative analysis," in *Proc. IEEE 19th Int. Symp. Netw. Comput. Appl. (NCA)*, Nov. 2020, pp. 1–8.

[2] B. McMahan and D. Ramage, "Federated learning: Collaborative machine learning without centralized training data," *Google Res. Blog*, vol. 3, Jun. 2017.

[3] A. M. Elbir, B. Soner, S. Çöleri, D. Gündüz, and M. Bennis, "Federated learning in vehicular networks," in *Proc. IEEE Int. Medit. Conf. Commun. Netw. (MeditCom)*, Sep. 2022, pp. 72–77.

[4] D. C. Nguyen, Q.-V. Pham, P. N. Pathirana, M. Ding, A. Seneviratne, Z. Lin, O. Dobre, and W.-J. Hwang, "Federated learning for smart healthcare: A survey," *ACM Comput. Surveys*, vol. 55, no. 3, pp. 1–37, Mar. 2023.

[5] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, "A survey on federated learning," *Knowl.-Based Syst.*, vol. 216, Jan. 2021, Art. no. 106775.

[6] Q. Li, Z. Wen, Z. Wu, S. Hu, N. Wang, Y. Li, X. Liu, and B. He, "A survey on federated learning systems: Vision, hype and reality for data privacy and protection," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 4, pp. 3347–3366, Apr. 2023.

[7] B. Yu, W. Mao, Y. Lv, C. Zhang, and Y. Xie, "A survey on federated learning in data mining," *WIREs Data Mining Knowl. Discovery*, vol. 12, no. 1, p. e1443, Jan. 2022.

[8] S. Banabilah, M. Aloqaily, E. Alsayed, N. Malik, and Y. Jararweh, "Federated learning review: Fundamentals, enabling technologies, and future applications," *Inf. Process. Manage.*, vol. 59, no. 6, Nov. 2022, Art. no. 103061.

[9] A. E. Ouadrhiri and A. Abdelhadi, "Differential privacy for deep and federated learning: A survey," *IEEE Access*, vol. 10, pp. 22359–22380, 2022.

[10] L. Caruccio, G. Cimino, V. Deufemia, G. Iuliano, and R. Stanzione, "Surveying federated learning approaches through a multi-criteria categorization," *Multimedia Tools Appl.*, vol. 83, no. 12, pp. 36921–36951, Aug. 2023.

[11] M. Ye, X. Fang, B. Du, P. C. Yuen, and D. Tao, "Heterogeneous federated learning: State-of-the-art and research challenges," *ACM Comput. Surv.*, vol. 56, no. 3, pp. 1–44, Mar. 2024.

[12] N. Rodríguez-Barroso, D. Jiménez-López, M. V. Luzón, F. Herrera, and E. Martínez-Cámara, "Survey on federated learning threats: Concepts, taxonomy on attacks and defences, experimental study and challenges," *Inf. Fusion*, vol. 90, pp. 148–173, Feb. 2023.

[13] E. T. M. Beltrán, M. Q. Pérez, P. M. S. Sánchez, S. L. Bernal, G. Bovet, M. G. Pérez, G. M. Pérez, and A. H. Celdrán, "Decentralized federated learning: Fundamentals, state of the art, frameworks, trends, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 4, pp. 2983–3013, 3rd Quart., 2023.

[14] Y. Zhang, D. Zeng, J. Luo, Z. Xu, and I. King, "A survey of trustworthy federated learning with perspectives on security, robustness, and privacy," 2023, *arXiv:2302.10637*.

[15] T. H. Rafi, F. A. Noor, T. Hussain, and D.-K. Chae, "Fairness and privacy preserving in federated learning: A survey," *Inf. Fusion*, vol. 105, May 2024, Art. no. 102198.

[16] B. Xiao, X. Yu, W. Ni, X. Wang, and H. V. Poor, "Over-the-air federated learning: Status quo, open challenges, and future directions," *Fundam. Res.*, vol. 2024, pp. 1–10, Feb. 2024.

[17] Y. Wan, Y. Qu, W. Ni, Y. Xiang, L. Gao, and E. Hossain, "Data and model poisoning backdoor attacks on wireless federated learning, and the defense mechanisms: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, Feb. 2024, doi: 10.1109/COMST.2024.3361451.

[18] X. Xie, C. Hu, H. Ren, and J. Deng, "A survey on vulnerability of federated learning: A learning algorithm perspective," *Neurocomputing*, vol. 573, Mar. 2024, Art. no. 127225.

[19] A. Chaddad, Y. Wu, and C. Desrosiers, "Federated learning for healthcare applications," *IEEE Internet Things J.*, vol. 11, no. 5, pp. 7339–7358, Mar. 2023.

[20] T. D. Nguyen, T. Nguyen, P. L. Nguyen, H. H. Pham, K. D. Doan, and K.-S. Wong, "Backdoor attacks and defenses in federated learning: Survey, challenges and future research directions," *Eng. Appl. Artif. Intell.*, vol. 127, Jan. 2024, Art. no. 107166.

[21] J. Pei, W. Liu, J. Li, L. Wang, and C. Liu, "A review of federated learning methods in heterogeneous scenarios," *IEEE Trans. Consum. Electron.*, Apr. 2024, doi: 10.1109/TCE.2024.3385440.

[22] L. Chen, X. Ding, Z. Bao, P. Zhou, and H. Jin, "Differentially private federated learning on non-IID data: Convergence analysis and adaptive optimization," *IEEE Trans. Knowl. Data Eng.*, Mar. 2024, doi: 10.1109/TKDE.2024.3379001.

[23] M. V. Luzón, N. Rodríguez-Barroso, A. Argente-Garrido, D. Jiménez-López, J. M. Moyano, J. D. Ser, W. Ding, and F. Herrera, "A tutorial on federated learning from theory to practice: Foundations, software frameworks, exemplary use cases, and selected trends," *IEEE/CAA J. Autom. Sinica*, vol. 11, no. 4, pp. 824–850, Apr. 2024.

[24] D. Cha, M. Sung, and Y.-R. Park, "Implementing vertical federated learning using autoencoders: Practical application, generalizability, and utility study," *JMIR Med. Informat.*, vol. 9, no. 6, Jun. 2021, Art. no. e26598.

[25] K. V. Sarma, S. Harmon, T. Sanford, H. R. Roth, Z. Xu, J. Tetreault, D. Xu, M. G. Flores, A. G. Raman, R. Kulkarni, B. J. Wood, P. L. Choyke, A. M. Priester, L. S. Marks, S. S. Raman, D. Enzmann, B. Turkbey, W. Speier, and C. W. Arnold, "Federated learning improves site performance in multicenter deep learning without data sharing," *J. Amer. Med. Inform. Assoc.*, vol. 28, no. 6, pp. 1259–1264, Jun. 2021.

[26] W. Ding, M. Abdel-Basset, H. Hawash, M. Pratama, and W. Pedrycz, "Generalizable segmentation of COVID-19 infection from multi-site tomography scans: A federated learning framework," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 8, no. 1, pp. 126–139, Feb. 2023.

[27] M. G. Crowson, D. Moukheiber, A. R. Arévalo, B. D. Lam, S. Mantena, A. Rana, D. Goss, D. W. Bates, and L. A. Celi, "A systematic review of federated learning applications for biomedical data," *PLOS Digit. Health*, vol. 1, no. 5, May 2022, Art. no. e0000033.

[28] F. Ullah, G. Srivastava, H. Xiao, S. Ullah, J. C. Lin, and Y. Zhao, "A scalable federated learning approach for collaborative smart healthcare systems with intermittent clients using medical imaging," *IEEE J. Biomed. Health Informat.*, vol. 28, no. 6, pp. 3293–3304, Jun. 2023.

[29] A. Qayyum, K. Ahmad, M. A. Ahsan, A. Al-Fuqaha, and J. Qadir, "Collaborative federated learning for healthcare: Multi-modal COVID-19 diagnosis at the edge," *IEEE Open J. Comput. Soc.*, vol. 3, pp. 172–184, 2022.

[30] R. Kumar, A. A. Khan, J. Kumar, N. A. Golilarz, S. Zhang, Y. Ting, C. Zheng, and W. Wang, "Blockchain-federated-learning and deep learning models for COVID-19 detection using CT imaging," *IEEE Sensors J.*, vol. 21, no. 14, pp. 16301–16314, Jul. 2021.

[31] I. Shiri et al., "Differential privacy preserved federated learning for prognostic modeling in COVID-19 patients using large multi-institutional chest CT dataset," *Med. Phys.*, pp. 1–12, Feb. 2024, doi: 10.1002/mp.16964.

[32] D. Byrd and A. Polychroniadou, "Differentially private secure multi-party computation for federated learning in financial applications," in *Proc. 1st ACM Int. Conf. AI Finance*, Oct. 2020, pp. 1–9.

[33] Y. Xianjia, J. P. Queralta, J. Heikkonen, and T. Westerlund, "Federated learning in robotic and autonomous systems," *Proc. Comput. Sci.*, vol. 191, pp. 135–142, Jan. 2021.

[34] S. Savazzi, M. Nicoli, M. Bennis, S. Kianoush, and L. Barbieri, "Opportunities of federated learning in connected, cooperative, and automated industrial systems," *IEEE Commun. Mag.*, vol. 59, no. 2, pp. 16–21, Feb. 2021.

[35] X. Zhou, W. Liang, K. I. Wang, Z. Yan, L. T. Yang, W. Wei, J. Ma, and Q. Jin, "Decentralized P2P federated learning for privacy-preserving and resilient mobile robotic systems," *IEEE Wireless Commun.*, vol. 30, no. 2, pp. 82–89, Apr. 2023.

[36] H. Zhang, J. Bosch, and H. H. Olsson, "End-to-end federated learning for autonomous driving vehicles," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2021, pp. 1–8.

[37] Y. Li, X. Tao, X. Zhang, J. Liu, and J. Xu, "Privacy-preserved federated learning for autonomous driving," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 8423–8434, Jul. 2022.

[38] S. Lee, J. Sung, and M.-K. Shin, "Layer-wise personalized federated learning for mobile traffic prediction," *IEEE Access*, vol. 12, pp. 53126–53140, 2024.

[39] T. Zhang, L. Gao, C. He, M. Zhang, B. Krishnamachari, and A. S. Avestimehr, "Federated learning for the Internet of Things: Applications, challenges, and opportunities," *IEEE Internet Things Mag.*, vol. 5, no. 1, pp. 24–29, Mar. 2022.

[40] S. Zuo, X. Yan, R. Fan, H. Hu, H. Shan, and T. Q. S. Quek, "Byzantine-resilient federated learning with adaptivity to data heterogeneity," 2024, *arXiv:2403.13374*.

[41] J. Zhao, H. Zhu, F. Wang, Y. Zheng, R. Lu, and H. Li, "Efficient and privacy-preserving federated learning against poisoning adversaries," *IEEE Trans. Services Comput.*, Mar. 2024, doi: 10.1109/TSC.2024.3377931.

[42] P. Tam, S. Math, and S. Kim, "Optimized multi-service tasks offloading for federated learning in edge virtualization," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 6, pp. 4363–4378, Nov. 2022.

[43] S. Dong, D. Zeng, L. Gu, and S. Guo, "Offloading federated learning task to edge computing with trust execution environment," in *Proc. IEEE 17th Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, Dec. 2020, pp. 491–496.

[44] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, "A survey on security and privacy of federated learning," *Future Gener. Comput. Syst.*, vol. 115, pp. 619–640, Feb. 2021.

[45] Y. Liu, Y. Kang, T. Zou, Y. Pu, Y. He, X. Ye, Y. Ouyang, Y.-Q. Zhang, and Q. Yang, "Vertical federated learning: Concepts, advances, and challenges," *IEEE Trans. Knowl. Data Eng.*, vol. 36, no. 7, pp. 3615–3634, Jul. 2024.

[46] C. Huang, J. Huang, and X. Liu, "Cross-silo federated learning: Challenges and opportunities," 2022, *arXiv:2206.12949*.

[47] Y. Jiang, X. Luo, Y. Wu, X. Zhu, X. Xiao, and B. C. Ooi, "On data distribution leakage in cross-silo federated learning," *IEEE Trans. Knowl. Data Eng.*, vol. 36, no. 7, pp. 3312–3328, Jul. 2024.

[48] Z. Li, H. Zhou, T. Zhou, H. Yu, Z. Xu, and G. Sun, "ESync: Accelerating intra-domain federated learning in heterogeneous data centers," *IEEE Trans. Services Comput.*, vol. 15, no. 4, pp. 2261–2274, Jul. 2022.

[49] Z. Zhen, Z. Wu, L. Feng, W. Li, F. Qi, and S. Guo, "A secure and effective energy-aware fixed-point quantization scheme for asynchronous federated learning," *Comput., Mater. Continua*, vol. 75, no. 2, pp. 2939–2955, 2023.

[50] D. Stripelis and J. Luis Ambite, "Semi-synchronous federated learning for energy-efficient training and accelerated convergence in cross-silo settings," 2021, *arXiv:2102.02849*.

[51] Z. Wang, Y. Hu, S. Yan, Z. Wang, R. Hou, and C. Wu, "Efficient ring-topology decentralized federated learning with deep generative models for medical data in eHealthcare systems," *Electronics*, vol. 11, no. 10, p. 1548, May 2022.

[52] S. Hosseinalipour, S. S. Azam, C. G. Brinton, N. Michelusi, V. Aggarwal, D. J. Love, and H. Dai, "Multi-stage hybrid federated learning over large-scale D2D-enabled fog networks," *IEEE/ACM Trans. Netw.*, vol. 30, no. 4, pp. 1569–1584, Aug. 2022.

[53] P. Silva, C. Gonçalves, N. Antunes, M. Curado, and B. Walek, "Privacy risk assessment and privacy-preserving data monitoring," *Expert Syst. Appl.*, vol. 200, Aug. 2022, Art. no. 116867.

[54] E. N. Witanto, Y. E. Oktian, and S.-G. Lee, "Toward data integrity architecture for cloud-based AI systems," *Symmetry*, vol. 14, no. 2, p. 273, Jan. 2022.

[55] W. Hummer, V. Muthusamy, T. Rausch, P. Dube, K. E. Maghraoui, A. Murthi, and P. Oum, "ModelOps: Cloud-based lifecycle management for reliable and trusted AI," in *Proc. IEEE Int. Conf. Cloud Eng. (IC2E)*, Jun. 2019, pp. 113–120.

[56] B. Camajori Tedeschini, S. Savazzi, R. Stoklasa, L. Barbieri, I. Stathopoulos, M. Nicoli, and L. Serio, "Decentralized federated learning for healthcare networks: A case study on tumor segmentation," *IEEE Access*, vol. 10, pp. 8693–8708, 2022.

[57] D. Madrigal Diaz, A. Manoel, J. Chen, N. Singal, and R. Sim, "Project florida: Federated learning made easy," 2023, *arXiv:2307.11899*.

[58] A. Rauniyar, D. H. Hagos, D. Jha, J. E. Håkegård, U. Bagci, D. B. Rawat, and V. Vlassov, "Federated learning for medical applications: A taxonomy, current trends, challenges, and future research directions," *IEEE Internet Things J.*, vol. 11, no. 5, pp. 7374–7398, Mar. 2024.

[59] J. Zhu, J. Cao, D. Saxena, S. Jiang, and H. Ferradi, "Blockchain-empowered federated learning: Challenges, solutions, and future directions," *ACM Comput. Surv.*, vol. 55, no. 11, pp. 1–31, Nov. 2023.

[60] A. Qammar, A. Karim, H. Ning, and J. Ding, "Securing federated learning with blockchain: A systematic literature review," *Artif. Intell. Rev.*, vol. 56, no. 5, pp. 3951–3985, May 2023.

[61] K. Wei, J. Li, C. Ma, M. Ding, W. Chen, J. Wu, M. Tao, and H. Vincent Poor, "Personalized federated learning with differential privacy and convergence guarantee," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3454–3469, Apr. 2023, doi: 10.1109/TIFS.2020.2988575.

[62] Y. Zhou, X. Liu, Y. Fu, D. Wu, J. H. Wang, and S. Yu, "Optimizing the numbers of queries and replies in convex federated learning with differential privacy," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 6, pp. 4823–4837, Nov. 2023.

[63] F. Sabah, Y. Chen, Z. Yang, M. Azam, N. Ahmad, and R. Sarwar, "Model optimization techniques in personalized federated learning: A survey," *Expert Syst. Appl.*, vol. 243, Jun. 2024, Art. no. 122874.

[64] M. Adnan, S. Kalra, J. C. Cresswell, G. W. Taylor, and H. R. Tizhoosh, "Federated learning and differential privacy for medical image analysis," *Sci. Rep.*, vol. 12, no. 1, p. 1953, Feb. 2022.

[65] W. Oh and G. N. Nadkarni, "Federated learning in health care using structured medical data," *Adv. Kidney Disease Health*, vol. 30, no. 1, pp. 4–16, Jan. 2023.

[66] L. Li, Y. Fan, M. Tse, and K.-Y. Lin, "A review of applications in federated learning," *Comput. Ind. Eng.*, vol. 149, Jan. 2020, Art. no. 106854.

[67] K. M. J. Rahman, F. Ahmed, N. Akhter, M. Hasan, R. Amin, K. E. Aziz, A. K. M. M. Islam, M. S. H. Mukta, and A. K. M. N. Islam, "Challenges, applications and design aspects of federated learning: A survey," *IEEE Access*, vol. 9, pp. 124682–124700, 2021.

[68] Z. Zheng, Y. Zhou, Y. Sun, Z. Wang, B. Liu, and K. Li, "Applications of federated learning in smart cities: Recent advances, taxonomy, and open challenges," *Connection Sci.*, vol. 34, no. 1, pp. 1–28, Dec. 2022.

[69] G. Dhiman, S. Juneja, H. Mohafez, I. El-Bayoumy, L. K. Sharma, M. Hadizadeh, M. A. Islam, W. Viriyasitavat, and M. U. Khandaker, "Federated learning approach to protect healthcare data over big data scenario," *Sustainability*, vol. 14, no. 5, p. 2500, Feb. 2022.

[70] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, and C. Miao, "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 2031–2063, 3rd Quart., 2020.

[71] X. Ma, L. Liao, Z. Li, R. X. Lai, and M. Zhang, "Applying federated learning in software-defined networks: A survey," *Symmetry*, vol. 14, no. 2, p. 195, Jan. 2022.

[72] F. A. Khokhar, J. H. Shah, M. A. Khan, M. Sharif, U. Tariq, and S. Kadry, "A review on federated learning towards image processing," *Comput. Electr. Eng.*, vol. 99, Apr. 2022, Art. no. 107818.

[73] L. Lavaur, M.-O. Pahl, Y. Busnel, and F. Autrel, "The evolution of federated learning-based intrusion detection and mitigation: A survey," *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 3, pp. 2309–2332, Sep. 2022.

[74] T. Wang, Y. Du, Y. Gong, K.-K.-R. Choo, and Y. Guo, "Applications of federated learning in mobile health: Scoping review," *J. Med. Internet Res.*, vol. 25, May 2023, Art. no. e43006.

[75] W. Issa, N. Moustafa, B. Turnbull, N. Sohrabi, and Z. Tari, "Blockchain-based federated learning for securing Internet of Things: A comprehensive survey," *ACM Comput. Surv.*, vol. 55, no. 9, pp. 1–43, Sep. 2023.

[76] Y. Chen, S. Huang, W. Gan, G. Huang, and Y. Wu, "Federated learning for metaverse: A survey," in *Companion Proc. ACM Web Conf.*, Apr. 2023, pp. 1151–1160.

[77] V. P. Chellapandi, L. Yuan, C. G. Brinton, S. H. Żak, and Z. Wang, "Federated learning for connected and automated vehicles: A survey of existing approaches and challenges," *IEEE Trans. Intell. Vehicles*, vol. 9, no. 1, pp. 119–137, Jan. 2024.

[78] D. Sirohi, N. Kumar, P. S. Rana, S. Tanwar, R. Iqbal, and M. Hijjii, "Federated learning for 6G-enabled secure communication systems: A comprehensive survey," *Artif. Intell. Rev.*, vol. 56, no. 10, pp. 11297–11389, Oct. 2023.
[79] G. Choi, W. C. Cha, S. U. Lee, and S.-Y. Shin, "Survey of medical applications of federated learning," *Healthcare Informat. Res.*, vol. 30, no. 1, pp. 3–15, Jan. 2024.
[80] F. Liu, Z. Zheng, Y. Shi, Y. Tong, and Y. Zhang, "A survey on federated learning: A perspective from multi-party computation," *Frontiers Comput. Sci.*, vol. 18, no. 1, Feb. 2024, Art. no. 181336.
[81] H. Woisetschläger, A. Isenko, S. Wang, R. Mayer, and H.-A. Jacobsen, "A survey on efficient federated learning methods for foundation model training," 2024, *arXiv:2401.04472*.
[82] A. Bentaleb and J. Abouchabaka, "A survey of federated learning approach for the sustainable development aspect: Elearning," in *Proc. E3S Web Conf.*, vol. 477, 2024, p. 55.
[83] H. Hafi, B. Brik, P. A. Frangoudis, A. Ksentini, and M. Bagaa, "Split federated learning for 6G enabled-networks: Requirements, challenges, and future directions," *IEEE Access*, vol. 12, pp. 9890–9930, 2024.
[84] N. Rana and H. Marwaha, "Federated learning for predictive healthcare analytics: From theory to real world applications," in *Proc. BIO Web Conf.*, vol. 86, 2024, p. 1003.
[85] N. Simić, S. Suzić, N. Milošević, V. Stanojev, T. Nosek, B. Popović, and D. Bajović, "Enhancing emotion recognition through federated learning: A multimodal approach with convolutional neural networks," *Appl. Sci.*, vol. 14, no. 4, p. 1325, Feb. 2024.
[86] X. Yang, H. Yu, X. Gao, H. Wang, J. Zhang, and T. Li, "Federated continual learning via knowledge fusion: A survey," *IEEE Trans. Knowl. Data Eng.*, pp. 1–20, Feb. 2024, doi: 10.1109/TKDE.2024.3363240.
[87] X. Tan, "Privacy preserving machine learning in energy services: A survey," in *Proc. 4th Int. Conf. Comput. Vis. Data Mining (ICCVDM)*, Feb. 2024, pp. 347–356.
[88] H. Guan, P.-T. Yap, A. Bozoki, and M. Liu, "Federated learning for medical image analysis: A survey," *Pattern Recognit.*, vol. 151, Jul. 2024, Art. no. 110424.
[89] S. O. Hwang and A. Majeed, "Analysis of federated learning paradigm in medical domain: Taking COVID-19 as an application use case," *Appl. Sci.*, vol. 14, no. 10, p. 4100, May 2024.
[90] G. Xu, H. Li, S. Liu, K. Yang, and X. Lin, "VerifyNet: Secure and verifiable federated learning," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 911–926, 2020.
[91] L. Wu, Y. Jin, Y. Yan, and K. Hao, "FL-OTCSEnc: Towards secure federated learning with deep compressed sensing," *Knowl.-Based Syst.*, vol. 291, May 2024, Art. no. 111534.
[92] R. Du, X. Li, D. He, and K.-K. R. Choo, "Towards secure and verifiable hybrid federated learning," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 2935–2950, Jan. 2024, doi: 10.1109/TIFS.2024.3357288.
[93] Z. Wang, G. Yang, H. Dai, and Y. Bai, "DAFL: Domain adaptation-based federated learning for privacy-preserving biometric recognition," *Future Gener. Comput. Syst.*, vol. 150, pp. 436–450, Jan. 2024.
[94] S. I. Hasan, S. F. Nimmy, and M. S. Kamal, "Counterfactual explanations and federated learning for enhanced data analytics optimisation," in *Applied Multi-objective Optimization*. Cham, Switzerland: Springer, 2024, pp. 21–43.
[95] M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, pp. 1–9, Mar. 2020.
[96] H. N. C. Neto, J. Hribar, I. Dusparic, D. M. F. Mattos, and N. C. Fernandes, "A survey on securing federated learning: Analysis of applications, attacks, challenges, and trends," *IEEE Access*, vol. 11, pp. 41928–41953, 2023.
[97] S. Trindade, L. F. Bittencourt, and N. L. S. D. Fonseca, "Resource management at the network edge for federated learning," *Digit. Commun. Netw.*, Oct. 2022, doi: 10.1016/j.dcan.2022.10.015.
[98] S. Wang, S. Hosseinalipour, V. Aggarwal, C. G. Brinton, D. J. Love, W. Su, and M. Chiang, "Towards cooperative federated learning over heterogeneous edge/fog networks," *IEEE Commun. Mag.*, vol. 61, no. 12, pp. 54–60, Dec. 2023.
[99] H. Zhou, Y. Zheng, and X. Jia, "Towards robust and privacy-preserving federated learning in edge computing," *Comput. Netw.*, vol. 243, Apr. 2024, Art. no. 110321.
[100] A. Kumar and S. N. Srirama, "FIDEL: Fog integrated federated learning framework to train neural networks," *Softw., Pract. Exper.*, vol. 54, no. 2, pp. 186–207, Feb. 2024.
[101] M. M. Salim, A. E. Azzaoui, X. Deng, and J. H. Park, "FL-CTIF: A federated learning based CTI framework based on information fusion for secure IIoT," *Inf. Fusion*, vol. 102, Feb. 2024, Art. no. 102074.
[102] T. Muazu, Y. Mao, A. U. Muhammad, M. Ibrahim, U. M. M. Kumshe, and O. Samuel, "A federated learning system with data fusion for healthcare using multi-party computation and additive secret sharing," *Comput. Commun.*, vol. 216, pp. 168–182, Feb. 2024.
[103] S. A. Rieyan, M. R. K. News, A. B. M. M. Rahman, S. A. Khan, S. T. J. Zaarif, M. G. R. Alam, M. M. Hassan, M. Ianni, and G. Fortino, "An advanced data fabric architecture leveraging homomorphic encryption and federated learning," *Inf. Fusion*, vol. 102, Feb. 2024, Art. no. 102004.
[104] S. H. Alsamhi, R. Myrzashova, A. Hawbani, S. Kumar, S. Srivastava, L. Zhao, X. Wei, M. Guizan, and E. Curry, "Federated learning meets blockchain in decentralized data sharing: Healthcare use case," *IEEE Internet Things J.*, vol. 11, no. 11, pp. 19602–19615, Jun. 2024.
[105] A. Lakhan, H. Hamouda, K. H. Abdulkareem, S. Alyahya, and M. A. Mohammed, "Digital healthcare framework for patients with disabilities based on deep federated learning schemes," *Comput. Biol. Med.*, vol. 169, Feb. 2024, Art. no. 107845.
[106] J. Tu, J. Huang, L. Yang, and W. Lin, "Personalized federated learning with layer-wise feature transformation via meta-learning," *ACM Trans. Knowl. Discovery Data*, vol. 18, no. 4, pp. 1–21, May 2024.
[107] X. Chen, Y. Huang, Z. Xie, and J. Pang, "HyperFedNet: Communication-efficient personalized federated learning via hypernetwork," 2024, *arXiv:2402.18445*.
[108] Y. Huang, S. Zhu, W. Chen, and Z. Huang, "FedAFR: Enhancing federated learning with adaptive feature reconstruction," *Comput. Commun.*, vol. 214, pp. 215–222, Jan. 2024.
[109] L. Wang, Y. Zhao, J. Dong, A. Yin, Q. Li, X. Wang, D. Niyato, and Q. Zhu, "Federated learning with new knowledge: Fundamentals, advances, and futures," 2024, *arXiv:2402.02268*.
[110] Z. Wang, J. Xiao, L. Wang, and J. Yao, "A novel federated learning approach with knowledge transfer for credit scoring," *Decis. Support Syst.*, vol. 177, Feb. 2024, Art. no. 114084.
[111] J. Wang, X. Yang, S. Cui, L. Che, L. Lyu, D. D. Xu, and F. Ma, "Towards personalized federated learning via heterogeneous model reassembly," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 36, 2024, pp. 1–12.
[112] K. Guo, Y. Ding, J. Liang, R. He, Z. Wang, and T. Tan, "Not all minorities are equal: Empty-Class-Aware distillation for heterogeneous federated learning," 2024, *arXiv:2401.02329*.
[113] Z. Liu, J. Guo, W. Yang, J. Fan, K.-Y. Lam, and J. Zhao, "Dynamic user clustering for efficient and privacy-preserving federated learning," *IEEE Trans. Dependable Secure Comput.*, Jan. 2024, doi: 10.1109/TDSC.2024.3355458.
[114] Z. Feng, "IoT data sharing technology based on blockchain and federated learning algorithms," *Intell. Syst. Appl.*, vol. 22, Jun. 2024, Art. no. 200359.
[115] H. Xu and T. Shu, "Defending against model poisoning attack in federated learning: A variance-minimization approach," *J. Inf. Secur. Appl.*, vol. 82, May 2024, Art. no. 103744.
[116] Y. Wang, Y. Xia, and Y. Zhan, "ELITE: Defending federated learning against Byzantine attacks based on information entropy," in *Proc. China Autom. Congr. (CAC)*, Oct. 2021, pp. 6049–6054.
[117] V. Shejwalkar and A. Houmansadr, "Manipulating the Byzantine: Optimizing model poisoning attacks and defenses for federated learning," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2021, pp. 1–19.
[118] A. Panda, S. Mahloujifar, A. N. Bhagoji, S. Chakraborty, and P. Mittal, "SparseFed: Mitigating model poisoning attacks in federated learning with sparsification," in *Proc. Int. Conf. Artif. Intell. Statist.*, 2022, pp. 7587–7624.
[119] Z. Zhang and R. Hu, "Byzantine-robust federated learning with variance reduction and differential privacy," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2023, pp. 1–9.
[120] H. Yang, D. Gu, and J. He, "DeMAC: Towards detecting model poisoning attacks in federated learning system," *Internet Things*, vol. 23, Oct. 2023, Art. no. 100875.
[121] C. Zhu, S. Roos, and L. Y. Chen, "LeadFL: Client self-defense against model poisoning in federated learning," in *Proc. Int. Conf. Mach. Learn.*, 2023, pp. 43158–43180.
[122] H. Yang, D. Gu, and J. He, "A robust and efficient federated learning algorithm against adaptive model poisoning attacks," *IEEE Internet Things J.*, vol. 11, no. 9, pp. 16289–16302, May 2024.

[123] J. Wang, X. Chang, J. Mišić, V. B. Mišić, L. Li, and Y. Yao, "CRS-FL: Conditional random sampling for communication-efficient and privacy-preserving federated learning," 2023, *arXiv:2306.00674*.

[124] R. Akai, M. Kuribayashi, and N. Funabiki, "A study on eliminating biased node in federated learning," in *Proc. Asia–Pacific Signal Inf. Process. Assoc. Annu. Summit Conf. (APSIPA ASC)*, Oct. 2023, pp. 620–627.

[125] A. Mora, A. Bujari, and P. Bellavista, "Enhancing generalization in federated learning with heterogeneous data: A comparative literature review," *Future Gener. Comput. Syst.*, vol. 157, pp. 1–15, Aug. 2024.

[126] Y. Tang, Y. Liang, Y. Liu, J. Zhang, L. Ni, and L. Qi, "Reliable federated learning based on dual-reputation reverse auction mechanism in Internet of Things," *Future Gener. Comput. Syst.*, vol. 156, pp. 269–284, Jul. 2024.

[127] W. Wei, L. Liu, M. Loper, K. H. Chow, and M. E. Gursoy, "A framework for evaluating client privacy leakages in federated learning," in *Proc. Eur. Symp. Res. Comput. Security*, 2020, pp. 545–566.

[128] S. Yagli, A. Dytso, and H. Vincent Poor, "Information-theoretic bounds on the generalization error and privacy leakage in federated learning," in *Proc. IEEE 21st Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, May 2020, pp. 1–5.

[129] X. Yuan, X. Ma, L. Zhang, Y. Fang, and D. Wu, "Beyond class-level privacy leakage: Breaking record-level privacy in federated learning," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2555–2565, Feb. 2022.

[130] J. Yang, S. Chen, G. Wang, Z. Wang, Z. Jie, and M. Arif, "GFL-ALDPA: A gradient compression federated learning framework based on adaptive local differential privacy budget allocation," *Multimedia Tools Appl.*, vol. 83, no. 9, pp. 26349–26368, Aug. 2023.

[131] S. A. Farooqi, A. A. Rahman, and A. Saad, "Differential privacy based federated learning techniques in IoMT: A review," in *Proc. 18th Int. Conf. Ubiquitous Inf. Manage. Commun. (IMCOM)*, Jan. 2024, pp. 1–7.

[132] Y. S. Narule and K. S. Thakre, "Privacy preservation using optimized federated learning: A critical survey," *Intell. Decis. Technol.*, vol. 18, no. 1, pp. 135–149, Feb. 2024.

[133] S. Mohammadi, A. Balador, S. Sinaei, and F. Flammini, "Balancing privacy and performance in federated learning: A systematic literature review on methods and metrics," *J. Parallel Distrib. Comput.*, vol. 192, Oct. 2024, Art. no. 104918.

[134] H. Duan, Z. Peng, L. Xiang, Y. Hu, and B. Li, "A verifiable and privacy-preserving federated learning training framework," *IEEE Trans. Dependable Secure Comput.*, Feb. 2024, doi: 10.1109/TDSC.2024.3369658.

[135] J. Wang, L. Xiong, Z. Liu, H. Wang, and C. Li, "A flexible and privacy-preserving federated learning framework based on logistic regression," *Comput. Electr. Eng.*, vol. 116, May 2024, Art. no. 109189.

[136] J. Xia, P. Li, Y. Mao, and M. Wu, "PT-ADP: A personalized privacy-preserving federated learning scheme based on transaction mechanism," *Inf. Sci.*, vol. 669, May 2024, Art. no. 120519.

[137] Y. Shi, H. Yu, and C. Leung, "Towards fairness-aware federated learning," *IEEE Trans. Neural Netw. Learn. Syst.*, early access, Apr. 10, 2023, doi: 10.1109/TNNLS.2023.3263594.

[138] Y. H. Ezzeldin, S. Yan, C. He, E. Ferrara, and A. S. Avestimehr, "FairFed: Enabling group fairness in federated learning," in *Proc. AAAI Conf. Artif. Intell.*, vol. 37, 2023, pp. 7494–7502.

[139] C. Lewis, V. Varadharajan, N. Noman, and U. Tupakula, "Ensuring fairness and gradient privacy in personalized heterogeneous federated learning," *ACM Trans. Intell. Syst. Technol.*, vol. 15, no. 3, pp. 1–30, Jun. 2024.

[140] F. Galli, K. Jung, S. Biswas, C. Palamidessi, and T. Cucinotta, "Advancing personalized federated learning: Group privacy, fairness, and beyond," *Social Netw. Comput. Sci.*, vol. 4, no. 6, p. 831, Oct. 2023.

[141] Z. Zhou, L. Chu, C. Liu, L. Wang, J. Pei, and Y. Zhang, "Towards fair federated learning," in *Proc.27th ACM SIGKDD Conf. Knowl. Discovery Data Mining*, Aug. 2021, pp. 4100–4101.

[142] O. T. Odeyomi, "Differentially private online federated learning with personalization and fairness," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2023, pp. 1955–1960.

[143] S. Rai, A. Kumari, and D. K. Prasad, "Client selection in federated learning under imperfections in environment," *AI*, vol. 3, no. 1, pp. 124–145, Feb. 2022.

[144] M. Duan, D. Liu, X. Chen, R. Liu, Y. Tan, and L. Liang, "Self-balancing federated learning with global imbalanced data in mobile systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 1, pp. 59–71, Jan. 2021.

[145] W. Zhang, X. Wang, P. Zhou, W. Wu, and X. Zhang, "Client selection for federated learning with non-IID data in mobile edge computing," *IEEE Access*, vol. 9, pp. 24462–24474, 2021.

[146] S. Abdulrahman, H. Tout, A. Mourad, and C. Talhi, "FedMCCS: Multicriteria client selection model for optimal IoT federated learning," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4723–4735, Mar. 2021.

[147] H. Zhang, Z. Xie, R. Zarei, T. Wu, and K. Chen, "Adaptive client selection in resource constrained federated learning systems: A deep reinforcement learning approach," *IEEE Access*, vol. 9, pp. 98423–98432, 2021.

[148] J. Leng, Z. Lin, M. Ding, P. Wang, D. Smith, and B. Vucetic, "Client scheduling in wireless federated learning based on channel and learning qualities," *IEEE Wireless Commun. Lett.*, vol. 11, no. 4, pp. 732–735, Apr. 2022.

[149] W. Xia, T. Q. S. Quek, K. Guo, W. Wen, H. H. Yang, and H. Zhu, "Multi-armed bandit-based client scheduling for federated learning," *IEEE Trans. Wireless Commun.*, vol. 19, no. 11, pp. 7108–7123, Nov. 2020.

[150] H. Ko, J. Lee, S. Seo, S. Pack, and V. C. M. Leung, "Joint client selection and bandwidth allocation algorithm for federated learning," *IEEE Trans. Mobile Comput.*, vol. 22, no. 6, pp. 3380–3390, Jun. 2023.

[151] Y. Fan, W. Xi, H. Zhu, and J. Zhao, "MiniPFL: Mini federations for hierarchical personalized federated learning," *Future Gener. Comput. Syst.*, vol. 157, pp. 41–50, Aug. 2024.

[152] L. Yang, J. He, Y. Fu, and Z. Luo, "Federated learning for medical imaging segmentation via dynamic aggregation on non-IID data silos," *Electronics*, vol. 12, no. 7, p. 1687, Apr. 2023.

[153] X. Huang, Y. Ding, Z. L. Jiang, S. Qi, X. Wang, and Q. Liao, "DP-FL: A novel differentially private federated learning framework for the unbalanced data," *World Wide Web*, vol. 23, no. 4, pp. 2529–2545, Jul. 2020.

[154] D. C. Verma, G. White, S. Julier, S. Pasteris, S. Chakraborty, and G. Cirincione, "Approaches to address the data skew problem in federated learning," *Proc. SPIE*, vol. 11006, pp. 542–557, Oct. 2019.

[155] S. A. Tijani, X. Ma, R. Zhang, F. Jiang, and R. Doss, "Federated learning with extreme label skew: A data extension approach," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2021, pp. 1–8.

[156] X. Fang, M. Ye, and X. Yang, "Robust heterogeneous federated learning under data corruption," in *Proc. IEEE/CVF Int. Conf. Comput. Vis. (ICCV)*, Oct. 2023, pp. 5020–5030.

[157] W. Huang, M. Ye, Z. Shi, and B. Du, "Generalizable heterogeneous federated cross-correlation and instance similarity learning," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 46, no. 2, pp. 712–728, Feb. 2024.

[158] S. Ayromlou, "Incremental learning and federated learning for heterogeneous medical image analysis," Ph.D. dissertation, Dept. Elect. Comput. Eng., Univ. British Columbia, Vancouver, BC, Canada, 2023.

[159] Y. Diao, Q. Li, and B. He, "Exploiting label skews in federated learning with model concatenation," 2023, *arXiv:2312.06290*.

[160] O. Shalom, A. Leshem, and W. U. Bajwa, "Mitigating data injection attacks on federated learning," 2023, *arXiv:2312.02102*.

[161] M. Vucovich, D. Quinn, K. Choi, C. Redino, A. Rahman, and E. Bowen, "FedBayes: A zero-trust federated learning aggregation to defend against adversarial attacks," 2023, *arXiv:2312.04587*.

[162] S. Bashir, T. Dagiuklas, K. Kassai, and M. Iqbal, "Architectural blueprint for heterogeneity-resilient federated learning," 2024, *arXiv:2403.04546*.

[163] V. Tolpegin, S. Truex, M. E. Gursoy, and L. Liu, "Data poisoning attacks against federated learning systems," in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2020, pp. 480–501.

[164] A. Schlesinger, K. P. O'Hara, and A. S. Taylor, "Let's talk about race: Identity, chatbots, and AI," in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, Apr. 2018, pp. 1–14.

[165] N. Bouacida and P. Mohapatra, "Vulnerabilities in federated learning," *IEEE Access*, vol. 9, pp. 63229–63249, 2021.

[166] P. Liu, X. Xu, and W. Wang, "Threats, attacks and defenses to federated learning: Issues, taxonomy and perspectives," *Cybersecurity*, vol. 5, no. 1, p. 4, Dec. 2022.

[167] X. Mu, K. Cheng, Y. Shen, X. Li, Z. Chang, T. Zhang, and X. Ma, "FedDMC: Efficient and robust federated learning via detecting malicious clients," *IEEE Trans. Dependable Secure Comput.*, pp. 1–16, Mar. 2024, doi: 10.1109/TDSC.2024.3372634.

[168] X. Li, M. Wen, S. He, R. Lu, and L. Wang, "A privacy-preserving federated learning scheme against poisoning attacks in smart grid," *IEEE Internet Things J.*, vol. 11, no. 9, pp. 16805–16816, May 2024.

[169] Y. Ren, M. Hu, Z. Yang, G. Feng, and X. Zhang, "BPFL: Blockchain-based privacy-preserving federated learning against poisoning attack," *Inf. Sci.*, vol. 665, Apr. 2024, Art. no. 120377.
[170] N. Dong, Z. Wang, J. Sun, M. Kampffmeyer, W. Knottenbelt, and E. Xing, "Defending against poisoning attacks in federated learning with blockchain," *IEEE Trans. Artif. Intell.*, vol. 1, no. 1, pp. 1–13, Feb. 2024.
[171] C. Shi, S. Ji, X. Pan, X. Zhang, M. Zhang, M. Yang, J. Zhou, J. Yin, and T. Wang, "Towards practical backdoor attacks on federated learning systems," *IEEE Trans. Dependable Secure Comput.*, pp. 1–16, Mar. 2024, doi: 10.1109/TDSC.2024.3376790.
[172] L. Fang, L. Wang, and H. Li, "Iterative and mixed-spaces image gradient inversion attack in federated learning," *Cybersecurity*, vol. 7, no. 1, p. 35, Apr. 2024.
[173] K. Li and C. Xiao, "CBFL: A communication-efficient federated learning framework from data redundancy perspective," *IEEE Syst. J.*, vol. 16, no. 4, pp. 5572–5583, Dec. 2022.
[174] J. Wang, X. Chang, J. Mišić, V. B. Mišić, Z. Chen, and J. Fan, "PA-iMFL: Communication-efficient privacy amplification method against data reconstruction attack in improved multilayer federated learning," *IEEE Internet Things J.*, vol. 11, no. 10, pp. 17960–17974, May 2024.
[175] J. Tong, Z. Chen, L. Fu, J. Zhang, and Z. Han, "From learning to analytics: Improving model efficacy with goal-directed client selection," *IEEE Trans. Mobile Comput.*, pp. 1–14, Mar. 2024, doi: 10.1109/TMC.2024.3383038.
[176] Z. Chen, D. Li, R. Ni, J. Zhu, and S. Zhang, "FedSeq: A hybrid federated learning framework based on sequential in-cluster training," *IEEE Syst. J.*, vol. 17, no. 3, pp. 4038–4049, Jul. 2023.
[177] Y. Li, F. Li, L. Chen, L. Zhu, P. Zhou, and Y. Wang, "Power of redundancy: Surplus client scheduling for federated learning against user uncertainties," *IEEE Trans. Mobile Comput.*, vol. 22, no. 9, pp. 5449–5462, Jul. 2023.
[178] M.-D. Nguyen, S.-M. Lee, Q.-V. Pham, D. T. Hoang, D. N. Nguyen, and W.-J. Hwang, "HCFL: A high compression approach for communication-efficient federated learning in very large scale IoT networks," *IEEE Trans. Mobile Comput.*, vol. 22, no. 11, pp. 6495–6507, Aug. 2023.
[179] Y. Jiang, S. Wang, V. Valls, B. J. Ko, W.-H. Lee, K. K. Leung, and L. Tassiulas, "Model pruning enables efficient federated learning on edge devices," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 34, no. 12, pp. 10374–10386, Nov. 2023.
[180] H. Zhu and Y. Jin, "Multi-objective evolutionary federated learning," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 31, no. 4, pp. 1310–1322, Apr. 2020.
[181] E. Hallaji, R. Razavi-Far, M. Saif, B. Wang, and Q. Yang, "Decentralized federated learning: A survey on security and privacy," *IEEE Trans. Big Data*, vol. 10, no. 2, pp. 194–213, Apr. 2024.
[182] M. Narula, J. Meena, and D. K. Vishwakarma, "A comprehensive review on federated learning for data-sensitive application: Open issues & challenges," *Eng. Appl. Artif. Intell.*, vol. 133, Jul. 2024, Art. no. 108128.
[183] Y. Sun, M. Kountouris, and J. Zhang, "How to collaborate: Towards maximizing the generalization performance in cross-silo federated learning," 2024, *arXiv:2401.13236*.
[184] Y. Sun, Y. Mao, and J. Zhang, "MimiC: Combating client dropouts in federated learning by mimicking central updates," *IEEE Trans. Mobile Comput.*, vol. 23, no. 7, pp. 7572–7584, Jul. 2024.
[185] M. Sameen and S. O. Hwang, "TIMPANY—Detection of model poisoning attacks usiNg accuracY," *IEEE Access*, vol. 9, pp. 139415–139425, 2021.
[186] Z. Yang, M. Chen, K.-K. Wong, H. V. Poor, and S. Cui, "Federated learning for 6G: Applications, challenges, and opportunities," *Engineering*, vol. 8, pp. 33–41, Jan. 2022.
[187] L. U. Khan, Z. Han, D. Niyato, and C. S. Hong, "Socially-aware-clustering-enabled federated learning for edge networks," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 3, pp. 2641–2658, Sep. 2021.
[188] S. Yang, W. Zheng, M. Xie, and X. Zhang, "Research of federated learning application methods and social responsibility," *IEEE Trans. Big Data*, pp. 1–12, Nov. 2022, doi: 10.1109/TBDATA.2022.3225688.
[189] Y. Yan, C.-M. Feng, M. Ye, W. Zuo, P. Li, R. S. M. Goh, L. Zhu, and C. L. P. Chen, "Rethinking client drift in federated learning: A logit perspective," 2023, *arXiv:2308.10162*.
[190] Y. J. Cho, D. Jhunjhunwala, T. Li, V. Smith, and G. Joshi, "To federate or not to federate: Incentivizing client participation in federated learning," in *Proc. Workshop Federated Learn., Recent Adv. New Challenges*, 2022, pp. 1–29.
[191] X. Ma, J. Zhu, Z. Lin, S. Chen, and Y. Qin, "A state-of-the-art survey on solving non-IID data in federated learning," *Future Gener. Comput. Syst.*, vol. 135, pp. 244–258, Oct. 2022.
[192] Z. Li, Y. Sun, J. Shao, Y. Mao, J. H. Wang, and J. Zhang, "Feature matching data synthesis for non-IID federated learning," *IEEE Trans. Mobile Comput.*, pp. 1–16, Feb. 2024, doi: 10.1109/TMC.2024.3365295.
[193] B. Yan, H. Zhang, M. Xu, D. Yu, and X. Cheng, "FedRFQ: Prototype-based federated learning with reduced redundancy, minimal failure, and enhanced quality," *IEEE Trans. Comput.*, vol. 73, no. 4, pp. 1086–1098, Apr. 2024.
[194] M. Moshawrab, M. Adda, A. Bouzouane, H. Ibrahim, and A. Raad, "Reviewing federated learning aggregation algorithms; strategies, contributions, limitations and future perspectives," *Electronics*, vol. 12, no. 10, p. 2287, May 2023.
[195] Y. Zhong, W. Tan, Z. Xu, S. Chen, J. Weng, and J. Weng, "WVFL: Weighted verifiable secure aggregation in federated learning," *IEEE Internet Things J.*, vol. 11, no. 11, pp. 19926–19936, Jun. 2024.
[196] X. Guo, Z. Liu, J. Li, J. Gao, B. Hou, C. Dong, and T. Baker, "VeriFL: Communication-efficient and fast verifiable aggregation for federated learning," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1736–1751, 2021.
[197] K. Pillutla, S. M. Kakade, and Z. Harchaoui, "Robust aggregation for federated learning," *IEEE Trans. Signal Process.*, vol. 70, pp. 1142–1154, 2022.
[198] J. So, C. He, C.-S. Yang, S. Li, Q. Yu, R. E. Ali, B. Guler, and S. Avestimehr, "LightSecAgg: A lightweight and versatile design for secure aggregation in federated learning," in *Proc. Mach. Learn. Syst.*, 2022, pp. 694–720.
[199] J. Nguyen, K. Malik, H. Zhan, A. Yousefpour, M. Rabbat, M. Malek, and D. Huba, "Federated learning with buffered asynchronous aggregation," in *Proc. Int. Conf. Artif. Intell. Statist.*, 2022, pp. 3581–3607.
[200] Y. Shi, P. Fan, Z. Zhu, C. Peng, F. Wang, and K. B. Letaief, "SAM: An efficient approach with selective aggregation of models in federated learning," *IEEE Internet Things J.*, vol. 11, no. 11, pp. 20769–20783, Jun. 2024.
[201] P. Qi, D. Chiaro, A. Guzzo, M. Ianni, G. Fortino, and F. Piccialli, "Model aggregation techniques in federated learning: A comprehensive survey," *Future Gener. Comput. Syst.*, vol. 150, pp. 272–293, Jan. 2024.
[202] E. T. Martínez Beltrán, Á. L. Perales Gómez, C. Feng, P. M. Sánchez Sánchez, S. López Bernal, G. Bovet, M. Gil Pérez, G. Martínez Pérez, and A. Huertas Celdrán, "Fedstellar: A platform for decentralized federated learning," *Expert Syst. Appl.*, vol. 242, May 2024, Art. no. 122861.
[203] G. Yu, X. Wang, C. Sun, Q. Wang, P. Yu, W. Ni, and R. P. Liu, "IronForge: An open, secure, fair, decentralized federated learning," *IEEE Trans. Neural Netw. Learn. Syst.*, pp. 1–15, Nov. 2024, doi: 10.1109/TNNLS.2023.3329249.
[204] M. K. Hasan, N. Jahan, M. Z. A. Nazri, S. Islam, M. A. Khan, A. I. Alzahrani, N. Alalwan, and Y. Nam, "Federated learning for computational offloading and resource management of vehicular edge computing in 6G-V2X network," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 3827–3847, Feb. 2024.
[205] B. Liu, Y. Cai, Z. Zhang, Y. Li, L. Wang, D. Li, Y. Guo, and X. Chen, "DistFL: Distribution-aware federated learning for mobile scenarios," *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 5, no. 4, pp. 1–26, Dec. 2021.
[206] L. Fu, H. Zhang, G. Gao, M. Zhang, and X. Liu, "Client selection in federated learning: Principles, challenges, and opportunities," *IEEE Internet Things J.*, vol. 10, no. 24, pp. 21811–21819, Dec. 2023.
[207] C. Xu, Y. Qu, Y. Xiang, and L. Gao, "Asynchronous federated learning on heterogeneous devices: A survey," *Comput. Sci. Rev.*, vol. 50, Nov. 2023, Art. no. 100595.
[208] W. Zellinger, V. Wieser, M. Kumar, D. Brunner, N. Shepeleva, R. Gálvez, J. Langer, L. Fischer, and B. Moser, "Beyond federated learning: On confidentiality-critical machine learning applications in industry," *Proc. Comput. Sci.*, vol. 180, pp. 734–743, Jan. 2021.
[209] A. Z. Tan, H. Yu, L. Cui, and Q. Yang, "Towards personalized federated learning," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 34, no. 12, pp. 9587–9603, Dec. 2022.
[210] S. Truex, N. Baracaldo, A. Anwar, T. Steinke, H. Ludwig, R. Zhang, and Y. Zhou, "A hybrid approach to privacy-preserving federated learning," in *Proc. 12th ACM Workshop Artif. Intell. Secur.*, Nov. 2019, pp. 1–11.
[211] R. Wang, J. Lai, X. Li, D. He, and M. K. Khan, "RPIFL: Reliable and privacy-preserving federated learning for the Internet of Things," *J. Netw. Comput. Appl.*, vol. 221, Jan. 2024, Art. no. 103768.

[212] J. Ling, J. Zheng, and J. Chen, "Efficient federated learning privacy preservation method with heterogeneous differential privacy," *Comput. Secur.*, vol. 139, Apr. 2024, Art. no. 103715.
[213] R. Wang, X. Yuan, Z. Yang, Y. Wan, M. Luo, and D. Wu, "RFLPV: A robust federated learning scheme with privacy preservation and verifiable aggregation in IoMT," *Inf. Fusion*, vol. 102, Feb. 2024, Art. no. 102029.
[214] H. Batool, A. Anjum, A. Khan, S. Izzo, C. Mazzocca, and G. Jeon, "A secure and privacy preserved infrastructure for VANETs based on federated learning with local differential privacy," *Inf. Sci.*, vol. 652, Jan. 2024, Art. no. 119717.
[215] V.-T. Tran, H.-H. Pham, and K.-S. Wong, "Personalized privacy-preserving framework for cross-silo federated learning," *IEEE Trans. Emerg. Topics Comput.*, pp. 1–12, Jan. 2024, doi: 10.1109/TETC.2024.3356068.
[216] R. Xiong, W. Ren, S. Zhao, J. He, Y. Ren, K.-K.-R. Choo, and G. Min, "CoPiFL: A collusion-resistant and privacy-preserving federated learning crowdsourcing scheme using blockchain and homomorphic encryption," *Future Gener. Comput. Syst.*, vol. 156, pp. 95–104, Jul. 2024.
[217] Z. Li, H. Chen, Y. Gao, Z. Ni, H. Xue, and H. Shao, "Staged noise perturbation for privacy-preserving federated learning," *IEEE Trans. Sustain. Comput.*, pp. 1–12, Apr. 2024, doi: 10.1109/TSUSC.2024.3381812.
[218] F. Wang, E. Hugh, and B. Li, "More than enough is too much: Adaptive defenses against gradient leakage in production federated learning," *IEEE/ACM Trans. Netw.*, pp. 1–15, Mar. 2024, doi: 10.1109/TNET.2024.3377655.
[219] Z. Li, M. Duan, S. Yu, and W. Yang, "DynamicNet: Efficient federated learning for mobile edge computing with dynamic privacy budget and aggregation weights," *IEEE Trans. Consum. Electron.*, Mar. 2024, doi: 10.1109/TCE.2024.3372696.
[220] H. Yu, Z. Liu, Y. Liu, T. Chen, M. Cong, X. Weng, D. Niyato, and Q. Yang, "A fairness-aware incentive scheme for federated learning," in *Proc. AAAI/ACM Conf. AI, Ethics, Soc.*, Feb. 2020, pp. 393–399.
[221] W. Huang, T. Li, D. Wang, S. Du, and J. Zhang, "Fairness and accuracy in federated learning," 2020, *arXiv:2012.10069*.
[222] W. Huang, T. Li, D. Wang, S. Du, J. Zhang, and T. Huang, "Fairness and accuracy in horizontal federated learning," *Inf. Sci.*, vol. 589, pp. 170–185, Apr. 2022.
[223] T. Huang, W. Lin, W. Wu, L. He, K. Li, and A. Y. Zomaya, "An efficiency-boosting client selection scheme for federated learning with fairness guarantee," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 7, pp. 1552–1564, Jul. 2021.
[224] Z. Li, Y. Zhou, D. Wu, T. Tang, and R. Wang, "Fairness-aware federated learning with unreliable links in resource-constrained Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17359–17371, Sep. 2022.
[225] Z. Fan, H. Fang, Z. Zhou, J. Pei, M. P. Friedlander, C. Liu, and Y. Zhang, "Improving fairness for data valuation in horizontal federated learning," in *Proc. IEEE 38th Int. Conf. Data Eng. (ICDE)*, May 2022, pp. 2440–2453.
[226] Z. Qu, R. Duan, L. Chen, J. Xu, Z. Lu, and Y. Liu, "Context-aware online client selection for hierarchical federated learning," *IEEE Trans. Parallel Distrib. Syst.*, vol. 33, no. 12, pp. 4353–4367, Dec. 2022.
[227] J. Pang, J. Yu, R. Zhou, and J. C. S. Lui, "An incentive auction for heterogeneous client selection in federated learning," *IEEE Trans. Mobile Comput.*, vol. 22, no. 10, pp. 5733–5750, Jun. 2022.
[228] M. Yang, H. Qian, X. Wang, Y. Zhou, and H. Zhu, "Client selection for federated learning with label noise," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 2193–2197, Feb. 2022.
[229] F. Shi, C. Hu, W. Lin, L. Fan, T. Huang, and W. Wu, "VFedCS: Optimizing client selection for volatile federated learning," *IEEE Internet Things J.*, vol. 9, no. 24, pp. 24995–25010, Dec. 2022.
[230] X. Tan, W. C. Ng, W. Y. B. Lim, Z. Xiong, D. Niyato, and H. Yu, "Reputation-aware federated learning client selection based on stochastic integer programming," *IEEE Trans. Big Data*, pp. 1–12, Jul. 2022, doi: 10.1109/TBDATA.2022.3191332.
[231] M. V. Shenoy, "HFedDI: A novel privacy preserving horizontal federated learning based scheme for IoT device identification," *J. Netw. Comput. Appl.*, vol. 214, May 2023, Art. no. 103616.
[232] A. Silvi, A. Rizzardi, D. Caldarola, B. Caputo, and M. Ciccone, "Accelerating federated learning via sequential training of grouped heterogeneous clients," *IEEE Access*, vol. 12, pp. 57043–57058, 2024.
[233] Y. Jiang, W. Zhang, and Y. Chen, "Data quality detection mechanism against label flipping attacks in federated learning," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 1625–1637, 2023.
[234] L. Zhang, T. Zhu, P. Xiong, W. Zhou, and P. S. Yu, "A game-theoretic federated learning framework for data quality improvement," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 11, pp. 10952–10966, Dec. 2022.
[235] B. Pejó and G. Biczók, "Quality inference in federated learning with secure aggregation," *IEEE Trans. Big Data*, vol. 9, no. 5, pp. 1430–1437, Oct. 2023.
[236] A. Li, L. Zhang, J. Tan, Y. Qin, J. Wang, and X.-Y. Li, "Sample-level data selection for federated learning," in *Proc. IEEE Conf. Comput. Commun.*, May 2021, pp. 1–10.
[237] Z. Zhang, G. Chen, Y. Xu, L. Huang, C. Zhang, and S. Xiao, "FedDQA: A novel regularization-based deep learning method for data quality assessment in federated learning," *Decis. Support Syst.*, vol. 180, May 2024, Art. no. 114183.
[238] Y. Chen, X. Yang, X. Qin, H. Yu, P. Chan, and Z. Shen, "Dealing with label quality disparity in federated learning," in *Federated Learning: Privacy and Incentive*. Berlin, Germany: Springer, 2020, pp. 108–121.
[239] Y. Zhao and X. Gong, "Quality-aware distributed computation and user selection for cost-effective federated learning," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, May 2021, pp. 1–6.
[240] W. Wu, L. He, W. Lin, and C. Maple, "FedProf: Selective federated learning with representation profiling," 2021, *arXiv:2102.01733*.
[241] S. Duan, C. Liu, Z. Cao, X. Jin, and P. Han, "Fed-DR-filter: Using global data representation to reduce the impact of noisy labels on the performance of federated learning," *Future Gener. Comput. Syst.*, vol. 137, pp. 336–348, Dec. 2022.
[242] Z. He, L. Yang, W. Lin, and W. Wu, "Improving accuracy and convergence in group-based federated learning on non-IID data," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 3, pp. 1389–1404, May 2023.
[243] L. Rokvic, P. Danassis, and B. Faltings, "Privacy-preserving data quality evaluation in federated learning using influence approximation," in *Proc. ICLR*. Austria: Messe Wien Exhibition Congress Center, 2023.
[244] E. M. Campos, A. G. Vidal, J. L. H. Ramos, and A. Skarmeta, "FedRDF: A robust and dynamic aggregation function against poisoning attacks in federated learning," 2024, *arXiv:2402.10082*.
[245] Y. Zhao, Y. Cao, J. Zhang, H. Huang, and Y. Liu, "FlexibleFL: Mitigating poisoning attacks with contributions in cloud-edge federated learning systems," *Inf. Sci.*, vol. 664, Apr. 2024, Art. no. 120350.
[246] Y. Huang, G. Yang, H. Zhou, H. Dai, D. Yuan, and S. Yu, "VPPFL: A verifiable privacy-preserving federated learning scheme against poisoning attacks," *Comput. Secur.*, vol. 136, Jan. 2024, Art. no. 103562.
[247] H. Kasyap and S. Tripathy, "Sine: Similarity is not enough for mitigating local model poisoning attacks in federated learning," *IEEE Trans. Dependable Secure Comput.*, pp. 1–13, Jan. 2024, doi: 10.1109/TDSC.2024.3353317.
[248] K. Li, J. Zheng, X. Yuan, W. Ni, O. B. Akan, and H. V. Poor, "Data-agnostic model poisoning against federated learning: A graph autoencoder approach," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 3465–3480, 2024.
[249] I. J. Mouri, M. Ridowan, and M. A. Adnan, "Data poisoning attacks and mitigation strategies on federated support vector machines," *Social Netw. Comput. Sci.*, vol. 5, no. 2, pp. 1–15, Jan. 2024.
[250] C. Xu, J. Ge, Y. Deng, L. Gao, M. Zhang, Y. Li, W. Zhou, and X. Zheng, "BASS: A blockchain-based asynchronous SignSGD architecture for efficient and secure federated learning," *IEEE Trans. Dependable Secure Comput.*, 2024.
[251] L. Sun, J. Tian, and G. Muhammad, "FedKC: Personalized federated learning with robustness against model poisoning attacks in the metaverse for consumer health," *IEEE Trans. Consum. Electron.*, Apr. 2024, doi: 10.1109/TCE.2024.3386932.
[252] L. Zhang, L. Shen, L. Ding, D. Tao, and L.-Y. Duan, "Fine-tuning global model via data-free knowledge distillation for non-IID federated learning," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2022, pp. 10164–10173.
[253] J. Yao, Z. Yang, W. Xu, M. Chen, and D. Niyato, "GoMORE: Global model reuse for resource-constrained wireless federated learning," *IEEE Wireless Commun. Lett.*, vol. 12, no. 9, pp. 1543–1547, Jun. 2023.
[254] Y. Jee Cho, D. Jhunjhunwala, T. Li, V. Smith, and G. Joshi, "Maximizing global model appeal in federated learning," Feb. 2022, *arXiv:2205.14840*, doi: 10.48550/arXiv.2205.14840.
[255] H. Wu and P. Wang, "Fast-convergent federated learning with adaptive weighting," *IEEE Trans. Cognit. Commun. Netw.*, vol. 7, no. 4, pp. 1078–1088, Dec. 2021.

[256] H. Wu and P. Wang, "Node selection toward faster convergence for federated learning on non-IID data," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 5, pp. 3099–3111, Sep. 2022.
[257] L. Li, X. Yu, X. Cai, X. He, and Y. Liu, "Contract-theory-based incentive mechanism for federated learning in health CrowdSensing," *IEEE Internet Things J.*, vol. 10, no. 5, pp. 4475–4489, Mar. 2023.
[258] G. Li, J. Cai, C. He, X. Zhang, and H. Chen, "Online incentive mechanism designs for asynchronous federated learning in edge computing," *IEEE Internet Things J.*, vol. 11, no. 5, pp. 7787–7804, Mar. 2024.
[259] P. Wang, Y. Yang, W. Sun, Q. Wang, B. Guo, J. He, and Y. Bi, "Federated learning with privacy-preserving incentives for aerial computing networks," *IEEE Trans. Netw. Sci. Eng.*, 2024.
[260] B. Li, S. Chen, and K. Yu, "FeDDkw—Federated learning with dynamic Kullback–Leibler-divergence weight," *ACM Trans. Asian Low-Resource Lang. Inf. Process.*, pp. 1–17, Apr. 2023, doi: 10.1145/3594779.
[261] M. Shahraki and A. J. Bidgoly, "Edge model: An efficient method to identify and reduce the effectiveness of malicious clients in federated learning," *Future Gener. Comput. Syst.*, vol. 157, pp. 459–468, Aug. 2024.
[262] S. Weng, L. Zhang, X. Zhang, and M. A. Imran, "Faster convergence on differential privacy-based federated learning," *IEEE Internet Things J.*, vol. 11, no. 12, pp. 22578–22589, Jun. 2024.
[263] X. Jiang, H. Hu, T. On, P. Lai, V. D. Mayyuri, A. Chen, D. M. Shila, A. Larmuseau, R. Jin, C. Borcea, and N. Phan, "FLSys: Toward an open ecosystem for federated learning mobile apps," *IEEE Trans. Mobile Comput.*, vol. 23, no. 1, pp. 501–519, Nov. 2022.
[264] X. Jiang, T. On, N. Phan, H. Mohammadi, V. D. Mayyuri, A. Chen, R. Jin, and C. Borcea, "Zone-based federated learning for mobile sensing data," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, Mar. 2023, pp. 141–148.
[265] G. Long, Y. Tan, J. Jiang, and C. Zhang, "Federated learning for open banking," in *Federated Learning: Privacy and Incentive*. Cham, Switzerland: Springer, 2020, pp. 240–254.
[266] N. P. Patel, R. Parekh, S. A. Amin, R. Gupta, S. Tanwar, N. Kumar, R. Iqbal, and R. Sharma, "LEAF: A federated learning-aware privacy preserving framework for healthcare ecosystem," *IEEE Trans. Netw. Service Manage.*, vol. 21, no. 1, pp. 1129–1141, Jun. 2023.
[267] J. Zhang, X. Li, K. Gu, W. Liang, and K. Li, "Secure aggregation in heterogeneous federated learning for digital ecosystems," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 1995–2003, Feb. 2024.
[268] M. M. Yaqoob, M. Alsulami, M. A. Khan, D. Alsadie, A. K. J. Saudagar, and M. AlKhathami, "Federated machine learning for skin lesion diagnosis: An asynchronous and weighted approach," *Diagnostics*, vol. 13, no. 11, p. 1964, Jun. 2023.
[269] Q. U. Ain, M. A. Khan, M. M. Yaqoob, U. F. Khattak, Z. Sajid, M. I. Khan, and A. Al-Rasheed, "Privacy-aware collaborative learning for skin cancer prediction," *Diagnostics*, vol. 13, no. 13, p. 2264, Jul. 2023.
[270] H. Fereidooni, S. Marchal, M. Miettinen, A. Mirhoseini, H. Möllering, T. D. Nguyen, P. Rieger, A.-R. Sadeghi, T. Schneider, H. Yalame, and S. Zeitouni, "SAFELearn: Secure aggregation for private federated learning," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2021, pp. 56–62.
[271] Y. Zheng, S. Lai, Y. Liu, X. Yuan, X. Yi, and C. Wang, "Aggregation service for federated learning: An efficient, secure, and more resilient realization," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 2, pp. 988–1001, Mar. 2023.
[272] J. Song, W. Wang, T. R. Gadekallu, J. Cao, and Y. Liu, "EPPDA: An efficient privacy-preserving data aggregation federated learning scheme," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 5, pp. 3047–3057, Feb. 2022.
[273] J. Tang, H. Xu, M. Wang, T. Tang, C. Peng, and H. Liao, "A flexible and scalable malicious secure aggregation protocol for federated learning," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 4174–4187, 2024.
[274] J. Gao, B. Zhang, X. Guo, T. Baker, M. Li, and Z. Liu, "Secure partial aggregation: Making federated learning more robust for industry 4.0 applications," *IEEE Trans. Ind. Informat.*, vol. 18, no. 9, pp. 6340–6348, Sep. 2022.
[275] S. Nabavirazavi, R. Taheri, and S. S. Iyengar, "Enhancing federated learning robustness through randomization and mixture," *Future Gener. Comput. Syst.*, vol. 158, pp. 28–43, Sep. 2024.
[276] N. Kourtellis, K. Katevas, and D. Perino, "FLaaS: Federated learning as a service," in *Proc. 1st Workshop Distrib. Mach. Learn.*, Dec. 2020, pp. 7–13.
[277] F. Mo, H. Haddadi, K. Katevas, E. Marin, D. Perino, and N. Kourtellis, "PPFL: Privacy-preserving federated learning with trusted execution environments," in *Proc. 19th Annu. Int. Conf. Mobile Syst., Appl., Services*, Jun. 2021, pp. 94–108.
[278] R. Parekh, N. Patel, R. Gupta, N. K. Jadav, S. Tanwar, A. Alharbi, A. Tolba, B.-C. Neagu, and M. S. Raboaca, "GeFL: Gradient encryption-aided privacy preserved federated learning for autonomous vehicles," *IEEE Access*, vol. 11, pp. 1825–1839, 2023.
[279] F. Mo, H. Haddadi, K. Katevas, E. Marin, D. Perino, and N. Kourtellis, "PPFL: Enhancing privacy in federated learning with confidential computing," *GetMobile, Mobile Comput. Commun.*, vol. 25, no. 4, pp. 35–38, Mar. 2022.
[280] A. A. Messaoud, S. B. Mokhtar, V. Nitu, and V. Schiavoni, "Shielding federated learning systems against inference attacks with ARM TrustZone," in *Proc. 23rd ACM/IFIP Int. Middleware Conf.*, Nov. 2022, pp. 335–348.
[281] F. Liu, X. Wu, S. Ge, W. Fan, and Y. Zou, "Federated learning for vision-and-language grounding problems," in *Proc. AAAI Conf. Artif. Intell.*, vol. 34, no. 7, 2020, pp. 11572–11579.
[282] M. J. Sheller, B. Edwards, G. A. Reina, J. Martin, S. Pati, A. Kotrotsou, M. Milchenko, W. Xu, D. Marcus, R. R. Colen, and S. Bakas, "Federated learning in medicine: Facilitating multi-institutional collaborations without sharing patient data," *Sci. Rep.*, vol. 10, no. 1, p. 12598, Jul. 2020.
[283] X. Li, Y. Gu, N. Dvornek, L. H. Staib, P. Ventola, and J. S. Duncan, "Multi-site fMRI analysis using privacy-preserving federated learning and domain adaptation: ABIDE results," *Med. Image Anal.*, vol. 65, Oct. 2020, Art. no. 101765.
[284] A. Saeed, F. D. Salim, T. Ozcelebi, and J. Lukkien, "Federated self-supervised learning of multisensor representations for embedded intelligence," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 1030–1040, Jan. 2021.
[285] B. Lei, Y. Liang, J. Xie, Y. Wu, E. Liang, Y. Liu, P. Yang, T. Wang, C. Liu, J. Du, X. Xiao, and S. Wang, "Hybrid federated learning with brain-region attention network for multi-center Alzheimer's disease detection," *Pattern Recognit.*, vol. 153, Sep. 2024, Art. no. 110423.
[286] M. Abdel-Basset, H. Hawash, N. Moustafa, I. Razzak, and M. A. Elfattah, "Privacy-preserved learning from non-i.I.d data in fog-assisted IoT: A federated learning approach," *Digit. Commun. Netw.*, vol. 10, no. 2, pp. 404–415, Apr. 2024.
[287] B. Xiong, X. Yang, F. Qi, and C. Xu, "A unified framework for multi-modal federated learning," *Neurocomputing*, vol. 480, pp. 110–118, Apr. 2022.
[288] J. Chen and A. Zhang, "FedMSplit: Correlation-adaptive federated multi-task learning across multimodal split networks," in *Proc. 28th ACM SIGKDD Conf. Knowl. Discovery Data Mining*, Aug. 2022, pp. 87–96.
[289] Y. Kang, Y. Liu, and X. Liang, "FedCVT: Semi-supervised vertical federated learning with cross-view training," *ACM Trans. Intell. Syst. Technol.*, vol. 13, no. 4, pp. 1–16, Aug. 2022.
[290] Z. Yan, J. Wicaksana, Z. Wang, X. Yang, and K.-T. Cheng, "Variation-aware federated learning with multi-source decentralized medical image data," *IEEE J. Biomed. Health Informat.*, vol. 25, no. 7, pp. 2615–2628, Jul. 2021.
[291] Z. Xiao, X. Xu, H. Xing, F. Song, X. Wang, and B. Zhao, "A federated learning system with enhanced feature extraction for human activity recognition," *Knowl.-Based Syst.*, vol. 229, Oct. 2021, Art. no. 107338.
[292] M. Zhang, L. Qu, P. Singh, J. Kalpathy-Cramer, and D. L. Rubin, "SplitAVG: A heterogeneity-aware federated deep learning method for medical imaging," *IEEE J. Biomed. Health Informat.*, vol. 26, no. 9, pp. 4635–4644, Sep. 2022.
[293] K. Wei, J. Li, M. Ding, C. Ma, H. H. Yang, F. Farokhi, S. Jin, T. Q. S. Quek, and H. Vincent Poor, "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3454–3469, 2020.
[294] C. Ma, J. Li, L. Shi, M. Ding, T. Wang, Z. Han, and H. V. Poor, "When federated learning meets blockchain: A new distributed learning paradigm," *IEEE Comput. Intell. Mag.*, vol. 17, no. 3, pp. 26–33, Aug. 2022.
[295] Z. Peng, J. Xu, X. Chu, S. Gao, Y. Yao, R. Gu, and Y. Tang, "VFChain: Enabling verifiable and auditable federated learning via blockchain systems," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 1, pp. 173–186, Jan. 2022.

[296] J. Cai, W. Shen, and J. Qin, "ESVFL: Efficient and secure verifiable federated learning with privacy-preserving," *Inf. Fusion*, vol. 109, Sep. 2024, Art. no. 102420.
[297] S. Ji, Y. Tan, T. Saravirta, Z. Yang, Y. Liu, L. Vasankari, S. Pan, G. Long, and A. Walid, "Emerging trends in federated learning: From model fusion to federated X learning," 2021, *arXiv:2102.12920*.
[298] A. Majeed, X. Zhang, and S. O. Hwang, "Applications and challenges of federated learning paradigm in the big data era with special emphasis on COVID-19," *Big Data Cognit. Comput.*, vol. 6, no. 4, p. 127, Oct. 2022.
[299] H. Zhang, G. Li, Y. Zhang, K. Gai, and M. Qiu, "Blockchain-based privacy-preserving medical data sharing scheme using federated learning," in *Proc. 14th Int. Conf. Knowl. Sci., Eng. Manag.* Cham, Switzerland: Springer, 2021, pp. 634–646.
[300] M. Zhou, Z. Yang, H. Yu, and S. Yu, "VDFChain: Secure and verifiable decentralized federated learning via committee-based blockchain," *J. Netw. Comput. Appl.*, vol. 223, Mar. 2024, Art. no. 103814.
[301] Z. Lei, K. Gai, J. Yu, S. Wang, L. Zhu, and K.-K. R. Choo, "Efficiency-enhanced blockchain-based client selection in heterogeneous federated learning," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Dec. 2023, pp. 289–296.
[302] M. Shayan, C. Fung, C. J. M. Yoon, and I. Beschastnikh, "Biscotti: A blockchain system for private and secure federated learning," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 7, pp. 1513–1525, Jul. 2021.
[303] Z. Yang, Y. Shi, Y. Zhou, Z. Wang, and K. Yang, "Trustworthy federated learning via blockchain," *IEEE Internet Things J.*, vol. 10, no. 1, pp. 92–109, Jan. 2023.
[304] B. Jia, X. Zhang, J. Liu, Y. Zhang, K. Huang, and Y. Liang, "Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT," *IEEE Trans. Ind. Informat.*, vol. 18, no. 6, pp. 4049–4058, Jun. 2022.
[305] J. A. Alzubi, O. A. Alzubi, A. Singh, and M. Ramachandran, "Cloud-IIoT-Based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 1080–1087, Jan. 2023.
[306] S. Ghosh and S. K. Ghosh, "FEEL: Federated learning framework for elderly healthcare using edge-IoMT," *IEEE Trans. Computat. Social Syst.*, vol. 10, no. 4, pp. 1800–1809, Jan. 2023.
[307] H. M. Khater, A. Tariq, F. Sallabi, M. A. Serhani, and E. Baraka, "Integrating cyber-physical system with federated-edge computing for diabetes detection and management," in *Proc. 5th Int. Conf. Big-data Service Intell. Comput.*, Oct. 2023, pp. 16–22.
[308] V. Stephanie, I. Khalil, M. Atiquzzaman, and X. Yi, "Trustworthy privacy-preserving hierarchical ensemble and federated learning in healthcare 4.0 with blockchain," *IEEE Trans. Ind. Informat.*, vol. 19, no. 7, pp. 7936–7945, Oct. 2022.
[309] W. Hao, N. Mehta, K. J. Liang, P. Cheng, M. El-Khamy, and L. Carin, "WAFFLe: Weight anonymized factorization for federated learning," *IEEE Access*, vol. 10, pp. 49207–49218, 2022.
[310] A. K. Nair, J. Sahoo, and E. D. Raj, "Privacy preserving federated learning framework for IoMT based big data analysis using edge computing," *Comput. Standards Interface*, vol. 86, Aug. 2023, Art. no. 103720.
[311] M. F. Khan and M. Abaoud, "Blockchain-integrated security for real-time patient monitoring in the Internet of Medical Things using federated learning," *IEEE Access*, vol. 11, pp. 117826–117850, 2023.
[312] Z. Alsulaimawi, "A non-negative matrix factorization framework for privacy-preserving and federated learning," in *Proc. IEEE 22nd Int. Workshop Multimedia Signal Process. (MMSP)*, Sep. 2020, pp. 1–6.
[313] H.-Y. Tran, J. Hu, X. Yin, and H. R. Pota, "An efficient privacy-enhancing cross-silo federated learning and applications for false data injection attack detection in smart grids," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 2538–2552, 2023.
[314] Q. Chen, Z. Wang, W. Zhang, and X. Lin, "PPT: A privacy-preserving global model training protocol for federated learning in P2P networks," *Comput. Secur.*, vol. 124, Jan. 2023, Art. no. 102966.
[315] Q. Chen, Z. Wang, J. Chen, H. Yan, and X. Lin, "Dap-FL: Federated learning flourishes by adaptive tuning and secure aggregation," *IEEE Trans. Parallel Distrib. Syst.*, vol. 34, no. 6, pp. 1923–1941, Jun. 2023.
[316] C. Wu, F. Wu, L. Lyu, Y. Huang, and X. Xie, "Communication-efficient federated learning via knowledge distillation," *Nature Commun.*, vol. 13, no. 1, p. 2032, Apr. 2022.
[317] L. Sun, R. Du, D. He, S. Zhu, R. Wang, and S. Chan, "Feature engineering framework based on secure multi-party computation in federated learning," in *Proc. IEEE 23rd Int. Conf. High Perform. Comput. Commun., 7th Int. Conf. Data Sci. Syst., 19th Int. Conf. Smart City, 7th Int. Conf. Dependability Sensor, Cloud Big Data Syst. Appl.*, Dec. 2021, pp. 487–494.
[318] C. Gu, X. Cui, X. Zhu, and D. Hu, "FL2DP: Privacy-preserving federated learning via differential privacy for artificial IoT," *IEEE Trans. Ind. Informat.*, vol. 20, no. 4, pp. 5100–5111, Apr. 2024.
[319] M. Asad, M. Aslam, S. F. Jilani, S. Shaukat, and M. Tsukada, "SHFL: K-Anonymity-Based secure hierarchical federated learning framework for smart healthcare systems," *Future Internet*, vol. 14, no. 11, p. 338, Nov. 2022.
[320] R. Gupta and T. Alam, "An efficient federated learning based intrusion detection system using LS2DNN with PBKA based lightweight privacy preservation in cloud server," *Multimedia Tools Appl.*, vol. 83, no. 15, pp. 44685–44697, Oct. 2023.
[321] J. Zhao, C. Huang, W. Wang, R. Xie, R. Dong, and S. Matwin, "Local differentially private federated learning with homomorphic encryption," *J. Supercomput.*, vol. 79, no. 17, pp. 19365–19395, Nov. 2023.
[322] A. Li, H. Yang, and Y. Chen, "Task-agnostic privacy-preserving representation learning via federated learning," in *Federated Learning: Privacy and Incentive*. Berlin, Germany: Springer, 2020, pp. 51–65.
[323] J. Jang, Y. An, and D. Choi, "Utility analysis of federated learning techniques through comparison of financial data performance," *J. Korea Inst. Inf. Secur. Cryptol.*, vol. 32, no. 2, pp. 405–416, 2022.
[324] P. Mehra and A. K. Varshney, "HFedRF: Horizontal federated random forest," in *Proc. Int. Congr. Workshop Ind. AI*. Cham, Switzerland: Springer, 2023, pp. 409–422.
[325] R. Xie, Z. Chen, C. Wu, and T. Li, "PPFGED: Federated learning for graphic element detection with privacy preservation in multi-source substation drawings," *Expert Syst. Appl.*, vol. 243, Jun. 2024, Art. no. 122758.
[326] R. Aziz, S. Banerjee, S. Bouzefrane, and T. Le Vinh, "Exploring homomorphic encryption and differential privacy techniques towards secure federated learning paradigm," *Future Internet*, vol. 15, no. 9, p. 310, Sep. 2023.
[327] C. Wu, L. Zhang, L. Xu, K.-K.-R. Choo, and L. Zhong, "Privacy-preserving serverless federated learning scheme for Internet of Things," *IEEE Internet Things J.*, vol. 11, no. 12, pp. 22429–22438, Jun. 2024.
[328] A. Kapoor and D. Kumar, "Computation and communication efficient approach for federated learning based urban sensing applications against inference attacks," *Pervas. Mobile Comput.*, vol. 98, Feb. 2024, Art. no. 101875.
[329] T. U. Islam, R. Ghasemi, and N. Mohammed, "Privacy-preserving federated learning model for healthcare data," in *Proc. IEEE 12th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2022, pp. 0281–0287.
[330] S. Deng, J. Zhang, L. Tao, X. Jiang, and F. Wang, "LSBlocFL: A secure federated learning model combining blockchain and lightweight cryptographic solutions," *Comput. Electr. Eng.*, vol. 111, Nov. 2023, Art. no. 108986.
[331] W. Li, S. Lu, and D.-L. Deng, "Quantum federated learning through blind quantum computing," *Sci. China Phys., Mech. Astron.*, vol. 64, no. 10, Oct. 2021, Art. no. 100312.
[332] P. Xu, M. Hu, T. Chen, W. Wang, and H. Jin, "LaF: Lattice-based and communication-efficient federated learning," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 2483–2496, 2022.
[333] X. Huang, P. Li, H. Du, J. Kang, D. Niyato, D. I. Kim, and Y. Wu, "Federated learning-empowered AI-generated content in wireless networks," *IEEE Netw.*, Jan. 2024, doi: 10.1109/MNET.2024.3353377.
[334] X. Wen and S. Xu, "When neural network architecture search meets federated learning parameter efficient fine tuning," in *Proc. 3rd Int. Conf. Intell. Commun. Comput. (ICC)*, Nov. 2023, pp. 180–185.
[335] H. Xu, K. P. Seng, J. Smith, and L. M. Ang, "Multi-level split federated learning for large-scale AIoT system based on smart cities," *Future Internet*, vol. 16, no. 3, p. 82, Feb. 2024.
[336] R. Yang, T. Zhao, F. R. Yu, M. Li, D. Zhang, and X. Zhao, "Blockchain-based federated learning with enhanced privacy and security using homomorphic encryption and reputation," *IEEE Internet Things J.*, vol. 11, no. 12, pp. 21674–21688, Jun. 2024.
[337] N. Marchang, "A federated learning privacy framework for missing data inference in environmental crowd sensing," *Trans. Emerg. Telecommun. Technol.*, vol. 35, no. 3, p. e4950, Mar. 2024.
[338] X. Zhang, Y. Kang, K. Chen, L. Fan, and Q. Yang, "Trading off privacy, utility, and efficiency in federated learning," *ACM Trans. Intell. Syst. Technol.*, vol. 14, no. 6, pp. 1–32, Dec. 2023.
[339] X. Gu, Z. Tianqing, J. Li, T. Zhang, W. Ren, and K.-K.-R. Choo, "Privacy, accuracy, and model fairness trade-offs in federated learning," *Comput. Secur.*, vol. 122, Nov. 2022, Art. no. 102907.
[340] Y. Yang, A. Xu, and T. Xie, "Personalized federated learning based on multi-objective optimization," SSRN, USA, 2024. [Online]. Available: https://ssrn.com/abstract=4685964

[341] D. Y. Zhang, Z. Kou, and D. Wang, "FairFL: A fair federated learning approach to reducing demographic bias in privacy-sensitive classification models," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2020, pp. 1051–1060.
[342] H. Chen, T. Zhu, T. Zhang, W. Zhou, and P. S. Yu, "Privacy and fairness in federated learning: On the perspective of tradeoff," *ACM Comput. Surv.*, vol. 56, no. 2, pp. 1–37, Feb. 2024.
[343] F. Hamman and S. Dutta, "Demystifying local and global fairness trade-offs in federated learning using partial information decomposition," 2023, *arXiv:2307.11333*.
[344] S. Javaherian, S. Panta, S. Williams, M. S. Islam, and L. Chen, "FedFair^3: Unlocking threefold fairness in federated learning," 2024, *arXiv:2401.16350*.
[345] M. Sirajul Islam, S. Javaherian, F. Xu, X. Yuan, L. Chen, and N.-F. Tzeng, "FedClust: Optimizing federated learning on non-IID data through weight-driven client clustering," 2024, *arXiv:2403.04144*.
[346] K. Sun, X. Zhang, X. Lin, G. Li, J. Wang, and J. Li, "Toward the tradeoffs between privacy, fairness and utility in federated learning," in *Proc. Int. Symp. Emerg. Inf. Secur. Appl.* Cham, Switzerland: Springer, 2023, pp. 118–132.
[347] W. Du, D. Xu, X. Wu, and H. Tong, "Fairness-aware agnostic federated learning," in *Proc. SIAM Int. Conf. Data Mining (SDM)*, 2021, pp. 181–189.
[348] J. So, R. E. Ali, B. Güler, J. Jiao, and A. S. Avestimehr, "Securing secure aggregation: Mitigating multi-round privacy leakage in federated learning," in *Proc. AAAI Conf. Artif. Intell.*, 2023, vol. 37, no. 8, pp. 9864–9873.
[349] T. Rückel, J. Sedlmeir, and P. Hofmann, "Fairness, integrity, and privacy in a scalable blockchain-based federated learning system," *Comput. Netw.*, vol. 202, Jan. 2022, Art. no. 108621.
[350] S. Lin, Y. Han, X. Li, and Z. Zhang, "Personalized federated learning towards communication efficiency, robustness and fairness," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 35, 2022, pp. 30471–30485.
[351] M. Naseri, J. Hayes, and E. De Cristofaro, "Local and central differential privacy for robustness and privacy in federated learning," 2020, *arXiv:2009.03561*.
[352] K. Wei, J. Li, C. Ma, M. Ding, C. Chen, S. Jin, Z. Han, and H. V. Poor, "Low-latency federated learning over wireless channels with differential privacy," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 1, pp. 290–307, Jan. 2022.
[353] J. Zhou, Z. Su, J. Ni, Y. Wang, Y. Pan, and R. Xing, "Personalized privacy-preserving federated learning: Optimized trade-off between utility and privacy," in *Proc. IEEE Global Commun. Conf.*, Dec. 2022, pp. 4872–4877.
[354] T. Qi, F. Wu, C. Wu, L. Lyu, T. Xu, H. Liao, Z. Yang, Y. Huang, and X. Xie, "FairVFL: A fair vertical federated learning framework with contrastive adversarial learning," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 35, 2022, pp. 7852–7865.
[355] M. Hosseinzadeh, N. Hudson, S. Heshmati, and H. Khamfroush, "Communication-loss trade-off in federated learning: A distributed client selection algorithm," in *Proc. IEEE 19th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2022, pp. 1–6.
[356] X. Lin, J. Wu, J. Li, C. Sang, S. Hu, and M. J. Deen, "Heterogeneous differential-private federated learning: Trading privacy for utility truthfully," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 6, pp. 5113–5129, Jan. 2023.
[357] J. Ma, Y. Zhou, L. Cui, and S. Guo, "An optimized sparse response mechanism for differentially private federated learning," *IEEE Trans. Dependable Secure Comput.*, pp. 1–12, Aug. 2024, doi: 10.1109/TDSC.2023.3302864.
[358] T. Salazar, M. Fernandes, H. Araújo, and P. H. Abreu, "Fair-fate: Fair federated learning with momentum," in *Proc. Int. Conf. Comput. Sci.* Cham, Switzerland: Springer, 2023, pp. 524–538.
[359] T. Salazar, J. Gama, H. Araújo, and P. Henriques Abreu, "Unveiling group-specific distributed concept drift: A fairness imperative in federated learning," 2024, *arXiv:2402.07586*.
[360] Y. M. Saputra, D. Nguyen, H. T. Dinh, Q.-V. Pham, E. Dutkiewicz, and W.-J. Hwang, "Federated learning framework with straggling mitigation and privacy-awareness for AI-based mobile application services," *IEEE Trans. Mobile Comput.*, vol. 22, no. 9, pp. 5296–5312, May 2022.
[361] M. Mestoukirdi, M. Zecchin, D. Gesbert, and Q. Li, "User-centric federated learning: Trading off wireless resources for personalization," *IEEE Trans. Mach. Learn. Commun. Netw.*, vol. 1, pp. 346–359, 2023.
[362] R. Teixeira, L. Almeida, P. Rodrigues, J. Corona, M. Antunes, and R. L. Aguiar, "Balancing privacy and explainability in federated learning," Res. Square, Durham, NC, USA, Tech. Rep., 2023, doi: 10.21203/rs.3.rs-3714454/v1.
[363] A. Li, J. Huang, J. Jia, H. Peng, L. Zhang, L. A. Tuan, H. Yu, and X.-Y. Li, "Efficient and privacy-preserving feature importance-based vertical federated learning," *IEEE Trans. Mobile Comput.*, vol. 23, no. 6, pp. 7238–7255, Jun. 2024.
[364] R. Hu, Y. Guo, and Y. Gong, "Federated learning with sparsified model perturbation: Improving accuracy under client-level differential privacy," *IEEE Trans. Mobile Comput.*, pp. 1–14, Dec. 2023, doi: 10.1109/TMC.2023.3343288.
[365] S. Lu, R. Li, W. Liu, C. Guan, and X. Yang, "Top-k sparsification with secure aggregation for privacy-preserving federated learning," *Comput. Secur.*, vol. 124, Jan. 2023, Art. no. 102993.
[366] Q. Lin, S. Jiang, Z. Zhen, T. Chen, C. Wei, and H. Lin, "Fed-PEMC: A privacy-enhanced federated deep learning algorithm for consumer electronics in mobile edge computing," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 4073–4086, Feb. 2024.
[367] M. Yang, H. Cheng, F. Chen, X. Liu, M. Wang, and X. Li, "Model poisoning attack in differential privacy-based federated learning," *Inf. Sci.*, vol. 630, pp. 158–172, Jun. 2023.
[368] L. Yin, S. Lin, Z. Sun, R. Li, Y. He, and Z. Hao, "A game-theoretic approach for federated learning: A trade-off among privacy, accuracy and energy," *Digit. Commun. Netw.*, vol. 10, no. 2, pp. 389–403, Apr. 2024.
[369] A. M. Girgis, D. Data, S. Diggavi, P. Kairouz, and A. T. Suresh, "Shuffled model of federated learning: Privacy, accuracy and communication trade-offs," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 464–478, Mar. 2021.
[370] Y. Li, X. Qin, H. Chen, K. Han, and P. Zhang, "Energy-aware edge association for cluster-based personalized federated learning," *IEEE Trans. Veh. Technol.*, vol. 71, no. 6, pp. 6756–6761, Jun. 2022.
[371] Z. Yao, J. Liu, H. Xu, L. Wang, C. Qian, and Y. Liao, "Ferrari: A personalized federated learning framework for heterogeneous edge clients," *IEEE Trans. Mobile Comput.*, pp. 1–15, Feb. 2024, doi: 10.1109/TMC.2024.3370961.
[372] Y. Zhu, J. Gong, K. Zhang, and H. Qian, "Malicious-resistant non-interactive verifiable aggregation for federated learning," *IEEE Trans. Dependable Secure Comput.*, pp. 1–17, Mar. 2024, doi: 10.1109/TDSC.2024.3380669.
[373] Z. Zhang, L. Wu, D. He, J. Li, N. Lu, and X. Wei, "Using third-party auditor to help federated learning: An efficient Byzantine-robust federated learning," *IEEE Trans. Sustain. Comput.*, pp. 1–14, Mar. 2024, doi: 10.1109/TSUSC.2024.3379440.
[374] S. Xu, H. Xia, P. Liu, R. Zhang, H. Chi, and W. Gao, "FLPM: A property modification scheme for data protection in federated learning," *Future Gener. Comput. Syst.*, vol. 154, pp. 151–159, May 2024.
[375] W. Issa, N. Moustafa, B. Turnbull, and K.-K.-R. Choo, "RVE-PFL: Robust variational encoder-based personalized federated learning against model inversion attacks," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 3772–3787, 2024.
[376] Z. Wu, S. Sun, Y. Wang, M. Liu, K. Xu, W. Wang, X. Jiang, B. Gao, and J. Lu, "FedCache: A knowledge cache-driven federated learning architecture for personalized edge intelligence," *IEEE Trans. Mobile Comput.*, pp. 1–15, Feb. 2024, doi: 10.1109/TMC.2024.3361876.
[377] W. Mao, Q. Ma, G. Liao, and X. Chen, "Game analysis and incentive mechanism design for differentially private cross-silo federated learning," *IEEE Trans. Mobile Comput.*, pp. 1–15, Feb. 2024, doi: 10.1109/TMC.2024.3364372.
[378] B. Li, P. Qi, B. Liu, S. Di, J. Liu, J. Pei, J. Yi, and B. Zhou, "Trustworthy AI: From principles to practices," *ACM Comput. Surv.*, vol. 55, no. 9, pp. 1–46, Sep. 2023.
[379] E. Barbierato and A. Gatti, "The challenges of machine learning: A critical review," *Electronics*, vol. 13, no. 2, p. 416, Jan. 2024.
[380] F. S. Grodzinsky, M. J. Wolf, and K. W. Miller, "Ethical issues from emerging AI applications: Harms are happening," *Computer*, vol. 57, no. 2, pp. 44–52, Feb. 2024.
[381] S. El-Sappagh, J. M. Alonso-Moral, T. Abuhmed, F. Ali, and A. Bugarín-Diz, "Trustworthy artificial intelligence in Alzheimer's disease: State of the art, opportunities, and challenges," *Artif. Intell. Rev.*, vol. 56, no. 10, pp. 11149–11296, Oct. 2023.
[382] B. Qi, B. Zhou, W. Zhang, J. Liu, and L. Wu, "Improving robustness of intent detection under adversarial attacks: A geometric constraint perspective," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 35, no. 5, pp. 6133–6144, May 2024.

[383] M. Mylrea and N. Robinson, "Artificial intelligence (AI) trust framework and maturity model: Applying an entropy lens to improve security, privacy, and ethical AI," *Entropy*, vol. 25, no. 10, p. 1429, Oct. 2023.
[384] W. Badawy, "Data-driven framework for evaluating digitization and artificial intelligence risk: A comprehensive analysis," *AI Ethics*, vol. 2023, pp. 1–26, Nov. 2023.
[385] G. Bonifazi, F. Cauteruccio, E. Corradini, M. Marchetti, G. Terracina, D. Ursino, and L. Virgili, "A model-agnostic, network theory-based framework for supporting XAI on classifiers," *Expert Syst. Appl.*, vol. 241, May 2024, Art. no. 122588.
[386] J. P. Lalor, A. Abbasi, K. Oketch, Y. Yang, and N. Forsgren, "Should fairness be a metric or a model? A model-based framework for assessing bias in machine learning pipelines," *ACM Trans. Inf. Syst.*, vol. 42, no. 4, pp. 1–41, Jul. 2024.
[387] H. Liu, Y. Wang, W. Fan, X. Liu, Y. Li, S. Jain, Y. Liu, A. Jain, and J. Tang, "Trustworthy AI: A computational perspective," *ACM Trans. Intell. Syst. Technol.*, vol. 14, no. 1, pp. 1–59, Feb. 2023.
[388] P. M. S. Sánchez, A. H. Celdrán, N. Xie, G. Bovet, G. M. Pérez, and B. Stiller, "FederatedTrust: A solution for trustworthy federated learning," *Future Gener. Comput. Syst.*, vol. 152, pp. 83–98, Mar. 2024.
[389] A. Tariq, M. Adel Serhani, F. Sallabi, T. Qayyum, E. S. Barka, and K. A. Shuaib, "Trustworthy federated learning: A survey," 2023, *arXiv:2305.11537*.
[390] Y. Zhang, D. Zeng, J. Luo, Z. Xu, and I. King, "A survey of trustworthy federated learning with perspectives on security, robustness and privacy," in *Proc. Companion ACM Web Conf.*, Apr. 2023, pp. 1167–1176.
[391] A. Psaltis, K. Zafeirouli, P. Leškovský, S. Bourou, J. C. Vásquez-Correa, A. García-Pablos, S. Cerezo Sánchez, A. Dimou, C. Z. Patrikakis, and P. Daras, "Fostering trustworthiness of federated learning ecosystem through realistic scenarios," *Information*, vol. 14, no. 6, p. 342, Jun. 2023.
[392] M. H. U. Rehman, A. M. Dirir, K. Salah, E. Damiani, and D. Svetinovic, "TrustFed: A framework for fair and trustworthy cross-device federated learning in IIoT," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 8485–8494, Dec. 2021.
[393] S. K. Lo, Y. Liu, Q. Lu, C. Wang, X. Xu, H.-Y. Paik, and L. Zhu, "Toward trustworthy AI: Blockchain-based architecture design for accountability and fairness of federated learning systems," *IEEE Internet Things J.*, vol. 10, no. 4, pp. 3276–3284, Feb. 2023.
[394] L. Wang, X. Zhao, Z. Lu, L. Wang, and S. Zhang, "Enhancing privacy preservation and trustworthiness for decentralized federated learning," *Inf. Sci.*, vol. 628, pp. 449–468, May 2023.
[395] M. Han, T. Zhu, and W. Zhou, "Fair federated learning with opposite GAN," *Knowledge-Based Syst.*, vol. 287, Mar. 2024, Art. no. 111420.
[396] G. Rjoub, O. A. Wahab, J. Bentahar, and A. Bataineh, "Trust-driven reinforcement selection strategy for federated learning on IoT devices," *Computing*, vol. 106, no. 4, pp. 1273–1295, Apr. 2024.
[397] Z. Yuan, Y. Tian, Z. Zhou, T. Li, S. Wang, and J. Xiong, "Trustworthy federated learning against malicious attacks in web 3.0," *IEEE Trans. Netw. Sci. Eng.*, pp. 1–14, Jan. 2024, doi: 10.1109/TNSE.2024.3350365.
[398] N. Bugshan, I. Khalil, M. S. Rahman, M. Atiquzzaman, X. Yi, and S. Badsha, "Toward trustworthy and privacy-preserving federated deep learning service framework for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 19, no. 2, pp. 1535–1547, Feb. 2023.
[399] J. Xu, J. Lin, W. Liang, and K.-C. Li, "Privacy preserving personalized blockchain reliability prediction via federated learning in IoT environments," *Cluster Comput.*, vol. 25, no. 4, pp. 2515–2526, Aug. 2022.
[400] J. Zhou, S. Pal, C. Dong, and K. Wang, "Enhancing quality of service through federated learning in edge-cloud architecture," *Ad Hoc Netw.*, vol. 156, Apr. 2024, Art. no. 103430.
[401] M. P. Singh, A. Anand, L. A. Prateek Janaswamy, S. Sundarrajan, and M. Gupta, "Trusted federated learning framework for attack detection in edge industrial Internet of Things," in *Proc. 8th Int. Conf. Fog Mobile Edge Comput. (FMEC)*, Sep. 2023, pp. 64–71.
[402] Z. Mahmood and V. Jusas, "Implementation framework for a blockchain-based federated learning model for classification problems," *Symmetry*, vol. 13, no. 7, p. 1116, Jun. 2021.
[403] H. A. Madni, R. M. Umer, and G. L. Foresti, "Blockchain-based swarm learning for the mitigation of gradient leakage in federated learning," *IEEE Access*, vol. 11, pp. 16549–16556, 2023.
[404] M. Guduri, C. Chakraborty, U. Maheswari, and M. Margala, "Blockchain-based federated learning technique for privacy preservation and security of smart electronic health records," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 2608–2617, Feb. 2024.
[405] Y. Zeng, H. Chen, and K. Lee, "Federated learning with local fairness constraints," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2023, pp. 1937–1942.
[406] N. Baracaldo, A. Anwar, M. Purcell, A. Rawat, M. Sinn, B. Altakrouri, D. Balta, M. Sellami, P. Kuhn, U. Schopp, and M. Buchinger, "Towards an accountable and reproducible federated learning: A FactSheets approach," 2022, *arXiv:2202.12443*.
[407] P. Chen, X. Du, Z. Lu, J. Wu, and P. C. K. Hung, "EVFL: An explainable vertical federated learning for data-oriented artificial intelligence systems," *J. Syst. Archit.*, vol. 126, May 2022, Art. no. 102474.
[408] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh, and G. Muhammad, "Secure and provenance enhanced Internet of Health Things framework: A blockchain managed federated learning approach," *IEEE Access*, vol. 8, pp. 205071–205087, 2020.
[409] L. Campanile, S. Marrone, F. Marulli, and L. Verde, "Challenges and trends in federated learning for well-being and healthcare," *Proc. Comput. Sci.*, vol. 207, pp. 1144–1153, Jan. 2022.
[410] Q. Yang, "Toward responsible AI: An overview of federated learning for user-centered privacy-preserving computing," *ACM Trans. Interact. Intell. Syst.*, vol. 11, nos. 3–4, pp. 1–22, Dec. 2021.
[411] L. Lyu, H. Yu, X. Ma, C. Chen, L. Sun, J. Zhao, Q. Yang, and P. S. Yu, "Privacy and robustness in federated learning: Attacks and defenses," *IEEE Trans. Neural Netw. Learn. Syst.*, 2022.
[412] X. Wu and H. Yu, "MarS-FL: Enabling competitors to collaborate in federated learning," *IEEE Trans. Big Data*, pp. 1–11, Jun. 2022, doi: 10.1109/TBDATA.2022.3186991.
[413] H. Gao, X. Pan, X. Zhang, K. Ye, P. Zhang, and L. Sun, "Towards trustworthy federated learning: A blockchain-based architecture for auditing, traceability, and verification," in *Proc. 4th Int. Conf. Comput. Sci. Commun. Technol. (ICCSCT)*, vol. 12918, Jan. 2023, pp. 580–590.
[414] W. Wei and L. Liu, "Trustworthy distributed AI systems: Robustness, privacy, and governance," *ACM Comput. Surv.*, Feb. 2024.
[415] M. Shen, J. Wang, J. Zhang, Q. Zhao, B. Peng, T. Wu, L. Zhu, and K. Xu, "Secure decentralized aggregation to prevent membership privacy leakage in edge-based federated learning," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 3, pp. 3105–3119, May 2024.
[416] Y. Tian, W. Zhang, A. Simpson, Y. Liu, and Z. L. Jiang, "Defending against data poisoning attacks: From distributed learning to federated learning," *Comput. J.*, vol. 66, no. 3, pp. 711–726, Oct. 2021.
[417] J. Castillo, P. Rieger, H. Fereidooni, Q. Chen, and A. Sadeghi, "FLEDGE: Ledger-based federated learning resilient to inference and backdoor attacks," in *Proc. Annu. Comput. Secur. Appl. Conf.*, Dec. 2023, pp. 647–661.
[418] Z. Zhou, C. Xu, M. Wang, X. Kuang, Y. Zhuang, and S. Yu, "A multi-shuffler framework to establish mutual confidence for secure federated learning," *IEEE Trans. Dependable Secure Comput.*, 2022.
[419] D. Pasquini, D. Francati, and G. Ateniese, "Eluding secure aggregation in federated learning via model inconsistency," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2022, pp. 2429–2443, doi: 10.1145/3548606.3560557.
[420] M. A. Agca, S. Faye, and D. Khadraoui, "A survey on trusted distributed artificial intelligence," *IEEE Access*, vol. 10, pp. 55308–55337, 2022.
[421] R. Zhang, H. Li, L. Tian, M. Hao, and Y. Zhang, "Vertical federated learning across heterogeneous regions for industry 4.0," *IEEE Trans. Ind. Informat.*, 2024.
[422] W. Xu, H. Zhu, Y. Zheng, F. Wang, J. Zhao, Z. Liu, and H. Li, "ELXGB: An efficient and privacy-preserving XGBoost for vertical federated learning," *IEEE Trans. Services Comput.*, vol. 17, no. 3, pp. 878–892, Apr. 2024.
[423] G. Wang, L. Zhou, Q. Li, X. Yan, X. Liu, and Y. Wu, "FVFL: A flexible and verifiable privacy-preserving federated learning scheme," *IEEE Internet Things J.*, Apr. 2024, doi: 10.1109/JIOT.2024.3385479.
[424] B. Buyukates, J. So, H. Mahdavifar, and S. Avestimehr, "LightVeriFL: A lightweight and verifiable secure aggregation for federated learning," *IEEE J. Sel. Areas Inf. Theory*, vol. 5, pp. 285–301, Apr. 2024, doi: 10.1109/JSAIT.2024.3391849.
[425] X. Mu, Y. Tian, Z. Zhou, S. Wang, and J. Xiong, "RVFL: Rational verifiable federated learning secure aggregation protocol," *IEEE Internet Things J.*, 2024.
[426] M. Kesici, B. Pal, and G. Yang, "Detection of false data injection attacks in distribution networks: A vertical federated learning approach," *IEEE Trans. Smart Grid*, May 2024, doi: 10.1109/TSG.2024.3399396.
[427] J. Liu, Z. Zhao, X. Luo, P. Li, G. Min, and H. Li, "SlaugFL: Efficient edge federated learning with selective GAN-based data augmentation," *IEEE Trans. Mobile Comput.*, pp. 1–18, May 2024, doi: 10.1109/TMC.2024.3397585.

[428] Z. Zhang and Y. Li, "NSPFL: A novel secure and privacy-preserving federated learning with data integrity auditing," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 4494–4506, Mar. 2024.
[429] S. Cheng, P. Li, R. Wang, and H. Xu, "Differentially private federated learning with non-IID data," *Computing*, vol. 2024, pp. 1–30, May 2024.
[430] L. Wu, S. Guo, Y. Ding, J. Wang, W. Xu, Y. Zhan, and A.-M. Kermarrec, "Rethinking personalized client collaboration in federated learning," *IEEE Trans. Mobile Comput.*, 2024.
[431] L. Zhong, L. Wang, L. Zhang, J. Domingo-Ferrer, L. Xu, C. Wu, and R. Zhang, "Dual-server based lightweight privacy-preserving federated learning," *IEEE Trans. Netw. Service Manage.*, May 2024, doi: 10.1109/TNSM.2024.3399534.
[432] H. Kang, M. Kim, B. Lee, and H. Kim, "FedAND: Federated learning exploiting consensus ADMM by nulling drift," *IEEE Trans. Ind. Informat.*, pp. 1–13, Apr. 2024, doi: 10.1109/TII.2024.3380742.
[433] A. Song, H. Li, K. Cheng, T. Zhang, A. Sun, and Y. Shen, "Guard-FL: An UMAP-assisted robust aggregation for federated learning," *IEEE Internet Things J.*, May 2024, doi: 10.1109/JIOT.2024.3399259.
[434] X. Sun, Z. Yuan, X. Kong, L. Xue, L. He, and Y. Lin, "Communication-efficient and privacy-preserving aggregation in federated learning with adaptability," *IEEE Internet Things J.*, May 2024, doi: 10.1109/JIOT.2024.3396217.
[435] C. Hu and B. Li, "MASKCRYPT: Federated learning with selective homomorphic encryption," *IEEE Trans. Dependable Secure Comput.*, pp. 1–14, Apr. 2024, doi: 10.1109/TDSC.2024.3392424.
[436] R. U. Haque, A. S. M. Touhidul Hasan, M. A. M. Al-Hababi, Y. Zhang, and D. Xu, "SSI-FL: Self-sovereign identity based privacy-preserving federated learning," *J. Parallel Distrib. Comput.*, vol. 191, pp. 1–13, Apr. 2024, Art. no. 104907, doi: 10.1016/j.jpdc.2024.104907.
[437] J. Li, Y. Tian, Z. Zhou, A. Xiang, S. Wang, and J. Xiong, "PSFL: Ensuring data privacy and model security for federated learning," *IEEE Internet Things J.*, 2024.
[438] E. S. Erdol, B. Ustubioglu, H. Erdol, and G. Ulutas, "Low dimensional secure federated learning framework against poisoning attacks," *Future Gener. Comput. Syst.*, vol. 158, pp. 183–199, Sep. 2024.
[439] F. Zhang, H. Huang, Z. Chen, and Z. Huang, "Robust and privacy-preserving federated learning with distributed additive encryption against poisoning attacks," *Comput. Netw.*, vol. 245, May 2024, Art. no. 110383.
[440] S. Lee, T. Zhang, S. Prakash, Y. Niu, and S. Avestimehr, "Embracing federated learning: Enabling weak client participation via partial model training," *IEEE Trans. Mobile Comput.*, 2024.
[441] M. Li, Y. Tian, J. Zhang, Z. Zhou, D. Zhao, and J. Ma, "IMFL: An incentive mechanism for federated learning with personalized protection," *IEEE Internet Things J.*, Apr. 2024, doi: 10.1109/JIOT.2024.3387973.
[442] G. Hu, J. Han, J. Lu, J. Yu, S. Qiu, H. Peng, D. Zhu, and T. Li, "Game-theoretic design of quality-aware incentive mechanisms for hierarchical federated learning," *IEEE Internet Things J.*, Apr. 2024, doi: 10.1109/JIOT.2024.3394170.
[443] X. Zhang, L. Fan, S. Wang, W. Li, K. Chen, and Q. Yang, "A game-theoretic framework for privacy-preserving federated learning," *ACM Trans. Intell. Syst. Technol.*, vol. 15, no. 3, pp. 1–35, May 2024.
[444] H. Nie and S. Lu, "FedCRMW: Federated model ownership verification with compression-resistant model watermarking," *Expert Syst. Appl.*, vol. 249, Sep. 2024, Art. no. 123776.
[445] N. Kumari and P. K. Jana, "Communication efficient federated learning with data offloading in fog-based IoT environment," *Future Gener. Comput. Syst.*, vol. 158, pp. 158–166, Sep. 2024.
[446] S. Hegde, C. S. Abhijit, and S. Ambesange, "FedCure: A heterogeneity-aware personalized federated learning framework for intelligent healthcare applications in IoMT environments," *IEEE Access*, vol. 12, pp. 15867–15883, 2024.
[447] S. S. Tripathy, S. Bebortta, M. I. U. Haque, Y. Zhu, and T. R. Gadekallu, "Toward multi-modal deep learning-assisted task offloading for consumer electronic devices over an IoT-fog architecture," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 1656–1663, Feb. 2024.
[448] W. Li, P. Yu, Y. Cheng, J. Yan, and Z. Zhang, "Efficient and privacy-enhanced federated learning based on parameter degradation," *IEEE Trans. Services Comput.*, 2024.
[449] Z. You, X. Dong, X. Liu, S. Gao, Y. Wang, and Y. Shen, "Location privacy preservation crowdsensing with federated reinforcement learning," *IEEE Trans. Dependable Secure Comput.*, pp. 1–18, 2024, doi: 10.1109/TDSC.2024.3398994.
[450] C. Yang, K. Jia, D. Kong, J. Qi, and A. Zhou, "DP-GSGLD: A Bayesian optimizer inspired by differential privacy defending against privacy leakage in federated learning," *Comput. Secur.*, vol. 142, Jul. 2024, Art. no. 103839, doi: 10.1016/j.cose.2024.103839.
[451] M. Chehimi and W. Saad, "Quantum federated learning with quantum data," in *Proc. ICASSP - IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2022, pp. 8617–8621.
[452] M. Popovic, M. Popovic, I. Kastelan, M. Djukic, and I. Basicevic, "Developing elementary federated learning algorithms leveraging the ChatGPT," in *Proc. 31st Telecommun. Forum (TELFOR)*, Nov. 2023, pp. 1–4.
[453] M. Al-Quraan, L. Mohjazi, L. Bariah, A. Centeno, A. Zoha, K. Arshad, K. Assaleh, S. Muhaidat, M. Debbah, and M. A. Imran, "Edge-native intelligence for 6G communications driven by federated learning: A survey of trends and challenges," *IEEE Trans. Emerg. Topics Comput. Intell.*, 2023.
[454] J. H. Yoo, H. Jeong, J. Lee, and T.-M. Chung, "Open problems in medical federated learning," *Int. J. Web Inf. Syst.*, vol. 18, no. 2/3, pp. 77–99, Oct. 2022, doi: 10.1108/IJWIS-04-2022-0080.
[455] Y. Zang, Z. Xue, S. Ou, L. Chu, J. Du, and Y. Long, "Efficient asynchronous federated learning with prospective momentum aggregation and fine-grained correction," in *Proc. AAAI Conf. Artif. Intell.*, 2024, vol. 38, no. 15, pp. 16642–16650.
[456] X. Zhang, S. Lin, C. Chen, and X. Chen, "MODA: Model ownership deprivation attack in asynchronous federated learning," *IEEE Trans. Dependable Secure Comput.*, pp. 1–16, 2024, doi: 10.1109/TDSC.2023.3348204.
[457] C. L. Stergiou, K. E. Psannis, and B. B. Gupta, "InFeMo: Flexible big data management through a federated cloud system," *ACM Trans. Internet Technol.*, vol. 22, no. 2, pp. 1–22, May 2022, doi: 10.1145/3426972.
[458] X. Li, H. Zhao, and W. Deng, "IOFL: Intelligent-optimization-based federated learning for non-IID data," *IEEE Internet Things J.*, vol. 11, no. 9, pp. 16693–16699, May 2024.
[459] E. Strickland, "Andrew ng, AI minimalist: The machine-learning pioneer says small is the new big," *IEEE Spectr.*, vol. 59, no. 4, pp. 22–50, Apr. 2022.
[460] S. Cui, W. Pan, J. Liang, C. Zhang, and F. Wang, "Addressing algorithmic disparity and performance inconsistency in federated learning," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 34, 2021, pp. 26091–26102.
[461] X. Fang and M. Ye, "Robust federated learning with noisy and heterogeneous clients," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2022, pp. 10062–10071.
[462] A.-R. Ottun, P. C. Mane, Z. Yin, S. Paul, M. Liyanage, J. Pridmore, A. Y. Ding, R. Sharma, P. Nurmi, and H. Flores, "Social-aware federated learning: Challenges and opportunities in collaborative data training," *IEEE Internet Comput.*, vol. 27, no. 2, pp. 36–44, Mar. 2023.
[463] M. Chen, H. V. Poor, W. Saad, and S. Cui, "Convergence time optimization for federated learning over wireless networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 4, pp. 2457–2471, Apr. 2021.
[464] T. Wang, Y. Liu, X. Zheng, H.-N. Dai, W. Jia, and M. Xie, "Edge-based communication optimization for distributed federated learning," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 4, pp. 2015–2024, Jul. 2022.
[465] Z. Hu, K. Shaloudegi, G. Zhang, and Y. Yu, "Federated learning meets multi-objective optimization," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 4, pp. 2039–2051, Jul. 2022.
[466] D. Gao, D. Chen, Z. Li, Y. Xie, X. Pan, Y. Li, B. Ding, and J. Zhou, "FS-real: A real-world cross-device federated learning platform," *Proc. VLDB Endowment*, vol. 16, no. 12, pp. 4046–4049, Aug. 2023.
[467] W. Bao, H. Wang, J. Wu, and J. He, "Optimizing the collaboration structure in cross-silo federated learning," in *Proc. Int. Conf. Mach. Learn.*, 2023, pp. 1718–1736.
[468] A. Durrant, M. Markovic, D. Matthews, D. May, J. Enright, and G. Leontidis, "The role of cross-silo federated learning in facilitating data sharing in the agri-food sector," *Comput. Electron. Agricult.*, vol. 193, Feb. 2022, Art. no. 106648.
[469] Z. Jiang, W. Wang, B. Li, and Q. Yang, "Towards efficient synchronous federated training: A survey on system optimization strategies," *IEEE Trans. Big Data*, vol. 9, no. 2, pp. 437–454, Apr. 2023.
[470] Z. Zhao, Y. Mao, Y. Liu, L. Song, Y. Ouyang, X. Chen, and W. Ding, "Towards efficient communications in federated learning: A contemporary survey," *J. Franklin Inst.*, vol. 360, no. 12, pp. 8669–8703, Aug. 2023.
[471] J.-H. Ahn, G.-Y. Kim, D. H. Kim, and C. You, "Model compression by count sketch for over-the-air stateless federated learning," *IEEE Internet Things J.*, vol. 11, no. 12, pp. 21689–21703, Jun. 2024.

[472] J. Á. Morell, Z. A. Dahi, F. Chicano, G. Luque, and E. Alba, "A multi-objective approach for communication reduction in federated learning under devices heterogeneity constraints," *Future Gener. Comput. Syst.*, vol. 155, pp. 367–383, Jun. 2024.
[473] H. Zhu, J. Xu, S. Liu, and Y. Jin, "Federated learning on non-IID data: A survey," *Neurocomputing*, vol. 465, pp. 371–390, Nov. 2021.
[474] X. Cao, M. Fang, J. Liu, and N. Zhenqiang Gong, "FLTrust: Byzantine-robust federated learning via trust bootstrapping," 2020, *arXiv:2012.13995*.
[475] L. Chen, D. Xiao, Z. Yu, and M. Zhang, "Secure and efficient federated learning via novel multi-party computation and compressed sensing," *Inf. Sci.*, vol. 667, May 2024, Art. no. 120481.
[476] H. Xiong, C. Jin, M. Alazab, K.-H. Yeh, H. Wang, T. R. Gadekallu, W. Wang, and C. Su, "On the design of blockchain-based ECDSA with fault-tolerant batch verification protocol for blockchain-enabled IoMT," *IEEE J. Biomed. Health Informat.*, vol. 26, no. 5, pp. 1977–1986, May 2022.
[477] D. Yang, S. Luo, J. Zhou, L. Pan, X. Yang, and J. Xing, "Efficient and persistent backdoor attack by boundary trigger set constructing against federated learning," *Inf. Sci.*, vol. 651, Dec. 2023, Art. no. 119743.
[478] S. Nabavirazavi, R. Taheri, M. Ghahremani, and S. S. Iyengar, "Model poisoning attack against federated learning with adaptive aggregation," in *Adversarial Multimedia Forensics*. Cham, Switzerland: Springer, 2023, pp. 1–27.
[479] C. Zhang, S. Ekanut, L. Zhen, and Z. Li, "Augmented multi-party computation against gradient leakage in federated learning," *IEEE Trans. Big Data*, pp. 1–10, Sep. 2022, doi: 10.1109/TBDATA.2022.3208736.
[480] G. Zhang, B. Liu, T. Zhu, M. Ding, and W. Zhou, "PPFed: A privacy-preserving and personalized federated learning framework," *IEEE Internet Things J.*, vol. 11, no. 11, pp. 19380–19393, Jun. 2024.
[481] A. Sharma and N. Marchang, "A review on client-server attacks and defenses in federated learning," *Comput. Secur.*, vol. 140, May 2024, Art. no. 103801.
[482] G. Shirvani, S. Ghasemshirazi, and B. Beigzadeh, "Federated learning: Attacks, defenses, opportunities, and challenges," 2024, *arXiv:2403.06067*.
[483] J.-P.-A. Yaacoub, H. N. Noura, and O. Salman, "Security of federated learning with IoT systems: Issues, limitations, challenges, and solutions," *Internet Things Cyber-Phys. Syst.*, vol. 3, pp. 155–179, Jan. 2023.
[484] X. Li, X. Yang, Z. Zhou, and R. Lu, "Efficiently achieving privacy preservation and poisoning attack resistance in federated learning," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 4358–4373, 2024.
[485] X. Luo, Y. Wu, X. Xiao, and B. C. Ooi, "Feature inference attack on model predictions in vertical federated learning," in *Proc. IEEE 37th Int. Conf. Data Eng. (ICDE)*, Apr. 2021, pp. 181–192.
[486] R.-Y. Huang, D. Samaraweera, and J. M. Chang, "Exploring threats, defenses, and privacy-preserving techniques in federated learning: A survey," *Computer*, vol. 57, no. 4, pp. 46–56, Apr. 2024.
[487] X. Wu, F. Huang, Z. Hu, and H. Huang, "Faster adaptive federated learning," in *Proc. AAAI Conf. Artif. Intell.*, 2023, vol. 37, no. 9, pp. 10379–10387.
[488] J. Zhang, S. Guo, Z. Qu, D. Zeng, Y. Zhan, Q. Liu, and R. Akerkar, "Adaptive federated learning on non-IID data with resource constraint," *IEEE Trans. Comput.*, vol. 71, no. 7, pp. 1655–1667, Jul. 2022.
[489] Y. Xia, Y. Liu, S. Dong, M. Li, and C. Guo, "SVCA: Secure and verifiable chained aggregation for privacy-preserving federated learning," *IEEE Internet Things J.*, vol. 11, no. 10, pp. 18351–18365, May 2024.
[490] J. Wu and W. Zhang, "On the security of verifiable and oblivious secure aggregation for privacy-preserving federated learning," *IEEE Trans. Dependable Secure Comput.*, pp. 1–2, Jan. 2024, doi: 10.1109/TDSC.2024.3352170.
[491] D. Chai, L. Wang, L. Yang, J. Zhang, K. Chen, and Q. Yang, "A survey for federated learning evaluations: Goals and measures," *IEEE Trans. Knowl. Data Eng.*, pp. 1–20, Mar. 2024, doi: 10.1109/TKDE.2024.3382002.
[492] C. Qiao, M. Li, Y. Liu, and Z. Tian, "Transitioning from federated learning to quantum federated learning in Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, May 2024, doi: 10.1109/COMST.2024.3399612.

ABDUL MAJEED received the B.S. degree in information technology from UIIT, PMAS-UAAR, Rawalpindi, Pakistan, in 2013, the M.S. degree in information security from COMSATS University, Islamabad, Pakistan, in 2016, and the Ph.D. degree in computer information systems and networks from Korea Aerospace University, South Korea, in 2021. He was a Security Analyst with Trillium Information Security Systems (TISS), Rawalpindi, from 2015 to 2016. He is currently an Assistant Professor with the Department of Computer Engineering, Gachon University, South Korea. His research interests include privacy-preserving data publishing, federated learning, statistical disclosure control, privacy-aware analytics, data-centric artificial intelligence, and machine learning.

SEONG OUN HWANG (Senior Member, IEEE) received the B.S. degree in mathematics from Seoul National University, in 1993, the M.S. degree in information and communications engineering from Pohang University of Science and Technology, in 1998, and the Ph.D. degree in computer science from Korea Advanced Institute of Science and Technology, South Korea, in 2004. He was a Software Engineer with LG-CNS Systems, Inc., from 1994 to 1996. He was a Senior Researcher with the Electronics and Telecommunications Research Institute (ETRI), from 1998 to 2007. He was a Professor with the Department of Software and Communications Engineering, Hongik University, from 2008 to 2019. He is currently a Full Professor with the Department of Computer Engineering, Gachon University, South Korea. His research interests include cryptography, data-centric artificial intelligence, cybersecurity, and machine learning.