International Journal of Machine Learning and Cybernetics (2023) 14:513–535
https://doi.org/10.1007/s13042-022-01647-y

ORIGINAL ARTICLE

A survey on federated learning: challenges and applications

Jie Wen[1] · Zhixia Zhang[1] · Yang Lan[2] · Zhihua Cui[2] · Jianghui Cai[2] · Wensheng Zhang[3]

Received: 16 May 2022 / Accepted: 29 August 2022 / Published online: 11 November 2022

Abstract

Federated learning (FL) is a secure distributed machine learning paradigm that addresses the issue of data silos in building a joint model. Its unique distributed training mode and the advantages of security aggregation mechanism are very suitable for various practical applications with strict privacy requirements. However, with the deployment of FL mode into practical application, some bottlenecks appear in the FL training process, which affects the performance and efficiency of the FL model in practical applications. Therefore, more researchers have paid attention to the challenges of FL and sought for various effective research methods to solve these current bottlenecks. And various research achievements of FL have been made to promote the intelligent development of all application areas with privacy restriction. This paper systematically introduces the current researches in FL from five aspects: the basics knowledge of FL, privacy and security protection mechanisms in FL, communication overhead challenges and heterogeneity problems of FL. Furthermore, we make a comprehensive summary of the research in practical applications and prospect the future research directions of FL.

Keywords Federated learning · Machine learning · Privacy protection · Personalized federated learning

1 Introduction

Since the concept of artificial intelligence (AI) was put forward in 1956, AI technology has more and more profound impact on human life [1–3]. As great progress has been made in AI technology in recent years, various application fields have stepped into intelligence [4, 5]. On the road of AI development, models, computing power, chip performance, and other technical issues have been the focus of academic research, so that AI technology can continue to evolve. For machines to truly approach the level of human thought, they need to be trained with vast amounts of real data [6, 7]. However, cloud computing power, data security, data silos and other risks will inevitably become constraints for AI to win user trust, collect private data, and achieve large-scale implementation [8]. Therefore, it is an urgent need for a practical and effective technique to alleviate the above problems and make the AI full of vitality again. Under this background, the concept of "federated learning (FL) " came into being.

The notion of FL is first proposed by Google in 2016, mainly to make android mobile phone users update models locally without revealing private personal data [9]. After then, Google implemented an application-oriented FL system. The designed FL system, which focused on running federated average (FedAvg) algorithms on mobile phones, can perform federated analytics and be applied to monitor statistics for large-scale cluster equipment without recording raw device data to the cloud server. FL is one of the most

✉ Zhihua Cui
cuizhihua@tyust.edu.cn

Jie Wen
wj_110926@163.com

Zhixia Zhang
15634969919@163.com

Yang Lan
lanyangvip1020@163.com

Jianghui Cai
jianghui@tyust.edu.cn

Wensheng Zhang
wensheng.zhang@ia.ac.cn

[1] School of Electronic Information Engineering, Taiyuan University of Science and Technology, Taiyuan, China

[2] School of Computer Science and Technology, Taiyuan University of Science and Technology, Taiyuan, China

[3] The State Key Laboratory of Intelligent Control and Management of Complex Systems, Institute of Automation Chinese Academy of Sciences, Beijing, China

concerned technologies in the field of privacy computing. With its advantages of lightweight technology pathway and deployment scheme, FL has become the mainstream solution and product choice in many privacy computing application scenarios. And as the development and perfection of FL applications, a large quantity of research achievements of FL field has emerged.

FL is a secure distributed machine learning technique that cooperatively performs FL algorithms on multiple scattered edge devices or servers under the condition that the private information is not leave local [10]. FL transfers the task of data training to each local client, and the communication between client and server is through parameter interaction rather than direct data interaction. The server only participates in simple parameter aggregation to update the global model. Such FL scheme can realize the protection of local user data on the basis of saving the computing and storage resources of the server. FL can obtain a global model with superior performance through the communication between client and server. This approach is contrasts with traditional centralized training, where all separate local datasets are gathered to a center server for training model [11]. Compared to the traditional centralized machine learning methods [12], FL techniques can realize multiple federated agencies to build a unified model between the safe, efficient, and compliance of multi-source data applications of the ecological system [13–15]. Meanwhile, the performance of federated model is similar to that of the model trained through data integration. FL realizes the interagency sharing of data fusion, through the system expansion of sample size and increase the data dimension for high-precision model building for big data and application support, which can provide high-quality big data services and create more value for social development.

However, with the explosion of privacy computing platforms and products, the number of FL products put into practical application gradually increases, and some challenges have also raised. At present, the research on FL technology is still in continuous improvement. By combing the existing literature, we concluded that research on current FL mainly faces three bottlenecks: privacy and security threats, heterogeneity challenges, and huge communication overhead of FL [16]. Compared with traditional privacy-protecting computing technologies, FL is essentially characterized by exposing certain parameter data and assuming that these data do not reveal sensitive information. However, a growing body of research has found that this hypothesis is not necessarily objective. In FL, there are still hidden dangers of parameters leakage and attack by malicious operations [17]. The research for effective privacy protection techniques and attack mitigation method remains a focus of FL. At the same time, when large quantities of clients participate in FL, the problem that communication overhead of FL is far greater than the computational overhead cannot be ignored. Therefore, communication efficiency problem is also the main challenges in FL. Additionally, any locally available data point distribution is not representing the overall data distribution because the data distribution varies widely between clients. The heterogeneity of client data distribution leads to global model drift. Also, each client is constrained by device resources and their tasks, and the models trained by clients participating in federated tasks are often different. All of these show the challenges of current FL techniques in practical applications.

FL continues to develop multiple practical applications while overcoming challenges. FL techniques have been deeply applied in many fields, such as: intelligent medical [18], recommendation systems, smart city [19], finance and insurance, edge of computing [20], intrusion detection et al. To meet the needs of practical applications, more efficient FL algorithms are sought to strike a balance between security and efficiency. Different institutions realize the application of FL through the secure connection of platforms so that the data cooperation model based on FL will develop in a legal and compliant direction. The motivation for this paper is to survey the existing literatures and summarize advanced methods and techniques in the FL field. We outlined the basic definition and categorization of FL, and reviewed the latest FL research, including different strategies for solving the challenges of privacy security, communication costs, and heterogeneity. Then we discussed how the FL framework can be applied to various application scenarios successfully, and the research achievements are introduced for several current application directions of FL. Additionally, we analyzed the current research status and prospect for the development of FL in the future.

The contributions of this paper to the FL research are as follows:

(1) It provides an in-depth survey and analysis of the latest papers on FL.
(2) It concerns the practical application prospects of FL and the challenges faced in the process of practical applications, and has unique views on the current development and future prospects of FL.

The rest of paper is organized as follows. The basics knowledge of FL is introduced in Sect. 2. Sect. 3 depicts privacy and security threats to FL and surveys and empirically evaluates mitigation methods. Sect. 4 surveys communication problem of FL and reviews various communication-efficient mechanisms. Sect. 5 discusses the solutions for the problem of heterogeneity in FL. Sect.6 introduces the current research status of FL in many fields. And in Sect. 7, the vision of the future of FL is pointed out. Finally, Sect. 8 gathers concluding remarks.

2 The basics knowledge of federated learning

For making a better overview of FL research, the basic concepts, training framework, and classification of FL are detailed introduced in this section.

2.1 Overview of federated learning

FL is a secure distributed learning framework in which a virtual model can be constructed to address the matter of dispersive clients collaborating needless to expose raw information [21]. The virtual model is an optimal global model for aggregating data from all participants and each participant serves the local objective using the obtained model. FL can achieve that the results of this modeling be much of similar to the traditional centralized training model [22], in which data from multiple clients are brought together in a same center server for modeling. In a federated mechanism, it is generally assumed that participants have the same identity and support the establishment of shared data policies. Because the data is not directly transferred, it does not affect data specifications or compromises user privacy.

First, we define the basic concept of FL: Define N participants in FL, all of whom want to merge their data $\{P_1, P_2, \cdots, P_N\}$ to train a global model. A frequently used approach is to gather all the data together and use total data$P = P_1 \cup P_2 \cup \cdots \cup P_N$ to train a model M_{sum} with a performance of V_{sum}. FL is a learning framework where participants co-training a common model M_{fed} with a performance of V_{fed}, in which no participant exposes its private data to others. Let ε be non-negative, then the performance loss of FL model is expressed as:

$$|V_{fed} - V_{sum}| < \varepsilon \tag{(1)}$$

The learning process of FL is achieved by minimizing a loss function, which is calculated on each client using a weighted aggregration method. And the goal of FL is to minimize the following objective function (2).

$$\min f(w) = \sum_{k=1}^{N} \frac{n_k}{n} F_k(w) \tag{(2)}$$

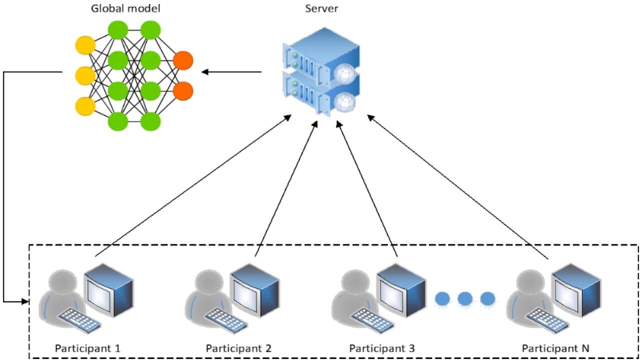

Fig. 1 The basic framework of FL

Where, N represents the number of clients, n_k is the amount of data on the $k-th$ client, $F_k(w)$ is the local objective function of the $k-th$ client.

FL allows a small range of performance deviation between the trained global federated model and the centralized training model. After several rounds of efficient federated global training, the performance of global model will continue to enhance and the convergence approaches to the performance of the centralized model [23]. In this basis, the basic framework of FL is introduced in Fig. 1. And the overall process of FL is as follows: Firstly, each client downloads the initial common model from the center server; Secondly, each client trains the model through their own local data until the local model converges; Thirdly, the client encrypts the model parameters and uploads them to the server; Finally, the server aggregates the uploaded gradients or parameters through the FL algorithm and updates the global model for next training. Looping through the above process, the client and the server communicate continuously until the global federated model converges.

2.2 The categorization of federated learning

In the light of the degree of overlap of data features in the client dataset, FL methods are usually subdivided into horizontal federated learning (HFL), vertical federated learning (VFL) and federated transfer learning (FTL), which are suitable for solving different practical problems. The specific categorization illustration is shown in Fig. 2. Then, each category is briefly introduced.

Horizontal federated learning For the dataset of each client, if the overlap of data features is larger than that of users, that is, there are more of the same data features and fewer of the same users, this is called horizontal federated learning (HFL) [24]. HFL is guided by the feature dimension of the data, and takes out the parts with the same characteristics of the participants but different users for joint training. In the process of HFL, the training sample space is enlarged by the

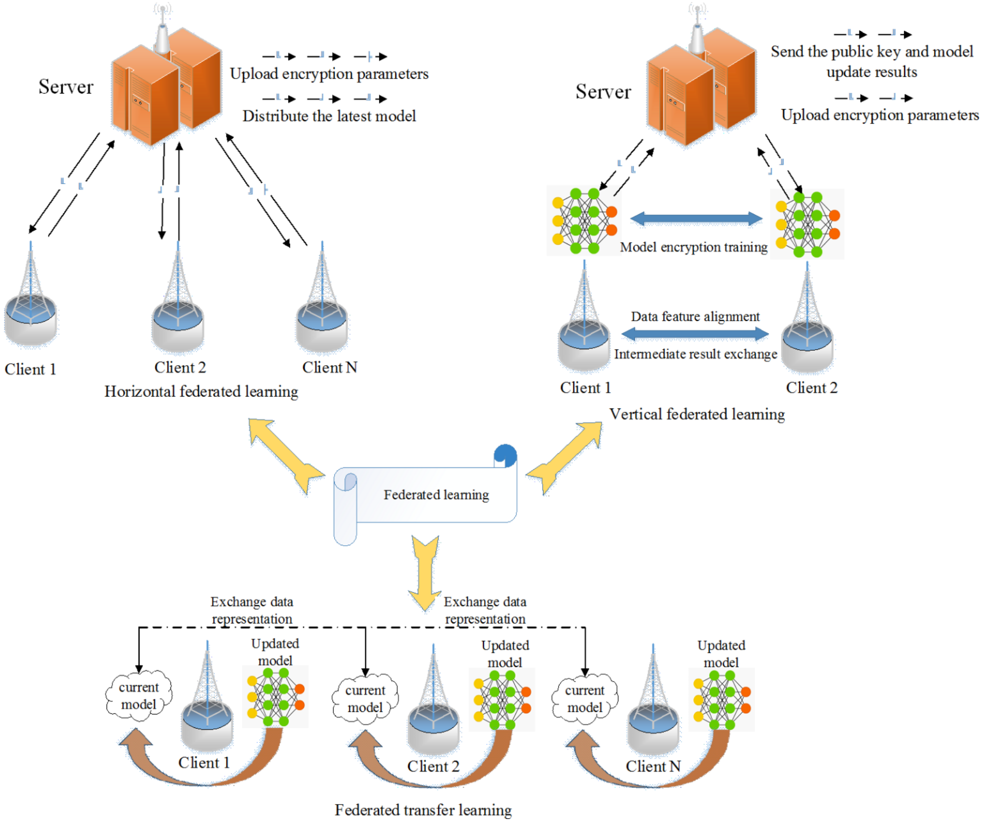
Server
Upload encryption parameters
Distribute the latest model
Client 1
Client 2
Client N
Horizontal federated learning
Server
Send the public key and model update results
Upload encryption parameters
Model encryption training
Data feature alignment
Intermediate result exchange
Client 1
Client 2
Vertical federated learning
Federated learning
Exchange data representation
Exchange data representation
Updated model
current model
Client 1
Updated model
current model
Client 2
Updated model
current model
Client N
Federated transfer learning

Fig. 2 The categories of FL

sample union between participants, thereby improving the accuracy and generalization ability of model [25].

Vertical federated learning Unlike HFL, the dataset characteristics of VFL are largely different between clients. For dataset of clients, the overlap of users is greater than that of data features, that is, each client dataset has more of the same users, and the data features are hardly duplicated [26]. HFL is a kind of FL based on feature dimensions, which is segmented according to feature dimensions. HFL takes common users as data alignment orientation and takes out the parts of participants with the same users but not completely the same characteristics for joint training [27]. Therefore, during the joint training, sample alignment of each participant's data is required first to obtain repeated data of users, and then training on selected data sets.

Federated transfer learning HFL and VFL require all participants to have the same feature space or sample space to build an efficient shared machine learning model. However, in more real scenarios, the datasets owned by each participant may be highly different [28, 29]. At the same time, it can help build an effective and accurate global model with only a small amount of data (samples and features do not overlap) and with less labels, while complying with data privacy and security regulations. This has given rise to a new category of FL, called federated transfer learning (FTL), which can deal with problems beyond the capabilities of existing HFL and VFL. FTL models can learn from source domain to target domain based on the similarity of data or models among participants [30]. In most applications, tags in the source domain are used to predict the accuracy of tags in the target domain [31].

3 Privacy and security challenges in federated learning

Before the FL was put forward, machine learning privacy protection problem has been always been a hot research topic [8]. As an innovative technology, the research direction of FL is also closely related to previous privacy protection techniques. FL provides a security mechanism to protect data privacy, which can secure the transmission of model while protecting local sensitive data. However, even under the protection of the FL security mechanism, there are still various types of attacks that can be against the FL system, thereby destroying the reliability of the FL system and threatening the data privacy of the participants [32]. In this section, we will briefly review three different privacy-protection technologies, identify the potential attacks and look for specific ways to prevent malicious hazards.

3.1 Privacy protection technique in federated learning

As a secure machine learning technology with privacy protection, the degree of protection of information privacy by FL is largely guaranteed by security encryption technology [33]. Since the advent of encryption technology, it has become the focus of many scholars, which greatly protects privacy information from disclosure. At present, the traditional encryption techniques accepted by most scholars include secure multi-party computing, differential privacy, and homomorphic encryption. These three privacy encryption methods provide basic guarantee for the secure transmission of parameters or gradients in FL. Next, these encryption techniques used in FL will be briefly introduced as follows.

3.1.1 Secure multi-party computing

Secure multi-party computing (SMC) was originated in 1982 with Yao's Millionaire problem [34], mainly used to protect the input data of each party participating in cooperation. In this process, sensitive data is protected by encryption between parties. The SMC security model typically involves multiparty and provides security guarantee in a zero-knowledge simulation framework. And the parties know nothing but inputs and outputs. Throughout the calculation process, parties always have absolute control over the data they own. In the related studies on SMC, one of the most advanced SMC frameworks is Sharemind [35], which is a secure multi-party computing system that allows user to process data without seeing it. With various research on private computing, SMC technology is becoming more mature. Xiong et al. [36] proposed a robust reversible image watermarking scheme using SMC technology based on lightweight encryption. And the proposed scheme based on bit prediction error extension (PEE) is guaranteed by SMC. An et al. [37] proposed a privacy-aware indoor location algorithm based on SMC to protect the private information of specific location. These efforts require users' data to be secretly shared between non-colluding client.

With the development of FL, SMC has been improved and migrated to federated system to protect sensitive data by encrypting parameters. Bonawitz et al. [38] built a privacy-preserving FL framework, where SMC can securely aggregate the clients' parameters, and be robust to clients' exit. Xu et al. [39] proposed a non-interactive and verifiable privacy protection FL model, and proposed a novel privacy gradient aggregation scheme using random matrix coding and secure two-party computation. These SMC models lead to huge communication cost because of multiple interactions involving in the learning process. However, in FL, because the number of parameters is typically several orders of magnitude smaller than the size of the data, the computational overhead of the encryption process is greatly reduced. Therefore, under the low safety requirements, using SMC technology to build a security model can be exchanged for improved efficiency.

3.1.2 Differential privacy

After user data is encrypted and uploaded to the center server, malicious server can use the encrypted data to infer the characteristics of the user group, but cannot parse the information of an individual. This attack method is called differential attack. Aiming at this threaten, differential privacy (DP) technology can use random noise to drown the original data, making it impossible for attackers to reverse the original data from the database. The main way to implement DP is to add noise to the result set to solve the privacy protection problem of a single query. DP has rigorous data theory, and its essence is the protection of computational results rather than computational process. The advantage of DP is that it has a privacy protection model that is strictly independent of background knowledge and can theoretically resist any attack.

In view of the advantages of DP in data privacy protection, researchers migrated it to the FL system, and by combining DP with other technologies, many models of privacy protection were generated. In the federated optimization process, certain malicious participants may launch the differential attack to affect the federated model security. For solving this issue, Geyer et al. [40] designed a federated optimization algorithm with DP protection strategy. The goal is to achieve a balance between privacy loss and model performance while hiding customer contributions and private data during training. Huang et al. [41] designed an asynchronous FL privacy protection computing model. It protects data privacy while reducing noise to be added by using an adaptive DP mechanism. Xiong et al. [42] conducted an in-depth analysis for privacy leakage problem in FL. Based on in-depth analysis, a new FL algorithm with differential privacy, 2DP-FL, is proposed to implement privacy protection by adding noise when training local models and distributed global models.

Most of the existing FL models train the deep neural networks, and the number of parameters transmitted during FL is often large [43, 44], so the communication cost of SMC cannot be ignored. Therefore, FL based on DP technology is often adopted in consideration of communication costs. The principle of FL based on DP is mainly to add noise to parameter information for data safe transmission, which will not generate a high communication cost or computing cost. However, since DP technique added noise to the parameters, this affected the availability of model. To alleviate this problem, Sun et al. [45] combined DP with functional encryption, proposed a hybrid privacy protection scheme for FL, and used an interactive key generation method, which avoided the collusion problem and obtained a good balance between privacy protection and model accuracy. Fan et al. [46] constructed an adaptive DP method to increase noise adaptively according to the importance of features during model training. And a multi-objective optimization model is established, which can balance the conflicting indexes of accuracy and privacy protection effectively by adopting multi-objective optimization algorithm [47–49].

3.1.3 Homomorphic encryption

Homomorphic encryption (HE) is an encryption algorithm which meets the homomorphic operation nature of the ciphertext. That is, it allows users to perform specific algebraic operations on ciphertext directly, and the result of ciphertext calculation is the same as that of plaintext encryption after the same operation. The design of an efficient HE algorithm involves some cryptography knowledge based on the complexity theory of mathematical computation. If a HE algorithm supports any form of ciphertext calculation, it is called fully homomorphic encryption (FHE) [50]. If partial ciphertext computation is supported, for example, only addition, multiplication, or a limited number of additions is supported, it is called semi-homomorphic encryption or partially homomorphic encryption (PHE). It is worth noting that when operating on an encrypted model using HE technique, all participants of these operations are required to share the same encryption key and the same decryption key.

In FL, HE allows the center server to carry out algebraic operations directly on encrypted parameters without decryption. Zhang et al. [51] proposed a privacy-protection and verifiable FL scheme. The scheme combines the chinese residual theorem and Paillier homomorphic encryption technology to deal with shared gradients, which can realize privacy-protected FL with low computational and communication costs. However, once participants who hold the same secret key collude with each other, the FL scheme will unable to guarantee user privacy security. In addition, in FL, the server can extract the information of the training dataset from the shared gradient by using the public key, which may maliciously tamper with the calculation results, thus influencing the accuracy of the federated global model. To solve above issues, Ma et al. [52] made a multi-key HE protocol, in which model updates are encrypted through aggregated public keys and decryption requires cooperation among all participating devices. Park et al. [53] used HE technique to design a privacy-protected FL algorithm that enables centralized servers to directly aggregate encrypted local parameters. The proposed algorithm allows each client to use different HE private keys in the same FL-based distributed cryptosystem, ensuring the privacy of parameters. These privacy-protected schemes effectively prevent privacy disclosure of shared parameters in FL and is robust to collusion between clients and servers. Meanwhile, the development of HE technology is limited by the large amount of time cost during encryption operation. In the light of this issue, Zhang et al. [54] optimized previous HE by scaling gradients in advance and then cutting and post-quantization encryption, which successfully decreases the encryption cost and the total number of ciphertext, as well as saving costs.

For clarity, we list the characteristic of three kinds of privacy protection techniques in Table 1.

3.2 Security attack and solutions in federated learning

In addition to improving the necessary data protection mechanism, it is also necessary to prevent malicious attacks from causing security risks of the federated system [55]. People often intuitively equate security and privacy, but there is actually a difference between the two. Security can guarantee the confidentiality and integrity of data, while privacy can further refine the privacy of personal information. Privacy prevails when dealing with private data, while security means protecting data from unauthorized access. In FL, there are various types of attacks that can against the FL system to compromise the security of federated model and local participants' model. In this segment, we introduce the two most common types of attacks that FL studies: poisoning attacks and Byzantine attacks. And the existing research works of each attack method are introduced to understand the current development of FL security protection mechanism.

3.2.1 Poisoning attack

In the FL mechanism, poisoning attack tends to tamper, destroy or pollute the client's local training dataset or model generated in the FL training process by means of poisoning, so as to affect the security of FL system [56]. The existing data poisoning types in FL are usually subdivided into data poisoning and model poisoning categories, which posed great threats to the security of FL.

Data poisoning attackers maliciously tamper with local client data's source tags or characteristics to influence the training result of federated models [57]. Because of the distributed nature of FL deployment, it is difficult to determine whether a client is participating in FL in good faith, so detecting data poisoning is a challenging task. Data

Table 1 The difference of several privacy protection techniques

Privacy mechanism	Reference	Contribution	Advantage	Disadvantage
Secure multi-party computing	[35]	Allow users to process data without seeing it	Throughout the calculation process, parties always have absolute control over the data they own	Cause huge communication cost in multi-party interaction
	[36]	Use SMC technology to achieve a robust reversible image watermarking scheme		
	[37]	Protect the private information of specific location in privacy-aware indoor location application		
	[38]	Can securely aggregate the clients' parameters in FL		
	[39]	Propose a novel privacy gradient aggregation scheme using random matrix coding and secure two-party computation		
Differential privacy	[40]	Achieve a balance between privacy loss and model performance while hiding customer contributions and private data during training.	Has a privacy protection model that is strictly independent of background knowledge and can theoretically resist any attack	Numerous noises will affect the availability of model
	[41]	Protect data privacy while reducing noise to be added by using an adaptive DP mechanism		
	[42]	2DP-FL is proposed to implement privacy protection by adding noise when training local models and distributed global models		
	[45]	Combine DP with functional encryption, which avoided the collusion problem and obtained a good balance between privacy protection and model accuracy.		
	[46]	Build a multi-objective optimization model to balance the conflicting indexes of accuracy and privacy protection effectively		
Homomorphic encryption	[51]	Realize privacy-protected FL with low computational and communication costs.	Allow the center server to carry out algebraic operations directly on encrypted parameters without decryption	Large amount of time cost during encryption operation
	[52]	Model updates are encrypted through aggregated public keys and decryption requires cooperation among all participating devices		
	[53]	Enables centralized servers to directly aggregate encrypted local parameters		
	[54]	Optimize previous HE by scaling gradients in advance and then cutting and post-quantization encryption		

poisoning is a more covert type of attack than model poisoning. While the principle of ensuring participants' privacy security, the central server is not clear about participants' personal data and local training process. When the attacker can only affect the data collection process of the client of FL system, but cannot directly destroy the model trained by FL, such attacks are often difficult to detect. In recent years, some defense schemes have been studied to against data poison attack that can delete outliers by calculating the similarity between data information [58]. In the aspect of this way, Tian et al. [59] proposed a strategy for detecting and suppressing potential outliers to defend against data poisoning attacks in FL. In the FL scenario of traffic flow prediction, Qi et al. [60] came up with a FL framework which using consortium blockchain technique. The model trained from distributed vehicles need be verified and then stored on the blockchain to effectively prevent data poisoning attacks. In addition, to further protect data security on blockchain, a DP approach with noise-adding mechanism is applied in the FL framework [61].

Another type of poisoning attack is caused by model poisoning. Some malicious attackers in FL can bring in hidden backdoor functionality to the local client model or global federated model, causing the model produce a specific error output. Model poisoning can take advantage of the fact that malicious participants in FL can directly influence the performance of federated global model, making the attack effect more powerful than training data poisoning attacks. In order to defense and reduce poisoning attack in FL, Zhao et al. [62] put forward a poisoning attack defense mechanism, which generates audit data through generative adversarial network during training [63], and then eliminates adversaries who upload malicious models through the accuracy of audit models. Observing the effect of local model poisoning on the global model of FL, Shi et al. [64] designed a federated exception analysis enhanced distributed learning framework to implement active defense in FL. In this framework, clients and server cooperate to analyze model exceptions and ensure the security and validity of the global model. Based on the characteristics of distributed learning mechanism for FL, the attack range of FL is larger than that of centralized learning, and the concealment is stronger. During the training and testing phases, any internal dishonest participant or external malicious attacker can have a very serious impact on the final performance of the federated global model. It is necessary to better understand the potential attacks of FL to improve the effectiveness and robustness of detection and defense methods.

3.2.2 Byzantine attack

Many FL usually encourages as many clients as possible with good data quality to participate in FL training by incentive mechanism, but does not consider the malicious clients attack problem in FL training process. In recent years, more individuals pay attention to the security of distributed learning, among which the Byzantine threat problem is the most important. Poisoning attack mainly considers the attack on a single user or a server, while Byzantine attack mainly considers the collusion of multiple users in distributed learning environment. In FL, a malicious attacker may control multiple clients, known as Byzantine users. Byzantine users can upload fake data due to unreliable communication channels, corrupted hardware, or even malicious attacks, lead to the global model is manipulated by attackers and cannot be converged. As an active internal attack pattern, Byzantine attack can easily harm the normal communication between client and server in FL. So, the defense and detection of Byzantine attack has been the hot issues in FL security research [65].

To better detect and defend attacks, researchers have conducted various research work on Byzantine attacks from different technologies and strategies. Ma et al. [66] put forward a credibility-based approach to defend against Byzantine attacks. For Byzantine attacks with non-independent and identical distributed (non-IID) datasets, reliability indicators were designed to evaluate the reliability of knowledge transmitted by clients, and the reliability was updated according to the knowledge information shared by clients each round. At the same time, in the basic of secure two-party computing protocol, an effective privacy protection parameter aggregation protocol is put forwarded. The proposed method can identify Byzantine attackers accurately and update global model securely. Similarly, Zhai et al. [67] designed a Byzantine robust model for FL by evaluating the reliability of non-IID data. However, the specific difference is that the reliability assessment method in this paper combines the adaptive anomaly detection model and data verification, in which adaptive mechanism and transfer learning [68] are introduced into the anomaly detection method to dynamically enhance the detection performance of Byzantine attacks with non-IID data. Different from the above methods of selecting trusted participants, Li et al. [69] focused on detecting the Byzantine model and identify the attacker in FL, puts forward a Byzantine resistant secure blockchained FL framework. the framework by introducing the validator to parallel execution of heavy validation workflow, improve the efficiency of the model validation, and through the Byzantine consistency validation to detect Byzantine attack resistance. The framework introduces validators to perform heavy validation workflows in parallel and detects Byzantine attacks through Byzantine anti-conformance validation, which greatly improves the efficiency of model verification. Based on the in-depth study of specific attack behavior of Byzantine attackers, various protection mechanisms and strategies provide a strong guarantee for the detection and defense methods of Byzantine attacks.

Furthermore, the differences of several attack and defense strategies are listed in Table 2.

4 Communication challenge in federated learning

Communication overhead is also a major bottleneck for FL, because the communication cost is far greater than the computation cost when numerous edge devices are sending their model parameters to central server. The communication cost is too large in the training process, resulting in low training efficiency of FL, which is not conducive to the application of FL in practical engineering field. Therefore, for an efficient FL algorithm, it is necessary to enhance the communication efficiency. In the existing research for reducing communication cost of FL, the respond solution strategies from three aspects are often considered: federated learning optimization algorithm, client selection, and model compression. In this section, we summarize the researchers' efforts to mitigate the communication cost challenge of FL in these three perspectives.

4.1 Federated Learning optimization algorithm

In the FL training process, the clients generate the local model after optimization processing steps such as gradient descent (GD) algorithm, and then transmit the trained model to the center server for aggregation. The performance of the local training model directly determines the performance of the federated model. Researchers have studied the influence of global communication iteration times between client and server and the local training times of client on FL performance [70]. And it is verified that increasing local iteration times and decreasing the global communication round can

Table 2 The difference of several attack and defense strategies

Attack mode		Attack characteristics	Reference	Defense method
Poisoning attack	Data poisoning	Maliciously tamper with local client data's source tags or characteristics	[59]	Detect and suppress potential outliers to defend attacks
			[60]	The model trained from distributed vehicles need be verified and then stored on the blockchain to prevent data poisoning attacks
	Model poisoning	Bring in hidden backdoor functionality to the local client model or global federated model, causing the model produce a specific error output	[62]	Came up with a FL framework which using consortium blockchain technique
			[64]	Clients and server cooperate to analyze model exceptions and ensure the security and validity of the global model
Byzantine attack		Exist malicious participants in FL training	[66]	Put forward a credibility-based approach to defend against Byzantine attacks.
			[67]	Designed a Byzantine robust model for FL by evaluating the reliability of non-IID data
			[69]	Introduce the validator to parallel execution of heavy validation workflow to improve the efficiency of the model validation

effectively boost the convergence efficiency of the global model while ensuring the performance of the federated model. Therefore, a useful way to reduce the communication overhead is to reduce the frequency of communication and increase the time interval of model aggregation by improving the efficiency and performance of local training.

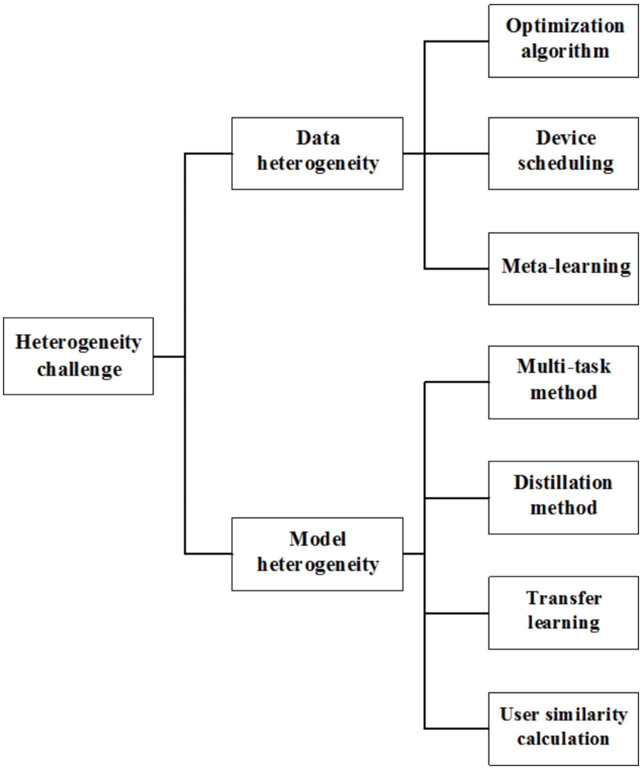

Fig. 3 Heterogeneity challenge and solutions in a federated learning environment

Based on it, the FedAvg algorithm proposed by McMahan can reduce the communication cost by increasing local training times to reduce the communication round [9]. However, when the model converges to a certain extent, increasing training times can no longer alleviate the communication cost challenge. More researchers try to optimize the FL framework algorithm to improve the training efficiency and convergence of federated model, lead to reduce the federated communication rounds. Liu et al. [71] considered the momentum term related to the last iteration optimization in gradient descent algorithm and proposed to use momentum gradient descent in the local model update process of FL system to realize the accelerated convergence of the local model and improve the communication efficiency of FL. Wu et al. [72] used adaptive a learning rate algorithm to optimize the GD process, avoiding model overfitting and fluctuation, and effectively ensure efficient training of FL under the condition of limited communication cost. On the other hand, optimization the aggregation mode of the model can also improve federated model convergence efficiency and greatly reduce the communication rounds. Wu et al. [73] proposed a federated adaptive weighting algorithm based on observing the contribution of client nodes to the aggregation of federated global model. In each round of communication, different weights are adaptively allocated according to the clients' contribution to update global model. And the contribution of client is first evaluated by the angle between local gradient vector and global gradient vector, and then quantified into weight coefficients by a nonlinear mapping function. These studies on federated learning optimization algorithms focus on accelerating the convergence time of global models by improving the training efficiency of local models and optimizing the aggregation mechanism, so as to achieve efficient communication.

4.2 Client selection

The classic FedAvg algorithm adopts the strategy of randomly selecting clients [9], which may slow down the training efficiency and performance of global model. Because in a synchronous FL environment, the server needs to wait for model updates from all clients selected to participate in the FL task until the last client completes uploading the local model. Meanwhile, the clients in FL have some differences in computing capacity and communication resources, which leads to the instability of participants and makes the high communication cost become one of the efficiency bottlenecks of FL. In practical FL applications, the client selection scheme participating in federated directly affects the efficiency and performance of federated model [74, 75].

Considering from this perspective, Liu et al. [76] studied an orthogonal method to identify irrelevant updates made by clients by detecting whether local model updates are consistent with the trend of global model updates, so as to avoid transmitting those irrelevant parameters to the server and reduce the occupation of network resources. Deng et al. [77] proposed an automated-quality-awareness based client selection framework, which taken into account various factors affecting learning performance, adopted reinforcement learning method [78, 79]. And it automatically evaluated the model quality of clients, and automatically selects high-quality clients for the federated task within a limited budget, which significantly improves learning efficiency. Lai et al. [80] proposed a framework that prioritized client participation in FL training using existing data that provided the greatest utility in improving model accuracy and the ability to run training quickly.

Additionally, in practical scenarios, some clients have limited computing resources or are in poor wireless channel conditions, which will lead to long global training delay of federated model. Therefore, the problem of client selection under resource constraints is also the focus of current research. For responding to this issue, Nishio [81] et al. proposed a new FL protocol, Fedcs, where the deadline for downloading, updating and uploading local models was preset. Then, greedy selection was adopted to enable the server to aggregate as many clients' update as possible during the restricted time, which made the whole training process efficient. Du et al. [82] adopted an efficient client selection scheme based on the shortest upload time to minimize the total training time of the FL, and designed a scheduling mechanism based on the maximum remaining bandwidth, which greatly reducing the upload time of each iteration and affecting the number of iterations. Nowadays, most of FL technology has been applied to the edge wireless network environment. With the complexity of the network environment of client devices and information of clients participating in practical federated tasks, the client selection problem has gradually become a complex optimization problem [83, 84] that needs to be studied urgently.

4.3 Model compression

In addition to reducing the communication rounds by optimizing the FL training algorithm and selecting the best client, model compression can also significantly reduce the scale of parameter transmission, which is a direct and useful strategy to improve the algorithm communication efficiency [85]. Especially in federated neural network, the parameters of deep neural network model are often millions, and the communication cost of transmission parameters is very big [86]. Li et al. [87] analyzed data redundancy in data set and propose a coreset-based FL framework. The novel framework used a smaller network model on the coreset instead of training the model on the whole dataset using the regular network model, thus achieving similar accuracy to training using the full data set while indirectly reducing the amount of data transferred by each client. Lu et al. [88] proposed an efficient asynchronous FL mechanism in edge network computing environment. In this mechanism, the client node adaptively calculates the threshold according to the parameter changes in each round during model training to compress and reduce parameter. Li et al. [89] proposed two communication-efficient FL frameworks based on CS method, which are called CS-FL and 1-bit CS-FL. In the CS-FL, local updates are compressed into analog compression measurements, which are then uploaded to the server by participants. Another 1-bit CS-FL method is to sparse local updates and compress them into 1-bit compressed measurements. Both of these methods can efficiently compress the uplink and downlink data during FL training.

Researchers have designed a variety of data compression methods to achieve efficient communication FL algorithm, but there is a general problem that the conflict between communication resources and computing resources, communication resources and model training performance needs to be paid attention [90]. Most data compression methods are lossy, and the improvement of communication efficiency is at the cost of model accuracy [91]. Aiming at this kind of optimization problem with conflict among multiple objectives [92, 93], researchers began to try to use multi-objective evolutionary algorithm (MOEA) to get the optimal solution [94–96]. Zhu et al. [97] tried to use MOEA to optimize the structure of neural network model in FL, and achieved optimal compression of network model parameters, thus achieving small communication cost and good global model performance synchronously. On the basis of the study of this problem, Lan et al. [98] applied FL to skin cancer detection applications to ensure efficient skin cancer detection while protecting patient data privacy. In the designed strategy, the communication cost of FL is reduced by sparse the global model, and an MOEA is used to balance the conflict between the communication overhead, accuracy, loss and AUC of global federated model.

5 Heterogeneity challenge in federated learning

Traditional FL usually aggregates all selected client-side model parameters or gradients to construct a common federated global model. In the process of aggregation, researchers gradually discovered the federated heterogeneity problems in practical applications, such as the data heterogeneity problem attribute to the non-IID of data for each client, and model heterogeneity problem with different size of each client model structure caused by different device resource constraints and personalized task, these heterogeneity problems may reduce the performance of the global model or makes it difficult to get convergence to some extent [99].

5.1 Data heterogeneity

In a real FL scenario, clients participating in FL are often scattered in different areas with different user activity, resulting in inconsistent data volume collected by each client and data distribution of each client. Therefore, the amount of data and data distribution of different clients participating in practical FL application are usually heterogeneous. For different clients with heterogeneous data, traditional direct average aggregation approach will lead to model drift problem and affect the convergence and precision of the global model [100]. As such, an effective FL method should be found according to the specific distribution of client data and the specific situation in the actual application environment.

To solve the statistical heterogeneity, scholars also have done lots of studies. Wang et al. [101] proposed an effective polynomial time algorithm to schedule workloads on different clients. For the problem of heterogeneous data, they converted it into an average cost minimization optimization problem and used a greedy algorithm to seek for balance between calculation time and calculation accuracy. Taik et al. [102] against the current challenges of federated edge learning (FEEL) with limited communication bandwidth, scarce energy, and heterogeneous data distribution, and proposed a device scheduling algorithm considering data quality, which prioritizes devices with high quality data while minimizing FEEL completion time and energy consumption of participating devices. It greatly improves the effectiveness and efficiency of FL training while alleviating the challenge of data heterogeneity. Furthermore, on the basis of considering this challenge, Li et al. [69] proposed a meta-learning-based personalized FL method which considering the non-IID characteristics of spatiotemporal data for solving he spatiotemporal prediction problem of urban construction. The global spatial-temporal schema diagram is automatically constructed through data federation, and each client customizes its own personalized model by evaluating the differences between the global schema diagram and the local schema diagram. For non-IID data with noisy, Hu et al. [103] proposed a FL framework based on federated Kalman filter (FKF) confidence. It used a convolutional adversarial generative network with advanced auxiliary classifiers as feature extraction to pre-train the data, and then the confidence parameters to each client are generated by the FKF, which overcomes the challenge of data heterogeneity and realizes efficient aggregation of FL. These methods greatly alleviate the heterogeneity of data between clients in FL, but it is obvious that the actual optimization focus of these methods is different, so they adopted different methods. Data heterogeneity problem will affect different stages of FL training process, such as client selection stage, model transmission stage and aggregation stage. Therefore, in the study of data heterogeneity, the influence of heterogeneity challenge on the training and application of FL model needs to be deeply analyzed when the data heterogeneity problem is studied.

5.2 Model heterogeneity

In the process of parameters aggregation in FL, the local model structure of each client is typically required to be uniform. However, such assumptions are not realistic in the actual scenario of FL. As each client is not necessarily the same and located in different spaces, and the resource profiles of mobile devices participating in FL tasks are not always the same. The communication volume, computing power and data possessed by each client are very different and these factors will strictly limit the model structure of each client's local training, resulting in structural differences among the client models. When the computing power and storage capacity of a client are small, only a simple model can be trained locally on the client, rather than overly complex models as required by the server. Meanwhile, in traditional FL, the common federated model is constructed through collaborative training of clients, while the model obtained by local training of clients essentially serves local tasks, and unified model type can limit the performance of local task execution, so the local model of clients is usually heterogeneous under the guidance of personalized tasks and local resources constrict [104]. The heterogeneity of the model allows different clients to design local models of different types and structural sizes based on their computational power. And overcoming the problem of inability to directly integrate models caused by heterogeneity while maintaining the personalization of the local model is the current challenge for FL. Aiming at above practical challenges caused by model heterogeneity in aggregation mechanism of FL, researchers have conducted many extensive studies.

In order to alleviate model heterogeneity problem and obtain high-quality personalized model for each client, some scholars have focused on personalized FL methods. Mills et al. [105] used the idea of multitasking to develop a multi-task FL algorithm for personalized federated model training, which introduced a non-federated batch normalization layer in federated deep neural network. The proposed algorithm allows users to personalize the training model according to their own local data, thus facilitating the performance and convergence speed of the local client model. Ni et al. [106] proposed a federated codistillation algorithm, which added a distillation term to the local objective function so that the local model could be trained based on the output of global model. In addition, the proposed algorithm was further extended to federated two-way codistillation to personalize the local model for each device. Yang et al. [107] designed a new FL framework, which trains the secure and personalized distributed model through FTL to implement the application of secure image steganography. Liu et al. [108] considered task individualization in the framework of federated random forest. It used locally sensitive hash method to calculate the similarity of users, carried out collaborative training for similar users, and made use of the characteristics of ensemble learning to incrementally select models, so as to carry out personalized training for the models.

Summarize the above research work on personalization of FL, we can see that the heterogeneity of model in FL can be roughly divided into the heterogeneity of model types and the heterogeneity of model structures. The model types (e.g. different neural networks, random tree, etc.) and the structures of model (e.g. different neural network depths etc.) used by different clients are different due to the limitation of client device resources or the influence of local task individuation [109]. When the local model types of each client are different, some feature extraction methods can be used to extract data features abstractly to achieve information fusion. In the shallow feature layer of each client model, FL can be used to achieve multi-features fusion, while the deep layer is specially designed to achieve local personalized tasks. On the other hand, when the client models are of the same type but have different model structures with personalized task requirements, the problem of model heterogeneity is also called parameter heterogeneity. In this case, each client can transform different model structures into the same structure through some mappings approach for federation. While in the local model training, each client can selectively learn the federated model to help guide the training of the local model [110], so as to build the local personalized model.

In Fig.3 below, we briefly summary the solutions proposed by these relevant literatures for the two heterogeneous challenges.

6 The application of federated learning

In the big data environment, users' personal information and behavioral data can be recorded in mobile smart devices or edge servers. So, data privacy protection provides a necessary guarantee for intelligent development, and various fields pay more attention to the security and privacy of private information. With the joint efforts of many scholars, FL has acted important role in the fields of various industries. And the current mainstream FL application areas are health care, finance, industry and urban services. In this section, we describe in detail the application of FL in these classic scenarios.

6.1 Federated learning in intelligent medical

In the medical field, individuals usually pay more attention to the privacy information of patients can not be disclosed, at the same time, various hospitals cannot exchange patient information privately, so it is quite suitable to use FL technique for protecting pathological information [111]. When applying FL to health care applications, each hospital represents the individual client, and the server can be the data center of the government agency. In this way, each hospital downloads the initial common model from the server and trains it with local data. After completion, the model information is encrypted and uploaded to the server, and the global model is updated through the federation algorithm. In this way, the data center will get a disease detection model with superior performance. The combination of FL and intelligent medicine application is shown in the Fig. 4.

FL has been used to build various disease detection models. Under the current severe epidemic situation, it solved COVID-19 detection, DNA sequencing and other problems,

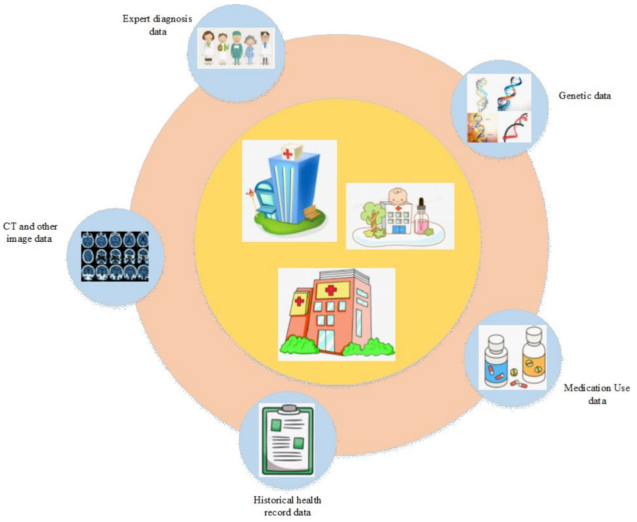

Fig. 4 Federated intelligent medicine

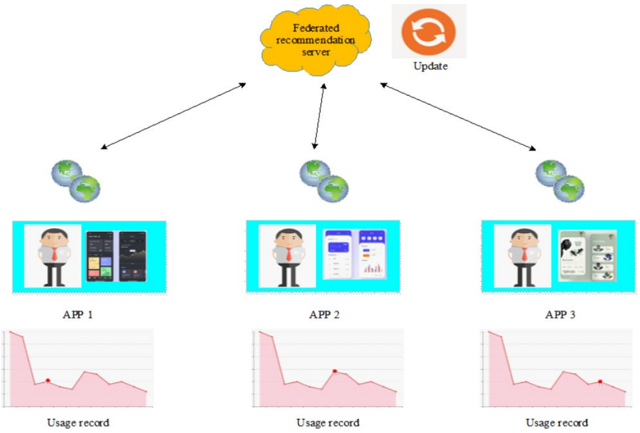

Fig. 5 Federated recommendation system

and showed good detection performance. For example, Ouyang et al. [112] proposed a COVID-19 collaborative early warning framework based on blockchain and intelligent contract to predict the detection results of new cases. This framework crowdsourced the task to medical establishments, social institutions and individuals to collaborate for early warning. And Dayan et al. [113] proposed a FL model, which predicts the future oxygen demand of patients with COVID-19 symptoms by inputting vital signs, laboratory data and chest x-rays, and better predicts the clinical outcome of patients with COVID-19, which lays a foundation for the wider application of FL in health care. Furthermore, an auxiliary diagnosis model for cancer patients based on FL is proposed by Ma et al. [114]. With the help of federated diagnostic model, doctors can provide personalized nutritional plans and treatment options for patients, and prolong the life of patients. This model has a certain guiding significance in the field of cancer rehabilitation medicine.

In the medical field, patient data is sensitive data, and many patients are reluctant to share their private data for intelligent testing services. In this situation, the security and effectiveness of FL technology provide feasible suggestions for the application of intelligent services in the medical field. The combination of FL and medical industry can build a disease detection model with good performance without harming private information of patient, which promotes the process of intelligence of medical industry [115].

6.2 Federated learning in recommended system

Traditional recommender systems need to collect and analyze large amounts of user data to recommend content or services [116, 117], but due to the concern of privacy security and data island problem, this operation is often not authorized by users. The emergence of FL provides a good paradigm to solve this problem, especially in cross-domain recommendation, including short video recommendation, social platform, online shopping platform and etc. The federated recommendation system typically includes federalization of recommendation algorithm based on collaborative filtering [118], federalization of recommendation algorithm based on deep learning and federation of recommendation algorithm based on meta-learning. In the vertical federated recommendation framework, the server is not limited to the data generated by users in this field, at the same time, we can also refer to the data of users in other areas, so as to provide users with high-quality content. The combination of FL and recommendation system is shown in the Fig. 5.

To further enhance the accuracy of the recommendation system and strengthen the deep integration of FL and recommendation system, many scholars have done carious research [119, 120]. Du et al. [121] proposed a user-level distributed matrix decomposition framework. Inspired by federation learning, the framework can learn the global model by collecting gradient information of client. Duan et al. [122] proposed a federated recommendation algorithm that allows each cloud to share weights and cooperatively train the global model, while combining matrix factorization with 8-bit quantization to reduce communication overhead and network bandwidth. Caballero et al. [123] proposed an activity recommendation model based on secure federated network Eduroam. The system can provide personalized information in the campus environment according to personal data of user. Muhammad et al. [124] proposed a FL-based recommendation algorithm: FedFast, which improves the classical FedAvg algorithm and accelerates the training of distributed recommendation model.

Under the premise that the user data is not local, the encrypted parameter information is transmitted between clients and server to train a federated recommendation model with good performance. Moreover, the combination of FL

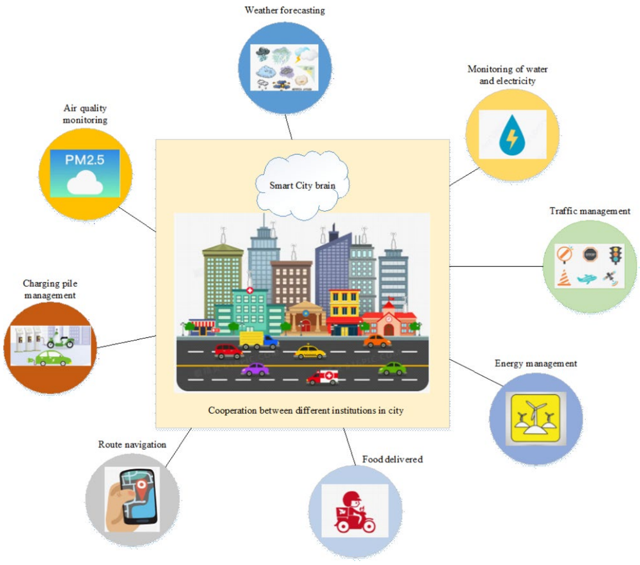

Fig. 6 Federated learning in smart city

and recommendation system aims to provide users with accurate and feasible recommend services on the premise of protecting privacy and trade secrets user, which promoting the progress of recommendation technology in various commerce institutions.

6.3 Federated learning in smart city

The development of the city is inseparable from the joint efforts of government agencies, private enterprises and individuals [125, 126], and the improvement of data privacy requirements leads to the data center can not provide data for third parties at will [127, 128]. This limits the exchange of data at different levels. The emergence of FL effectively solves the problem of data isolated island and integrates data at all levels of the city in order to provide better urban applications and transportation services for citizens [129, 130]. When FL is applied to smart city construction, government agencies and private enterprises will act as data owners, that is, clients. And the urban data management center will become the service. In order to solve various problems in the construction of smart cities, the service will unite with different levels of institutions in the city to train a global model, it will deal with different tasks, so as to provide more convenient urban services for citizens [131]. The combination of FL and smart city application is shown in the Fig. 6.

In view of this, many researchers have conducted a series of studies on the application of FL in urban development. Jiang et al. [132] made an in-depth description on the feasibility of FL in smart city perception, and summarized the open problems and challenges in applications, so as to provide guidance for scholars on this topic. Putra et al. [133] proposed federated compression learning, which ensures the privacy of PM2.5 prediction data, but also reduces transmission consumption in smart city sensing applications. Li et al. [69] proposed a spatio-temporal prediction technology to protect privacy through combining FL, which ensured spatio-temporal prediction accurate under the premise of protecting data privacy in construction of smart cities. Yuan et al. [134] proposed a federated deep learning algorithm based on spatio-temporal long-term and short-term network, which used observed historical traffic data to predict traffic flow, ensuring data privacy and effectively alleviating traffic congestion in smart cities.

The emergence of FL provides a new paradigm for building smart city. This effectively protects the data privacy, promotes the sharing and fusion of data at all levels of city, taps the potential value of urban data, and further promoting the process of urban intelligent construction, so that citizens could fully enjoy high-quality urban services.

6.4 Federated learning in finance and insurance

In order to fully analyze and utilize big data, cooperation among financial institutions has gradually become the transformation trend of financial and insurance industry [135]. In recent years, some financial institutions have carried out FL applications, mainly focusing on risk control, marketing, anti-money laundering and other aspects. The application of FL in financial scenarios, including HFL helps many banks train credit of depositor forecasting models, and VFL helps different financial institutions predict loan repayment ability. No matter which kind of FL is used, it will help financial scenarios to better understand investment ability of customers and credit rating scores. Similarly, participants in FL in the financial field will be different financial institutions, which keep investment information of user, and will train different global models for different financial tasks under the assumption that the data are not exposed [136]. The combination of FL and finance application is shown in the Fig. 7.

However, most of the combinations of FL and finance application are still in the early research stage and have not been put into large-scale application. At present, there is a classic application of FL in the financial field is WeBank institution used FL in the risk management of small and micro business credit and personal loans, which helps bank solve third-party data for risk control modeling. And then better predict and score the credit information of enterprises, as well as the insurance claims of users. Based on the credit risk assessment applications, Cheng et al. [137] proposed an efficient privacy-protection boosting tree framework based on VFL, which implements privacy-preserving joint machine learning training on vertically segmented client credit score data.

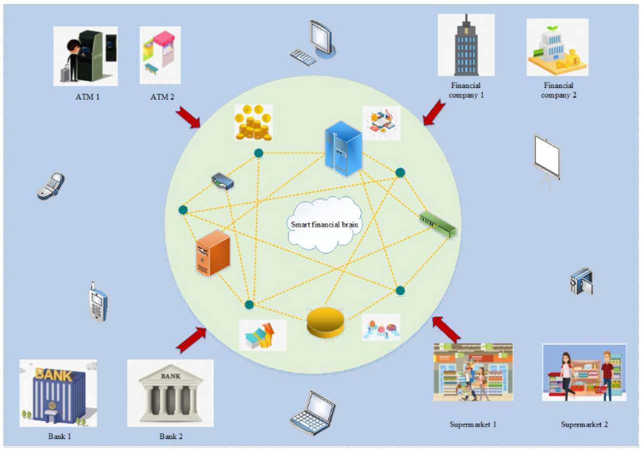

Fig. 7 Federated learning applications in financial

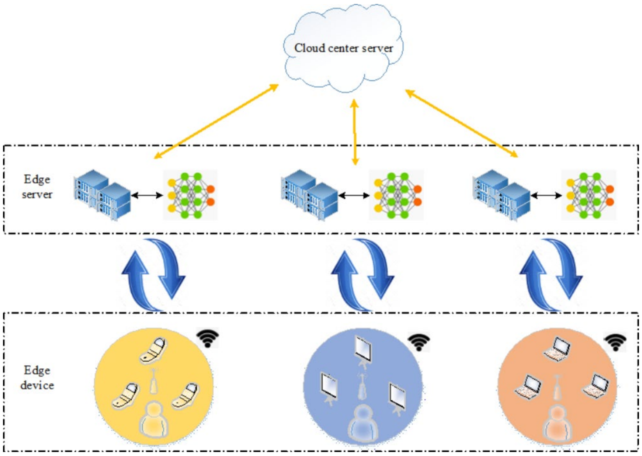

Fig. 8 Federated learning in edge computing

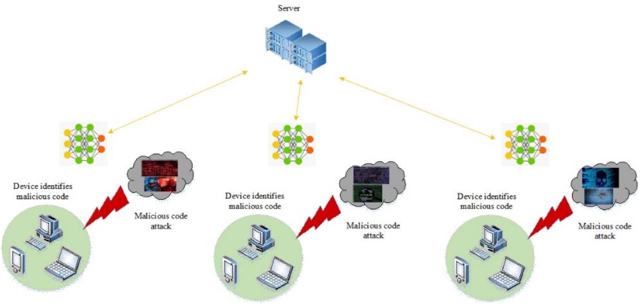
Server
Device identifies malicious code
Malicious code attack
Device identifies malicious code
Malicious code attack
Device identifies malicious code
Malicious code attack

Fig. 9 Federated intrusion detection

As a field with strong demand for privacy protection, the combination of financial industry with FL effectively provides a very superior paradigm for breaking down the barriers of financial data and promoting the intelligent application of financial and insurance enterprises.

6.5 Federated learning in edge computing

As the information technology rapid evolves, the functions of personal mobile devices have gradually become intelligent, which provides an effective guarantee for processing distributed edge data safely in FL [138]. The combination of edge computing and FL enables edge devices to train a common machine learning model with superior performance without sending source data to cloud devices [139]. And the Fig. 8 provides a diagram of this combination.

To effectively combine marginal computing with FL, scholars have carried out research from different angles. Ye et al. [140] proposed an edge FL framework, which separates the local model update process that should be implemented independently by mobile devices. Then the outputs of the mobile device are aggregated to the server, which improves the training efficiency and reduces the interaction frequency. Jiang et al. [141] proposed a novel FL algorithm with adaptive learning rate to meet different precision requirements and speed up the local training process. And a fair aggregation strategy is designed to minimize the precision difference between terminal devices. For improving the communication efficiency of federated edge computing, the network resources and training rate of the edge side is considered in practical learning, and an asynchronous federation learning is designed in edge computing. Wang et al. [142] proposed an efficient asynchronous joint learning method to alleviate the inefficiency caused by the heterogeneity and autonomy of edge nodes. This method allows edge clients to choose some models from cloud to update asynchronously according to the local data distribution, so as to decrease the amount of computation and communication and promote the efficiency of FL. To further protect the data privacy at the edge, Liu et al. [143] considered the asynchronous convergence FL of obsolete coefficients and uses blockchain networks to aggregate and generate global model. It not only protects privacy, but also avoids communication interruption caused by abnormal training failure of local equipment, special attacks and etc. At the same time, Chen et al. [144] proposed a FL parameter aggregation method based on mutual information, which can resist malicious node attacks and maintain the robustness of FL.

With the progress of the Internet of things, FL also provides the possibility for the secure interconnection of edge computing data [145]. On the other hand, with the deepening of the concept of privacy protection, federated edge computing has more and more potential and potential value. further make edge computing towards the direction of integration.

Table 3 The research work of FL applications

Reference	Application	Contribution	Major FL challenges solved
[112], [113], [114]	Intelligent medical	Applying federated learning techniques to disease detection	protect patients' sensitive data and eliminate the data island challenge
[121], [123]	Recommendation system	Proposed a user-level distributed matrix decomposition framework	Learn the global model under strict privacy requirements
[122], [124]	Recommendation system	Allow each cloud to share weights and cooperatively train the global model,	Reduce communication overhead
[132]	Smart city	Made an in-depth description on the feasibility of FL in smart city perception, and summarized the open problems and challenges in applications	Provide guidance for scholars on FL topic
[133]	Smart city	Proposed federated compression learning	Protect the privacy of PM2.5 prediction data, and reduce transmission consumption
[69], [134]	Smart city	Proposed a spatio-temporal prediction technology	Protect personal privacy
[137]	Finance and insurance	Proposed an efficient privacy-protection boosting tree framework for the credit risk assessment applications	protect users' sensitive data and eliminate the data island challenge
[140], [141], [143]	Edge computing	Proposed an edge FL framework	Improve the training efficiency and reduce the interaction frequency
[142]	Edge computing	Proposed an efficient asynchronous joint learning method	Alleviate the heterogeneity challenge and decrease the amount of computation and communication
[144]	Edge computing	Proposed a FL parameter aggregation method based on mutual information	Resist malicious node attacks
[150], [151], [143], [152]	Intrusion detection	Proposed a FL-based network intrusion detection method and designed secure protection mechanisms	Reduce the resource utilization of the central server and ensures data security and privacy

6.6 Federated leaning in intrusion detection

Intrusion detection is a commonly used network security defense technology. Nowadays, the deep learning techniques are usually used to achieve network intrusion detection to achieve higher detection accuracy [146, 147]. However, deep learning machine learning model training often requires plenty of data, in reality, some institutions lack of network intrusion detection data sets, which is disadvantageous to the training of the model [148, 149]. At the same time, uploading data from all institutions for centralized in-depth learning and training will face privacy issues.

The emergence of FL alleviates the above problems to some extent, and the Fig. 9 shows a effective diagram of this combination To further improve the recognition accuracy of intrusion detection under the federated framework, Tang et al. [150] proposed a FL-based network intrusion detection method, which allows multiple institutions to jointly carry out in-depth learning and training under the condition of retaining local data. At the same time, Zhao et al. [151] proposed an intelligent intrusion detection method based on FL-assisted long short-term memory. Liu et al. [143] proposed a cooperative intrusion detection mechanism based on FL, which reduces the resource utilization of the central server and ensures data security and privacy. Furthermore, in order to ensure the security of the global model, the blockchain is employed to store and share the training model. Li et al. [152] proposed a new federated deep learning scheme, which used convolution neural network and gated loop unit to build an efficient intrusion detection model, which allows multiple industrial clusters to build this model in the way of privacy protection. And a reliable communication protocol based on Paillier cryptosystem is designed to protect the security of the model parameters transmission.

The application of FL in intrusion detection not only ensures a high detection rate, but also protects the data privacy of various institutions, and alleviates the problem of data island faced by intrusion detection.

Furthermore, these are the papers on the applied work of FL technology and we list them in Table 3. The papers in Table 3 are categorized according to the type of FL application domain and the FL challenges it addresses. Some papers mainly focus on the privacy challenge of federated learning technology in different domain scenarios, and the other part focuses on other communication and heterogeneity challenges faced by federated learning in applications.

7 Prospect for federated learning

Nowadays, the rapid development of AI accelerates the process of intelligent digitization in various industries, which brings the problems of data fragmentation and data island [153, 154], it hinders the data sharing among various fields and can not fully tap the potential value of data. The emergence of FL has alleviated the above issues to a certain degree and became the focus of many scholars. The development of FL is faced with multiple challenges, and no single strategy can comprehensively solve these bottlenecks in the practical application of FL technology. Although scholars have conducted some research on all aspects of FL which being as a kind of new-developed privacy-protection machine learning technique, there are still some aspects worth paying attention for scholars to studying and exploring in depth.

(1) Research on more efficient encryption algorithms and defensive attack methods to improve the security of FL. With the continuous breakthrough of information technology, the means of lawbreakers to steal user information are increasing [155]. The emergence of new DOS and DDOS attacks and new computer viruses increases the disclosure risk of user private information [156]. This hinders the data sharing among the enterprises participating in FL, and cannot fully tap the potential value of the data, resulting in huge economic losses. It is necessary to design more superior encryption method and attack detection method to enhance the security of FL and defend more kinds of attack dangers [157]. To ensure data security and improve encryption efficiency, some hardware-based encryption techniques should also be focused on. Some researchers also are considering the combination of emerging protection technologies such as block chain and FL to ensure the cross-domain learning security of FL. Meanwhile, due to the increasing scale of current FL deployments involving servers and a large number of client nodes, the types and number of attacks that may be attacked are far greater than centralized training methods. In the future, whether large-scale client participation can effectively continue to ensure the security of FL is debatable. Since the client uploads parameters instead of local data in FL, it is difficult for the server to identify malicious clients directly. Therefore, in addition to the existing client-side statistical information, it is necessary to use external source information that can be obtained in practical applications. External source information largely can help service providers find safe and efficient defense methods and accurately identify attacks and intrusions that are not easy to detect.

(2) Research on more efficient federated learning algorithms. In the period of big data, more requirements have been raised for the computing power of equipment and the communication ability between devices. In the traditional federated algorithm, researchers often focused on the convergence of global federated model. While the convergence of the global model often requires many communications between the client and the server, which undoubtedly results in a lot of communication costs [158]. And due to the influence of regional economy, network bandwidth and other factors, different enterprises participating in FL have different communication resource restriction. At the same time, the fairness of cooperation in FL is also a problem to be considered in the design of federated learning algorithm. The traditional FL mechanism makes the clients obtain the same global model, ignores the different contributions of participants and the incentive mechanism in the cooperative system, which is not conducive to the participation of more participants in the FL system, thus hindering the sustainable development of the FL system. These considerations have gradually led to the design of FL algorithms more efficient and comprehensive. At present, there is still no a universal FL algorithm can solve all the challenges in practical application. With the implementation of the practical application platform of FL, the optimization objectives and training methods of FL under different requirements and resource constraints should also be appropriately readjusted, and the FL algorithm also needs to be combined with specific training methods and aggregation mechanisms. Therefore, it is still particularly important to optimize FL framework and design efficient FL algorithm to improve the overall efficiency of FL, reduce the communications cost between clients and servers, ensure the model fairness, and encourage enterprises to invest more awards for enhancing the training performance of global model.

(3) Develop the selection strategy of large-scale clients in FL. In the training of FL global model, the global performance is greatly affected by client data quality, client reputation and credibility, training resources, energy consumption and other factors [159]. Meanwhile, because many of the clients participating in FL are intelligent user devices, they are in the mobile geographical location and dynamic network environment, which result in unstable training efficiency. With the popularization and large-scale applications of FL, the number of mobile clients participating in FL is increasing exponentially. Subsequently, it is necessary to consider both scheduling strategy efficiency and how to select high-quality [160, 161], stable performance clients in a complex FL environment to balance more selection targets [162]. On the other hand, as a key step in FL algorithm, client selection is performed for each communication round, which makes client selection a dynamic scheduling problem [163]. Therefore, it has become the focus and difficulty of many scholars to study an efficient client dynamic selection scheme, which dynamically select high-quality clients from

a large number of clients to optimize the global model and enhance the robustness of FL. In the future development of FL, the problem of client selection is bound to develop in large scale and complexity, and it is gradually important to efficiently select the client suitable for FL in the changing environment.

(4) Research on new model fusion method in multi-modal FL. Due to the diversity and heterogeneity of data of enterprise devices in different fields, clients participating in FL can provide different forms of data, including pictures, voice, text, and etc., this is the multi-modal data. Different data types make it necessary for clients to train different local models to perform locally personalized tasks. When the clients carry out FL, it is very difficult for the server to directly aggregate the different modal models uploaded by the client. This heterogeneity mentioned here is different from the model heterogeneity challenge in Sect. 5.2. The heterogeneity here refers to the different structures and types of models due to different data forms, not just different structures. For example, one client trains text data, another client trains image data, and the types and structures of network models suitable for processing local tasks are different. Therefore, how to mine the huge value hidden in different modal data, establish the relationship between different modal models, realize the fusion of multi-modal models, and improve the performance of local models, is the current research focus of multi-modal FL. In this case, when updating the global model, the server needs to design a new model fusion method to deal with the model uploaded by the client before the update, in order to better update the global model, and enable FL to provide personalized services for the different clients.

(5) Deepen the research and application of FL in various fields. The development of FL has experienced three stages: traditional privacy protection, FL and security FL. Basically, all kinds of commonly used machine learning algorithms can adopt FL method for model training, support structured, text, image and other types of data sources, and can be applied in sample classification, path programming [164], regression prediction, image recognition [165, 166], gene analysis, natural language and other tasks. In recent years, FL has played an important role in health care, finance, Internet of things, urban services and other fields where there is a strictly requirement for privacy protection. Based on the characteristics of distributed learning approach in FL, it also plays a prominent part in relieving the storage pressure and computing pressure of central server, adjusting data distribution structure and optimizing federated training mode. Besides to promote cooperation between different regions and different fields and further promote commercial development, scholars should pay some attention to the application of FL in education, e-government, meteorology, coal [167], power dispatching [168] and other fields. For example, in the education field, a multi-data source student information sharing platform can be build due to the accumulation of a large amount of data in students' physical and mental health research, and the data value sharing is realized under the condition of guaranteeing the privacy of data source, so security FL becomes a worthy solution. And in the process of dealing with government data, many government departments are reluctant to share personal data because the lack of credible data asset right confirmation scheme. Under such circumstances, FL can be integrated with big data development components to solve the data island of government departments and achieve secure cross-departmental sharing and sharing of government and social data, effectively reducing the risk of data leakage.

At the moment, the FL has a promising application prospect. But the FL technique applied to more fields is very much a blank area, which need to be explore to make FL applied to all aspects of people daily lives and lower the risk of privacy information disclosure in the big data era [169].

In recent years, the amount of literature on FL has grown exponentially, which show that people have paid more attention to the importance of privacy protection. As a solution of traditional machine learning in security protection, FL can fully release the productivity of big data and solve the problem of privacy protection. However, in the face of various application requirements in the actual complex environment and the deficiency of FL, it is necessary to dynamically optimize FL training according to objectives and constraints. FL is not only the union of models, but also the union of knowledge and non-sensitive information. The idea of federated learning can provide a feasible solution for other areas of research that are not only machine learning area.

8 Conclusion

FL technique, as one of the important solutions of privacy protection, has gained rapid development and enough attention in recent years. From the basic knowledge and framework of FL to the methods and strategies for solving above challenges, researchers have carried out careful research on the various branches of FL, and have done a lot of research work in each branch. Researchers have a more in-depth understanding of FL, and based on this to achieve a perfect combination of FL with various applications.

This paper summarized the current research achievements of FL, systematically introduced the concept of FL, the challenges faced by the development of FL, and the research direction of FL combined with various applications. On the basis of these, we made a deep thinking and analysis on the development of FL in the future and the bottleneck problems to be broken. This research work is expected to help scholars in the field of FL to understand the development and current research status of FL, and provide strong support for the further development of FL. In the field of FL, future research will continue to focus on privacy and security protection mechanism, client cooperation training mode and fairness, robustness, personalized federated learning mechanism, so as to facilitate the deployment and application of FL technology for in-depth exploration.

Acknowledgements This work is supported by the National Key Research and Development Program of China under Grant No.2018YFC1604000, the National Natural Science Foundation of China under Grant No.61806138, No.U1636220, No.61961160707 and No.61976212; Science and Technology Development Foundation of the Central Guiding Local under Grant No. YDZJSX2021A038; China University Industry-University-Research Collaborative Innovation Fund (Future Network Innovation Research and Application Project) under Grant No. 2021FNA04014; Outstanding Innovation Project for Graduate Students of Taiyuan University of Science and Technology under Grant No. XCX211004 and No. XCX212081.

Data Availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

References

1. Zhang Z, Zhao M et al (2022) An efficient interval many-objective evolutionary algorithm for cloud task scheduling problem under uncertainty. Inf Sci 583:56–72
2. Wang H, Xie F, Li J, Miu F (2022) Modelling, simulation and optimisation of medical enterprise warehousing process based on FlexSim model and greedy algorithm. Int J Bio-Inspired Comput 19(1):59–66
3. Cai X, Hu Z, Chen J (2020) A many-objective optimization recommendation algorithm based on knowledge mining. Inf Sci 537:148–161
4. Ren Y, Sun Y et al (2019) Adaptive Makeup Transfer via Bat Algorithm. Mathematics 7(3):273
5. Yang Y, Cai J, Yang H, Zhao X (2021) Density clustering with divergence distance and automatic center selection. Inf Sci 596:414–438
6. Hemalatha B, Rajkumar N (2021) A modified machine learning classification for dental age assessment with effectual ACM-JO based segmentation. Int J Bio-Inspired Comput 17(2):95–104
7. Cui Z, Zhao P et al (2021) An improved matrix factorization based model for many-objective optimization recommendation. Inf Sci 579:1–14
8. Kuze N, Ishikura S et al (2021) Classification of diversified web crawler accesses inspired by biological adaptation. Int J Bio-Inspired Comput 17(3):165–173
9. Mcmahan H et al (2017) Communication-Efficient Learning of Deep Networks from Decentralized Data. In: *proceedings of the 20th International Conference on Artificial Intelligence and Statistics, PMLR* 54: 1273–1282
10. Yang Q, Liu Y, Chen T, Tong Y (2019) Federated Machine Learning: Concept and Applications. ACM Trans Intell Syst Technol 10(2):1–19
11. Wang L, Meng Z, Yang L (2022) A multi-layer two-dimensional convolutional neural network for sentiment analysis. Int J Bio-Inspired Comput 19(2):97–107
12. Li H (2021) Image error correction of hockey players' step-by-step pull shooting based on Bayesian classification. Int J Comput Sci Math 14(2):185–195
13. Li A, Zhang L, Wang J, Han F, Li X (2022) Privacy-Preserving Efficient Federated-Learning Model Debugging. IEEE Trans Parallel Distrib Syst 33(10):2291–2303
14. Pereira A, Mazza L, Pinto P et al (2022) Deep convolutional neural network applied to Trypanosoma cruzi detection in blood samples. Int J Bio-Inspired Comput 19(1):1–17
15. Zhou Y, Sai Y, Yan L (2021) An improved extension neural network methodology for fault diagnosis of complex electromechanical system. Int J Bio-Inspired Comput 18(4):250–258
16. Liu J, Huang J, Zhou Y et al (2022) From distributed machine learning to federated learning: a survey. Knowl Inf Syst 64(4):885–917
17. Cui Z, Zhao Y, Cao Y et al (2021) Malicious Code Detection under 5G HetNets Based on a Multi-Objective RBM Model. IEEE Network 35(2):82–87
18. Liang B, Cai J, Yang H (2022) A new cell group clustering algorithm based on validation & correction mechanism. Expert Syst Appl 193:116410
19. Long T, Jia Q (2021) Matching Uncertain Renewable Supply with Electric Vehicle Charging Demand—A Bi-Level Event-Based Optimization Method. Complex Syst Model Simul 1(1):33–44
20. Zhou H, Yang G, Dai H, Liu G (2022) PFLF: Privacy-Preserving Federated Learning Framework for Edge Computing. IEEE Trans Inf Forensics Secur 17:1905–1918
21. Jiang J, Hu L et al (2020) BACombo-Bandwidth-Aware Decentralized Federated Learning. Electronics 9(3):440
22. Wang C, Liu Z, Wei H, Chen L, Zhang H (2021) Hybrid Deep Learning Model for Short-Term Wind Speed Forecasting Based on Time Series Decomposition and Gated Recurrent Unit. Complex Syst Model Simul 1(4):308–321
23. Cui Z, Wen J, Lan Y et al (2022) Communication-efficient federated recommendation model based on many-objective evolutionary algorithm. Expert Syst Appl 201:116963
24. Zhang K, Song X, Zhang C, Yu C (2022) Challenges and future directions of secure federated learning: a survey. Front Comput Sci 16(5):165817
25. Feng C, Liu B et al (2022) Blockchain-Empowered Decentralized Horizontal Federated Learning for 5G-Enabled UAVs. IEEE Trans Industr Inf 18(5):3582–3592
26. Dai M, Xu A, Huang Q, Zhang Z, Lin X (2021) Vertical federated DNN training. Phys Communication 49:101465
27. Gu B, Xu A et al (2020) Privacy-Preserving Asynchronous Vertical Federated Learning Algorithms for Multiparty Collaborative Learning. arXiv preprint arXiv: 2008. 06233
28. Li B, Liang Y, Gan Z et al (2021) Research on multi-UAV task decision-making based on improved MADDPG algorithm and transfer learning. Int J Bio-Inspired Comput 18(2):82–91
29. Guan J, Cai J, Bai H, You I (2021) Deep transfer learning-based network traffic classification for scarce dataset in 5G IoT systems. Int J Mach Learn Cybernet 12(11):3351–3365
30. Yang Y, Cai J, Yang H, Zhang J, Zhao X (2020) TAD: A trajectory clustering algorithm based on spatial-temporal density analysis. Expert Syst Appl 139:112846
31. Xu J, Zhang Z et al (2021) A many-objective optimized task allocation scheduling model in cloud computing. Appl Intell 51(6):3293–3310
32. Cai X, Geng S, Zhang J et al (2021) A Sharding Scheme-Based Many-Objective Optimization Algorithm for Enhancing Security in Blockchain-Enabled Industrial Internet of Things. IEEE Trans Industr Inf 17(11):7650–7658
33. Cavusoglu U, Kokcam AH (2021) A new approach to design S-box generation algorithm based on genetic algorithm. Int J Bio-Inspired Comput 17(1):52–62

34. Yao A (1982) Protocols for secure computations. *In: Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science* pp. 160–164
35. Bogdanov D, Willemson J (2008) Sharemind: A Framework for Fast Privacy-Preserving Computations. *In: Proceedings of European Symposium on Research in Computer Security*, Springer, pp. 192–206
36. Xiong L, Han X, Yang C, Shi Y (2022) Robust Reversible Watermarking in Encrypted Image With Secure Multi-Party Based on Lightweight Cryptography. IEEE Trans Circuits Syst Video Technol 32(1):75–91
37. An J, Wang Z et al (2021) Know Where You are: A Practical Privacy-Preserving Semi-Supervised Indoor Positioning via Edge-Crowdsensing. IEEE Trans Netw Serv Manage 18(4):4875–4887
38. Bonawitz K, Ivanov V, Kreuter B et al (2017) Practical Secure Aggregation for Privacy-Preserving Machine Learning. Presented at the Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, available: https://doi.org/10.1145/3133956.3133982
39. Xu Y, Peng C, Tan W et al (2022) Non-interactive verifiable privacy-preserving federated learning. Future Generation Computer Systems 128:365–380
40. Geyer R, Klein T, Nabi M (2017) Differentially Private Federated Learning: A Client Level Perspective. arXiv preprint arXiv: 1712. 07557
41. Huang J, Cheng X, Ji Z et al (2022) AFLPC: An Asynchronous Federated Learning Privacy-Preserving Computing Model Applied to 5G-V2X. Security and Communication Networks 2022: 9334943
42. Xiong Z, Cai Z, Takabi D, Li W (2022) Privacy Threat and Defense for Federated Learning With Non-i.i.d. Data in AIoT. IEEE Trans Industr Inf 18(2):1310–1321
43. Sattler F, Wiedemann S et al (2020) Robust and Communication-Efficient Federated Learning From Non-i.i.d. Data. IEEE Trans Neural Networks Learn Syst 31(9):3400–3413
44. Taşkıran M, Yetiş S (2021) Deep learning based tobacco products classification. Int J Comput Sci Math 13(2):167–176
45. Sun Z, Feng J, Yin L et al (2022) Fed-DFE: A Decentralized Function Encryption-Based Privacy-Preserving Scheme for Federated Learning. Cmc-Computers Mater Continua 71(1):1867–1886
46. Fan T, Cui Z (2021) Adaptive differential privacy preserving based on multi-objective optimization in deep neural networks. Concurrency and Computation-Practice & Experience 33(20):e6367
47. Cai X, Zhang M et al (2019) Analyses of inverted generational distance for many-objective optimisation algorithms. Int J Bio-Inspired Comput 14(1):62–68
48. Li W, Ye X, Huang Y, Mahmoodi S (2022) Adaptive Dimensional Learning with a Tolerance Framework for the Differential Evolution Algorithm. Complex Syst Model Simul 2(1):59–77
49. Xi J, Zheng L (2021) Cuckoo search with dual-subpopulation and information-sharing strategy. Int J Comput Sci Math 14(4):315–327
50. Wang W, Gan Y, Vong C, Chen C (2020) Homo-ELM: fully homomorphic extreme learning machine. Int J Mach Learn Cybernet 11(7):1531–1540
51. Zhang X, Fu A, Wang H et al (2020) A Privacy-Preserving and Verifiable Federated Learning Scheme. *In: proceedings of the ICC 2020–2020 IEEE International Conference on Communications (ICC)* pp. 1–6
52. Ma J, Naas S, Sigg S, Lyu X (2021) Privacy-preserving federated learning based on multi-key homomorphic encryption.arXiv preprint arXiv:2104. 06824
53. Park J, Lim H (2022) Privacy-Preserving Federated Learning Using Homomorphic Encryption. Appl Sci 12(2):734
54. Zhang C, Li S, Xia J et al (2020) BatchCrypt: Efficient Homomorphic Encryption for Cross-Silo Federated Learning. In: Proceedings of the 2020 USENIX Conference on Usenix Annual Technical Conference, USENIX Association, USA, pp. 493–506
55. Cai X, Niu Y, Geng S et al (2020) An under-sampled software defect prediction method based on hybrid multi-objective cuckoo search. Concurrency and Computation-Practice & Experience 32(5):e5478
56. Cui Z, Du L, Wang P et al (2019) Malicious code detection based on CNNs and multi-objective algorithm. J Parallel Distrib Comput 129:50–58
57. Chan P, He Z, Li H, Hsu C (2018) Data sanitization against adversarial label contamination based on data complexity. Int J Mach Learn Cybernet 9(6):1039–1052
58. Yang Y, Cai J, Yang H et al (2022) ISBFK-means: A new clustering algorithm based on influence space. Expert Syst Appl 201:117018
59. Tian Y, Zhang W, Simpson A, Jiang Z (2021) Defending Against Data Poisoning Attacks: From Distributed Learning to Federated Learning.The Computer Journal,bxab192
60. Qi Y, Hossain M, Nie J, Li X (2021) Privacy-preserving blockchain-based federated learning for traffic flow prediction. Future Generation Computer Systems-the International Journal of Escience 117:328–337
61. Cui Z, Xue F, Zhang S et al (2020) A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN. IEEE Trans Serv Comput 13(2):241–251
62. Zhao Y, Chen J, Zhang J et al (2022) Detecting and mitigating poisoning attacks in federated learning using generative adversarial networks. Concurrency and Computation: Practice and Experience 34(7):e5906
63. Li X, Cao S, Gao L, Wen L et al (2021) A Threshold-Control Generative Adversarial Network Method for Intelligent Fault Diagnosis. Complex Syst Model Simul 1(1):55–64
64. Shi S, Hu C, Wang D, Zhu Y, Han Z (2022) Federated Anomaly Analytics for Local Model Poisoning Attack. IEEE J Sel Areas Commun 40(2):596–610
65. Zhai K, Ren Q, Wang L, Yan C (2022) Byzantine-robust federated learning via credibility assessment on non- IID data. Math Biosci Eng 19(2):1659–1676
66. Ma X, Jiang Q, Shojafar M et al (2022) DisBezant: Secure and Robust Federated Learning Against Byzantine Attack in IoT-Enabled MTS. IEEE Trans Intell Transp Syst. DOI: https://doi.org/10.1109/TITS.2022.3152156
67. Zhai K, Ren Q, Wang J, Yan C (2022) Byzantine-robust federated learning via credibility assessment on non-IID data. Math Biosci Eng 19(2):1659–1676
68. Zhang M, Mo L (2021) MGWHD-SVM: maximum weighted heteroscedastic migration learning algorithm. Int J Comput Sci Math 14(1):89–106
69. Li W, Wang S (2022) Federated meta-learning for spatial-temporal prediction. Neural Comput Appl. DOI: https://doi.org/10.1007/s00521-021-06861-3
70. McMahan H, Moore E, Ramage D, Arcas B (2016) Federated Learning of Deep Networks using Model Averaging.arXiv preprint arXiv:1602. 05629
71. Liu W, Chen L, Chen Y, Zhang W (2020) Accelerating Federated Learning via Momentum Gradient Descent. IEEE Trans Parallel Distrib Syst 31(8):1754–1766
72. Wu X, Zhang Y, Shi M et al (2022) An adaptive federated learning scheme with differential privacy preserving. Future Generation Computer Systems 127:362–372
73. Wu H, Wang P (2021) Fast-Convergent Federated Learning With Adaptive Weighting. IEEE Trans Cogn Commun Netw 7(4):1078–1088
74. Bao W, Wu C et al (2021) Edge Computing-Based Joint Client Selection and Networking Scheme for Federated Learning in Vehicular IoT. China Commun 18(6):39–52

75. Hu M, Wu D, Zhou Y et al (2020) Incentive-Aware Autonomous Client Participation in Federated Learning. IEEE Trans Parallel Distrib Syst 33(10):2612–2627
76. Liu S, Yu G, Yin R, Yuan J, Shen L, Liu C (2022) Joint Model Pruning and Device Selection for Communication-Efficient Federated Edge Learning. IEEE Trans Commun 70(1):231–244
77. Deng Y, Lyu F, Ren J et al (2022) AUCTION: Automated and Quality-Aware Client Selection Framework for Efficient Federated Learning. IEEE Trans Parallel Distrib Syst 33(8):1996–2009
78. Liao Z, Li S (2021) Solving Nonlinear Equations Systems with an Enhanced Reinforcement Learning Based Differential Evolution. Complex Syst Model Simul 2(1):78–95
79. Luo L, Zhao N, Lodewijks G (2021) Scheduling Storage Process of Shuttle-Based Storage and Retrieval Systems Based on Reinforcement Learning. Complex Syst Model Simul 1(2):131–144
80. Lai F, Zhu X, Madhyastha H, Chowdhury M (2021) Oort: Efficient federated learning via guided participant selection. In: Proceedings of the *15th USENIX Symposium on Operating Systems Design and Implementation*, OSDI 2021, pp. 19–35
81. Nishio T, Yonetani R (2019) Client Selection for Federated Learning with Heterogeneous Resources in Mobile Edge. *In: Proceedings of ICC 2019–2019 IEEE International Conference on Communications (ICC)* pp. 1–7
82. Du C, Xiao J, Guo W (2022) Bandwidth constrained client selection and scheduling for federated learning over SD-WAN. IET Commun 16(2):187–194
83. Gong W, Liao Z, Mi X et al (2021) Nonlinear Equations Solving with Intelligent Optimization Algorithms: A Survey. Complex Syst Model Simul 1(1):15–32
84. Zhao F, Di S, Cao J et al (2021) A Novel Cooperative Multi-Stage Hyper-Heuristic for Combination Optimization Problems. Complex Syst Model Simul 1(2):91–108
85. Li J, Cao F, Cheng H, Qian Y (2021) Learning the number of filters in convolutional neural networks. Int J Bio-Inspired Comput 17(2):75–84
86. Hu Y, Yan X (2021) Neural network-assisted expensive optimisation algorithm for pollution source rapid positioning of drinking water. Int J Bio-Inspired Comput 17(4):227–235
87. Li K, Xiao C (2021) CBFL: A Communication-Efficient Federated Learning Framework From Data Redundancy Perspective. IEEE Syst J. DOI: https://doi.org/10.1109/JSYST.2021.3119152
88. Lu X, Liao Y, Lio P, Pan H (2020) An Asynchronous Federated Learning Mechanism for Edge Network Computing. J Comput Res Dev 57(12):2571–2582
89. Li C, Li G, Varshney P (2021) Communication-Efficient Federated Learning Based on Compressed Sensing. IEEE Internet of Things Journal 8(20):15531–15541
90. Cheng X, You M, Ma X (2021) Bi-level optimisation model of modular product family with adaptability consideration. Int J Comput Sci Math 14(4):357–368
91. Cai J, Yang Y, Yang H, Zhao X, Hao J (2022) ACM Trans Knowl Discovery Data. DOI: https://doi.org/10.1145/3522592. ARIS: A Noise Insensitive Data Pre-processing Scheme for Data Reduction Using Influence Space
92. Cui Z, Zhao L, Zeng Y et al (2021) A Novel PIO Algorithm with multiple selection strategies for many-objective optimization problems. Complex Syst Model Simul 4(1):291–307
93. Cai X, Wang P et al (2019) Multi-Objective Three-Dimensional DV-Hop Localization Algorithm With NSGA-II. IEEE Sens J 19(21):10003–10015
94. Hou Z, Hou J (2021) Joint estimation of battery state-of-charge based on the genetic algorithm - adaptive unscented Kalman filter. Int J Comput Sci Math 14(1):1–16
95. Wang P, Xue F, Li H et al (2019) A Multi-Objective DV-Hop Localization Algorithm Based on NSGA-II in Internet of Things. Mathematics 7(2):184
96. Qiao K, Liang J, Qu B et al (2022) Differential Evolution with Level-Based Learning Mechanism. Complex Syst Model Simul 2(1):35–58
97. Zhu H, Jin Y (2020) Multi-Objective Evolutionary Federated Learning. IEEE Trans Neural Networks Learn Syst 31(4):1310–1322
98. Lan Y, Xie L, Cai X, Wang L (2022) A many-objective evolutionary algorithm based on integrated strategy for skin cancer detection. KSII Trans Internet Inf Syst 16(1):80–96
99. Wang Q, Li Q et al (2021) Efficient federated learning for fault diagnosis in industrial cloud-edge computing. Computing 103(10):2319–2337
100. Zhang J, Chen X, Wang C et al (2022) FedAda: Fast-convergent adaptive federated learning in heterogeneous mobile edge computing environment. World Wide Web-Internet and Web Information Systems. DOI: https://doi.org/10.1007/s11280-021-00989-x
101. Wang C, Yang Y, Zhou P (2021) Towards Efficient Scheduling of Federated Mobile Devices Under Computational and Statistical Heterogeneity. IEEE Trans Parallel Distrib Syst 32(2):394–410
102. Taïk A, Mlika Z, Cherkaoui S (2022) Data-Aware Device Scheduling for Federated Edge Learning. IEEE Trans Cogn Commun Netw 8(1):408–421
103. Hu K, Wu J, Weng L (2021) A novel federated learning approach based on the confidence of federated Kalman filters. Int J Mach Learn Cybernet 12(12):3607–3627
104. Tan A, Yu H, Cui L, Yang Q (2022) Toward Personalized Federated Learning. IEEE Trans Neural Networks Learn Syst. DOI: https://doi.org/10.1109/TNNLS.2022.3160699
105. Mills J, Hu J, Min G (2022) Multi-Task Federated Learning for Personalised Deep Neural Networks in Edge Computing. IEEE Trans Parallel Distrib Syst 33(3):630–641
106. Ni X, Shen X, Zhao H (2022) Federated optimization via knowledge codistillation. Expert Syst Appl 191:116310
107. Yang H, He H, Zhang W, Cao X (2021) FedSteg: A Federated Transfer Learning Framework for Secure Image Steganalysis. IEEE Trans Netw Sci Eng 8(2):1084–1094
108. Liu S, Wang J, Zhang W (2022) Federated personalized random forest for human activity recognition. Math Biosci Eng 19(1):953–971
109. Rao C, Li R (2021) Research on prediction method on RUL of motor of CNC machine based on deep learning. Int J Comput Sci Math 14(4):338–346
110. Liang B, Cai J, Yang H (2022) Grid-DPC: Improved density peaks clustering based on spatial grid walk. Appl Intell DOI. https://doi.org/10.1007/s10489-022-03705-y
111. Xu X, Peng H, Bhuiyan M et al (2022) Privacy-Preserving Federated Depression Detection From Multisource Mobile Health Data. IEEE Trans Industr Inf 18(7):4788–4797
112. Ouyang L, Yuan Y, Cao Y, Wang F (2021) A novel framework of collaborative early warning for COVID-19 based on blockchain and smart contracts. Inf Sci 570:124–143
113. Dayan I, Poth H, Zhong A et al (2021) Federated learning for predicting clinical outcomes in patients with COVID-19. Nat Med 27(10):1735–
114. Ma Z, Zhang M, Liu J et al (2022) An Assisted Diagnosis Model for Cancer Patients Based on Federated Learning. Front Oncol 12:860532
115. Mabrouk M, Afify H, Marzouk S (2021) 3D reconstruction of structural magnetic resonance neuroimaging based on computer aided detection. Int J Bio-Inspired Comput 17(3):174–181
116. Cai X, Hu Z, Zhao P et al (2020) A hybrid recommendation system with many-objective evolutionary algorithm. Expert Syst Appl 159:113648
117. Xie L, Hu Z, Cai X et al (2021) Explainable recommendation based on knowledge graph and multi-objective optimization. Complex & Intelligent Systems 7(3):1241–1252

118. Cui Z, Xu X, Xue F et al (2020) Personalized Recommendation System Based on Collaborative Filtering for IoT Scenarios. IEEE Trans Serv Comput 13(4):685–695
119. Lin G, Liang F, Pan W, Ming Z (2021) FedRec: Federated Recommendation With Explicit Feedback. IEEE Intell Syst 36(5):21–29
120. Jie Z, Chen S, Lai J, Arif M, He Z (2022) Personalized federated recommendation system with historical parameter clustering. J Ambient Intell Humaniz Comput. DOI: https://doi.org/10.1007/s12652-022-03709-z
121. Du Y, Zhou D, Xie Y, Shi J, Gong M (2021) Federated matrix factorization for privacy-preserving recommender systems. Appl Soft Comput 111:107700
122. Duan S, Zhang D, Wang Y et al (2020) JointRec: A Deep-Learning-Based Joint Cloud Video Recommendation Framework for Mobile IoT. IEEE Internet of Things Journal 7(3):1655–1666
123. Caballero A, Garcia-Valverde T, Pereniguez F, Botia J (2016) Activity recommendation in intelligent campus environments based on the Eduroam federation. J Ambient Intell Smart Environ 8(1):35–46
124. Muhammad K, Wang Q, O'Reilly-Morgan D et al (2020) FedFast: Going beyond Average for Faster Training of Federated Recommender Systems. In: Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD 2020, pp. 1234–1242
125. Wang F, Xu X, Chen M et al (2021) Simulation Research on Fire Evacuation of Large Public Buildings Based on Building Information Modeling. Complex Syst Model Simul 1(2):122–130
126. Shen Y, Yu L, Li J (2022) Robust Electric Vehicle Routing Problem with Time Windows under Demand Uncertainty and Weight-Related Energy Consumption. Complex Syst Model Simul 2(1):18–34
127. Zhang J, Zhu Z, Chang Y et al (2019) Demand Estimation of Water Resources based on Coupling Algorithm. In: Proceedings of the 31st Chinese Control and Decision Conference (2019 CCDC), pp. 714–719
128. Wang H, Wang W, Cui Z et al (2018) A new dynamic firefly algorithm for demand estimation of water resources. Inf Sci 438:95–106
129. Lu H, Dong X, Cao X (2022) Motion Model of Floating Weather Sensing Node for Typhoon Detection. Complex Syst Model Simul 2(1):96–111
130. Zhang Y, Xin D (2021) Short-term traffic flow prediction model based on deep learning regression algorithm. Int J Comput Sci Math 14(2):155–166
131. Jiang C, Li R, Chen J et al (2021) Modelling the green supply chain of hotels based on front-back stage decoupling: perspective of ant colony labour division. Int J Bio-Inspired Comput 18(2):176–188
132. Jiang J, Kantarci B, Oktug S, Soyata T (2020) Federated learning in smart city sensing: Challenges and opportunities. Sensors 20(21):6230
133. Putra K, Chen H, Prayitno (2021) Federated compressed learning edge computing framework with ensuring data privacy for pm2.5 prediction in smart city sensing applications. Sensors 21(13):4586
134. Yuan X, Chen J, Yang J et al (2022) FedSTN: Graph Representation Driven Federated Learning for Edge Computing Enabled Urban Traffic Flow Prediction. IEEE Trans Intell Transp Syst. DOI: https://doi.org/10.1109/TITS.2022.3157056
135. Liu L, Song M, Wang X et al (2021) Aircraft pushback slot allocation bi-level programming model based on congestion pricing. Int J Comput Sci Math 14(3):249–262
136. Li Y, Chen C, Liu N, Huang H et al (2021) A Blockchain-Based Decentralized Federated Learning Framework with Committee Consensus. IEEE Network 35(1):234–241
137. Cheng K, Fan T, Jin Y et al (2021) SecureBoost: A Lossless Federated Learning Framework. IEEE Intell Syst 36(6):87–98
138. Salawudeen A, Umoh I, Sadiq B, Oyenike O, Mu'azu M (2022) An adaptive ant colony optimisation for improved lane detection in intelligent automobile vehicles. Int J Bio-Inspired Comput 19(2):108–123
139. Chen Z, Chen Z, Geng Y (2022) Modelling and empirical analysis of the VMI-3PL system of cloud service platform in industry supply chain. Int J Comput Sci Math 15(1):60–71
140. Ye Y, Li S, Liu F et al (2020) EdgeFed: Optimized Federated Learning Based on Edge Computing. IEEE Access 8:209191–209198
141. Jiang H, Liu M, Yang B et al (2020) Customized Federated Learning for accelerated edge computing with heterogeneous task targets. Comput Netw 183:107569
142. Wang Q, Li Q, Wang K et al (2021) Efficient federated learning for fault diagnosis in industrial cloud-edge computing. Computing 103(10):2319–2337
143. Liu H, Zhang S, Zhang P et al (2021) Blockchain and Federated Learning for Collaborative Intrusion Detection in Vehicular Edge Computing. IEEE Trans Veh Technol 70(6):6073–6084
144. Chen N, Li Y, Liu X, Zhang Z (2021) A mutual information based federated learning framework for edge computing networks. Comput Commun 176:23–30
145. Zheng Z, Wu S, Huang Q, Yang J (2022) Research on localisation algorithm of large irregular workpiece for industrial robot. Int J Comput Sci Math 15(1):30–42
146. Zhang Y, Cai X, Zhu H, Xu Y (2020) Application an improved swarming optimisation in attribute reduction. Int J Bio-Inspired Comput 16(4):213–219
147. Cai X, Geng S, Wu D, Chen J (2021) Unified integration of many-objective optimization algorithm based on temporary offspring for software defects prediction. Swarm Evol Comput 63:100871
148. Zhang Z, Xie L (2020) A many-objective integrated evolutionary algorithm for feature selection in anomaly detection. Concurrency and Computation-Practice & Experience 32(22):e5861
149. Melis M, Scalas M et al (2022) Do gradient-based explanations tell anything about adversarial robustness to android malware? Int J Mach Learn Cybernet 13(1):217–232
150. Tang Z, Hu H, Xu C (2022) "A federated learning method for network intrusion detection. Concurrency and Computation: Practice and Experience 34(10):e6812
151. Zhao R, Yin Y, Shi Y, Xue Z (2020) Intelligent intrusion detection based on federated learning aided long short-term memory. Phys Communication 42:101157
152. Li B, Wu Y, Song J et al (2021) DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber-Physical Systems. IEEE Trans Industr Inf 17(8):5615–5624
153. Fallahpour A, Barri K, Wong K et al (2021) An integrated data mining approach to predict electrical energy consumption. Int J Bio-Inspired Comput 17(3):142–153
154. Cai X, Cao Y et al (2021) Multi-objective evolutionary 3D face reconstruction based on improved encoder-decoder network. Inf Sci 581:233–248
155. Zhang Z, Cao Y, Cui Z et al (2021) A Many-Objective Optimization Based Intelligent Intrusion Detection Algorithm for Enhancing Security of Vehicular Networks in 6G. IEEE Trans Veh Technol 70(6):5234–5243
156. Ko I, Chambers D, Barrett E (2021) Recurrent autonomous autoencoder for intelligent DDoS attack mitigation within the ISP domain. Int J Mach Learn Cybernet 12(11):3145–3167
157. Al-Hazaimeh O, Al-Jamal M, Alomari A et al (2022) Image encryption using anti-synchronisation and Bogdanov transformation map. Int J Comput Sci Math 15(1):43–59
158. Qin Z, Li G, Ye H (2021) Federated Learning and Wireless Communications. IEEE Wirel Commun 28(5):134–140

159. Yang M, Qian H, Wang X, Zhou Y, Zhu H (2022) Client Selection for Federated Learning With Label Noise. IEEE Trans Veh Technol 71(2):2193–2197
160. Wang L, Pan Z, Wang J (2021) A Review of Reinforcement Learning Based Intelligent Optimization for Manufacturing Scheduling. Complex Syst Model Simul 1(4):257–270
161. Wu X, Cao Z, Wu S (2021) Real-Time Hybrid Flow Shop Scheduling Approach in Smart Manufacturing Environment. Complex Syst Model Simul 1(4):335–350
162. Cai X, Wang P et al (2020) Weight convergence analysis of DV-hop localization algorithm with GA. Soft Comput 24(23):18249–18258
163. Peng W, Lin J, Ma X (2021) A bi-objective optimisation approach for the critical chain project scheduling problem. Int J Comput Sci Math 13(4):311–330
164. Bai H, Fan T, Niu Y (2022) Multi-UAV Cooperative Trajectory Planning Based on Many-Objective Evolutionary Algorithm. Complex Syst Model Simul 2(2):130–141
165. Lv D (2022) Scale parameter recognition of blurred moving image based on edge combination algorithm. Int J Comput Sci Math 15(2):168–182
166. Swain D, Bijawe S, Akolkar P et al (2021) Diabetic retinopathy using image processing and deep learning. Int J Comput Sci Math 14(4):397–409
167. Cai X, Zhang J, Ning Z et al (2021) A Many-Objective Multistage Optimization-Based Fuzzy Decision-Making Model for Coal Production Prediction. IEEE Trans Fuzzy Syst 29(12):3665–3675
168. Chen S, Zhang J, Bai Y et al (2021) Blockchain Enabled Intelligence of Federated Systems (BELIEFS): An attack-tolerant trustable distributed intelligence paradigm. Energy Rep 7:8900–8911
169. Cui Z, Zhang J et al (2020) Hybrid many-objective particle swarm optimization algorithm for green coal production problem. Inf Sci 518:256–271

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.