Computers and Electrical Engineering 99 (2022) 107818

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

A review on federated learning towards image processing☆

Fahad Ahmed KhoKhar [a], Jamal Hussain Shah [a], Muhammad Attique Khan [b], Muhammad Sharif [a], Usman Tariq [c], Seifedine Kadry [d,*]

[a] Department of Computer Science,COMSATS University Islamabad, Wah Campus, 47040, Pakistan
[b] Department of Computer Science,HITEC Unnversity Taxila, Taxila 47080, Pakistan
[c] College of Computer Engineering and Science, Prince Sattam Bin Abdulaziz University, Al-Kharaj, Saudi Arabia
[d] Faculty of Applied Computing and Technology, Noroff University College, Kristiansand, Norway

ARTICLE INFO

Keywords:
Ederated learning
Data privacy
Edge computing
Secure communication
Tensorflow federated

ABSTRACT

Nowadays, data privacy is an important consideration in machine learning. This paper provides an overview of how Federated Learning can be used to improve data security and privacy. Federated Learning is made up of three distinct architectures that ensure that privacy is never jeopardised. Federated learning is a type of collective learning in which individual edge devices are trained and then aggregated on the server without sharing edge device data. On the other hand, federated learning provides secure models with no data sharing, resulting in a highly efficient privacy-preserving solution that also provides security and data access. We discuss the various frameworks used in federated learning, as well as how federated learning is used with machine learning, deep learning, and datamining. This paper focuses on image processing applications that ensure that data trained on the model is secure and protected. We provide a comprehensive overview of the key issues raised in recent literature, as well as an accurate description of the related research work.

1. Introduction

Federated Learning (FL) [1] is now a novel technology which catches attention to explore its applicability and its potential by the researchers [2,3]. Federated learning only provide the solution [4] either is it able to train the model without compromising the privacy of any individuals at a central location? In the FL architecture main concern is to move towards collaboration, which cannot be achieved using traditional machine learning methods [5]. Moreover, Federated Learning tends to gain training without dispersal of data, which is not done before using standard algorithms of machine learning [6,7].

Mobile phones and other cutting-edge devices are becoming more prevalent in our daily lives. The use of these cutting-edge devices causes us to become addicted to them. Because of the widespread use of these devices, a massive amount of data is generated and growing on a daily basis. These devices are connecting over the distributed networks [8] and communicate with each other. Because the computing capacity of these edge devices associated with the transmission of private information is increasing. There is a mechanism that instead of performing computations on the network, these computations should be performed on edge devices and pushed to the edge [9].

☆ This paper is for special section VSI-cei. Reviews were processed by Guest Editor Dr. Imran Razzak and recommended for publication.

* Corresponding author.
E-mail address: skadry@gmail.com (S. Kadry).

https://doi.org/10.1016/j.compeleceng.2022.107818
Received 16 April 2021; Received in revised form 7 February 2022; Accepted 10 February 2022
Available online 17 February 2022

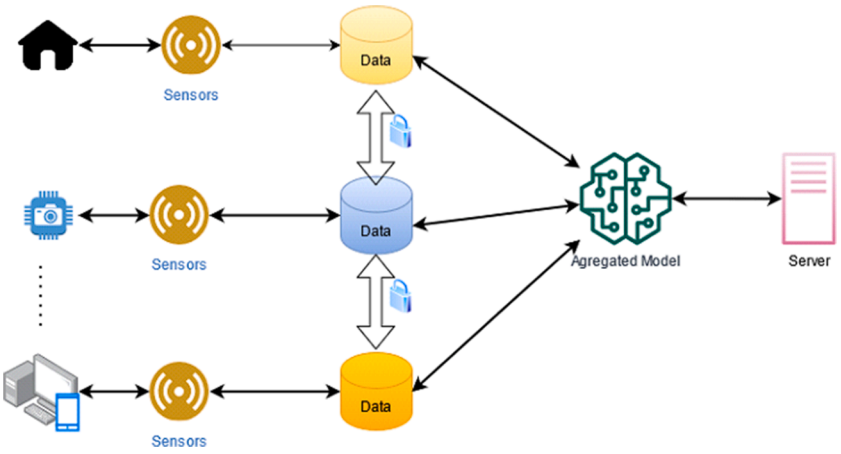

Fig. 1. Federated Learning with IoT

The art of edge computing is not new in the field there are many concepts related to edge computing i.e. FOG computing, Sensor Networks acquisition search control system, and computing at the edge [10,11]. Many Machine Learning models support storing and serve the devices locally e.g. common approach is user modeling and personalization in the mobile devices [12]. However, as the devices' storage and computational capacities within distributed networks expand, enhanced local resources can be leveraged on each node. Furthermore, Security issues regarding the transmission of raw data that would allow data generated by user data should stay on edge devices. This has resulted in an emerging awareness in federated learning [13] that discovers statistical models of training straight on remote and edge devices. The word system that utilizes in the paper is to elaborate communications network entities such that nodes, clients, or sensors.

Network devices on the Internet of Things, such that wearable technology, driverless cars [14], or home automation [15], might include many sensors that enable them to gather, respond and react in real-time to incoming data. For Instance, a group of automated driving might involve an up-to-date framework of traffic, development, or pedestrian behavioral patterns to operate safely; however, it may be difficult to build aggregate models in these situations because the data is of private nature and each device have limited connectivity. Techniques of federated learning can help train models that react successfully to variations in such environments while protecting the privacy of users.

Nowadays, Modern devices are increasing rapidly which causes a lot of data generation. These devices used many sensors that generate the data and the data is very important for the end-users [16]. These sensors collect the data and take reaction on that data and then adapt that data for the learning. For Example, there are a bunch of cameras are deployed in the Organization and there is Image Recognition System [17] is working. With the increase of IoT devices i.e. sensors which generate lot of data which cause the drifting of the data. In this [18] author briefly emphasize the concept of the drifts in data stream that is originated and generated by different end devices and sensors. Almost, 48 different datasets are used and evaluated to represent the real-world sensor data pattern that is shown in Fig. 1.

Cameras need to be trained to check the activity or recognition of the person. Instead of training the data on the server, the data should be trained on the camera and then the camera makes a centralized model and then send it to the server. For this purpose, Federated Machine Learning is used that helps in training the model without knowing the local data of the Cameras and without compromising the privacy of any camera to make a trained model [19].

As we address in this paper, learning in such an environment varies greatly from conventional distributed environments [20], requiring fundamental developments in environments i.e. anonymity, machine learning, and adaptive computation, and posing new concerns in the convergence of disparate categories such as deep neural network and systems. Big organizations have been implemented federated learning frameworks in practice [21,22] which performs a vital role in promoting privacy-sensitive systems where the training of data is dispersed on the edge devices [23,24].

Another example of GBoard which is utilized in every smartphone and mandatory part of daily life. In a virtual keyboard for smartphones, they train a coevolutionary artificial neural network (ANN) framework based on a distributed edge learning system called Next-Word Federated Learning prediction. Using the Federated Averaging algorithm, client-server testing using the gradient descent method [25] is contrasted with testing on client computers. A strong predictive recall is performed by the federated algorithm, which allows testing on higher-quality data for this usage scenario. This research shows the viability and value of the client system training classification algorithms without sending confidential personal data to servers [26]. Similary, Face Recoginition [27] is another biometric solution which is used for the security and surveillance system [28]. Authors of [29] suggest the efficient and effective method for the Face Recogniton of the human which is Particle Swarm Optimization (PSO). Moreover, this technique used the Discrete Fourier Transform to overcome the translational variance problem. The adapted method perform on different datasets i.e. CK, MMI, and JAFFE with the average accuracy of 90%.

In this paper, section II explains the architecture of the FL with their schemas which are elaborated in the Fig. 2. Section III

Table 1
List of abbrevations used throughout the manuscript.

Abbrevation	Description
FL	Federated learning
ANN	Artificial neural network
SVM	Support vector machine
SGD	Stochastic gradient descent
SGXs	Software guard extensions
CIFG	Coupled input and forget gate
fMRI	Functional MRI
CBFL	Community based federated learning
QSAR	Quantitative structure activity relationship
ESNs	Echo state networks
DNN	Deep neural network
TFF	Tensorflow federation
GANs	Generative adversarail networks
IoT	Internet of Things
MEC	Mobile edge computing
DRL	Deep reinforcement learning

comprises of the Related work with their protocols and frameworks which is used in the FL. Different kinds of application which use the support of the FL to make their data secure are elaborated in the Section IV. In this section main focus is about application used in image processing by FL are discussed. In Section V, Optimization techniques used in the FL are discussed with the benefits of each technique also elaborated. In Section VI, Privacy Outflow in FL are discussed with the exploiting attacks done on Machine Learning. In Section VII how the FL operated at edge are explained with the examples. Benefits of the FL are also discussed in the Section VII. The List of abbreviations are given in Table 1.

1.1. The architecture of the federated learning system

In this section, we elaborate on the Architecture of Federated Learning by giving examples and introduce each architecture type separately.

1.2. Horizontal federated learning

In given Fig. 2 describes a standard framework for a horizontal federated learning network. Multiple organizations have different clients which consider as K respondents with the same form of data collectively train on a model of machine-learning with the support of a cloud server or parameter using this framework. An assumption is made that the edge devices are precise and the server is truthful however, interested in learning; henceforth, there is no data loss from any kind of sample respondents is allowed [30]. Usually, the following four phases are included in the planning process for such a program.

- Edge devices compute the training gradient locally, selection of gradients is with encryption [30], confidential sharing [31] techniques, and then transmit mask results to the cloud server.
- There will be a more secure and encrypted form of aggregation which performs on the server without knowing any learning information regarding the edge devices.
- Once the server received the aggregated results it sends back that result to the edge devices.
- Edge devices then update their learning according to the decrypted gradients.

The above four steps are making continuous iteration so that the loss function becomes low, while the training process is completed. This Horizontal Architecture is free from a dedicated Machine- Learning Algorithm and all edge devices share the final model parameters.

1.3. Vertical federated learning

Suppose there are two companies i.e. Company A and B want to train the machine-learning model jointly and each company owns its data each with their business systems. However, Company B also has mark data that must be modeled by the algorithm. For purposes of data protection and confidentiality both companies A and B unable to share data directly. A third-party person C is introduced in the training process of Company A and B to make sure the security of the results. There we believe person C is trustworthy and is not colluding with Company A or B, however, Team A and B considered trustworthy but interested in one another. Team A, trustworthy third person C that is a rational presumption because Person C could be operated with the system such as authorities or substituted with protected computing nodes such as Intel Software Guard Extensions (SGXs) [33]. This FL system comprises of two portions that are shown in Fig. 3.

Part 1 Encrypted Entity Alignment: Both companies are not identical, the method used by Encrypted based user ID technique which

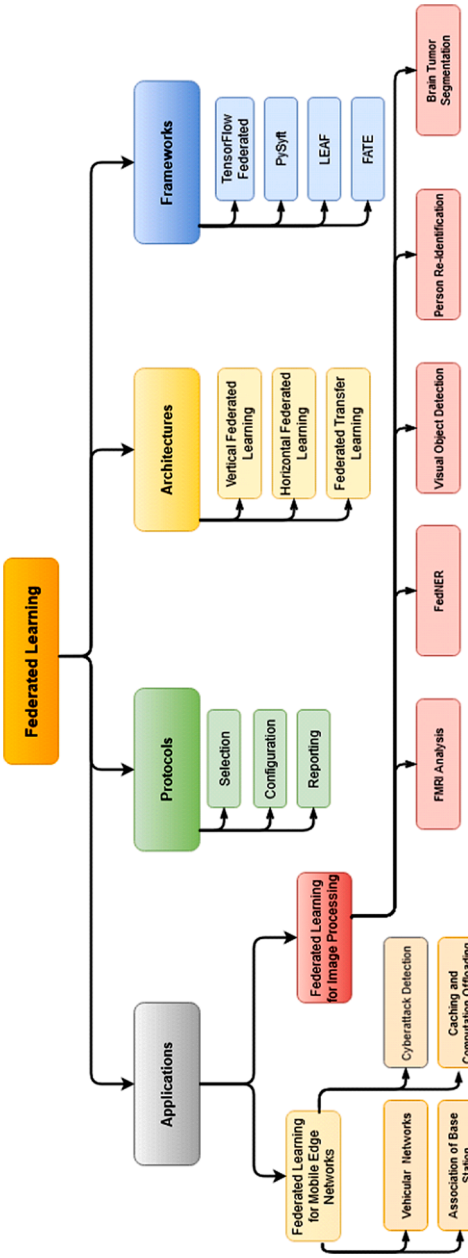

Fig. 2. Overview of federated learning.

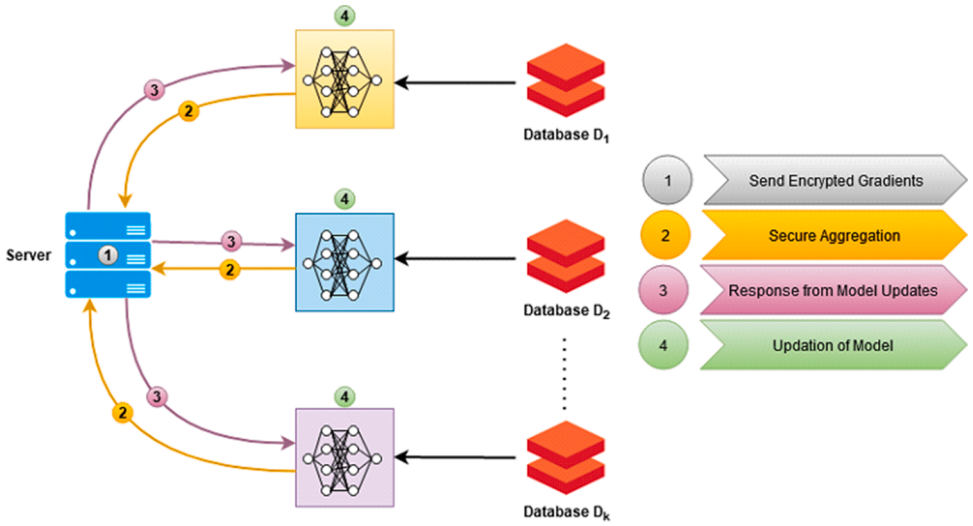

Fig. 3. Horizontal federated learning architecture [32].

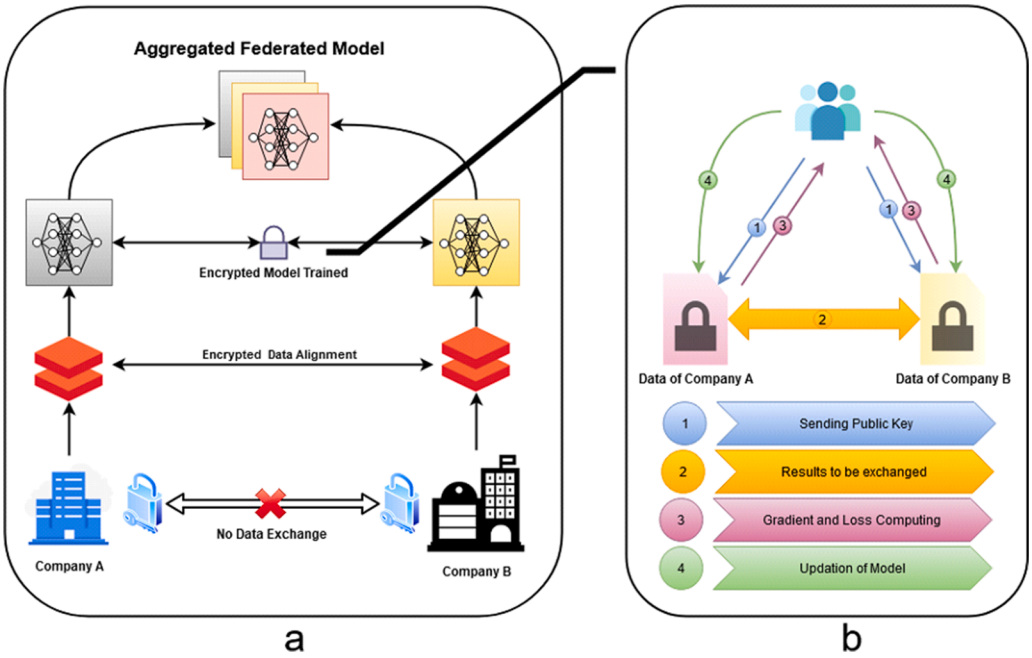

Fig. 4. Federated learning vertical architecture[32].

is well explained in [34,35] to ensure that same end-user of both companies without A and B revealing their data. During this method i. e. Entity Alignment, the system ensures that data will not be exposed and data do not intersect respectively.

Part 2 Encrypted Model Training: Once common objects are determined then these mutual objects used a machine-learning model to train their data. Thus, the training method will be divided into the following steps which are given in the Fig. 3.

- A public key and encryption pairs that are created by person C are sent to company A and B
- Company A and company B make encryption and share the intermediate results for focal loss calculation and gradient.
- Company A and company B make a computation of encrypted gradient and adding mask. A and B have to compute encrypted loss as well and then send encoded data to person C.
- Then person C performs decryption to transfer their decrypted gradient and the focal loss towards Company A and Company B. Then both companies unmask the gradients and perform updating to their models respectively.

1.4. Federated transfer learning

Transfer learning (TL) is genrally employed to reused a pre-traiend model for another task [164] and recently used in several applications such as surveillance, biometric, medical, and agriculture [165,166,167,168,169,170,171,172,173,174]. As described above example of Vertical Federated Learning, company A and company B have overlapping samples but they are very rare and we are trying to learn the labels for all data about company A. Vertical Federated Learning performs well on the overlapping data as elaborated above. To learn about all data of company A or company B the new concept of Transfer Learning [36] is introduced. Transfer Learning do not change the entire design of vertical federated Learning i.e. shown in Fig. 2 however make some changes in the results which are collaborated among company A and company B. Transfer Learning uses the same illustration as shown in Fig. 4 of feature among the company A and company B and supports in minimizing the error of label prediction for the target company with the help of source company like company B in this scenario. Henceforth, both companies A and B have different gradient computation as advised in the Federated Learning scenario.

2. Related work

Federated Learning keeps private training data while making the machine learning model. As we know that it's a novel technology, it has many branches in which Federated Learning used and some roots are already in existing fields. Here, we elaborated on Federated Learning and its relationship with other fields from multiple perspectives.

2.1. Machine learning and federated machine learning

At first glance, horizontal federated learning and distributed machine learning are both close. Distributed Machine Learning involves a variety of areas, such as the distribution of training data, the distribution of computer tasks, and the distribution of predictive models. Parameter server [38] is also a function of distributed machine learning. On distributed work nodes the parameter server stores data as a tool to speed up the training cycles. Then allocates data, computational resources to train the model more effectively through the central scheduling node. The working node represents the data holder for horizontally federated learning. It should have complete autonomy for its local data that can determine when to enter into federated learning and how to do so. The central node still regulates the server parameter; thus, a more dynamic learning system is confronted with federated learning.

Federated learning also stresses the security of data-privacy in their data. Good data protection policies will help in the future to tackle the increasingly strict regulatory climate for data privacy and data security. Federated learning, Non-IID data would also need to be discussed, as in distributed machine-learning environments. The authors of [39] have shown that output for federated learning can be greatly reduced with non-IID local data. Besides, the authors presented a new approach for tackling the problem similar to learning transfer.

2.2. Computing at edge and federated machine learning

Federated Learning has great importance and is mostly found as an edge computing operating system since it provides synchronization and protection for the learning protocol. The authors of [40] found generalized machine learning models that were learned with gradient-centric approaches. The merging boundary of the gradient descent is analyzed from a theoretical perspective, based on this a control system is proposed that will evaluate the complete method between the changes occurring and the response parameter of aggregation to reduce the gradient descent under the defined budget.

2.3. Federated databases system and federated machine learning

Federated databases system [41] are the system that includes different units in the database that control their whole system. This suggests the idea of a federated database for interoperability with different individual databases. The federated databases system mostly uses distributed database storage systems [42], and their data is of a heterogeneous type in each database unit. This indicates towards Federated Learning in the form of data structure and storage has many similarities with it. However, in the course of interacting with each other, the federated databases system doesn't require any sort of privacy protection, and their management team has full access to all database units. The federated database system, therefore, focuses on simple data operations [43] including adding, searching, deleting, and merging, while federated learning aims to build a normally utilized model and data owner to better represent the various principles and legislation obtained from the data.

2.4. Privacy-preserving machine learning

Federated Learning can be described as distributed machine learning which preserves privacy and is decentralized. This is also directly connected to multiparty, machine learning that protects anonymity. Over the past, a bunch of work has been devoted to this field. For instance, the authors of [44,45] existing methodology for vertically partitioned data to protect multiparty decision trees. Vaidyaand Clifton suggested encrypted mining rules for the association [46], secure K Means Clustering [47], and Naive Bayes classifier [48] for data that is Vertically Partitioned. The writers of [49]'s suggested rules of alignment algorithm on horizontally partitioned data.

Table 2
Frameworks and platform of FL.

Ref No.	Year	Framework	Description
[73]	2019	Tensorflow Federated	TFF is used with the combination of TensorFlow with DL. It is best to use for the distributed computations and decentralizes ML.
[74]	2018	PySyft	As Defined with the name it is used with the combination of the PyTorch. Mainly used in the privacy-preserving of the DL model as well as Secure Multiparty Computation (SMPC)
[75]	2018	LEAF	It is well helpful in Dataset that can be used in FL as a benchmark.
[76]	2018	FATE	It supports the secure and federated implementation of the ML models by WeBank

For data that is vertically partitioned [50] and for horizontally partitioned data [45] the authors proposed stable support vector machines (SVM) algorithms, In the paper [51] safe protocols for multiple party linear regression and classification were proposed. The authors of [25] suggested stable descent methods for multiparty gradients. All SMC [52] used for privacy assurances functions on these. Nikolaenko et al. [53] introduced a privacy-conserving protocol on horizontally partitioned data for linear regression using homomorphic cryptography and Yao's garbled circuits. For vertically partitioned data a linear regression approach was suggested by the authors of [54,55]. Both systems specifically solved the problem of linear regression. The authors of [56] addressed the SGD problem and also for functional regression and neural networks they suggested a privacy-preserving protocol.

Recently, there is a follow-up study was conducted for a three-server model [57]. Aono et al. [58] proposed to use homomorphic encryption to establish a secure logistic regression protocol. In the paper of [59], Shokri and Shmatikov used training of neural networks with the exchange of updated parameters on horizontally partitioned data. Thus, the recent developments in deep learning, inference of privacy-preserving artificial neural networks also receives extensive attention in the research field [60,61,62,63,64,65].

2.5. Federated machine learning and big data

Federated learning does not apply only quality in education but it also leads to business practice. The first thing that happens to people as they understand the implications of big data is to compile the large data, train the models remotely, and then import their generated results for further use. Under these demands there is technology arises i.e. cloud computing. That said, the cloud storage paradigm has been challenged by rapidly increasing the importance of data protection and a close partnership among the income of an organization and its assets.

Thus, the Federated Learning business model [66] has been introduced, however, created modern architecture for Big Data applications [67]. If the autonomous data occupied by each entity does not generate an optimal model, the federated learning system enables organizations and companies to share a single and unique model without their local data sharing. However, the Federated Learning model may render equal rules for benefit distribution using a consensus framework based on blockchain techniques [68]. The data possessors should be encouraged to join the data coalition and make their own money, irrespective of the amount of data they have. We are optimistic that the generation of the business model for the data shared between the companies and the technological framework for Federated Learning should be jointly implemented [69].

2.6. Frameworks and protocols used in federated learning

For making the privacy factor more authentic and reliable FL protocol has been introduced in [21]. All issues related to the devices which have connectivity issues as well as security of communication etc. are handled using the protocol. In each training round, there are three phases i.e. Selection, Configuration, and Reporting. Each phase of the FL protocol has a significant role in the training round.

Selection: This part as described it makes a selection of the subset of the edge device which takes part in a training model. Selection of the edge device may vary according to the need of the server. E.g. efficient training [70]. All server participants must complete the parametric updates in the round until weighted average of both the model takes place [13]. For the selection of new edge computers, protocol are analyzed to respond to the training constraint in Federated Learning.

Configuration: Thus, the server is designed and according to chosen aggregate model, such as the protected aggregation [67]. The main server then executes the planned training and generates a model for each client.

Reporting: In this updation from the participant are send to the server. Therefore, updation is also aggregated using the algorithm i.e., FedAvg algorithm.

Moreover, a connection between edge devices changing according to the FL population size as well as pace steering. The optimal Time window is managed by pace steering for edge devices to reconnecting with the FL server [21]. Pace Steering is used when the FL population is small which makes sure that the devices are connected to the server continuously and there is no distortion in the communication. Besides efficiency in communication, there is another problem that is getting attention more which is communication security:

- Protected Aggregate Model: In this identity of the FL clients are utilized and traced to infer for prevention of updates which are done locally, a server which is virtually deployed for local aggregated model [71]. The transmission of the local updates with authorized encryption is done by the Secret Sharing mechanism [72].

Table 3
Various applications with the help of FL.

Ref No.	Year	Applications	Methodology
[83]	2020	Google Keyboard Query Suggestions	Client-Server Architecture of Federated Learning
[84]	2020	Mobile Keyboard Prediction	Used Coupled Input and Forget Gate (CIFG) Network and Recurrent Neural Network Trained using FL
[85]	2019	Ranking Browser History Suggestion	RMSProp Optimization Technique used
[86]	2020	Visual Object Detection	FedVision with its components
[87]	2020	FMRI Analysis	FL on Functional MRI (fMRI) data
[88]	2019	Patient Clustering for Prediction Mortality and Stay Time at Hospital	Community-Bas ed Federated Learning (CBFL) used
[89]	2020	Biased Data Dilemma Drug Discovery	Client-Server Architecture of FL used
[90]	2020	Collaborative Drug Discovery	FL using Quantitative Structure-Activity Relationship (QSAR)
[91]	2020	Brain Tumor Segmentation	Applying differential-privacy techniques to keep the patient data in an FL
[92]	2020	Distributed Medical Databases: Meta-Analysis of Large-Scale Subcortical Brain Data	Analyzing brain structure relationships for different diseases using FL
[93]	2020	FedNER	FL for Medical Named Entity Recognition (NER)
[70]	2019	Mobile Edge Computing	Linear Regression, SVM and CNN using Federated Averaging
[81]	2020	Recommender System	Federated Stochastic Gradient Approach
[98]	2020	Persong *Re*-Identification	*Re*-Identification of the person using Federated Learning via Benchmark Analysis
[99]	2020	Number Classificaiton	Classification of the Numbers using TensorFlow with the help of Federated Learning
[94]	2018	Cyberattack Detection	Cyberattack detection model for a FL-enabled edge network
[95]	2018	Edge Caching and Computation Offloading	DRL for caching and offloading in UEs
[96]	2018	Base Station Association	FL based echo state network (ESNs) approach
[97]	2018	Vehicular Networks	Extreme Value Theory is used with the FL

Some of the applications related to Image processing are elaborated with their detailed structure using FL.

- Differential Privacy: As I directed upward in the protected aggregated model, Differential Privacy (DP) helps prevent the FL server from knowing the owner of a local update. In this regard, the main goal is to maintain privacy. In FL, the Differential Privacy [69] applied a different kind of noise factor to the existing source update, which gives security provided for the accuracy of the model.

These concepts of privacy are detailed discussed in Section VI. Some of the open-source and freely available frameworks for FL have been developed and discussed in Table 2.

3. Applications

FL is an emerging field and it is growing rapidly concerning time. Due to privacy and security consciousness, many companies and industries are moving their working towards Federated Learning. In this section, some of the applications are discussed with their methodology. Most applications of Federated Learning are related to Edge Computing [77,78,79,80] where edge devices are used as end devices. Recent researches try to combine Federated Learning with the Edge Mobile System and it shows the best performance on the recommended system [81,82]as well as Natural Language Processing.

4. FMRI analysis

Within Xiaoxiao Li, Yufeng Gu, et al. work, the main focus is standard data in the settings of healthcare. Usually, in the settings of healthcare, data fundamentally endures out of deficiency of generalizability & accuracy. Since the data of high quality isn't regularly accessible in the settings of healthcare because of concerns related to dependability, models endure in performance as well. Moreover, patients are concerned regarding their medical information that is being shared with their managers and used in the future for insurance decisions of health.

Moreover, doctors stress that in the case that their statistics of health are made publicly accessible, the patients will lose by them or they endure tremendous results when they can't evaluate the performance. Authors investigate such a problem by pertaining to FL concerning user data of MRI (fMRI). Data of fMRI is associated with numerous types of neural disorders or diseases. Authors oversaw to make their suggested system deprived of sharing of data. The suggested system comprises two primary components. About testing, the writers included resting-state fMRIs out of the Autism Brain Imaging Data Exchange dataset (ABIDE). At this time, the authors used this to identify ASDs (autism spectrum disorders) & a stable control group. The proposed method highlighted the pros of the use of FL & has imaginable use-cases for the identification of rare diseases with few patients [88].

4.1. Brain tumor segmentation

One more illustration of FL that is being applied for numerous settings of medical, was used for the segmentation of brain tumors [100]. Moreover, the specific application of FL covers medical imaging. Whereas the methods i.e. DNN (Deep Neural Networks) have

Table 4
Optimization techniques for FL models.

Optimization Technique	Benefit (s)
Ada-grad	Reliable and faster
Mini-batch Gradient Descent	More model updation and efficient
RMSProp	Minimum memory required
Fed Adagrad	Adaptable
FedAdam	More accurate
FedYogi	Adaptable

described noteworthy results, they are exceptionally contingent on the diversity & quantity of the training data [22,101,102,103]. This is tricky since desired training data might not be accessible because of possessing fewer rates of incidents of some disorders/diseases & a smaller number of individuals . Concerning such FL application, authors of [91] and [104] used the dataset of BraTS 2018, which accommodate Magnetic resonance imaging (MRI) scans of nearly three hundred people having brain tumors. Authors contrast their strategies in opposition to centralized data training. Outcomes demonstrated the best performance of the proposed method of authors.

4.2. Distributed medical databases–Meta-analysis of large-scale subcortical brain data

Now, authors of [92] oversee to suggest a system of FL for getting & examining biomedical data deprived of data sharing. Particularly, the main focus is on examining the structure of brain connections over different diseases. A huge data is comprising of images of the brain [105], hence there is a huge chance to completely understand genetic procedures concerning different diseases brain-related. Shockingly, datasets that are kept in distinctive places, can't continuously be shared due to privacy concerns, hence we are constrained in completely damaging data for considering disorders of the brain. THE proposed FL system of authors was firstly assessed using artificial data, afterward applied at various databases. The authors were able to verify their suggested system was adequate concerning the deliberate reason. A further illustration by [97] was that FL was willing to apply a system authentication framework, in particular towards imaging frameworks. At this time, the authors have been able to present their system for medical imaging platforms as an account of improvement in safety and reliability.

5. FedNER

Within such a specific FL application, a key focus is on applying FL with regard to the NER (Medical Named Entity Recognition). It consists of numerous applications in a setting of healthcare, however, adequate data that is tagged is vital with regard to training & getting a precise NER model. Unsuccessfully, in the medical community tagged data is restricted because of sensitivity. NER is centered on recognizing numerous entities of medical i.e., names of drugs, signs & symptoms out from medical texts which are unstructured & classify them into various groups. Authors in this application presented a system of FL known as FedNER to make better use of medical data & get a precise NER model deprived of exchanging medical data that is sensitive.

Within the system of FedNER, the server communicates with numerous models of clients sharing models and updating them. Clients are from distinctive medical stages. Additionally, authors assess FedNER through using data-sets of three medical NER, & uses a ratio of 80 to 20 (80% Training, 20% Testing). FedNER system was a contrast in opposition to some standard methods of NER. Authors discover that their model of FedNER is overseen to defeat other methods of NER, consequently accomplishing progressing performance generally [93]. In general, In various industries FL has numerous applications, i.e. being an FL method known as FedRec, wherever it focuses on suggestions of news [106]. Further works i.e. as [107,108,109] include the FL application with regard to handling the shortcomings of FL, i.e. collaboration & quality of data.

5.1. A way for optimization towards federated learning

There are different Optimization Techniques which is adapted by the Federated Learning Models [110] which are described in given Table 4. According to the author of the latest method, Federated Learning uses a mini-batch gradient descent. The optimization technique has been used to optimize the models. This divides the training set by small chunks used only to calculate the inconsistency of the result derived as well as to change the parameters of the model [103]. Mini-Batch Gradient Descent is used to make a compromise between the gradient descent and its results. Mini-Batch gradient descent has many benefits and drawbacks [104,105].

Moreover, other optimization techniques are also used i.e. Ada-grad, Adam, and RMSProp. These techniques of Optimization are molded for the FL. The optimization technique named Adam is the combination of RMSProp and SGD which is presented by this paper [111]. As early described Adam combine two optimization technique due to which it has multiple advantages Low memory parameters, but it also includes Works effectively although there is a slight parameter calibration. The RMSProp is also focused on the Gradient Descent process. The benefit to use the RMSProp mechanism is that it would be capable of automatically tuning the learning

algorithm, so there is no need to do it manually [106].

Also, different optimization methods are proposed by the author of [112] which are FedYogi, FedAdam, and FedAdaGrad. According to the algorithm of FedAdaGrad three steps are included i.e., initialization, make sample subsets, compute estimation. The other two methods, FedYogi and FedAdam, both have the same architecture, but there is still a significant difference in the parameters [113]. Both algorithms are dependent on the adaptivity degree which means how the algorithm can well adapt. If the parametric value is smaller than it indicated the adaptivity is high. All of these three algorithms are implemented in the Tensor Flow Federated (TFF) [73] and these are compared with the Federated Average Algorithm which gives greater accuracy than the Federated Averaging Algorithm. Summary of few optimization technique is given in Table 4.

In Wireless Networks Federated Learning has interesting facts regarding optimization techniques of the FL [114,115]. However, wireless network has some common issue like bandwidth. Some researchers found the solution for this problem which is illustrated in the [116,117,118,119] and they performed it efficiently. So, there are still flaws that should be overcome for the architecture of the Wireless Networks to put up the Federated Learning. The author of [120] intends to provide the FL's indulgence in the wireless network for improvement of communication which improves the 10 to 16% reduction of communication loss. Before the inference of the FL, it seems to be very difficult for the healthcare and wireless network [121]. Other approaches that are defined in [122,123,124] and [125] are also trying to convince the Wireless Networks [126] to include the FL and some of them try to add FL into the Internet of Things (IoT) [128,129]. As I describe earlier FL is more conscious about the Security and Privacy hence, [127] includes the FL for detection of Malicious activity done by the Clients that play a very important role while Clients are involved in the FL. FL is growing rapidly in term of their availability and applicability, this tends to lead the FL into the more edge devices as well [105]

5.2. Privacy outflow in federated learning

According to Federated Learning the main objective is that to protect the privacy of the end-users or clients that is end-user needs only to share the specified parameter of their well-trained model as a replacement for sharing the whole data. Though, with the passage of time and novelty in information Technology, some of the privacy outflow issues are raised in the FL when clients or servers are malicious. Since the primary objective of the FL is dead, the main server global model may also be distorted or even just the client may also have violated privacy while training. Although FL ensures that there is no exchange of the data between the clients for the training of the model, there are still some same classes that can interfere with the sensitive information of the model e.g., location, gender, and occupation on their shared model can be based upon client's data. In [130] while training on Face Scrub [131] data set for the binary gender classifier. They present that input of the client can be changed by inferring the dataset just working on the shared model, which causes an increase in accuracy of up to 90%. In this part, we briefly elaborate on the Privacy overflow problems that correspond to their share models in the FL.

5.3. Data exploiting attacks in machine learning

In [132] authors present that information can be retrieved from the trained model. According to this paper, Correlations are implied on the training samples which are present inside the trained model. An unexpected interfere in the model if the trained model is out. An example of an adversarial attack can interfere with the gender of an end-user using their trained model of voice recognition system. In [133], authors introduced a new algorithm for reversing a very efficient model and make effective in attacking the information from face recognition [134] or decision tree-based approach trained models. The main concern about the idea is to compare the possible value with each target feature vector, then produced a weighted estimation of the probability that is an accurate value. According to their experiments, it is shown that their technique about the adversarial can make a predicted face from the image with high accuracy from their label.

A few years ago, the authors of [135] present that attack can be done by inferring information of the victim by the queries for prediction of the model. Moreover, it usually occurs when a vulnerable edge device has access to perform prediction queries on the trained model. The vulnerable edge device could be used for the query prediction to retrieve the trained model by the owner of the data. Moreover, the author committed that this type of adversary attack might be successful in extracting the information of model from a large amount of the training models which are logistic regression, decision trees, Support Vector Machines (SVMs), and also in the complex form of training models which includes CNN and DNNs. Few of the researchers also explain the vulnerabilities and adversarial effects of DNN based trained model against the model extraction attacks [136,137,138]. Henceforth, this is the most prior concern of privacy for the edge devices in regards to sharing the trained model of the FL.

5.4. Differential privacy-based protection solutions for fl members

For the protection of the parameters privacy which is trained through DNNs, in [139] authors proposed a method, known as differentially private stochastic gradient descent that may be applied to deep learning algorithms effectively. This method's main concept is to add a few "noise" to parameters that are trained through a mechanism of differential privacy-preserving randomized

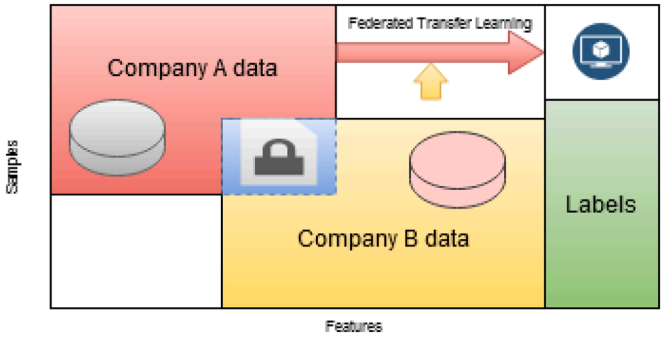

Fig. 5. Federated transfer learning architecture [37].

[140], For example, Gaussian method, before transmitting these parameters to the server. Especially, in the step of gradient averaging a basic FL member, to approach the differentially private stochastic gradient descent Gaussian distribution is applied. Afterward, at the phase of training, members continue to calculate the probability so that malicious members can harm the data from its parameters that are shared. When a predefined threshold is approached, the training process will stop by a member.

So, the member can overcome the risk of leaking information that is private from its parameters that are shared. To be inspired by this proposal, the authors in [141] create a method that can get a solution of privacy-protection for members which is better. In this approach, their authors propose two significant steps to analyze the data prior passing the trained parameter to a server. Especially, about every step of learning, firstly aggregate server chooses a number that is random among members for the training of the Global Model. Afterward, whether a member is chosen for the training of the Global model in the step of learning a member will accept the proposed method in [139], Such as using a method of Gaussian Distribution for adding noise to the model which is trained before transmitting training parameters to the server. As a result, a malicious participant cannot collect data from certain participants while using parameters of such a common global model as it does not have data such as who has participated in each training phase.

5.5. Collaborative training solutions

Although deep learning solutions can secure data that is private of authorized members from other participants who are malicious in FL, they work properly only whenever the server is trustworthy. Whenever the server is harmful or malicious, on the network there is a serious threat regarding privacy to the entire members. So, in [59] the authors present a framework of collaborative deep learning to provide various members to learn the global model deprived of sending their definite training models to the server. The main concept of this method is rather than sending entire trained parameters set to the server & improving Global parameters concerning its local model, every member carefully chooses a list of gradients to send & many parameters depriving of a global model for updating like elaborated in Fig. 5.

Regarding this, harmful members can't harm private data from the model that is shared. The important outcome of this paper is that whenever Global parameters Local training dataset Aggregator SGD choose parameters to improve select parameters to send Server member Local parameters. Members don't share entire parameters that are trained & don't improve entire parameters through the model that is shared, proposed solution's accuracy is yet near to that of the stage once a server has an entire set of data for the training of the Global model. e.g., in regards to the dataset of MNIST [142], prediction model accuracy once members admit for the sharing of 10% & 1% of their trained parameters that's entire at once 99.14% & 98.71%, correlated with the 99.17% regarding integrated output once entire data need to train on the sever.

So, the method is yet to be tested on additional complicated classification duties. Whereas sharing of selective parameter & deep learning solutions can make data manipulating threats further critical, in [143] the authors present that such solutions are impressionable to a kind of new attack, known as forceful attack, created based on Generative Adversarial Networks [144]. GANs (Generative Adversarial Networks) is a machine learning method class that uses binary neural networks, called discriminator networks and generator networks, which challenge one another to train the data. The Generator network seeks to generate the forged data in addition to little noise to original data. Afterward, for classification for generating forged data is send to the discriminator network. Then after the process of training, Generative Adversarial Networks can generate data that is new with identical statistics like the dataset of training. Influenced by such concept, in [143] the authors make a forceful attack that permits a harmful member to harm data that is sensitive from a victim member alike with totally a component of shared parameters along with the victim.

To handle with Generative Adversarial Networks attack, in [145] authors proposed a solution using a confidential scheme of sharing regarding the greatest boosting algorithm. This method implements a delicate confidential sharing protocol before sending up to date trained model within plaintext to the server in every step. So, in the network, other members can't change information from the

model that is shared. Therefore, the restrictions of this method are the dependence on a trustworthy third party to create signature key sets.

In contrast to the entire mentioned works, the authors in [146] proposed a cooperative training model in which entire members collaborate to train a Generative Adversarial Networks model which is federated. An important concept of this technique is that the model of federated Generative Adversarial Networks can create artificial data that may be substitute members' original data, & so securing the confidentiality of original data for the legal members.

Especially, to make sure that the privacy of members' data and yet sustaining stretchability in training duties, this method gives a federated generative model. This federated generative model can result in artificial data that doesn't associate with any legal member especially, yet comes from the usual data distribution of cross-user. Subsequently, this method can importantly decrease the probability of harmful misuse of information from the original information. Therefore, this method assumes existing restrictions of Generative Adversarial Networks that already exist, such that, the uncertainty of training because of the generated forges data, that can effectively decrease the functioning of cooperative learning models.

5.6. Encryption-based solutions

Encryption is a successful method for securing the privacy of data regarding members once they desire to share their trained parameters in the FL. In [30], a technique of homomorphic encryption is presented for securing the member's privacy by sharing their parameters from a trustworthy yet strange server. The trustworthy but inquisitive server remains explained to a member that desires to retrieve data from their shared parameters of members, In good condition yet retains entire processes in FL. The idea of such a solution seems to be that the client's qualified parameters that will be encoded by using a technique called homomorphic encryption technique before uploading to the server. This method also successful in securing data that is sensitive or confidential from that kind of server and it also has the same precision and accuracy as that of the consolidated deep learning algorithm.

Another related idea that is proposed in [71] using the confidential method of sharing which are used to secure their information of FL members. Even though both methods of encryption are proposed in [30,71] can intercept the strange server from getting information, they need various stages of communications & can't prevent collaborations among server & members [148]. So, in [149] the authors introduce a novel hybrid solution that combines both deep learning & homomorphic encryption within FL. Especially, before the parameters that are trained and transmitted to the server, their might be encryption by using the additional encryption method i.e. homomorphic encryption method combines with additional noises to disturbed real parameters. Consequently, this novel hybrid approach at the same time intercept the strange server from harming information moreover resolve the problem of collusion among the server & harmful members. Therefore, the authors don't contrast the presented method accuracy with the condition without homomorphic encryption & deep learning.

5.7. Federated learning at edge

As previously discuss FL never compromises on the Privacy of the end devices which enables the revolutionary IoT devices to use the FL in the Edge devices. Authors of [150] discuss the novel idea of Mobile Edge Computing with the use of FL. There is two major work done in which one is about the Communication gap between the wireless networks in Edge Computing and configure them dynamically using machine learning algorithm with the increase in efficiency of training of FL. Moreover, the global model of the FL accuracy never compromises according to their algorithm. In another article [151] they found different four design aspects i.e. learning Algorithm design, hardware-software co-design based edge devices, resource optimization, and incentive mechanism. Another novel approach is game-theoretic incentive mechanisms [152] used for making effective interaction between the edge devices and servers of the FL. There are two main branches of edge computing each is described below:

5.8. Cloud edge

Nowadays, Different IoT devices are interlinked and make a global connection with each other. While the connection with each other there is a communication gap which makes the distortion in the communication of the devices which is termed as Access Time. In [153] a new methodology is proposed which is named as PerFit, a personalized FL framework in Cloud Edge for IoT application [154] with extensive data privacy protection. Through aggregating local changes from the global Edge system [155] and exploiting the strengths of edge computing, PerFit helps you to learn a globally shared paradigm. PerFit can naturally incorporate a range of customized federated learning methods to solve the system, statistical, and framework heterogeneities in Cloud devices and thereby achieve personalization and improved efficiency for systems in IoT applications. To minimize the straggle result, PerFit architecture simplifies edge computing to increase the computational capacity of individual devices through cloud computing.

5.9. Mobile edge

In the past few years, Edge Devices are increasing rapidly with the magnificent sensing and computational capabilities. With the time Deep Learning introduced in Mobile devices and It brings versatility to mobile applications e.g., for medical purposes and in the Vehicle network. As data servers are present outside the cloud these days, Mobile Edge Computing adopted a new generous solution in which storage and computing functionalities [156] of Mobile edge devices and Server Edge are bring training model closer to the source of the data [157] i.e. edge devices. As defined in [158] end-edge cloud computing network is made up of the following i.e. edge devices, edge nodes, and cloud servers. Different approaches to Cloud-based machine learning enables the data to be centralized in a data center or any cloud server. Another framework introduced is Mobile Edge Computing (MEC) which makes all devices close the data which reduced the communication problem. In [147] the concept of Federated Learning is used to train the data locally instead of globally and send the data model to the server for the aggregation of the model.

5.10. Benefits of federated learning

As we know that Federated Learning is more caring about Privacy so many industries are encouraged to apply the Federated Learning and ensure that their privacy is not vanished [159]. In FL the data is always on the Consumer edge device which is also the main reason for moving towards this novel technology. Federated Learning provides the new framework of working while In traditionally, training algorithms are dependent on the centralized architecture [160]. A new approach of decentralizing solution is offered by FL which gives more performance as well as efficiency on large data sets. To encourage the industries to apply the federated learning model, we have to perform the cost and benefit analysis carefully [161].

As far as we concern about the Benefits of FL, there are a lot. One of the most crucial benefits of FL is the removal of privacy concerns [145]. Federated Learning is most usable where the privacy concerns are most like data access and management of data. Due to which it is perfect for those companies and industries where are more concerned with the privacies. Because FL is working on the decentralized approach, we don't worry about the training algorithm and the data. The training Algorithm is responsible to train the edge devices and only share the relevant data which is required [162]. Federated Learning carried out their process even the edge devices are on charging, may be connected through WIFI, or in use. So end-user doesn't need to worry about their battery and data leakage [163]. There is a summary of the major benefits which are illustrated as follows.

- **Real-time prediction:** As far as the concern with the FL all prediction is done on the edge devices themselves so there is no need to worry about a time-lag issue while sending and receiving the data.
- **Privacy and security of data:** Because the training is done on itself, there is the only model that needs to be transferred. Due to which there is no issue of the privacy and security of the confidential or personal data in the centralized location.
- **Offline prediction:** The process of prediction is also carried out even the devices are offline. Hence, there is no need to worry about the devices either it is online or offline. As far as devices get to input the model can utilize them to do their work.
- **Smart framework:** As FL does not need any kind of complex hardware to carry out their operations, however, infrastructure requirements are very minimum.

Overall, FL providing a lot of benefits that compel the different industries to utilize their framework for different reasons. Unfortunately, FL is not a good approach, so we consider some preventions about which device needs to be useful and which framework of FL is used to get the most benefits. However, it can be employed in many applications such as medical and named a few more [175,176,177,178,179].

6. Conclusion

Data security is becoming a more sensitive and important challenge with the increase of Artificial Intelligence. There are many issues related to security and data thefting in past but Federated Learning gives us new hope to work secure and smart way. Their encryption technology ensures that the communication between edge devices is encrypted and there is no loss of data or any privacy issue. Using Federated Learning make a model for different industries without compromising on the local data so that the industries could work along with others on data security. Different systems and server use their infrastructure and hardware which can also affect the efficiency of the FL and also provide a bad impact on data privacy. FL also help the end user if they don't have labeled data for training, it enables the training of the model without sharing the data to other end user. In the future Federated Learning become more valuable and demanding in the industry because everyone is ready to pay for the security of data and it trains the other model without knowing the data of any company or participant. Artificial Intelligence makes our lives easier in the future using this Federated Learning. Moreover, FL is more concerned about the communication between edge devices and the server and tries to minimize the lack of issues between them. FL should need to address the privacy outflow issues which are still mandatory to overcome because no one is ready to compromise on the privacy of their data.

Uncited link

(Table 1), (Table 3), Fig. 6

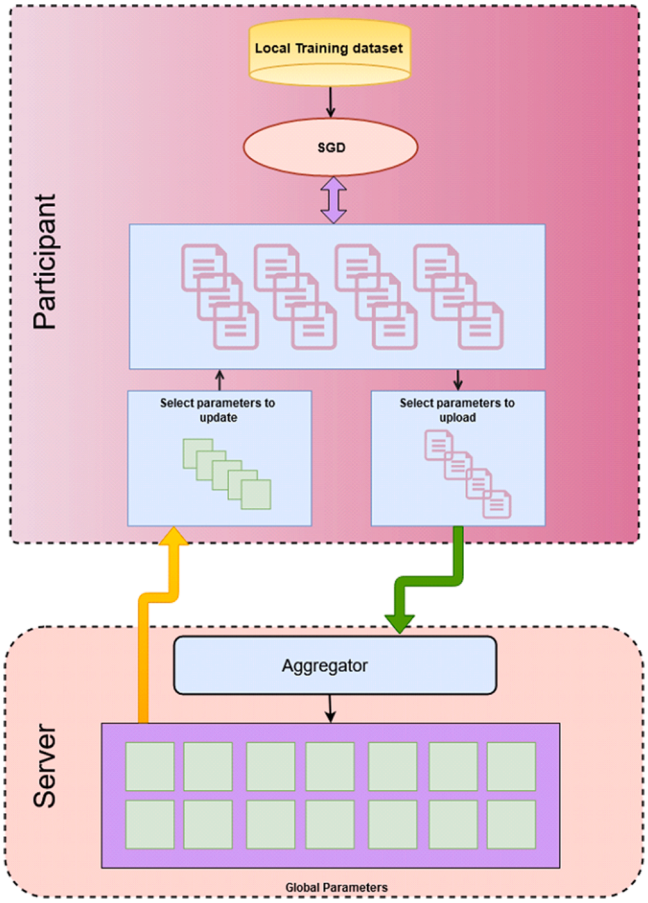

Fig. 6. Sharing model for selective parameters [147].

Declaration of Competing Interest

All authors declare that they have no conflict of interest in this work. All authors contributed equally.

References

[1] P.P. Liang et al., "Think locally, act globally–Federated learning with local and global representations," ArXiv200101523 Cs Stat, Jul. 2020, Accessed: Nov. 12, 2020. [Online]. Available: http://arxiv.org/abs/2001.01523.
[2] H.H. Zhuo, W. Feng, Y. Lin, Q. Xu, and Q. Yang, "Federated deep reinforcement learning," ArXiv190108277 Cs, Feb. 2020, Accessed: Nov. 12, 2020. [Online]. Available: http://arxiv.org/abs/1901.08277.
[3] "A fairness-aware incentive scheme for federated learning | Proceedings of the AAAI/ACM conference on AI, Ethics, and Society." https://dl.acm.org/doi/abs/10.1145/3375627.3375840 (accessed Nov. 12, 2020).
[4] "A. Hybrid Approach to privacy-preserving federated learning | Proceedings of the 12th ACM workshop on artificial intelligence and security." https://dl.acm.org/doi/abs/10.1145/3338501.3357370?casa_token=v0r8hPlAzLAAAAAA:0vS0oc2CCrU5dhwscT3-PF_Gww2WRop2go_uWZBnWNsxuiNzIn5hW28YXGXc314cO6cjLGwAGeeu (accessed Nov. 12, 2020).
[5] "(PDF) A novel approach to machine learning application to protection privacy data in healthcare–Federated learning | Ahmet Ali Süzen - Academia.edu." https://www.academia.edu/42883324/A_NOVEL_APPROACH_TO_MACHINE_LEARNING_APPLICATION_TO_PROTECTION_PRIVACY_DATA_IN_HEALTHCARE_FEDERATED_LEARNING (accessed Nov. 12, 2020).
[6] S. Lin, G. Yang, and J. Zhang, "Real-time edge intelligence in the making–A collaborative learning framework via federated meta-learning," ArXiv200103229 Cs Stat, May 2020, Accessed: Nov. 12, 2020. [Online]. Available: http://arxiv.org/abs/2001.03229.
[7] Pandey SR, Tran NH, Bennis M, Tun YK, Manzoor A, Hong CS. A crowdsourcing framework for on-device federated learning. IEEE Trans Wirel Commun May 2020;19(5):3241–56. https://doi.org/10.1109/TWC.2020.2971981.
[8] D. Remédios, A. Teófilo, H. Paulino, and J. Lourenço, "Mobile device-to-device distributed computing using data sets," Aug. 2015. doi: 10.4108/eai.22-7-2015.2260273.

[9] R. Alameh, W.S. Hede, L.J. Vannatta, M.W. Schellinger, and K.A. Paitl, "Method and system for conducting communication between mobile devices," US8391719B2, Mar. 05, 2013 Accessed: Nov. 12, 2020. [Online]. Available: https://patents.google.com/patent/US8391719B2/en.
[10] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," p. 3.
[11] Madden SR, Franklin MJ, Hellerstein JM, Hong W. TinyDB–An acquisitional query processing system for sensor networks. ACM Trans Database Syst Mar. 2005; 30(1):122–73. https://doi.org/10.1145/1061318.1061322.
[12] Kuflik T, Kay J, Kummerfeld B. Challenges and solutions of ubiquitous user modeling. Cogn Technol Apr. 2012. https://doi.org/10.1007/978-3-642-27663-7_2.
[13] H.B. McMahan, E. Moore, D. Ramage, S. Hampson, and B.A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," ArXiv160205629 Cs, Feb. 2017, Accessed: Nov. 03, 2020. [Online]. Available: http://arxiv.org/abs/1602.05629.
[14] "[PDF] Visual SLAM for driverless cars –A brief survey | Semantic scholar." www.semanticscholar.org/paper/Visual-SLAM-for-Driverless-Cars-%3A-A-Brief-Survey-Ros-Sappa/5229c6781deb77dec8499985943ab3e057a86d26 (accessed Nov. 12, 2020).
[15] Kodali RK, Jain V, Bose S, Boppana L. IoT based smart security and home automation system. In: 2016 international conference on computing, communication and automation (ICCCA); Apr. 2016. p. 1286–9. https://doi.org/10.1109/CCAA.2016.7813916.
[16] V. Natarajan, K. Ranganathan, J.J. Sydir, and A. Vyas, "Efficient mesh network data gathering," US10778556B2, Sep. 15, 2020 Accessed: Nov. 12, 2020. [Online]. Available: https://patents.google.com/patent/US10778556B2/en.
[17] "[2001.05566] Image segmentation using deep learning–A survey." https://arxiv.org/abs/2001.05566 (accessed Nov. 12, 2020).
[18] Toor AA, Usman M, Younas F, Fong ACM, Khan SA, Fong S. Mining massive E-health data streams for IoMT enabled healthcare systems. Sensors Jan. 2020;20 (7). https://doi.org/10.3390/s20072131. Art7.
[19] Wang C, Wang Q, Ren K, Lou W. Privacy-preserving public auditing for data storage security in cloud computing. In: 2010 proceedings IEEE INFOCOM; Mar. 2010. p. 1–9. https://doi.org/10.1109/INFCOM.2010.5462173.
[20] "(PDF) A comparison of conventional distributed computing environments and computational grids." https://www.researchgate.net/publication/215759989_A_Comparison_of_Conventional_Distributed_Computing_Environments_and_Computational_Grids (accessed Nov. 12, 2020).
[21] K. Bonawitz et al., "Towards federated learning at scale–System design," ArXiv190201046 Cs Stat, Mar. 2019, Accessed: Nov. 03, 2020. [Online]. Available: http://arxiv.org/abs/1902.01046.
[22] Sharif Muhammad Imran, Alhussein Musaed, Aurangzeb Khursheed, Raza Mudassar. A decision support system for multimodal brain tumor classification using deep learning. Complex Intell Syst 2021:1–14.
[23] Brisimi TS, Chen R, Mela T, Olshevsky A, Ch I, lidis Pasch, Shi W. Federated learning of predictive models from federated electronic health records. Int. J. Med. Inf. Apr. 2018;112:59–67. https://doi.org/10.1016/j.ijmedinf.2018.01.007.
[24] Huang L, Yin Y, Fu Z, Zhang S, Deng H, Liu D. LoAdaBoost–Loss-based AdaBoost federated machine learning with reduced computational complexity on IID and non-IID intensive care data. PLoS One Apr. 2020;15(4):e0230706. https://doi.org/10.1371/journal.pone.0230706.
[25] L. Wan, W.K. Ng, S. Han, and V.C. S. Lee, "Privacy-preservation for gradient descent methods," in Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining, New York, USA, Aug. 2007, pp. 775–783. doi: 10.1145/1281192.1281275.
[26] A. Hard et al., "Federated learning for mobile keyboard prediction," ArXiv181103604 Cs, Feb. 2019, Accessed: Nov. 03, 2020. [Online]. Available: http://arxiv.org/abs/1811.03604.
[27] M. Murtaza, M. Raza, and J.H. Shah, "Face recognition using adaptive margin fisher's criterion and linear discriminant analysis," vol. 11, no. 2, p. 10, 2014.
[28] Javed Kashif, Khan Sajid Ali, Saba Tanzila, Habib Usman, Khan Junaid Ali, Abbasi Aaqif Afzaal. Human action recognition using fusion of multiview and deep features: an application to video surveillance. Multimed Tools Appl 2020:1–27.
[29] Khan SA, Ishtiaq M, Nazir M, Shaheen M. Face recognition under varying expressions and illumination using particle swarm optimization. J Comput Sci Sep. 2018;28:94–100. https://doi.org/10.1016/j.jocs.2018.08.005.
[30] L.T. Phong, Y. Aono, T. Hayashi, L. Wang, and S. Moriai, "Privacy-preserving deep learning via additively homomorphic encryption," p. 18.
[31] K. Bonawitz et al., "Practical secure aggregation for privacy-preserving machine learning," in Proceedings of the 2017 ACM SIGSAC conference on computer and communications security, Dallas Texas USA, Oct. 2017, pp. 1175–1191. doi: 10.1145/3133956.3133982.
[32] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning–Concept and applications," ArXiv190204885 Cs, Feb. 2019, Accessed: Nov. 03, 2020. [Online]. Available: http://arxiv.org/abs/1902.04885.
[33] Bahmani R, et al. Secure multiparty computation from SGX. In: Kiayias A, editor. Financial cryptography and data security, 10322. Cham: Springer International Publishing; 2017. p. 477–97. https://doi.org/10.1007/978-3-319-70972-7_27.
[34] M. Scannapieco, I. Figotin, E. Bertino, and A.K. Elmagarmid, "Privacy preserving schema and data matching," in Proceedings of the 2007 ACM SIGMOD international conference on Management of data, New York, USA, Jun. 2007, pp. 653–664. doi: 10.1145/1247480.1247553.
[35] Liang G, Chawathe SS. Privacy-preserving inter-database operations. In: Chen H, Moore R, Zeng DD, Leavitt J, editors. Intelligence and security informatics, 3073. Berlin, Heidelberg: Springer Berlin Heidelberg; 2004. p. 66–82. https://doi.org/10.1007/978-3-540-25952-7_6.
[36] Pan SJ, Yang Q. A survey on transfer learning. IEEE Trans Knowl Data Eng 2009;22(10):1345–59.
[37] S. Saha and T. Ahmad, "Federated transfer learning–Concept and applications," ArXiv201015561 Cs, Sep. 2020, Accessed: Dec. 04, 2020. [Online]. Available: http://arxiv.org/abs/2010.15561.
[38] Ho Q, et al. More effective distributed ML via a stale synchronous parallel parameter server. In: Proceedings of the 26th International Conference on Neural Information Processing Systems. 1. NY, USA: Red Hook; Dec. 2013. p. 1223–31.
[39] Y. Zhao, M. Li, L. Lai, N. Suda, D. Civin, and V. Chandra, "Federated learning with non-IID data," ArXiv180600582 Cs Stat, Jun. 2018, Accessed: Nov. 03, 2020. [Online]. Available: http://arxiv.org/abs/1806.00582.
[40] Wang S, et al. When edge meets learning–Adaptive control for resource-constrained distributed machine learning. In: IEEE INFOCOM 2018 - IEEE conference on computer communications. HI: Honolulu; Apr. 2018. p. 63–71. https://doi.org/10.1109/INFOCOM.2018.8486403.
[41] Sheth AP, Larson JA. Federated database systems for managing distributed, heterogeneous, and autonomous databases. ACM Comput Surv Sep. 1990;22(3): 183–236. https://doi.org/10.1145/96602.96604.
[42] R. Murthy and R. Goel, "System and method for distributed database query engines," US9081826B2, Jul. 14, 2015 Accessed: Nov. 12, 2020. [Online]. Available: https://patents.google.com/patent/US9081826B2/en.
[43] R. Ziglin, "Methods and apparatus for interfacing application programs with database functions," US20030033317A1, Feb. 13, 2003 Accessed: Nov. 12, 2020. [Online]. Available: https://patents.google.com/patent/US20030033317A1/en.
[44] W. Du and Z. Zhan, "Building decision tree classifier on private data," p. 9.
[45] Yu H, Vaidya J, Jiang X. Privacy-preserving SVM classification on vertically partitioned data. In: Ng W-K, Kitsuregawa M, Li J, Chang K, editors. Advances in knowledge discovery and data mining, 3918. Berlin, Heidelberg: Springer Berlin Heidelberg; 2006. p. 647–56. https://doi.org/10.1007/11731139_74.
[46] J. Vaidya and C. Clifton, "Privacy preserving association rule mining in vertically partitioned data," p. 6.
[47] Vaidya J, Clifton C. Privacy-preserving k-means clustering over vertically partitioned data. In: Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining. NY, USA: New York; Aug. 2003. p. 206–15. https://doi.org/10.1145/956750.956776.
[48] J. Vaidya and C. Clifton, "Privacy Preserving Näive Bayes Classifier for Vertically Partitioned Data," p. 5.
[49] Kantarcioglu M, Clifton C. Privacy-preserving distributed mining of association rules on horizontally partitioned data. IEEE Trans Knowl Data Eng Sep. 2004; 16(9):1026–37. https://doi.org/10.1109/TKDE.2004.45.
[50] Yu H, Jiang X, Vaidya J. Privacy-preserving SVM using nonlinear kernels on horizontally partitioned data. In: Proceedings of the 2006 ACM symposium on applied computing. NY, USA: New York; Apr. 2006. p. 603–10. https://doi.org/10.1145/1141277.1141415.
[51] Du W, Han YS, Chen S. Privacy-preserving multivariate statistical analysis–Linear regression and classification. In: Proceedings of the 2004 SIAM international conference on data mining; Apr. 2004. p. 222–33. https://doi.org/10.1137/1.9781611972740.21.
[52] A.C. Yao, "Protocols for secure computations," p. 5.

[53] Nikolaenko V, Weinsberg U, Ioannidis S, Joye M, Boneh D, Taft N. Privacy-preserving ridge regression on hundreds of millions of records. In: Proceedings of the 2013 IEEE symposium on security and privacy. USA; May 2013. p. 334–48. https://doi.org/10.1109/SP.2013.30.

[54] A. Gascón et al., "Secure linear regression on vertically partitioned datasets," IACR Cryptol EPrint Arch, 2016.

[55] Giacomelli I, Jha S, Joye M, Page CD, Yoon K. Privacy-preserving ridge regression with only linearly-homomorphic encryption. In: Preneel B, Vercauteren F, editors. Applied cryptography and network security, 10892. Cham: Springer International Publishing; 2018. p. 243–61. https://doi.org/10.1007/978-3-319-93387-0_13.

[56] Mohassel P, Zhang Y. SecureML–A system for scalable privacy-preserving machine learning. In: 2017 IEEE symposium on security and privacy (SP). CA, USA: San Jose; May 2017. p. 19–38. https://doi.org/10.1109/SP.2017.12.

[57] Mohassel P, Rindal P. ABY^3–A mixed protocol framework for machine learning. In: Proceedings of the 2018 ACM SIGSAC conference on computer and communications security. NY, USA: New York; Jan. 2018. p. 35–52. https://doi.org/10.1145/3243734.3243760.

[58] Aono Y, Hayashi T, Trieu Phong L, Wang L. Scalable and secure logistic regression via homomorphic encryption. In: Proceedings of the sixth ACM on conference on data and application security and privacy - CODASPY '16. Louisiana, USA: New Orleans; 2016. p. 142–4. https://doi.org/10.1145/2857705.2857731.

[59] Shokri R, Shmatikov V. Privacy-preserving deep learning. In: Proceedings of the 22nd ACM SIGSAC conference on computer and communications security - CCS '15. Colorado, USA: Denver; 2015. p. 1310–21. https://doi.org/10.1145/2810103.2813687.

[60] H. Chabanne, A. de Wargny, J. Milgram, C. Morel, E. Prouff, and S. Identity, "PrivaCY-PRESERVING CLASSIfiCATION ON DEEP NEURAL NETwork," p. 18.

[61] N. Dowlin, R. Gilad-Bachrach, K. Laine, K. Lauter, M. Naehrig, and J. Wernsing, "CryptoNets–Applying neural networks to encrypted data with high throughput and accuracy," p. 10.

[62] E. Hesamifard, H. Takabi, and M. Ghasemi, "CryptoDL–Deep neural networks over encrypted data," ArXiv171105189 Cs, Nov. 2017, Accessed: Nov. 03, 2020. [Online]. Available: http://arxiv.org/abs/1711.05189.

[63] Liu J, Juuti M, Lu Y, Asokan N. Oblivious neural network predictions via MiniONN transformations. In: Proceedings of the 2017 ACM SIGSAC conference on computer and communications security. USA: Dallas Texas; Oct. 2017. p. 619–31. https://doi.org/10.1145/3133956.3134056.

[64] Riazi MS, Weinert C, Tkachenko O, Songhori EM, Schneider T, Koushanfar F. Chameleon–A hybrid secure computation framework for machine learning applications. In: Proceedings of the 2018 on Asia conference on computer and communications security - ASIACCS '18. Republic of Korea: Incheon; 2018. p. 707–21. https://doi.org/10.1145/3196494.3196522.

[65] Rouhani BD, Riazi MS, Koushanfar F. Deepsecure: scalable provably-secure deep learning. In: Proceedings of the 55th annual design automation conference. California: San Francisco; Jun. 2018. p. 1–6. https://doi.org/10.1145/3195970.3196023.

[66] "Federated learning–A new AI business model | by alexandre gonfalonieri | Towards data science." https://towardsdatascience.com/federated-learning-a-new-ai-business-model-ec6b4141b1bf (accessed Nov. 12, 2020).

[67] "Big data application architecture | SpringerLink." https://link.springer.com/chapter/10.1007/978-1-4302-6293-0_2 (accessed Nov. 12, 2020).

[68] Gao W, Hatcher WG, Yu W. A survey of blockchain–Techniques, applications, and challenges. In: 2018 27th international conference on computer communication and networks (ICCCN); Jul. 2018. p. 1–11. https://doi.org/10.1109/ICCCN.2018.8487348.

[69] K. Cheng, T. Fan, Y. Jin, Y. Liu, T. Chen, and Q. Yang, "SecureBoost–A lossless federated learning framework," ArXiv190108755 Cs Stat, Jan. 2019, Accessed: Nov. 12, 2020. [Online]. Available: http://arxiv.org/abs/1901.08755.

[70] Nishio T, Yonetani R. Client selection for federated learning with heterogeneous resources in mobile edge. In: ICC 2019 - 2019 IEEE international conference on communications (ICC); May 2019. p. 1–7. https://doi.org/10.1109/ICC.2019.8761315.

[71] K. Bonawitz et al., "Practical secure aggregation for privacy-preserving machine learning," in Proceedings of the 2017 ACM SIGSAC conference on computer and communications security, New York, NY, USA, Oct. 2017, pp. 1175–1191. doi: 10.1145/3133956.3133982.

[72] "How to share a secret | Communications of the ACM." https://dl.acm.org/doi/abs/10.1145/359168.359176?casa_token=I1VwrZdw0dEAAAAA:7HrDGHnl2sCSIwf50OE-Eq3X1nDfLVMZ5_80PD4U0TJXHX7Q3yrcBVisjWhF6uvIMKN7HgGyDo2aYz0 (accessed Dec. 30, 2020).

[73] "TensorFlow Federated." https://www.tensorflow.org/federated (accessed Dec. 01, 2020).

[74] T. Ryffel et al., "A generic framework for privacy preserving deep learning," ArXiv181104017 Cs Stat, Nov. 2018, Accessed: Dec. 30, 2020. [Online]. Available: http://arxiv.org/abs/1811.04017.

[75] S. Caldas et al., "LEAF–A Benchmark for Federated Settings," ArXiv181201097 Cs Stat, Dec. 2019, Accessed: Dec. 30, 2020. [Online]. Available: http://arxiv.org/abs/1812.01097.

[76] FedAI, "HOME," Fate. https://fate.fedai.org/(accessed Dec. 30, 2020).

[77] M. Duan et al., "Astraea–Self-balancing federated learning for improving classification accuracy of mobile deep learning applications," ArXiv190701132 Cs Stat, May 2020, Accessed: Nov. 19, 2020. [Online]. Available: http://arxiv.org/abs/1907.01132.

[78] S. Niknam, H.S. Dhillon, and J.H. Reed, "Federated learning for wireless communications–Motivation, opportunities and challenges," ArXiv190806847 Cs Eess Stat, May 2020, Accessed: Nov. 19, 2020. [Online]. Available: http://arxiv.org/abs/1908.06847.

[79] Qian Y, Hu L, Chen J, Guan X, Hassan M, Alelaiwi A. Privacy-aware service placement for mobile edge computing via federated learning. Inf Sci 2019. https://doi.org/10.1016/J.INS.2019.07.069.

[80] "[PDF] Federated learning based proactive content caching in edge computing | Semantic scholar." https://www.semanticscholar.org/paper/Federated-Learning-Based-Proactive-Content-Caching-Yu-Hu/91f7e3856b9ac81bdaceb67e322084c811ed22b3 (accessed Nov. 19, 2020).

[81] M. Ammad-ud-din et al., "Federated collaborative filtering for privacy-preserving personalized recommendation system," ArXiv190109888 Cs Stat, Jan. 2019, Accessed: Nov. 19, 2020. [Online]. Available: http://arxiv.org/abs/1901.09888.

[82] D. Chai, L. Wang, K. Chen, and Q. Yang, "Secure federated matrix factorization," ArXiv190605108 Cs, Jun. 2019, Accessed: Nov. 19, 2020. [Online]. Available: http://arxiv.org/abs/1906.05108.

[83] T. Yang et al., "Applied federated learning–Improving google keyboard query suggestions," ArXiv181202903 Cs Stat, Dec. 2018, Accessed: Nov. 19, 2020. [Online]. Available: http://arxiv.org/abs/1812.02903.

[84] D. Leroy, A. Coucke, T. Lavril, T. Gisselbrecht, and J. Dureau, "Federated learning for keyword spotting," ArXiv181005512 Cs Eess Stat, Feb. 2019, Accessed: Nov. 19, 2020. [Online]. Available: http://arxiv.org/abs/1810.05512.

[85] F. Hartmann, S. Suh, A. Komarzewski, T.D. Smith, and I. Segall, "Federated learning for ranking browser history suggestions," ArXiv191111807 Cs Stat, Nov. 2019, Accessed: Nov. 19, 2020. [Online]. Available: http://arxiv.org/abs/1911.11807.

[86] Y. Liu et al., "FedVision–An online visual object detection platform powered by federated learning," ArXiv200106202 Cs Stat, Jan. 2020, Accessed: Nov. 19, 2020. [Online]. Available: http://arxiv.org/abs/2001.06202.

[87] X. Li, Y. Gu, N. Dvornek, L. Staib, P. Ventola, and J.S. Duncan, "Multi-site fMRI analysis using privacy-preserving federated learning and domain adaptation–ABIDE results," ArXiv200105647 Cs Eess, Apr. 2020, Accessed: Nov. 19, 2020. [Online]. Available: http://arxiv.org/abs/2001.05647.

[88] Huang L, Shea AL, Qian H, Masurkar A, Deng H, Liu D. Patient clustering improves efficiency of federated machine learning to predict mortality and hospital stay time using distributed electronic medical records. J Biomed Inform 2019;99:103291. https://doi.org/10.1016/j.jbi.2019.103291.

[89] "Facing small and biased data dilemma in drug discovery with federated learning | bioRxiv." https://www.biorxiv.org/content/10.1101/2020.03.19.998898v1 (accessed Nov. 19, 2020).

[90] "FL-QSAR: a federated learning based QSAR prototype for collaborative drug discovery | bioRxiv." https://www.biorxiv.org/content/10.1101/2020.02.27.950592v1 (accessed Nov. 19, 2020).

[91] W. Li et al., "Privacy-preserving federated brain tumour segmentation," ArXiv191000962 Cs, Oct. 2019, Accessed: Nov. 19, 2020. [Online]. Available: http://arxiv.org/abs/1910.00962.

[92] S. Silva, B. Gutman, E. Romero, P.M. Thompson, A. Altmann, and M. Lorenzi, "Federated learning in distributed medical databases–Meta-analysis of large-scale subcortical brain data," ArXiv181008553 Cs Q-Bio Stat, Mar. 2019, Accessed: Nov. 19, 2020. [Online]. Available: http://arxiv.org/abs/1810.08553.

[93] S. Ge, F. Wu, C. Wu, T. Qi, Y. Huang, and X. Xie, "FedNER–Privacy-preserving medical named entity recognition with federated learning," ArXiv200309288 Cs, Mar. 2020, Accessed: Nov. 19, 2020. [Online]. Available: http://arxiv.org/abs/2003.09288.

[94] Abeshu A, Chilamkurti N. Deep learning–The frontier for distributed attack detection in fog-to-things computing. IEEE Commun Mag Feb. 2018;56(2):169–75. https://doi.org/10.1109/MCOM.2018.1700332.

[95] Wang X, Han Y, Wang C, Zhao Q, Chen X, Chen M. In-Edge AI–Intelligentizing mobile edge computing, caching and communication by federated learning. IEEE Netw Sep. 2019;33(5):156–65. https://doi.org/10.1109/MNET.2019.1800286.

[96] M. Chen, O. Semiari, W. Saad, X. Liu, and C. Yin, "Federated echo state learning for minimizing breaks in presence in wireless virtual reality networks," ArXiv181201202 Cs Math, Sep. 2019, Accessed: Dec. 21, 2020. [Online]. Available: http://arxiv.org/abs/1812.01202.

[97] S. Samarakoon, M. Bennis, W. Saad, and M. Debbah, "Federated learning for ultra-reliable low-latency V2V communications," ArXiv180509253 Cs Stat, May 2018, Accessed: Dec. 21, 2020. [Online]. Available: http://arxiv.org/abs/1805.09253.

[98] Zhuang W, et al. Performance optimization of federated person re-identification via benchmark analysis. In: Proceedings of the 28th ACM international conference on multimedia. NY, USA: New York; Oct. 2020. p. 955–63. https://doi.org/10.1145/3394171.3413814.

[99] "Federated learning for image classification | tensorflow federated," TensorFlow. https://www.tensorflow.org/federated/tutorials/federated_learning_for_image_classification (accessed Jul. 18, 2021).

[100] Amin J, Yasmin M, Fernandes SL. Big data analysis for brain tumor detection–Deep convolutional neural networks. Future Gener Comput Syst Oct. 2018;87:290–7. https://doi.org/10.1016/j.future.2018.04.065.

[101] Nazar Umaira, Khan Muhammad A, Lali Ikram Ullah, Lin Hong, Ali Hashim, Ashraf Imran, Tariq Junaid. Review of automated computerized methods for brain tumor segmentation and classification. Curr Med Imaging 2020;16(7):823–34.

[102] Manic KSuresh, Biju Roshima, Patel Warish, Khan Muhammad Attique, Raja N, Uma S. Extraction and evaluation of corpus callosum from 2D brain MRI slice–A study with cuckoo search algorithm. Comput Math Methods Med 2021:2021.

[103] Aziz Ahsan, Tariq Usman, Nam Yunyoung, Nazir Muhammad, Jeong Chang-Won, Mostafa Reham R, Sakr Rasha H. An ensemble of optimal deep learning features for brain tumor classification. Comput Mater Contunua 2021;70:2.

[104] Zahoor Saliha, Lali Ikram U, Javed Kashif, Mehmood Waqar. Breast cancer detection and classification using traditional computer vision techniques: a comprehensive review. Curr Med Imaging 2020;16(10):1187–200.

[105] Khan Sajid Ali, Song Oh-Young, Nazir Muhammad. Medical imaging fusion techniques–A survey benchmark analysis, open challenges and recommendations. J Med Imaging Health Inform 2020;10(11):2523–31.

[106] T. Qi, F. Wu, C. Wu, Y. Huang, and X. Xie, "Privacy-preserving news recommendation model learning," ArXiv200309592 Cs, Oct. 2020, Accessed: Dec. 30, 2020. [Online]. Available: http://arxiv.org/abs/2003.09592.

[107] F. Yin et al., "FedLoc–Federated learning framework for data-driven cooperative localization and location data processing," ArXiv200303697 Cs Eess Stat, May 2020, Accessed: Dec. 30, 2020. [Online]. Available: http://arxiv.org/abs/2003.03697.

[108] R. Zeng, S. Zhang, J. Wang, and X. Chu, "FMore–An incentive scheme of multi-dimensional auction for federated learning in MEC," ArXiv200209699 Cs Stat, Feb. 2020, Accessed: Dec. 30, 2020. [Online]. Available: http://arxiv.org/abs/2002.09699.

[109] Y. Chen, X. Yang, X. Qin, H. Yu, B. Chen, and Z. Shen, "FOCUS–Dealing with label quality disparity in federated learning," ArXiv200111359 Cs Stat, Jan. 2020, Accessed: Dec. 30, 2020. [Online]. Available: http://arxiv.org/abs/2001.11359.

[110] Y. Deng, M.M. Kamani, and M. Mahdavi, "Adaptive personalized federated learning," ArXiv200313461 Cs Stat, Nov. 2020, Accessed: Dec. 01, 2020. [Online]. Available: http://arxiv.org/abs/2003.13461.

[111] D.P. Kingma and J. Ba, "Adam–A method for stochastic optimization," ArXiv14126980 Cs, Jan. 2017, Accessed: Dec. 01, 2020. [Online]. Available: http://arxiv.org/abs/1412.6980.

[112] S. Reddi et al., "Adaptive federated optimization," ArXiv200300295 cs math stat, Jul. 2020, Accessed: Dec. 01, 2020. [Online]. Available: http://arxiv.org/abs/2003.00295.

[113] ur Rehman MH, Gaber MM, editors. Federated learning systems–Towards next-generation AI. Springer International Publishing; 2021. https://doi.org/10.1007/978-3-030-70604-3.

[114] "(PDF) Federated learning for UAVs-enabled wireless networks–Use cases, challenges, and open problems." https://www.researchgate.net/publication/339948127_Federated_Learning_for_UAVs-Enabled_Wireless_Networks_Use_Cases_Challenges_and_Open_Problems (accessed Dec. 01, 2020).

[115] S. Wang et al., "Federated learning for task and resource allocation in wireless high altitude balloon networks," ArXiv200309375 Cs Eess Math Stat, Mar. 2020, Accessed: Dec. 01, 2020. [Online]. Available: http://arxiv.org/abs/2003.09375.

[116] M. Chen, H.V. Poor, W. Saad, and S. Cui, "Convergence time optimization for federated learning over wireless networks," ArXiv200107845 cs math stat, Jan. 2020, Accessed: Dec. 01, 2020. [Online]. Available: http://arxiv.org/abs/2001.07845.

[117] Tran NH, Bao W, Zomaya A, Nguyen MNH, Hong CS. Federated learning over wireless networks:–Optimization model design and analysis. In: IEEE INFOCOM 2019 - IEEE conference on computer communications; Apr. 2019. p. 1387–95. https://doi.org/10.1109/INFOCOM.2019.8737464.

[118] "(PDF) Performance optimization of federated learning over wireless networks." https://www.researchgate.net/publication/339559317_Performance_Optimization_of_Federated_Learning_over_Wireless_Networks (accessed Dec. 01, 2020).

[119] K. Wei et al., "Performance analysis and optimization in privacy-preserving federated learning," ArXiv200300229 Cs, Feb. 2020, Accessed: Dec. 01, 2020. [Online]. Available: http://arxiv.org/abs/2003.00229.

[120] M. Chen, Z. Yang, W. Saad, C. Yin, H.V. Poor, and S. Cui, "A joint learning and communications framework for federated learning over wireless networks," ArXiv190907972 Cs Stat, Oct. 2020, Accessed: Dec. 01, 2020. [Online]. Available: http://arxiv.org/abs/1909.07972.

[121] Yang HH, Liu Z, Quek TQS, Poor HV. Scheduling policies for federated learning in wireless networks. IEEE Trans Commun Jan. 2020;68(1):317–33. https://doi.org/10.1109/TCOMM.2019.2944169.

[122] Fantacci R, Picano B. A federated learning framework for mobile edge computing networks. CAAI Trans Intell Technol Nov. 2019;5. https://doi.org/10.1049/trit.2019.0049.

[123] S. Savazzi, M. Nicoli, and V. Rampa, "Federated learning with cooperating devices–A consensus approach for massive IoT networks," ArXiv191213163 Cs Eess, Dec. 2019, doi: 10.1109/JIOT.2020.2964162.

[124] Zhang C. Thesis. 2018. https://doi.org/10.32657/10220/47928.

[125] J. Kang, Z. Xiong, D. Niyato, Y. Zou, Y. Zhang, and M. Guizani, "Reliable federated learning for mobile networks," ArXiv191006837 Cs, Oct. 2019, Accessed: Dec. 01, 2020. [Online]. Available: http://arxiv.org/abs/1910.06837.

[126] Khan BA, Sharif M, Raza M, Umer T, Hussain K, Khan AU. An approach for surveillance using wireless sensor networks (WSN. J Inf Commun Technol JICT 2007;1(2). Art2.

[127] S. Li, Y. Cheng, W. Wang, Y. Liu, and T. Chen, "Learning to detect malicious clients for robust federated learning," ArXiv200200211 Cs Stat, Feb. 2020, Accessed: Dec. 01, 2020. [Online]. Available: http://arxiv.org/abs/2002.00211.

[128] "[1909.12567] cell-free massive MIMO for wireless federated learning." https://arxiv.org/abs/1909.12567 (accessed Dec. 01, 2020).

[129] E. Bakopoulou, B. Tillman, and A. Markopoulou, "A federated learning approach for mobile packet classification," ArXiv190713113 Cs Stat, Jul. 2019, Accessed: Nov. 12, 2020. [Online]. Available: http://arxiv.org/abs/1907.13113.

[130] L. Melis, C. Song, E. De Cristofaro, and V. Shmatikov, "Exploiting unintended feature leakage in collaborative learning," ArXiv180504049 Cs, Nov. 2018, Accessed: Dec. 24, 2020. [Online]. Available: http://arxiv.org/abs/1805.04049.

[131] Ng H-W, Winkler S. A data-driven approach to cleaning large face datasets. In: 2014 IEEE international conference on image processing (ICIP). France: Paris; Oct. 2014. p. 343–7. https://doi.org/10.1109/ICIP.2014.7025068.

[132] G. Ateniese, G. Felici, L.V. Mancini, A. Spognardi, A. Villani, and D. Vitali, "Hacking smart machines with smarter ones–How to extract meaningful data from machine learning classifiers," ArXiv13064447 Cs Stat, Jun. 2013, Accessed: Dec. 27, 2020. [Online]. Available: http://arxiv.org/abs/1306.4447.

[133] Fredrikson M, Jha S, Ristenpart T. Model inversion attacks that exploit confidence information and basic countermeasures. In: Proceedings of the 22nd ACM SIGSAC conference on computer and communications security. NY, USA: New York; Oct. 2015. p. 1322–33. https://doi.org/10.1145/2810103.2813677.
[134] Shah JH, Yasmin M, Fernandes SL. Facial expressions classification and false label reduction using LDA and threefold SVM. Pattern Recognit Lett Nov. 2020; 139:166–73. https://doi.org/10.1016/j.patrec.2017.06.021.
[135] F. Tramèr, F. Zhang, A. Juels, M.K. Reiter, and T. Ristenpart, "Stealing machine learning models via prediction APIs," ArXiv160902943 Cs Stat, Oct. 2016, Accessed: Dec. 27, 2020. [Online]. Available: http://arxiv.org/abs/1609.02943.
[136] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership inference attacks against machine learning models," ArXiv161005820 Cs Stat, Mar. 2017, Accessed: Dec. 27, 2020. [Online]. Available: http://arxiv.org/abs/1610.05820.
[137] N. Papernot, P. McDaniel, and I. Goodfellow, "Transferability in machine learning: from phenomena to black-box attacks using adversarial samples," ArXiv160507277 Cs, May 2016, Accessed: Dec. 27, 2020. [Online]. Available: http://arxiv.org/abs/1605.07277.
[138] rndic N, Laskov P. Practical evasion of a learning-based classifier–A case study. In: 2014 IEEE symposium on security and privacy. CA: San Jose; May 2014. p. 197–211. https://doi.org/10.1109/SP.2014.20.
[139] Abadi M, et al. Deep learning with differential privacy. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security; Oct. 2016. p. 308–18. https://doi.org/10.1145/2976749.2978318.
[140] Dwork C, McSherry F, Nissim K, Smith A. Calibrating noise to sensitivity in private data analysis. Theory of cryptography. ,Heidelberg: Berlin; 2006. p. 265–84. https://doi.org/10.1007/11681878_14.
[141] R.C. Geyer, T. Klein, and M. Nabi, "Differentially private federated learning–A client level perspective," ArXiv171207557 Cs Stat, Mar. 2018, Accessed: Dec. 28, 2020. [Online]. Available: http://arxiv.org/abs/1712.07557.
[142] Lecun Y, Bottou L, Bengio Y, Haffner P. Gradient-based learning applied to document recognition. In: Proc. IEEE, 86; Nov. 1998. p. 2278–324. https://doi.org/10.1109/5.726791.
[143] Hitaj B, Ateniese G, Perez-Cruz F. Deep models under the GAN–Information leakage from collaborative deep learning. In: Proceedings of the 2017 ACM SIGSAC conference on computer and communications security. NY, USA: New York; Oct. 2017. p. 603–18. https://doi.org/10.1145/3133956.3134012.
[144] I.J. Goodfellow et al., "Generative adversarial networks," ArXiv14062661 Cs Stat, Jun. 2014, Accessed: Dec. 28, 2020. [Online]. Available: http://arxiv.org/abs/1406.2661.
[145] Y. Liu, Z. Ma, X. Liu, S. Ma, S. Nepal, and R. Deng, "Boosting privately–Privacy-preserving federated extreme boosting for mobile crowdsensing," ArXiv190710218 Cs, Apr. 2020, Accessed: Nov. 21, 2020. [Online]. Available: http://arxiv.org/abs/1907.10218.
[146] Triastcyn A, Faltings B. Federated generative privacy. IEEE Intell Syst Jul. 2020;35(4):50–7. https://doi.org/10.1109/MIS.2020.2993966.
[147] Lim WYB, et al. Federated learning in mobile edge networks–A comprehensive survey. IEEE Commun Surv Tutor 2020;22(3):2031–63. https://doi.org/10.1109/COMST.2020.2986024.
[148] Shahid MA, Sharif M. Cloud computing security models, architectures, issues and challenges–A survey. Smart Comput Rev Dec. 2015:602–16. https://doi.org/10.6029/smartcr.2015.06.010.
[149] Hao M, Li H, Xu G, Liu S, Yang H. Towards efficient and privacy-preserving federated deep learning. In: ICC 2019 - 2019 IEEE international conference on communications (ICC); May 2019. p. 1–6. https://doi.org/10.1109/ICC.2019.8761267.
[150] S. Jere, Q. Fan, B. Shang, L. Li, and L. Liu, "Federated learning in mobile edge computing–An edge-learning perspective for beyond 5G," ArXiv200708030 Cs Eess, Jul. 2020, Accessed: Dec. 17, 2020. [Online]. Available: http://arxiv.org/abs/2007.08030.
[151] L.U. Khan et al., "Federated learning for edge networks–Resource optimization and incentive mechanism," ArXiv191105642 Cs, Sep. 2020, Accessed: Dec. 17, 2020. [Online]. Available: http://arxiv.org/abs/1911.05642.
[152] "Full article–A review on game-theoretic incentive mechanisms for mobile data offloading in heterogeneous networks." https://www.tandfonline.com/doi/full/10.1080/02564602.2017.1396936 (accessed Dec. 17, 2020).
[153] Wu Q, He K, Chen X. Personalized federated learning for intelligent IoT applications–A cloud-edge based framework. IEEE Comput Graph Appl May 2020. https://doi.org/10.1109/OJCS.2020.2993259. 1–1.
[154] Lin J, Yu W, Zhang N, Yang X, Zhang H, Zhao W. A survey on internet of things–Architecture, enabling technologies, security and privacy, and applications. IEEE Internet Things J Oct. 2017;4(5):1125–42. https://doi.org/10.1109/JIOT.2017.2683200.
[155] Sittón-Candanedo I, Alonso RS, Corchado JM, Rodríguez-González S, Casado-Vara R. A review of edge computing reference architectures and a new global edge proposal. Future Gener Comput Syst Oct. 2019;99:278–94. https://doi.org/10.1016/j.future.2019.04.016.
[156] Mao Y, You C, Zhang J, Huang K, Letaief KB. A survey on mobile edge computing–The communication perspective. IEEE Commun Surv Tutor 2017;19(4): 2322–58. https://doi.org/10.1109/COMST.2017.2745201. Fourthquarter.
[157] Shi W, Cao J, Zhang Q, Li Y, Xu L. Edge computing–Vision and challenges. IEEE Internet Things J Oct. 2016;3(5):637–46. https://doi.org/10.1109/JIOT.2016.2579198.
[158] "[1907.08349] Convergence of edge computing and deep learning–A comprehensive survey." https://arxiv.org/abs/1907.08349 (accessed Dec. 20, 2020).
[159] Burger M. The Risk to Population Health Equity Posed by Automated Decision Systems–A Narrative Review. ArXiv200106615 Cs Jan. 2020. AccessedNov212020[Online]Available, http://arxiv.org/abs/2001.06615.
[160] M. Seif, R. Tandon, and M. Li, "Wireless federated learning with local differential privacy," ArXiv200205151 Cs Math, Feb. 2020, Accessed: Nov. 21, 2020. [Online]. Available: http://arxiv.org/abs/2002.05151.
[161] L. Lyu, H. Yu, and Q. Yang, "Threats to federated learning–A survey," ArXiv200302133 Cs Stat, Mar. 2020, Accessed: Nov. 21, 2020. [Online]. Available: http://arxiv.org/abs/2003.02133.
[162] "Towards faster and better federated learning–A feature fusion approach semantic scholar." https://www.semanticscholar.org/paper/Towards-Faster-and-Better-Federated-Learning%3A-A-Yao-Huang/d7605c16b035379c15de614d0f5335ec92ba227e (accessed Nov. 21, 2020).
[163] Y. Mansour, M. Mohri, J. Ro, and A.T. Suresh, "Three approaches for personalization with applications to federated learning," ArXiv200210619 Cs Stat, Jul. 2020, Accessed: Nov. 21, 2020. [Online]. Available: http://arxiv.org/abs/2002.10619.
[164] Alqahtani Abdullah, Khan Aimal, Alsubai Shtwai, Binbusayyis Adel, Ch M, Yong Hwan-Seung, Cha Jaehyuk. Cucumber leaf diseases recognition using multi level deep entropy-ELM feature selection. Appl Sci 2022;12(2):593.
[165] Nawaz M, Nazir T, Javed A, Tariq U, Yong HS, Cha J. An efficient deep learning approach to automatic glaucoma detection using optic disc and optic cup localization. Sensors 2022;22(2):434.
[166] Yasmeen Usra, Tariq Usman, Junaid Ali, Khan Muhammad, Asfand E, Ch Yar, Hanif Avais, Mey Senghour, Nam Yunyoung. Citrus diseases recognition using deep improved genetic algorithm. Comput Mater Continua 2021;70(2):1–15.
[167] Muhammad Khan, Sharif Muhammad, Akram Tallha, Kadry Seifedine. Intelligent fusion-assisted skin lesion localization and classification for smart healthcare. Neural Comput Appl 2021:1–16.
[168] Bibi Amina, Javed Muhammad Younus, Tariq Usman, Kang Byeong-Gwon, Nam Yunyoung, Mostafa Reham R, Sakr Rasha H. Skin lesion segmentation and classification using conventional and deep learning based framework. CMC-Comput Mater Continua 2022;71(2):2477–95.
[169] Khan Seemab, Alhaisoni Majed, Tariq Usman, Yong Hwan-Seung, Armghan Ammar, Alenezi Fayadh. Human action recognition–A paradigm of best deep learning features selection and serial based extended fusion. Sensors 2021;21(23):7941.
[170] Syed HH, Tariq U, Armghan A, Alenezi F, Khan JA, Rajinikanth V. A rapid artificial intelligence-based computer-aided diagnosis system for COVID-19 classification from CT images. Behav Neurol 2021:2021.
[171] Rajinikanth V, Satapathy SC, Taniar D, Mohanty JR, Tariq U, Damaševičius R. VGG19 network assisted joint segmentation and classification of lung nodules in CT Images. Diagnostics 2021;11(12):2208.
[172] Saleem F, Alhaisoni M, Tariq U, Armghan A, Alenezi F, Kadry S. Human gait recognition–A single stream optimal deep learning features fusion. Sensors 2021; 21(22):7584.

[173] Arshad M, Tariq U, Armghan A, Alenezi F, Younus Javed M, Kadry S. A computer-aided diagnosis system using deep learning for multiclass skin lesion classification. Computational intelligence and neuroscience. 2021. p. 2021.
[174] Alhaisoni M, Tariq U, Hussain N, Majid A, Damaševičius R, Maskeliūnas R. COVID-19 case recognition from chest CT images by deep learning, entropy-controlled firefly optimization, and parallel feature fusion. Sensors 2021;21(21):7286.
[175] M. Sharif M, Akram T, Kadry S, Hsu CH. A two-stream deep neural network-based intelligent system for complex skin cancer types classification Int J Intell Syst 2021.
[176] Hussain N, Kadry S, Tariq U, Mostafa RR, Choi JI, Nam Y. Intelligent deep learning and improved whale optimization algorithm based framework for object recognition. Hum Cent Comput Inf Sci 2021;11:34.
[177] Kanwal S, Shah JH, Nisa M, Kadry S, Sharif M, Maheswari M. Person re-identification using adversarial haze attack and defense–A deep learning framework. Comput Electr Eng 2021;96:107542.
[178] Zhang YD, Alhusseni M, Kadry S, Wang SH, Saba T, Iqbal T. A fused heterogeneous deep neural network and robust feature selection framework for human actions recognition. Arab J Sci Eng 2021:1–16.
[179] Zia F, Irum I, Qadri NN, Nam Y, Khurshid K, Ali M, Khan MA. A multilevel deep feature selection framework for diabetic retinopathy image classification. Comput Mater Continua 2022;70:2261–76.

Fahad Ahmed Khokar: he is currently a master student at Department of Computer science, COMSATS University Islamabad, Wah campus. His research interest including machine learning, federated learning, and deep learning for several applications.

Jamal Hussain Shah: He received the Ph.D. degree in pattern recognition from the University of Science and Technology China, Hefei, China. Since 2008, he has been in the education field. He is currently an Assistant Professor with COMSATS University Islamabad, Wah Cantt, Pakistan. His areas of specialization are automation and pattern recognition. He has 21 publications in IF, SCI and ISI journals and in national and international conferences. His research interests include deep learning, algorithms design and analysis, machine learning, image processing, and big data.

Muhammad Attique Khan (Member IEEE) earned his Master and Ph.D degree in Human Activity Recognition for Application of Video Surveillance and Skin Lesion Classification using Deep Learning from COMSATS University Islamabad, Pakistan. He is currently Lecturer of Computer Science Department in HITEC University Taxila, Pakistan. His primary research focus in recent years is medical imaging, COVID19, MRI analysis, Video Surveillance, Human Gait Recognition, and Agriculture Plants. He has above 180 publications that have more than 4720 citations and impact factor 500+ with h-index 43.

Muhammad Sharif, PhD (IEEE Senior Member) is Associate Professor at COMSATS University Islamabad, Wah Campus Pakistan. He has worked one year in Alpha Soft UK based software house in 1995. He is OCP in Developer Track. He is in teaching profession since 1996 to date. He published more than 200 papers in to date with more than 6000 citations.

Usman Tariq holds a Ph.D. from the Ajou University, South Korea and led the design of a global data infrastructure simulator modeling, to evaluate the impact of competing architectures on the performance, availability, and reliability of the system for Industrial IoT infrastructure. Currently he is interested in applied cyber security, advanced topics in Internet of Things, and health informatics. His research focus is on the theory of large complex networks, which includes network algorithms, stochastic networks, network information theory, and large-scale statistical inference.

Seifedine Kadry received the bachelor's degree from Lebanese University, in 1999, the M.S. degree from the University of Reims, France, in 2002, and the EPFL, Lausanne, the Ph.D. degree from Blaise Pascal University, France, in 2007, and the H.D.R. degree from the University of Rouen Normandy, in 2017. He is currently a Full Professor of data science with Noroff University College, Norway. He is also an ABET Program Evaluator of computing and an ABET Program Evaluator of engineering technology. His current research interests include data science, education using technology, system prognostics, stochastic systems, and probability and reliability analysis.