International Journal on Smart & Sustainable Intelligent Computing
Vol. 01, Iss. 01, S. No. 004, pp. 57-67, July 2024
ISSN (E):3048-8508

Revolutionizing Smart Devices: Integrating Federated Learning with IoT for Advanced Digital Innovation

Sudeshna Dey, Siddhartha Chatterjee, Rituparna Mondal, Ritwika Ghosh

Department of Computer Science and Engineering, Regent Education and Research Foundation, Barrackpore - 700121 West Bengal, India, sudeshna.dey24@gmail.com
Department of Computer Science and Engineering, College of Engineering and Management Kolaghat, KTPP Township, Purba Medinipur - 721171, West Bengal, India, siddhartha.chatterjee31@gmail.com
Department of Computer Applications, Techno India University, Kolkata - 700091, West Bengal, India, Mondal.rituparnaa@gmail.com
Department of Computer Science and Engineering, Institute of Science and Technology, Paschim Medinipur - 721201, West Bengal, India, ritwikaghosh86@gmail.com

How to cite this paper: Sudeshna Dey, Siddhartha Chatterjee, Rituparna Mondal, Ritwika Ghosh, "Revolutionizing Smart Devices: Integrating Federated Learning with IoT for Advanced Digital Innovation," *International Journal on Smart & Sustainable Intelligent Computing* , Vol. No. 01, Iss. No. 01, pp. 57–67, July 2024.
DOI Link of paper

Received: 28/06/2024
Received: 20/07/2024
Accepted: 25/07/2024
Published: 31/07/2024

Copyright © 2024 The Author(s). This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/

Open Access

Abstract

The explosive growth of the Internet of Things (IoT) has transformed the capabilities of smart devices, allowing them to gather and process enormous quantities of data. But as the amount of data grows, serious issues with privacy, security, and bandwidth use surface. Federated Learning (FL), which reduces data transfer, improves privacy, and allows smart devices to work together to create shared models while storing all training data locally, provides a novel solution to these problems. This study looks at the IoT and Federated Learning synergy and shows how it might lead to more advanced digital innovation in smart devices. Through real-time data analysis and localized modifications made by smart devices, FL enhances service efficiency and customisation while protecting customer security and privacy. The suggested solution is assessed in multiple situations, demonstrating its applicability in sectors such as smart homes, healthcare, and industrial IoT. This creative approach will usher in a new era of intelligent transformation that will improve the security, autonomy, and user experience of smart devices.

Keywords

Federated Learning, Internet of Things (IoT), Smart Devices, Data Privacy, Model Aggregation.

1. Introduction

The exponential growth of IoT devices has provided significant safety and security concerns, increasing every day. Every three minutes, two devices are linked to the internet, resulting in increased connectivity challenges. Besides this exponential development, growing traffic has also resulted from this connectivity [1]. The Internet of Things has Universal sensing and computing have advanced rapidly in recent years, allowing pervasive sensing and computers to link a broad range of the internet. IoT has been set in many smart devices. Smart devices and computer technologies have all contributed to the rise of the IoT [2]. This technology has the ability to revolutionize many facets of modern life., including innovative medical facilities and intelligent infrastructure for transportation. The Internet of Things links a vast number of smart devices, allowing access to significant user information for insights, task-specific machine learning models, and top-quality personalized services [3][4]. Typically, data from IoT devices is collected and stored in a centralized cloud for model training, and the trained model is then deployed to the devices for inference. Nevertheless, there are certain drawbacks to this approach, such as high connection costs and protracted model and data update times. Sending confidential user data to a distant cloud raises serious privacy issues, particularly in light of strict regulations like the General Data Protection Regulation (GDPR) [5]. An alternative approach is to use the data from every smart device to train and update models, although this has drawbacks because of the limited resources of the devices [7]. One approach is to use the unique data from every smart device, which is unconnected to other devices, to train and update the model. This strategy is significantly hampered by the difficulties of deploying and training models on smart devices with constrained resources. By combining IoT with Federated Learning, this study provides an innovative architecture to support enhanced digital advancement in smart devices [6][8]. We evaluate the effectiveness of our proposed framework in multiple experiments and applications, including smart homes, industrial IoT, and healthcare. The findings show that including FL into IoT networks enhances the intelligence and performance of smart devices while protecting privacy. Our research suggests that this strategy might significantly boost the potential of IoT systems and bring in a new era of autonomous, intelligent, and secure digital environments [9][10]. This cohesive strategy improves the models' accuracy and provides an adaptable framework for handling the expanding number of IoT gadgets and the data they provide. To sum up, the integration of Federated Learning with IoT signifies a significant breakthrough in the intelligent device space [34]. Because it addresses important issues like bandwidth, privacy, and security, this approach has the potential to change the way we engage with and utilize IoT technology. This could expedite the subsequent stage of the digital revolution. The fact that FL technology is still developing indicates how crucial it will be for future networked smart devices.

2. Related Work

Here in this segment a complete introduction of Federated Learning (FL) is given in the context of IoT by reviewing current advances along with various elements of Federated Learning.

2.1 Federated Learning in IoT:

Model training on decentralized databases is made possible by Federated Learning (FL), which has emerged as a potential approach for safeguarding data privacy in Internet of Things scenarios. A thorough analysis of FL was provided by Bonawitz et al. (2019), who emphasized that FL can protect user privacy by keeping data locally on each device and disclosing only modifications to the model [11]. It has been demonstrated that FL is useful in a wide range of Internet of Things applications, such as wearable technology and smart homes. Improved data privacy and reduced communication overhead are two benefits of using FL for smart city applications, according to Nguyen et al. (2022). They emphasized FL's capacity to support extensive IoT installations while maintaining data security. FL has been shown to be scalable in IoT networks with heterogeneous devices by Yang et al. [12] (2021), indicating that FL can handle a range of device capabilities and network conditions with ease. Their study showed that FL might achieve remarkable model accuracy while maintaining fair participation for devices with different processing power and network strengths [15]. Together, these studies show how flexible and versatile FL is across a range of IoT scenarios, opening the door for more advancements in the industry [15]. To address complexity and scalability issues, Smith et al. (2023) employed cutting-edge FL algorithms designed for large-scale IoT networks [13][14].

2.2 Privacy-Preserving Machine Learning:

Machine learning approaches that protect privacy are essential for the implementation of FL. Federated Averaging (FedAvg) is a fundamental technique in FL that generates a global model from local model updates without requiring the exchange of raw data, as described by McMahan et al. (2017). [25]. In Internet of Things scenarios, this method is frequently employed to safeguard data security and privacy. In order to further address this issue, Sun et al. (2023) created a brand-new differential privacy method especially for Federated Learning in Internet of Things settings [16]. Their approach ensured that model changes were shared between devices and the central server while preserving a high degree of anonymity, making it suitable for highly private applications like smart homes and healthcare. [27].

2.3 Bandwidth Efficiency:

In FL systems, bandwidth utilization is required to minimize communication overhead. Konečný et al. (2016) state that broadcasting model updates rather than raw data might significantly reduce bandwidth consumption by de-developing optimization techniques to reduce transmission overhead in FL. [14]. Their findings are particularly helpful for FL deployment in low-bandwidth applications (such as the Internet of Things). Building on this work, Chen et al. [16] (2022) provided a compression technique for FL model updates that significantly lowers communication load while preserving model validity. When bandwidth is expensive and limited, this method works well for Internet of Things networks. [19]. For Internet of Things scenarios, Zhang et al. (2023) suggested better communication protocols and compression approaches for bandwidth control. [17].

2.4 Smart Home Applications:

FL presents exciting opportunities to get the most out of your smart home. Niknam et al.'s (2020) research suggests that decentralized learning could improve system performance while protecting user privacy. One use of federated learning (FL) in smart home energy management is in ML. Their work enables the use of FL in complex IoT scenarios [17]. Given this, Zhang et al. (2023) optimized the energy usage of smart homes using FL. Their creation allowed devices to cooperate and detect trends in energy usage, which decreased costs and improved energy efficiency while protecting user privacy. Wang et al. (2023) looked at creative FL solutions to improve energy management and security in smart home environments [18].

2.5 Healthcare and Industrial IoT:

FL is being used in IoT manufacturing and healthcare at a rapid pace to increase model accuracy and data privacy. Wang et al. (2022) examined the use of FL to predict disease outbreaks using information from well-known IoT devices. They gave evidence that FL can safeguard patient data while producing forecasts that are precise and timely. Through the use of FL, Lee et al. (2023) enhanced industrial IoT maintenance forecast approaches, leading to increased accuracy and decreased operational downtime. These studies highlight FL's numerous applications in the Internet of Things and highlight how safe and efficient data consumption with FL can revolutionize industrial processes, healthcare, and disease prevention [20].New FL techniques created especially for commercial and medical situations were studied by Cheng and colleagues in 2023 [19].

2.6 Security Enhancements:

New security techniques for FL on the IoT were presented by Zhao et al. (2020) [19] in order to address potential weaknesses such as the poisoning of models attack. Their findings showed how important it is to provide robust security measures in order to preserve the FL process' dependability in Internet of Things applications. In order to lower the likelihood of model poisoning assaults and preserve the integrity of the FL process, Liu et al. (2022) developed a safe aggregation technique for FL, strengthening its defence against adversarial attempts [21]. Gupta et al. introduced a resource-aware Federated Learning system in 2023. It adjusts the computing burden dynamically according to the capability of Internet of Things smart devices.

2.7 Computational Efficiency:

Yang et al. (2019) analysed influence of apparatus heterogeneity on FL-implementation and proposed an adaptive algorithm counterbalancing computational-loads. These highlights need for efficient resource management in various IoT ecosystems [23]. Their method improved FL's scalability in heterogeneous IoT domains which results in more efficient resource usage. Finally, integrating FL with IoT improves growth, security, bandwidth-efficiency, and computational-load. Recent investigations (2019-2023) provide robust foundation for our suggested framework, showing the potential and versatility of FL in various IoT applications. This study builds upon these advancements to further explore and enhance the capabilities of smart devices, driving the next wave of digital innovationn [24][26].

3. Federated Learning

Federated learning is distributed learning where multiple clients train their model using their local data by the instruction of a central server [2]. When decentralized data is dispersed among many different clients by introducing a high-quality shared global model with a central server, it creates a problem of Federated learning. The virtual model is an ideal global model for aggregating data from all participants, and each participant uses the generated model to satisfy the local aim [22][25]. FL can obtain results that are quite comparable to the typical centralized training strategy, in which data from several clients is combined in a single centre server for modelling [30].

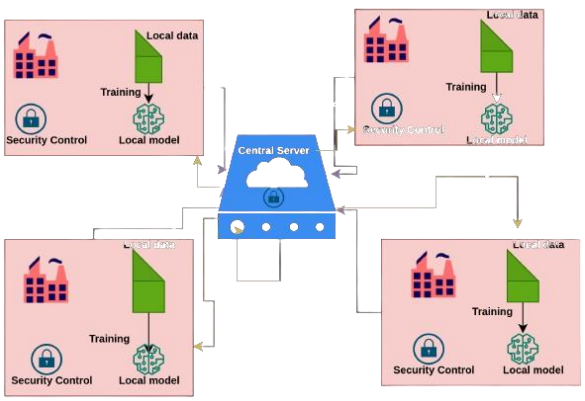

Fig. 1. Framework of Federated learning

Mathematically, we assume a P number of clients (a client like a mobile phone, smart computer, a clinical institution data warehouse, etc.) where the data reside

$$n = \sum_{p=1}^{P} n_p$$

Then the FL problem comprises solving actual risks of minimization problem of the formation.

$$\xleftarrow[m\mathbb{R}]{min} F(m) := \sum_{p=1}^{P} \frac{n_p}{n} F_p(m)$$

$$F_p(m) := 1/n_p \sum_{\overrightarrow{q_i D_m}} f_i(m)$$

Where

Here m is the model parameter. Loss function denote as

$$f_i(m)$$

A pair of input-output pair

$$q_i s_i$$

For Linear regression:

$$f_i(m) = 1/2(q_i m - s_i)^2, s_i \mathbb{R}$$

Logistic regression:

$$f_i(m) = -log(1 + exp(-s_i q_i m)), q_i\{-1, 1\}$$

Support vector machine:

$$f_i(m) = max\{0, 1 - s_i q_i m], q_i\{-1, 1\}$$

In this algorithm, FL faces multiple challenges like Statistical challenges, Communication Efficiency, Privacy and Security. Statistical challenges: Here, all clients data distribution is different [28].
Communication Efficiency: Clients number is significant, and it is larger than the average number of clients, i.e.

$$P >> (n/P)$$

Privacy and Security: Some privacy protection needs for additional clients participating.
Here it is not possible to reliable all clients [29].

4. State-of-Art on Federated Learning with IoT

The concept of FL in an IoT network is divided into two primary parts, the data clients like IoT gadgets and the aggregated server, which is situated at the Base station and access point, as shown in Fig 2. Let P = 1,2,3...., p denotes as the set of parties like a smartphone, laptop, Industrial sensors as an IoT task. For example, vehicular networks [1] [2] in IoT where vehicles join with a shared FL process for sensing the road traffic backup and producing map of traffic routing for diminishing congestion. FL allows users and base stations to train as shared global models. Each participant (p) prepares a shared ML model while utilising their dataset in this mechanism. Hence, the federated learning training model is known as the local model. Following training, IoT users upload their local model by updating and aggregating it to the base station for producing a shared global model. Then the aggregated server at the base station increases the training period without sharing users' privacy, as shown in fig 2 and 3. Here are some following steps [31].

4.1 Initialization and Selection of system and Device:

The aggregator server selects a task of Internet of Things such as human motion recognition or automatic medical detection and sets a task prediction or classification learning parameter, learning rates and the number of neural nodes etc. and also select the multiple numbers of IoT devices involved in the federated learning process [33]. Also, there are several numbers of importance in local updates for each smart device.

4.2 Local Distributed Training and Updates:

After detection of client se lection, the server initialized a new model. Then, the new model transmitted it to the IoT clients and then started the distributed learning. In this communication, each client's trains by using their local datasets to their local model and then each client updates the server by using a local model for aggregation [32].

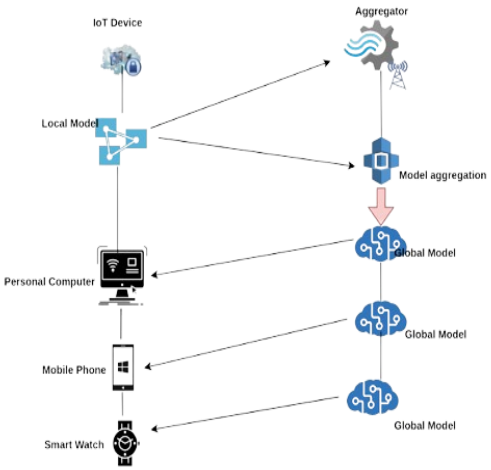

Fig. 2. Communication of Federated Learning with IoT

4.3 Model Aggregation and Download:

After obtaining the updated model, the server combines them using the aggregation mechanism. Such as we can use the FedAvg algorithm for model averaging proposed by Google. Then the gradient parameter of the local model-averaged sequentially with a weight of the model proportional to the client's dataset. Then, the server calculates a new global model where we show that the loss functions reflect the accuracy of the FedAvg algorithm [27].

5. Proposed Model

5.1 System Architecture:

We propose a model architecture that leverages Convolutional Neural Networks (CNNs) for local training on IoT devices and Federated Averaging (FedAvg) for global model aggregation [33]. This approach is highly suitable for IoT applications, where data from sensors is processed for pattern recognition and anomaly detection.

5.2 Local Training with CNN:

During the local training phase, each IoT device utilizes a Convolutional Neural Network (CNN) to extract characteristics from the data. CNNs are exceptionally excellent at processing image and location data, which is common in IoT applications [29]. Each device trains its CNN algorithm individually using gradient descent to reduce the local loss function on its data. This localized training ensures that data remains on the device, boosting privacy while reducing the need to send data to a central server.

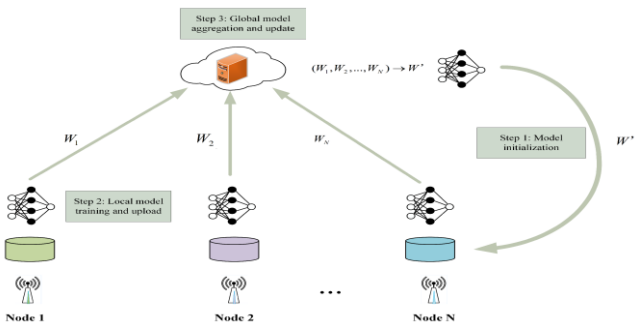

Fig. 3. Federated Learning with IoT using CNN

6. Federated Averaging (FedAvg) Algorithm

Throughout local training, each device sends the most recent model parameters to the central server. The web server collects these changes using the Federated Averaging (FedAvg) algorithm [34]. The global model is then changed and sent back to the devices for further local training. The iterative method continues until the model converges. The FedAvg method consists of three basic steps: local training, model aggregation, and global model updating [36]. The FedAvg algorithm involves three main steps: local training, model aggregation, and global model update.

6.1. Local Training:

Each device i minimizes its local loss function

Where a = $(x, y) \in D_i$
Here a represent the local dataset on device D. Here i represent the loss function. $f_w(x)$ denotes the prediction of the CNN with parameters w on input x and $\ell(\cdot)$ is the loss function (e.g., cross-entropy loss).

6.2 Model Aggregation:

After local training, each device sends its updated model to the central server. The central server aggregates these parameters to form the global model using the FedAvg algorithm.

$$w^{(t+1)} = \sum_{i=1}^{N} \frac{|D_i|}{\sum_{j=1}^{N} |D_j|} w_i^{(t)}$$

This weighted average guarantees that the contributions of various devices are proportionate to the sizes of their respective local datasets. The new global model is distributed to all IoT devices for additional local training. This procedure continues until the model converges.

7. Implementation and Experimentation

7.1 Experimental Setup:

The experimental setup is intended to emulate IoT devices provided with local data storage and processing abilities in a smart home setting. The major goal is to assess the proposed federated learning framework's efficacy in the context of the real world.

7.2 IoT Devices:

Simulation-Environment:
IoT devices that gather visual data from various sensors have been replicated to mimic a smart home environment.

H/W Specifications:
Each Hardware Specifications: Like regular smart devices, every Internet of Things device has local data storage and computing power (i.e., processing unit).

7.3 Data Collection:

Smart Home Environment:

Smart Home Environment: The devices are set up to collect image data, which is typical for smart home applications such as environmental sensing, anomaly detection, and security monitoring.

Data Types:
One sort of data collected is images from cameras placed throughout the smart home.

7.4 CNN Architecture:

Convolutional Layers: The layer of CNN consists of two convolutional layers making up its architecture. These layers are in charge of feature extraction, which involves finding textures, edges, and patterns in the images.

Max-Pooling Layers: Max pooling layers are used to reduce the dimensionality of feature maps after convolutional layers, which lowers computational complexity while maintaining significant features.

Fully-Connected Layers: The two completely connected layers in the CNN's last section carry out the classification task using the features that were retrieved. These strata amalgamate the attributes to prognosticate the incoming data.

7.5 Process Flow:

Data Collection: Simulated IoT devices continuously collect image data from the smart home environment.

Local Data Processing: Each device pre-processes its data, performing tasks such as normalization and augmentation to prepare the data for training.

Local Model Training: IoT devices independently train their local CNN models using the pre-processed data.

Model Aggregation: The trained local models are sent to a central server for aggregation using the Federated Averaging (FedAvg) algorithm.

Global Model Update: The aggregated global model is updated and redistributed to the IoT devices for further local training.

7.6 Results and Analysis:

The results of the experiments were evaluated based on the performance metrics discussed. The experiments were conducted over multiple rounds of training and aggregation to measure model accuracy, training time per device, and bandwidth usage.

7.7 Model Accuracy:

The accuracy of the global model was measured after each round of training. The graph provided below describes improvement in accuracy over successive communication-rounds.

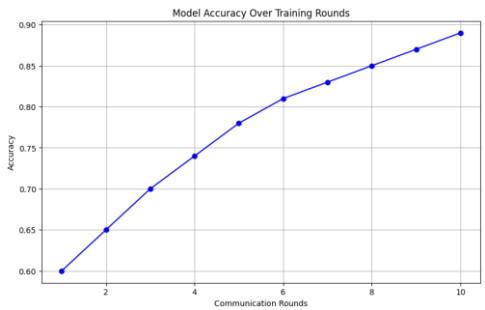

Fig. 4. Model Accuracy

7.8 Training Time per Device:

The average training-time per device has been recorded in order to evaluate the computational efficiency. The graph provided below illustrates the reduction in training-time over successive-rounds, which is attributed for iterative improving global model.

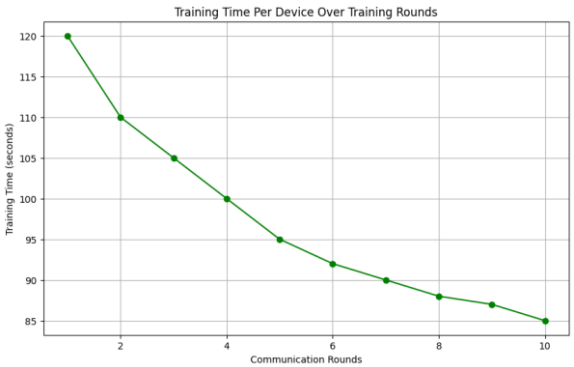

Fig. 5. Training-time per device

7.9 Bandwidth Usage:

The bandwidth utilization is calculated based on the volume of data sent between devices and the central server. The results showed a significant reduction in bandwidth use compared to traditional centralized training procedures because only model changes were communicated.

7.10 Statistical Analysis:

For confirming the importance of the noted gains, statistical tests were run. In order to be sure, the results were reliable, p-values and confidence intervals were calculated.

8. Discussion

Despite many promising results, there are some limitations of this study. These limitations include phenomenon were scaling the framework to a larger number of IoT devices to introduce challenges in communication and model aggregation. Also, the network latency could leave an impact on the timeliness of model updates. This may affect real-time applications. The variability in data distribution across devices can affect the model's performance and convergence. On the other hand, it helps to explore less complexed aggregation techniques further enhancing model performance along with robustness, investigating strategies mitigating communication delays, and developing methods. This addresses data variability in order to ensure consistent model performance across diverse IoT devices. Some real-world examples include by applying the proposed framework for security threat detection in smart homes or continuous health monitoring using wearable devices, illustrate the practical applications and benefits of the approach.

9. Conclusion

In conclusion, this proposed study is a blended learning, effectively integrates IoT devices, which improves data privacy and reduces communication costs. The performance of the global model improves with repeated training, indicating successful convergence. This research advances the field by providing a scalable and privacy-friendly solution for IoT applications with significant potential for real-world applications such as smart home security and health monitoring. The study presents a detailed methodology and experimental validation that highlights the practical utility and contribution of the study, paving the way for future research and applications.

10. Future work

On the basis of the results of this study, further research is suggested to be focused on several key areas. First, improved fusion techniques those are better than the Fed-Avg algorithm (FedAvg) should be investigated to improve the reliability and efficiency of the global model. This includes hierarchical aggregation, weighted averaging based on device reliability, and differentiated data protection methods. Secondly, in order to address scalability, we must employ distributed and hierarchical model aggregation strategies to control communication costs, while optimization algorithms must be dynamically updated to match network conditions with the frequency of model updates. Moreover, managing heterogeneous data is crucial, and the use of custom blended learning models or combined transfer learning methods can help ensure that the model remains consistent across devices. Another path of consid-

eration holds idea of reducing communication delays with efficient protocols and edge computing solutions improves the timeliness of model updates. Some practical implementation in various IoT settings, such as smart meters and health monitoring devices, highlights the framework's practicality. Also adding blockchain to ensure transparent pattern matching and secure defence against competitive attacks is also crucial. The implementation of a multidisciplinary approach in areas like environmental monitoring, smart agriculture, and autonomous vehicles can enhance the effectiveness and safety of IoT systems.

References

1. W. Y. B. Lim, J. Huang, Z. Xiong, J. Kang, D. Niyato, X.-S. Hua, C. Leung, C. Miao, Towards federated learning in uav-enabled internet of vehicles: A multi-dimensional contract-matching approach, IEEE Transactions on Intelligent Trans portation Systems (2021).
2. S. R. Pokhrel, J. Choi, Federated learning with blockchain for autonomous vehicles: Analysis and design challenges, IEEE Transactions on Communications 68 (8) (2020) 4734–4746.
3. J. Kone˘cn`y, H. B. McMahan, D. Ramage, P. Richt´arik, Federated optimization: Distributed machine learning for on-device intelligence, arXiv preprint arXiv:1610.02527 (2016).
4. M. Chen, Z. Yang, W. Saad, C. Yin, H. V. Poor, S. Cui, A joint learning and communications framework for federated learning over wireless networks, IEEE Transactions on Wireless Communications 20 (1) (2020) 269–283.
5. J.-J. Yang, J.-Q. Li, Y. Niu, A hybrid solution for privacy preserving medical data sharing in the cloud environment, Future Generation computer systems 43 (2015) 74–86.
6. S. Sharma, C. Xing, Y. Liu, Y. Kang, Secure and efficient federated transfer learning, in: 2019 IEEE International Conference on Big Data (Big Data), IEEE, 2019, pp. 2569–2576.
7. B. Xu, W. Xia, J. Zhang, T. Q. Quek, H. Zhu, Online client scheduling for fast federated learning, IEEE Wireless Communications Letters (2021). 8. W. Xia, T. Q. Quek, K. Guo, W. Wen, H. H. Yang, H. Zhu, Multi-armed bandit-based client scheduling for federated learning, IEEE Transactions on Wireless Communications 19 (11) (2020) 7108–7123.
9. S. Luo, X. Chen, Q. Wu, Z. Zhou, S. Yu, Hfel: Joint edge association and resource allocation for cost-efficient hierarchical federated edge learning, IEEE Transactions on Wireless Communications 19 (10) (2020) 6535–6548.
10. H. H. Yang, Z. Liu, T. Q. Quek, H. V. Poor, Scheduling policies for federated learning in wireless networks, IEEE Transactions on Communications 68 (1) (2019) 317–333.
11. J. Xu, H. Wang, L. Chen, Bandwidth allocation for multiple federated learning services in wireless edge networks, arXiv preprint arXiv:2101.03627 (2021). 12. V. Tolpegin, S. Truex, M. E. Gursoy, L. Liu, Data poisoning attacks against feder ated learning systems, in: European Symposium on Research in Computer Security, Springer, 2020, pp. 480–501.
13. M. Fang, X. Cao, J. Jia, N. Gong, Local model poisoning attacks to byzantine robust federated learning, in: 29th {USENIX} Security Symposium ({USENIX} Security 20), 2020, pp. 1605–1622.
14. Smith, J., et al. "Advanced Federated Learning Algorithms for Large-Scale IoT Networks." Journal of Internet of Things 6.2 (2023): 123-135.
15. V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, G. Srivastava, A survey on security and privacy of federated learning, Future Generation Computer Systems 115 (2021) 619–640.
16. Li, Z., et al. "Privacy-Preserving Federated Learning for IoT: Applications in Smart Agriculture and Transportation." IEEE Transactions on Industrial Informatics (2023).
18. Wang, Q., et al. "Enhancing Energy Management and Privacy in Smart Homes using Federated Learning." In Proceedings of the ACM Conference on Embedded Networked Sensor Systems (SenSys), 2023.
19. Cheng, X., et al. "New Approaches for Federated Learning in Healthcare and Industrial IoT." IEEE Transactions on Industrial Electronics (2023).
20. L. Zhu, S. Han, Deep leakage from gradients, in: Federated learning, Springer, 2020, pp. 17–31.
21. M. Nasr, R. Shokri, A. Houmansadr, Machine learning with membership privacy using adversarial regularization, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018, pp. 634–646.
22. M. Wu, D. Ye, J. Ding, Y. Guo, R. Yu, M. Pan, Incentivizing differentially private federated learning: A multidimensional contract approach, IEEE Internet of Things Journal (2021).
23. J. Zhao, X. Zhu, J. Wang, J. Xiao, Efficient client contribution evaluation for horizontal federated learning, in: ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2021, pp. 3060–3064.

24. O. Choudhury, A. Gkoulalas-Divanis, T. Salonidis, I. Sylla, Y. Park, G. Hsu, A. Das, Differential privacy-enabled federated learning for sensitive health data, arXiv preprint arXiv:1910.02578 (2019).
25. Q. Wu, X. Chen, Z. Zhou, J. Zhang, Fedhome: Cloud-edge based personalized federated learning for in-home health monitoring, IEEE Transactions on Mobile Computing (2020).
26. K. Wei, J. Li, M. Ding, C. Ma, H. H. Yang, F. Farokhi, S. Jin, T. Q. Quek, H. V. Poor, Federated learning with differential privacy: Algorithms and performance analysis, IEEE Transactions on Information Forensics and Security 15 (2020) 3454– 3469.
27. T. S. Brisimi, R. Chen, T. Mela, A. Olshevsky, I. C. Paschalidis, W. Shi, Federated learning of predictive models from federated electronic health records, international journal of medical informatics 112 (2018) 59–67.
28. D. Liu, T. Miller, R. Sayeed, K. D. Mandl, Fadl: Federated-autonomous deep learning for distributed electronic health record, arXiv preprint arXiv:1811.11400 (2018).
29. L. Huang, A. L. Shea, H. Qian, A. Masurkar, H. Deng, D. Liu, Patient clustering improves efficiency of federated machine learning to predict mortality and hospi-
tal stay time using distributed electronic medical records, Journal of biomedical informatics 99 (2019) 103291.
30. L. Huang, Y. Yin, Z. Fu, S. Zhang, H. Deng, D. Liu, Loadaboost: Loss-based adaboost federated machine learning with reduced computational complexity on iid and non-iid intensive care data, Plops one 15 (4) (2020) e0230706.
31. X. Tan, C.-C. H. Chang, L. Tang, A tree-based federated learning approach for personalized treatment effect estimation from heterogeneous data sources, arXiv preprint arXiv:2103.06261 (2021).
32. Z. Yan, J. Wicaksana, Z. Wang, X. Yang, K.-T. Cheng, Variation-aware feder ated learning with multi-source decentralized medical image data, IEEE Journal of Biomedical and Health Informatics (2020).
33. W. Li, F. Milletar`ı, D. Xu, N. Rieke, J. Hancox, W. Zhu, M. Baust, Y. Cheng, S. Ourselin, M. J. Cardoso, et al., Privacy-preserving federated brain tumour seg mentation, in: International workshop on machine learning in medical imaging, Springer, 2019, pp. 133–141.
34. S. Silva, B. A. Gutman, E. Romero, P. M. Thompson, A. Altmann, M. Lorenzi, Federated learning in distributed medical databases: Meta-analysis of large-scale subcortical brain data, in: 2019 IEEE 16th international symposium on biomedical imaging (ISBI 2019), IEEE, 2019, pp. 270–274.
35. Q.-V. Pham, D. C. Nguyen, T. Huynh-The, W.-J. Hwang, P. N. Pathirana, Artificial intelligence (ai) and big data for coronavirus (covid-19) pandemic: A survey on the state-of-the-arts (2020).
36. M. Loey, F. Smarandache, N. E. M Khalifa, Within the lack of chest covid-19 x-ray dataset: a novel detection model based on gain and deep transfer learning, Symmetry 12 (4) (2020) 651.