Federated Learning for Industrial Internet of Things in Future Industries

Dinh C. Nguyen, Ming Ding, Pubudu N. Pathirana, Aruna Seneviratne, Jun Li,
Dusit Niyato, *Fellow, IEEE*, and H. Vincent Poor, *Fellow, IEEE*

***Abstract*—The Industrial Internet of Things (IIoT) offers promising opportunities to transform the operation of industrial systems and becomes a key enabler for future industries. Recently, artificial intelligence (AI) has been widely utilized for realizing intelligent IIoT applications where AI techniques require centralized data collection and processing. However, this is not always feasible in realistic scenarios due to the high scalability of modern IIoT networks and growing industrial data confidentiality. Federated Learning (FL), as an emerging collaborative AI approach, is particularly attractive for intelligent IIoT networks by coordinating multiple IIoT devices and machines to perform AI training at the network edge while helping protect user privacy. In this article, we provide a detailed overview and discussions of the emerging applications of FL in key IIoT services and applications. A case study is also provided to demonstrate the feasibility of FL in IIoT. Finally, we highlight a range of interesting open research topics that need to be addressed for the full realization of FL-IIoT in industries.**

***Index Terms*—Federated learning, Industrial Internet of Things, Industry 4.0, future industries, privacy.**

I. Introduction

Recent advances in communication and smart device technologies along with the rapid development of industrial informatization have promoted the proliferation of the Industrial Internet of Things (IIoT), with its capability to increase productivity and efficiency in industries [1]. It is anticipated that IIoT will play an increasingly significant role in the development of new applications, from smart manufacturing, smart factory to smart transportation and smart healthcare in the future industrial revolutions, including Industry 4.0. For example, IIoT can provide innovative solutions to drive smart manufacturing processes due to its ubiquitous sensing and computation capabilities.

To realize intelligent IIoT services and applications in industries, artificial intelligence (AI) techniques such as machine learning (ML) have been widely exploited to train data models. Traditionally, AI functions are placed at the cloud or the data center for data learning and modeling, which remains some critical limitations with respect to the rapid increase in IIoT data volumes. The transfer of a massive volume of IIoT data to a remote server for AI training requires much network bandwidth and incurs high communication overhead, both of which are unacceptable to time-sensitive IIoT applications such as autonomous driving and real-time healthcare. Importantly, the reliance on such a central server or third party for data learning raises critical privacy issues, e.g., user information leakage, since these data may contain sensitive information. Moreover, in the future industries, such a centralized AI architecture may be no longer suitable because IIoT data are not centrally located, but distributed over a large-scale network. Therefore, there is an urgent need to go toward distributed AI approaches for enabling scalable and privacy-promoting intelligent IIoT applications at the network edge.

Recently, federated learning (FL) [2] has emerged as a promising solution for realizing cost-effective intelligent IIoT applications with improved privacy protection. Conceptually, FL is a collaborative AI approach that enables training of high-quality AI models by averaging local updates aggregated from multiple learning clients, e.g., IIoT devices, without the need for direct access to the local data which thus mitigates privacy leakage risks. Moreover, since FL attracts large computation and dataset resources from a number of IIoT devices to train AI models, the IIoT data training quality, e.g., accuracy, would be significantly improved which might not be achieved by using centralized AI approaches with less data and limited computational capabilities [3].

Motivated by these appealing characteristics, a flurry of research activities combining FL with IIoT in industries has been sparked [2]–[4]. However, these works only focus on certain application domains in IIoT, such as cognitive computing [2], industrial artificial intelligence [3], and digital twin-enabled IIoT [4], while a holistic overview on the use of FL in key IIoT services and applications is still missing.

To fill this gap, this article presents and details an integration of FL and IIoT. Specifically, we present the principle of FL and explain its benefits in IIoT. Then, we provide the state-of-the-art review of the use of FL in important IIoT services, i.e., IIoT data offloading and caching, IIoT attack detection, and IIoT mobile crowdsensing. Notably, we explore and discuss the roles of FL in key industrial IIoT applications, including smart manufacturing, smart transportation, smart grid, and smart healthcare. A case study is provided in the area of federated healthcare to demonstrate the feasibility of FL in IIoT. We also highlight interesting open issues for future FL-IIoT research. The new contributions of this article compared to the state-of-the-art are summarized in Table I.

Dinh C. Nguyen and Pubudu N. Pathirana are with School of Engineering, Deakin University, Australia

Ming Ding is with Data61, CSIRO, Australia

Aruna Seneviratne is with School of Electrical Engineering and Telecommunications, University of New South Wales, Australia

Jun Li is with School of Electrical and Optical Engineering, Nanjing University of Science and Technology, China

Dusit Niyato is with School of Computer Science and Engineering, Nanyang Technological University, Singapore

H. Vincent Poor is with the Department of Electrical Engineering, Princeton University, USA.

TABLE I: Comparison with related work and new contributions of this article.

Related works	Topic	Key contributions
[2]	FL for cognitive computing in Industry 4.0	An FL-based solution for big data driven cognitive computing in Industry 4.0, aiming to improve the performances of poisoning attack resistance, accuracy, and incentive mechanisms for industrial automation.
[3]	FL for industrial artificial intelligence	An efficient and privacy-enhanced FL solution for industrial artificial intelligence with user privacy awareness.
[4]	FL and digital twin empowered IIoT	An architecture of digital twin-enabled IIoT, by using digital twins to capture the characteristics of industrial devices to assist FL.
This article	FL and IIoT in industries	A holistic discussion of the use of FL in IIoT. Particularly, • We identify and discuss the potential of FL in various key IIoT services, i.e., IIoT data offloading and caching, IIoT attack detection, and mobile IIoT crowdsensing. • We then provide a detailed investigation of using FL in four important applications, namely smart manufacturing, smart transportation, smart grid, and smart healthcare. • We then present a case study toward FL-based smart healthcare. Several interesting open research topics for FL-IIoT in industries are also highlighted.

The remainder of the article is organized as follows. Section II describes the key principle of FL and its benefits in IIoT. We then present the overview of the potential of FL in IIoT services in Section III. In Section IV, we provide an detailed discussion on the integration of FL into key IIoT applications. A case study in FL-based smart healthcare is provided in Section V. Finally, Section VI concludes the article.

II. Integration of FL and IIoT: Key Principle and Benefits

A. Key Principle

The typical FL-IIoT network is composed of two main entities: the data clients, e.g., IIoT devices and industrial sensors, and an aggregator (e.g., an edge server) located at a base station (BS) or an access point (AP), as illustrated in Fig. 1. FL allows IIoT devices and the server to train a shared global model while the raw data are kept at local devices. Here, each IIoT user participates in training a shared AI model by using its own dataset and then uploads its local model to the aggregator for building a new global model. By relying on the distributed data training at IIoT devices, the aggregation server can enrich the training performance without completely compromising user data privacy [3]. As shown in Fig. 1, the generic FL-IIoT process includes the following key steps:

1) *System Initialization and Device Selection:* The aggregation server selects an IIoT task, e.g., road traffic evaluation or healthcare analytic, along with model requirements such as task classification or task prediction, and learning parameters such as learning rate. Moreover, the server selects a subset of IIoT devices as the learning clients that should be involved in the FL process.
2) *Distributed Local Training and Updates:* Once the subset of the learning clients is determined, the server sends an initial model to the clients to trigger the distributed training. In every communication round, each client trains a local model using its own dataset and calculates an update. Then, each client uploads its computed update to the server for aggregation.
3) *Model Aggregation and Download:* After receiving all updates from clients, the server aggregates them and calculates a new version of global model. Subsequently, the server broadcasts the new global update to all clients for optimizing the local models in the next learning round.
4) *Iterated Training:* The FL training is iterated until the global loss function converges or a desired accuracy is achieved. Here, the accuracy of FL can be defined as the ratio of total accuracies of all clients to the total number of clients, according to the popular Federated Averaging (FedAvg) algorithm proposed by Google [3].

B. Key Benefits of FL Integration in IIoT

With its innovative operational concept, FL can offer some important benefits for IIoT applications in industries as follows:

- *Data Privacy Enhancement:* In the FL system, only the local updates are required by the central server for the AI training, while the local data are kept at local devices, which thus provides a degree of data privacy. Following the increasingly stringent data privacy protection legislation such as the General Data Protection Regulation (GDPR), the capability of protecting user information of FL is significant for building sustainable and safe IIoT systems.
- *Low-latency Network Communication:* By avoiding the offloading of huge data volumes to the server, FL can significantly reduce communication costs in intelligent IIoT networks, e.g., latency, consumed by raw data transmission. Therefore, FL also helps save much network spectrum resources required for data training.
- *Improved Learning Quality:* FL attracts large computation and dataset resources from a number of IIoT devices over the distributed IIoT network to train AI models. This cooperation would accelerate the convergence rate of the overall training process and improve learning accuracy, which might not be achieved by using centralized AI approaches.

Compared to traditional distributed learning [5], [6], which mostly performs parallel data training without federation, FL can better exploit similar experienced data from distributed data sources located at distributed IIoT devices, which might otherwise result in ignoring rarely occurring yet important exemplars. Hence, FL is able to gain benefits from data feature

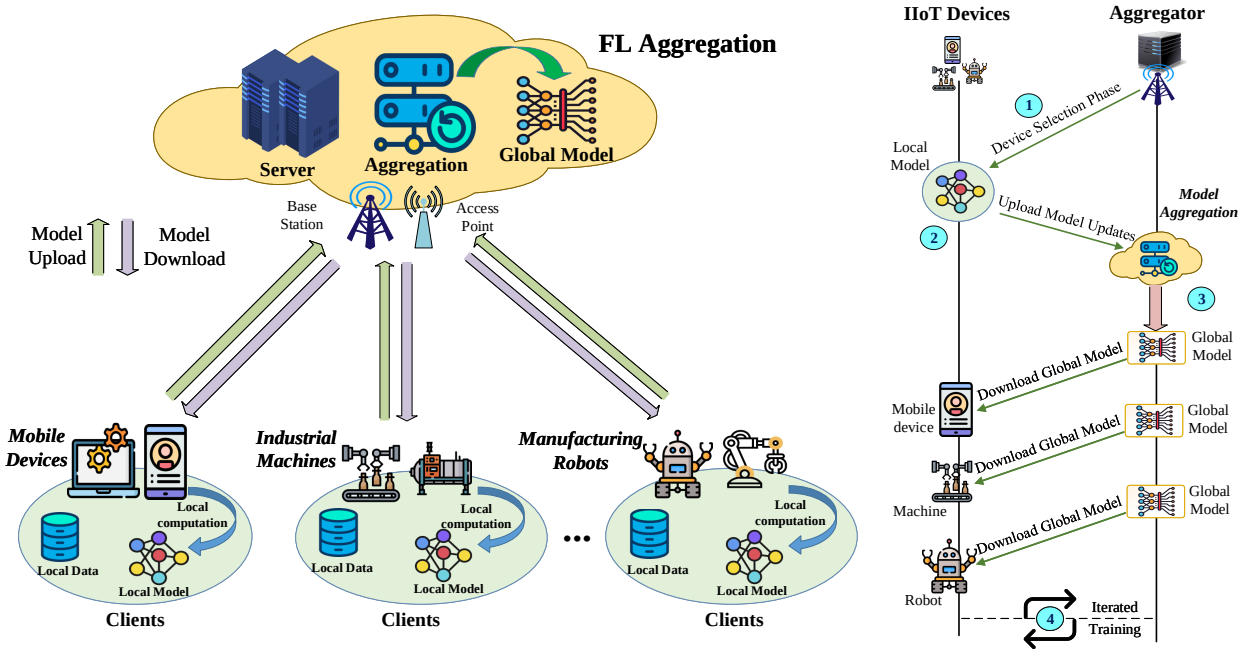


Fig. 1: The network architecture and communication process for FL-IIoT.

diversity across the distributed dataset which helps improve the generalizability of the global AI model for better training performance, e.g., enhanced training accuracy.

III. FL for IIoT Services

A. FL for the Optimization of IIoT Data Offloading and Caching

To meet the ever-increasing computation demands of IIoT users and industrial operators in Industry 4.0, data offloading has been widely regarded as an efficient solution which enables IIoT devices and machines to offload their data tasks to resourceful edge servers. In this context, FL can be used to implement offloading optimization where multiple IIoT devices like actuators in smart manufacturing work as intelligent agents to collaboratively train an AI model to learn the policy of offloading industrial data, e.g., production-related data packages. This solution not only enhances data privacy due to the distribution of data learning in different IIoT devices but also mitigates the computation burden posed on the industrial system in the centralized offloading architecture. For example, FL can support data offloading for the transportation industry [7], where each vehicle collaboratively performs data training for offloading optimization. It prevents sharing actual data and thus helps address privacy concerns of vehicle drivers.

Data offloaded from IIoT devices can be cached by edge servers where FL can play an important role in establishing intelligent caching policies, in order to cope with the explosive growth of industrial data in modern IIoT networks. As shown in [8], FL is very useful to build proactive data caching schemes in urban informatics where an IIoT-based transportation system is created by the federation of vehicular entities, including macrobase stations, road side units, and moving vehicles. Here, each vehicle equipped with caching resources trains a local model using a noise-added gradient-descent algorithm and collaborates with other entities to build a shared content caching policy.

B. FL for IIoT Attack Detection

Industrial devices have become targets of malicious adversaries who can attack AI/ML models in smart manufacturing and operations, by modifying data inputs or changing learning network weights which can lead to erroneous predicted outputs. Many solutions have been proposed to cope with attacks on IIoT devices such as ensemble diversity or adversarial training, but they are mostly applied to a specific type of attack and do not scale well to distributed IIoT networks. FL has emerged as a strong alternative to provide collaborative intelligence for IIoT systems with the ability to detect and prevent various attacks for safe industrial processes. Enabled by the privacy-promoting feature of FL, a federated attack detection and defense solution is built in [9] where each IIoT machine joins to run a deep neural network locally, in order to retrain the threat model to fight against adversaries. An example for federated attack detection in IIoT is illustrated in Fig. 2. Here, each IIoT device first produces adversarial samples to create a retraining set that is then used to build a local attack detection model. Subsequently, the trained gradient is transmitted to the cloud server for aggregation and synchronization to produce a shared model, and this process is iterated in several communication rounds until the attack model converges. In this regard, the built model can effectively detect attacks thereby building a strong defense solution in the IIoT network. Through simulations with MINIST datasets, the FL-based approach can achieve a high attack detection accuracy of 87.8%, compared to 73.8% in the standalone method.

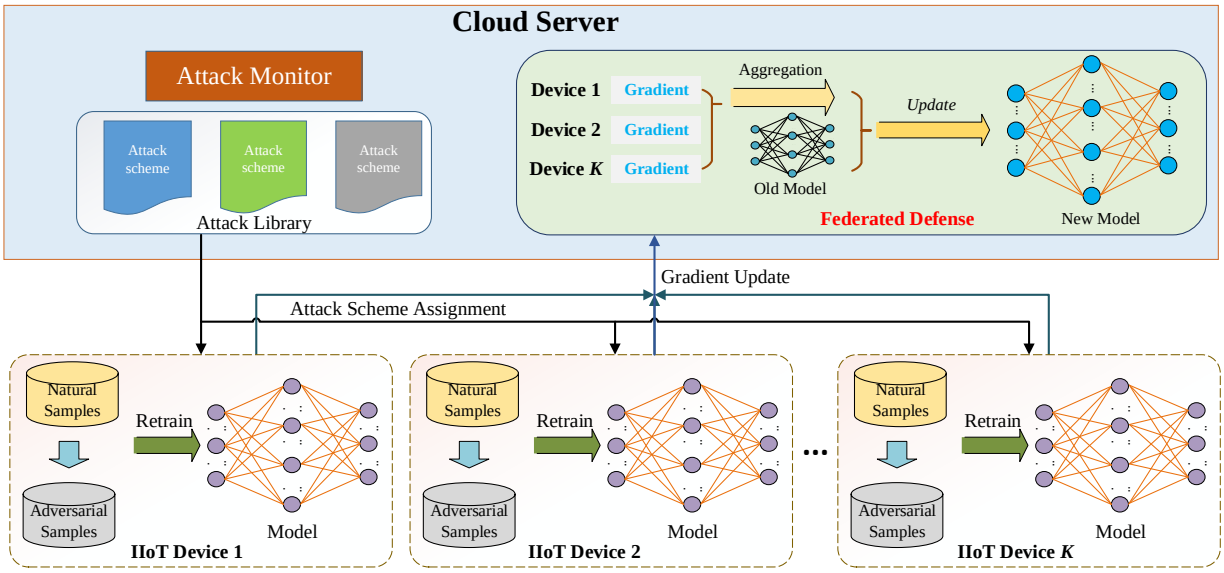


Fig. 2: Federated attack detection and defense in FL-based IIoT networks.

C. FL for IIoT Mobile Crowdsensing

With the rapid development of IIoT, mobile crowdsensing is designed to take advantage of pervasive industrial devices for sensing and collecting data from physical environments. For example, operators in smart factories can make decisions based on environmental information collected from ambient sensors distributed across the whole factory, e.g., sensing abnormal machinery noise to monitor operating status of machines. To realize intelligent mobile crowdsensing, centralized AI/ML techniques are used which usually require direct access to user data, which in turn makes the data vulnerable to privacy leakage. Moreover, the use of a central server to handle all sensing industrial data is not a scalable solution, making it hard to cope with massive data volumes in large-scale industrial systems. FL is a promising tool to accelerate the learning and training for crowdsensing models. As an example, the study in [10] shows an FL-based mobile crowdsensing scheme, with a focus on privacy-enhancing extreme gradient boosting with the cooperation of multiple clients like industrial machines. A secure gradient aggregation algorithm is designed by integrating homomorphic encryption with secret sharing, which prevents the central server from guessing decryption result before operating aggregation. Simulations reveal a high accuracy rate of 98%, and a reduction of 23.9% runtime, and 33.3% communication latency for gradient aggregation.

IV. FL for IIoT Applications

In this section, we present the use of FL in IIoT applications in details.

A. FL for Smart Manufacturing

Smart manufacturing refers to the integration of intelligence into manufacturing processes where AI techniques play important roles in learning big data generated from industrial machines for process modeling, monitoring, prediction and control in production stages. The AI functions often require data sharing among manufacturers and factories which is not an ideal solution due to growing user privacy concerns. FL can realize intelligence for industrial systems without data exchange, by the collaborative data learning of distributed industrial devices and machines. Given the fact that there are diverse industrial services in industries, e.g., production monitoring with robots, product assembly with automatic manipulator arms, package delivery and logistics with vehicles, it is desired to develop a multiple FL services solution to deal with different industrial services in the co-working IIoT ecosystem, as illustrated in Fig. 3. Each group of industrial machines participates in the collaborative AI training using their local industrial datasets within their working environments, e.g., machinery fault data in production lines and productivity information in the assembly process, before offloading the learned parameter to the cloud via its edge server. Here, each virtual machine in the cloud will compute a global model of the industrial service that it manages. In this regard, a multiple FL services solution is realized, and all industrial machines in different service lines can benefit from the exchanged knowledge.

B. FL for Smart Transportation

Recent advances in sensing and communication technologies along with the growth of data volume from road cameras, embedded devices, and vehicular sensors have empowered vehicular networks. AI/ML has been adopted to realize intelligent transportation systems (ITS) where massive vehicular data are often processed at a data center before sending back to vehicles and roadside units. However, this approach remains some critical issues such as privacy leakage and communication overhead caused by raw data sharing. FL can support ITS by running ML models directly at vehicles based on their datasets such as road geometry, collision avoidance, and traffic flow [11]. A cloud server can be employed to aggregate the local updates of all vehicles to make overall decisions on the

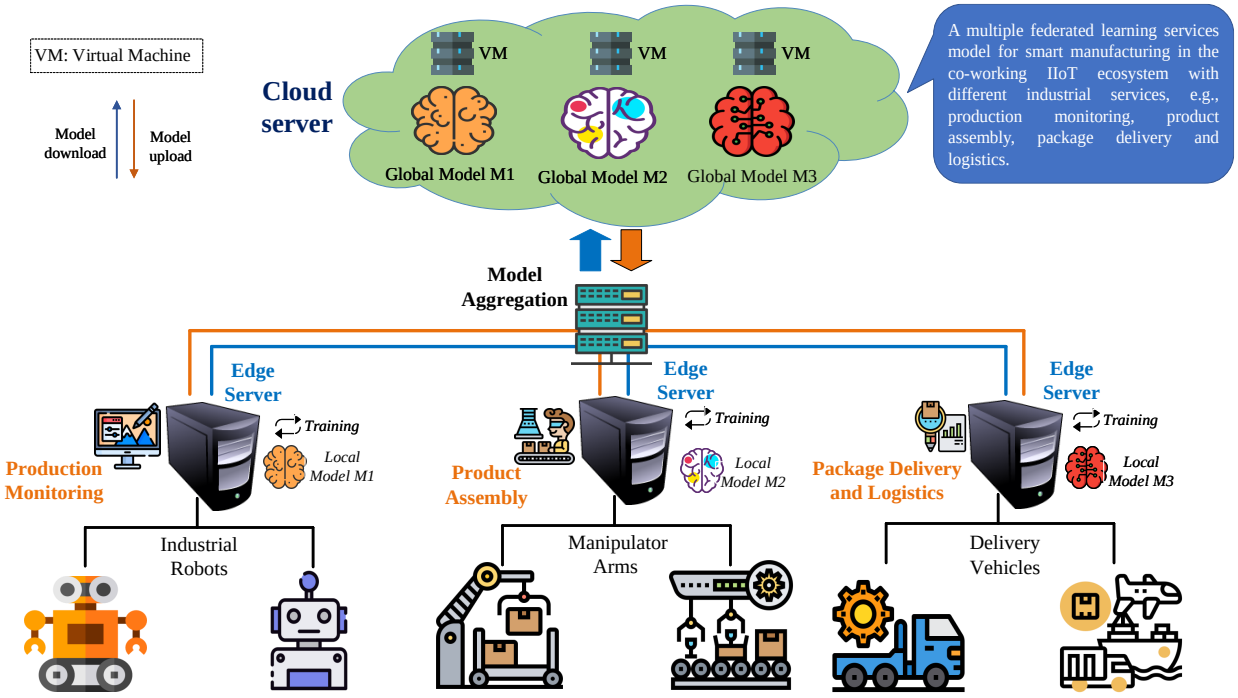


Fig. 3: Federated learning for smart manufacturing.

traffic flow. The use of massive data from multiple vehicles and huge computation capability of all participants helps provide better traffic prediction outcomes, which cannot be met by using centralized ML techniques with less dataset and limited computation. FL can also support privacy-enhanced smart transport logistics, e.g., package delivery services. In this context, postal operators and customers can federate to run a shared ML model for delivery time prediction based on their local data sources, e.g., traffic conditions, drivers' behaviors, and weather, for delivery latency optimization and thus facilitating logistic activities. Moreover, FL can be also used in Unmanned Aerial Vehicles (UAVs)-based vehicular networks where UAVs can be employed as mobile FL clients to join the collaborative model training via aerial links with an ITS entity such as a road side unit. This federated mobile model can enable interesting ITS services such as dynamic traffic prediction and road weather monitoring, in which ground-based communications are unavailable.

C. FL for Smart Grid

Smart grid plays an integral part in building smart city architectures which not only provides energy resources to smart city applications such as transportation, manufacturing, but also has impacts on environmental, security, and social aspects in Industry 4.0. FL can enable intelligent solutions for smart grid management and energy transmissions in a decentralized manner while helping promote privacy. FL is used to establish federated predictive power schemes in a network of edge data centers for smart grid [12]. In this case, each edge equipment such as a smart meter cooperatively trains AI models, e.g., neural networks, using its own electrical consumption data while the edge server coordinates local updates to build a global model to estimate future household electrical demands. In this way, user information such as energy preference and home addresses is not revealed to the server which promotes privacy protection. Simulations are conducted with over 800 homes in the United States, showing a reduction in networking load, compared to standalone learning approaches. Further, due to the increasing privacy concerns, the shareholders of distributed electric generators and consumers may not willing to provide information of their electricity loads/consumption, but these datasets would be critical to the safe operation of smart grids. FL can help address this issue by allowing the distributed participants to collaboratively learn the patterns of electricity generation/consumption, without sharing raw data to each other. FL is also an efficient solution to bring together different stakeholders from energy systems (heat, cool, gas, etc.), aiming to achieve privacy-enhanced energy information exchange in the electricity production ecosystem.

D. FL for Smart Healthcare

In the past few years, AI/ML technologies have been widely used in the healthcare sector to gain insights into health issues and diseases by learning digital medical information extracted from electronic health records (EHRs) for facilitating diagnosis and severity assessment as well as promoting medical research. One of the challenges in such traditional AI techniques is privacy leakage during data analytics. Indeed, compared to other domains, data in healthcare systems are highly sensitive subject to health regulations. Moreover, collecting a large volume of clinical datasets from isolated medical centers is a critical challenge. FL can provide much more efficient solutions for data learning and potentially reshapes the current intelligent healthcare systems by providing intelligent healthcare services while promoting well user privacy based on the cooperation of multiple entities such as health users and

healthcare providers across medical institutions. Indeed, FL can offer flexible and privacy-promoting EHRs management solutions [13], by facilitating the cooperation of multiple hospital institutions to perform health data analytics without the need for EHRs data sharing. Moreover, FL with its privacy-enhanced nature can promote secure healthcare cooperation for better medical service delivery, by allowing for aggregating the model updates from separate hospital organizations with multiple devices, e.g., magnetic resonance imaging (MRI) scanners, to build stronger AI models for medical tasks, such as medical imaging.

V. Case Study

We present a case study on FL-IIoT, by designing an FL-health system for COVID-19 detection [14]. In the pandemic, collecting sufficient data for training becomes challenging with privacy concerns caused by public data sharing. Hence, we propose a new FL scheme to generate realistic COVID-19 images for facilitating privacy-enhanced COVID-19 detection with generative adversarial networks (GANs) [15]. Compared to the traditional FL scheme [14], our advanced FL solution can achieve federated data augmentation for generating high-quality synthetic COVID-19 images that can enhance the training performances with privacy awareness. The details of our FL design will be provided in the following.

A. System Model

We consider a system model for FL-based COVID-19 detection as illustrated in Fig. 4, including a set of medical institutions and a cloud server. Each institution participates in the FL process using its own COVID-19 image dataset, e.g., X-ray images, to build a global GAN with the cloud, aiming to generate high-quality synthetic COVID-19 images for improving the overall COVID-19 detection. Specifically, at each institution we design a GAN consisting of two components, namely a generator and a discriminator based on CNNs which alternatively train via a min-max game [15]. Given a noise sample from a standard Gaussian distribution, the CNN-based generator learns to generate a fake COVID-19 image data point. Moreover, we design another CNN as a discriminator at each institution which tries to classify the real COVID-19 image data point against the one produced from the generator. The discriminator outputs 1 if the input is real data samples or 0 if the input is fake data samples. Accordingly, the generator and the discriminator at each institution interact to obtain the optimal parameters in a fashion that the generator can generate the fake COVID-19 image data distribution close to the real image data as much as possible to fool the discriminator while the discriminator tries to differentiate between fake and real image samples. As a result, the generator can synthesize realistic COVID-19 image samples which are similar to the real COVID-19 image data after a training period, aiming to achieve an efficient data augmentation for later classification tasks.

B. FL Training for COVID-19 Detection

Each institution joins the FL training with the cloud server, by updating the parameters of the discriminator and the generator in each global round and exchange them with the cloud server for aggregation. For every global epoch, each institution collaboratively trains its discriminator and generator. Specifically, the generator produces minibatchs of fake samples from the noise probability distribution. Also, the discriminator samples minibatchs of real data from the actual image distribution. Then, each institution updates simultaneously the discriminator and generator by ascending its stochastic gradients to update its own weights. After local training, all institutions transmit the learned updates to the cloud server for model averaging, while actual COVID-19 images are kept at local institutions which thus ensures data privacy. Then, the cloud server broadcasts the new global updates to all institutions for the next round of GAN learning. The FL process is iterated until the global loss function converges with a desired accuracy.

C. Illustrative Results

We report simulation results obtained when training a COVID-19 dataset [14] of total 620 X-ray images in three classes: COVID-19, normal, and pneumonia in an FL system with five institutions. By using the proposed FL model, we generate 1500 synthetic X-ray images which are then combined with an actual dataset for COVID-19 classification. We use a CNN-based classifier with three convolutional layers and Adam optimizer, and the configurations of GANs are shown in Fig. 4. We evaluate our approach and compare with state-of-the-art schemes, including the standalone scheme (training dataset at only an institution without federation), the standalone scheme with GAN [15], the FL scheme without GAN [14], and the centralized scheme.

In Fig. 5(a), we compare the discriminator loss of our advanced FL scheme and the standalone scheme with GAN [15]. It can be seen that the the performance of the standalone scheme cannot achieve its optimum due to the lack of access to the full dataset. Meanwhile, our advanced FL scheme can learn over the entire data span from distributed datasets which is able to extract better image features for efficient data augmentation.

We then investigate the detection accuracy for different FL schemes and our advanced FL scheme, where the standalone scheme is used as the baseline. As shown in Fig. 5(b), the more participating institutions in data training, the higher accuracy achieved. The intuition behind this observation is the improved image feature learning efficiency thanks to the use of diverse data sources. Nevertheless, the accurate rate of our FL scheme is the best among all approaches and is close to the centralized scheme.

Additionally, we compare the accuracy performance of our scheme with other COVID-19 detection schemes, as indicated in Fig. 5(c). Our advanced FL scheme can significantly improve the accuracy performance due to its GAN and federated learning combination. Our scheme yields the highest accuracy of 0.963 after 200 iterative epochs, while other schemes including the FL scheme without GAN, the standalone scheme with GAN, and the standalone scheme without GAN have lower performances, with 0.922, 0.856, and 0.705, respectively.

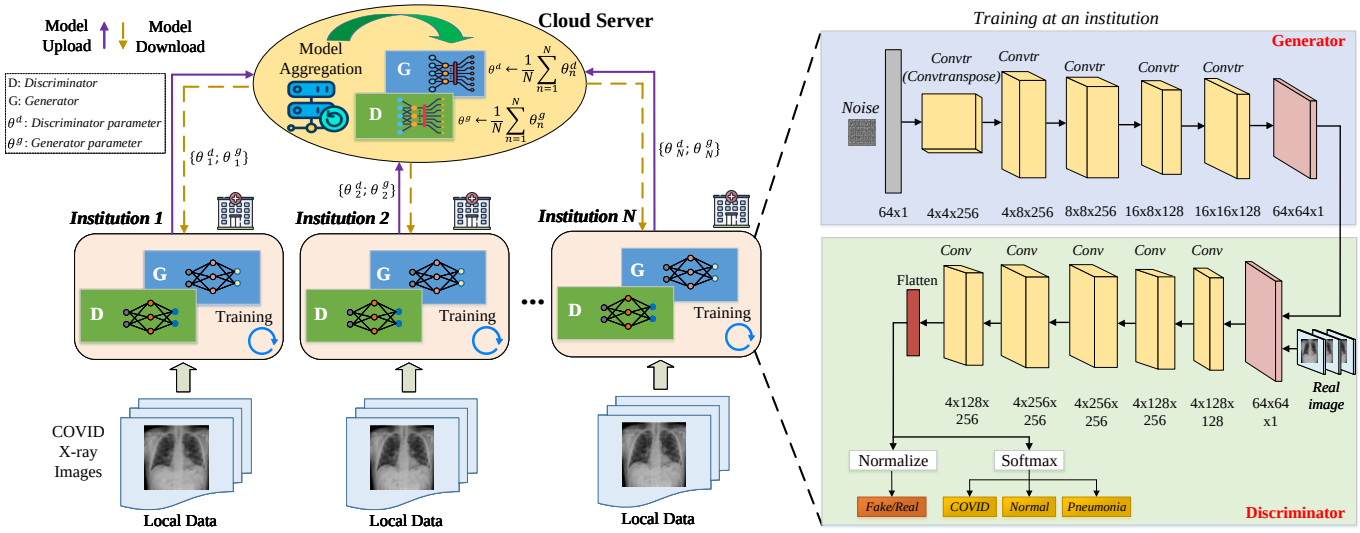
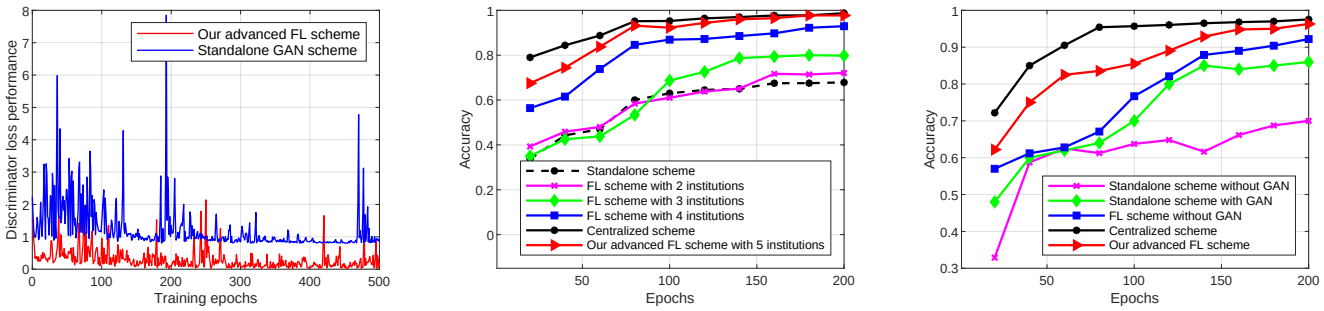


Fig. 4: Our advanced FL model for COVID-19 detection.



(a) Performance of discriminator loss.

(b) Performance of COVID-19 detection accuracy.

(c) Performance of COVID-19 detection accuracy.

Fig. 5: Performance comparison of different approaches for COVID-19 detection.

VI. Conclusions and Open Research Topics

This paper provided a detailed overview on the integration of FL into IIoT in industries. The roles of FL in important IIoT services and applications were identified and analyzed. The feasibility of FL in IIoT was demonstrated via a case study and simulations. Several interesting open research topics for FL-IIoT in industries are highlighted as follows:

- *Communication Issues in FL-IIoT:* Communications in FL-IIoT training in both uplinks and downlinks rely heavily on the level of interconnection among machines, AI software, and the computation server. This communication network also differs from traditional ones due to environmental constraints, such as high temperature and corrosive substances in manufacturing processes. Further, the high frequency bands, e.g., above 2.4GHz for WiFi networks, which are essential for low-latency FL communications, may be not available in realistic industrial environments like hospitals. New designs of efficient communication protocols specific to IIoT settings are desired to facilitate the FL training.
- *Resource Management Issues in FL-IIoT:* The concept of FL-IIoT mostly relies on scalable data parallelism and on-device training at IIoT devices. To achieve a synchronous update at the server, all IIoT devices need to devote their computational resources for training. Unfortunately, this requirement is not always met due to the resource constraints of certain IIoT devices with weak computation capacities, e.g., industrial wearable sensors, which can cause significant delays in model aggregation. Thus, resource-aware FL algorithms and resource allocation solutions should be considered in FL-IIoT system design.

- *Economic Issues in FL-IIoT:* In FL-IIoT, when an industrial user serves as training nodes, how to encourage them to join the FL process is a key challenge. A user may not be willing to devote its resources to perform data training if it does not have much economic benefits to compensate the consumption of computational resources. Incentive mechanisms such as credit-based support and revenue payment are highly needed to attract more users to join FL training which also enhances the robustness of industrial FL-IIoT systems.

Acknowledgments

This work was supported in part by the CSIRO Data61, Australia, and in part by U.S. National Science Foundation under Grant CCF-1908308. The work of Jun Li was supported by National Natural Science Foundation of China under Grant 61872184.

REFERENCES

[1] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018.

[2] Y. Qu, S. R. Pokhrel, S. Garg, L. Gao, and Y. Xiang, "A Blockchained Federated Learning Framework for Cognitive Computing in Industry 4.0 Networks," *IEEE Transactions on Industrial Informatics*, pp. 1–1, Jul. 2020.

[3] M. Hao, H. Li, X. Luo, G. Xu, H. Yang, and S. Liu, "Efficient and Privacy-Enhanced Federated Learning for Industrial Artificial Intelligence," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6532–6542, Oct. 2020.

[4] W. Sun, S. Lei, L. Wang, Z. Liu, and Y. Zhang, "Adaptive Federated Learning and Digital Twin for Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, pp. 1–1, Oct. 2020.

[5] H. Liao, Z. Zhou, X. Zhao, L. Zhang, S. Mumtaz, A. Jolfaei, S. H. Ahmed, and A. K. Bashir, "Learning-Based Context-Aware Resource Allocation for Edge-Computing-Empowered Industrial IoT," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4260–4277, May 2020.

[6] H. Liao, Z. Zhou, X. Zhao, and Y. Wang, "Learning-Based Queue-Aware Task Offloading and Resource Allocation for Space-Air-Ground-Integrated Power IoT," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5250–5263, Apr. 2021.

[7] J. Cao, K. Zhang, F. Wu, and S. Leng, "Learning Cooperation Schemes for Mobile Edge Computing Empowered Internet of Vehicles," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, Seoul, Korea (South), May 2020, pp. 1–6.

[8] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Differentially Private Asynchronous Federated Learning for Mobile Edge Computing in Urban Informatics," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2134–2143, Mar. 2020.

[9] Y. Song, T. Liu, T. Wei, X. Wang, Z. Tao, and M. Chen, "FDA3: Federated Defense Against Adversarial Attacks for Cloud-Based IIoT Applications," *IEEE Transactions on Industrial Informatics*, pp. 1–1, Jun. 2020.

[10] Y. Liu, Z. Ma, X. Liu, S. Ma, S. Nepal, and R. Deng, "Boosting Privately: Privacy-Preserving Federated Extreme Boosting for Mobile Crowdsensing," *arXiv:1907.10218*, Apr. 2020.

[11] Z. Du, C. Wu, T. Yoshinaga, K.-L. A. Yau, Y. Ji, and J. Li, "Federated Learning for Vehicular Internet of Things: Recent Advances and Open Issues," *IEEE Open Journal of the Computer Society*, vol. 1, pp. 45–61, May 2020.

[12] A. Taik and S. Cherkaoui, "Electrical Load Forecasting Using Edge Computing and Federated Learning," in *Proc. IEEE International Conference on Communications (ICC)*, Dublin, Ireland, Jun. 2020, pp. 1–6.

[13] M. Hao, H. Li, G. Xu, Z. Liu, and Z. Chen, "Privacy-aware and Resource-saving Collaborative Learning for Healthcare in Cloud Computing," in *Proc. IEEE International Conference on Communications (ICC)*, Dublin, Ireland, Jun. 2020, pp. 1–6.

[14] B. Liu, B. Yan, Y. Zhou, Y. Yang, and Y. Zhang, "Experiments of Federated Learning for COVID-19 Chest X-ray Images," Jul. 2020, arXiv: 2007.05592.

[15] Y. Jiang, H. Chen, M. H. Loew, and H. Ko, "COVID-19 CT Image Synthesis with a Conditional Generative Adversarial Network," *IEEE Journal of Biomedical and Health Informatics*, pp. 1–1, Dec. 2020.

Dinh C. Nguyen is currently pursuing the Ph.D. degree at the School of Engineering, Deakin University, Victoria, Australia. He is also affiliated with the Information Security and Privacy Research Group, CSIRO Data61, Docklands, Melbourne, Australia. His research interests focus on federated learning, blockchain, Internet of Things, and edge computing.

Ming Ding is currently a Senior Research Scientist with the CSIRO Data61, Sydney, NSW, Australia. His research interests include information technology, data privacy and security, machine learning and AI. He has authored over 100 articles in IEEE journals and conferences. He is an Editor of the IEEE Transactions on Wireless Communications and the IEEE Wireless Communications Letters.

Pubudu N. Pathirana is a full Professor and the Director of Networked Sensing and Control group at the School of Engineering, Deakin University, Geelong, Australia. He was a visiting professor at Yale University in 2009. His current research interests include bio-medical assistive device design, mobile/wireless networks, and Internet of Things.

Aruna Seneviratne is currently a Foundation Professor of telecommunications with the University of New South Wales, Australia, where he holds the Mahanakorn Chair of telecommunications. His current research interests are in physical analytics: technologies that enable applications to interact intelligently and securely with their environment in real time.

Jun Li received Ph. D degree in Electronic Engineering from Shanghai Jiao Tong University, China in 2009. His research interests include network information theory, game theory, distributed intelligence, multiple agent reinforcement learning. He has co-authored more than 200 papers in IEEE journals and conferences, and holds 1 US patents and more than 10 Chinese patents in these areas. He was serving as an editor of IEEE Communication Letters and TPC member for several flagship IEEE conferences.

Dusit Niyato (F'17) received the B.Eng. degree from the King Mongkuts Institute of Technology Ladkrabang, Thailand, in 1999, and the Ph.D. degree from the University of Manitoba, Canada, in 2008. He is currently a Professor with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research interests are in the areas of energy harvesting for wireless communication, the Internet of Things, and sensor networks.

H. Vincent Poor (F'87) is the Michael Henry Strater University Professor of Electrical Engineering at Princeton University. His interests include information theory, machine learning and networks science, and their applications in wireless networks, energy systems, and related fields. Dr. Poor is a Member of the National Academy of Engineering and the National Academy of Sciences, and a Foreign Member of the Chinese Academy of Sciences and the Royal Society. He received the Marconi and Armstrong Awards of the IEEE Communications Society in 2007 and 2009, respectively, and the IEEE Alexander Graham Bell Medal in 2017.