Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol X No. Y (20--)

Federated Learning: A Comprehensive Survey on Types, Applications, Challenges, and Future Directions

Nagaraj Naik,

Manipal Institute of Technology, MAHE, Manipal, India, Corresponding Author Email:Nagaraj.naik@manipal.edu

Vikranth B M

B.M.S College of Engineering, Bangalore, India, Email: vikranth.cse@bmsce.ac.in

Article History:

Received: *dd-mm-yyyy*

Revised: *dd-mm-yyyy*

Accepted: *dd-mm-yyyy*

Abstract: Federated Learning (FL) is a new machine learning (ML) paradigm where multiple parties jointly train a model without sharing each other's raw data, which is beneficial for predictive analytics with privacy protection and low data transmission cost. This work surveys the basic concepts in FL such as the three categories of FL: horizontal FL, vertical FL, and federated transfer learning, which are suitable for different types of data partitioning. With that in mind, FL is fitting for applications in healthcare, finance, edge computing, and IoT devices as it is able to maintain privacy-aware AI development. FL, however, has its own challenges, including communication overhead, computational costs, data heterogeneity, security, and fairness. The decentralized nature of the clients thus requires frequent exchanging of model updates, leading to more bandwidth-centric and high-latency constraints which may hinder their scaling silently. Furthermore, an ongoing challenge in FL concerns fairness, i.e., reducing potential biases that emerge from unbalanced data distributions. The next chapter of FL research would be a little more on the side of communication efficiency and probably leveraging adaptive compression mechanisms and zero-aggregation. To improve accuracy when dealing with heterogeneous environments, federated learning personalization (FL) is also gaining ground toward modifying models for each client while leveraging global knowledge. Additionally, continuing breakthroughs in federated reinforcement learning could further broaden the applicability of FL to dynamic, autonomous decision-making systems. Addressing these challenges will be key to creating scalable, secure and efficient FL frameworks for mainstream integration into privacy-sensitive fields. This survey presents a thorough introduction to FL, covering its advantages along with its disadvantages and future research trends. As FL tackles essential technical constraints and enhances its algorithmic architecture, it could potentially transform decentralized AI space and foster innovation in various fields.

Keywords: Federated learning, Privacy-Preserving AI, Decentralized Machine Learning, Data Heterogeneity.

1. Introduction

Federated Learning (FL) has emerged to address the growing need for privacy-preserving distributed machine learning, al- allowing clients to collaboratively train a model without sharing their raw data. Conventional centralized training approaches ask for aggregating all data at one server which invites privacy, issues, and regulatory hurdles [1],[2]. Federated Learning (FL) serves as a suitable solution where it keeps data local while enabling collaborative training, which is especially useful for applications in sensitive domains such as healthcare, finance, and the Internet of Things [3],[4]. Federated learning is a concept that was introduced by Google back in 2016 to help train AI models on decentralized data without compromising user privacy. In contrast to conventional centralized

training, in which data is sent to a central repository, FL allows model training on edge devices [5],[6]. This is reflected in areas such as personalized recommendation systems, predictive maintenance, and smart infrastructure, where FL is being widely adopted [7]. The federated learning framework is described in Figure 1.

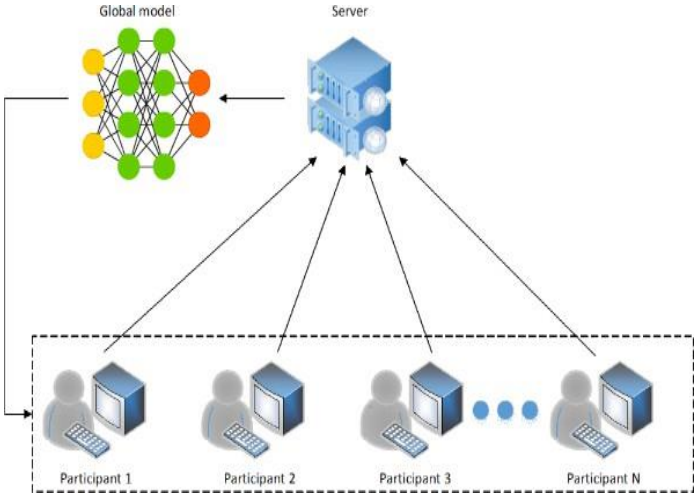

Fig. 1. Federated Learning Framework [1].

FL has many advantages over traditional centralized machine learning. A major advantage of such a traditional alternative is the privacy preservation target since clients never share their data, which eliminates the risk of data breach [8],[9]. Also, FL minimizes communication overheads because it sends only model updates (gradients or parameters) and not large datasets significantly saving bandwidth. The decentralized property of FL lets clients update their local models without the necessity of requiring a central dataset and also be a participant in the aggregation process of the global model [10]. FL additionally aids regulatory compliance (e.g., GDPR and HIPAA)since it guarantees that data never leaves its source. A significant benefit is its ability to support non-IID data, enabling clients to participate in a shared model despite disparate data distributions. Through many rounds of training and aggregation, FL facilitates the iterative enhancement of the model, ensuring that the performance of the global model converges to that of a centralized model.

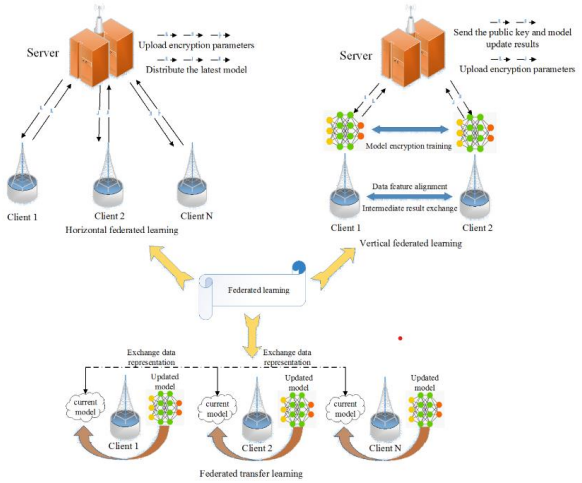

Fig. 2. Types of Federated Learning [1].

2. Key Features of Federated Learning

- Federated learning is a completely fresh paradigm of machine learning, where local models are trained without sharing training data on remote sites, preserving the privacy and security of the data. In the case of federated learning, the iterative data cleaning step helps users (clients) to only train the local models without disclosing raw data and thus safeguards the end-user from information leakage. While FL may incur a slight performance gap compared to their centralized model counterparts, performance is aggravated over the iterations of global training, preserving model robustness. Despite these benefits, still faced with issues surrounding communication efficiency, model heterogeneity, and security vulnerabilities with FL. This is also to say, that solving these problems will be key to unlocking the full potential of FL in real-world applications across multiple domains.
- Federated Learning (FL) has arisen as an effective de-centralized machine learning paradigm that allows associative model training while preserving data privacy. Federated learning (FL), in contrast to traditional centralized learning, enables multiple clients to jointly build a global model collaboratively without sharing raw data, which makes FL especially applicable to privacy-sensitive domains including healthcare, finance, and IoT [11].
- Concerning FL, it offers many benefits such as preserving the privacy of training data, decreased overhead in communication, decentralized model updates, and the meekness of data protection regulations such as GDPR. Moreover, FL naturally deals with non-IID data on heterogeneous clients, which adapts well to real-world tasks. FL improves the data privacy and freshness of the data, however, high communication cost, model heterogeneity and cybersecurity threats such as adversarial attacks and privacy threats are the challenges of FL.

3. Types of Federated Learning

Depending upon the nature of the data distribution, the Federated Learning approach can be classified into three broad categories, 1) Federation Transfer learning (FTL), 2) Vertical Federated learning(VFL), 3) Horizontal Federated Learning(HFL).

1.1. Federation Transfer learning

Federated Transfer Learning (FTL), an advanced parallel of Federated Learning (FL), allows collaborative training of models using different data while addressing crucial issues such as data heterogeneity and privacy preservation. FL (Federal Learning), on the other hand, assumes that all participations hold data from the same feature and label space. FTL (Federated Transfer Learning), however, assumes that different parties will have different feature distributions, label distributions, or both. This is especially beneficial for cases when organizations or devices have different datasets and they still need to construct a common model without risking data privacy. FTL harnesses Transfer Learning (TL) mechanics to transfer be shared from one specific area (domain) to another (target), to enable participants with dissimilar data properties to close others to the global model. In contrast to centralized Transfer Learning where data needs to be shared with a central entity, FTL provides knowledge transfer without sharing raw data. It does so through secure computation (e.g. homomorphic encryption (HE), differential privacy (DP), and secure multi-party computation (SMPC)). These techniques also enable organizations or devices to work together without revealing sensitive data. The different types of federated learning are depicted in Figure 2. This method is useful in cross-silo FL, where participants like educational institutes, banks, or hospitals want to train a global model while keeping their datasets private. It can also be used for cross-device FL, for which local devices with different distributions of private data can still be used to train a federated model. In general, the FTL process aligns either the shared or similar features among parties, transfers the knowledge between participants through

fine-tuning the pre-trained model, and employs secure algorithms to facilitate privacy-preserving learning. FTL can greatly improve the efficiency and usability of federated learning by filling the gaps of data heterogeneity, thus enabling more real-world applications

1.2. Horizontal Federated Learning (HFL)

When entities or devices share similar feature space but have different data samples, Horizontal Federated Learning or Sample-based Federated Learning applies. Meaning that all participant's organizations have the same kinds of data attributes (or features) while the individual records (or users) they have data on is different. This scenario commonly applies to applications in with many organizations working in the same industry to address varied user demands. Imagine several hospitals spread out across different regions interested in training a common machine-learning model to predict disease outcomes. Every hospital manages patient records with shared characteristics such as age, symptoms, medical history, and test results. However, since each hospital serves different patients, the datasets do not share individual records. In classical machine learning, all the hospitals need to gather their data and upload them to one place to train, which raises privacy concerns. Using HFL, each hospital can train a local model, and then, share only the learned parameters (e.g., gradients) with a central server that can aggregate them and improve a global model.

1.3. VFL (Vertical Federated Learning)

Feature-based Federated Learning (or Vertical Federated Learning) is applied when different entities have overlapping data samples (i.e., they have data about the same users), but (in addition) their datasets have different features. This form is appropriate when organizations in dissimilar sectors wish to collaborate without exposing their proprietary information. Consider a bank and an e-commerce company, both of which have records of the same customers. The bank has data on financial transactions, and the e-commerce company has data on customers' shopping behaviour. For example, both institutions may wish to jointly train a model for credit risk evaluation. But, privacy issues and competition, they cannot share raw data. Instead, with VFL they can train a model together as user records are aligned with encryption techniques such as Secure Multi-Party Computation (SMPC) or Homo-morphic Encryption, so they do not expose any sensitive data.

4. Application of Federated Learning

- FL is highly promising in the healthcare Analytic domain. It allows the providers to create predictive models of the hospital readmission risk from Electronic Health Records (EHR) without compromising data privacy. Also, consumer-facing applications, such as atrial fibrillation detection from electrocardiograms acquired via smartwatches, could use FL without exposing the end-user data. This paper, provides an overview of the federated learning framework, addresses its challenges and solutions, and its applications in healthcare. The authors [12] proposed a federated learning communication protocol to support this in emergency management applications. The main goal of this paper is to tackle the communication difficulties that arise in critical emergency management situations. This paper proposes a new protocol that overcomes the limitations of these centralized server architectures and thus represents a stronger alternative. Specifically, CATA supports communication via a certain protocol, allowing the framework to interact with various centralized servers, and facilitating knowledge sharing and model training among servers while ensuring data security and confidentiality. Consequently, it allows critical infrastructure systems, especially those running on an Android platform, to gain performance and resilient capabilities as supporting

systems for the real-time system. This study as a whole offers an improved mode of communication between various centralized servers with seamless communication, which is crucial for efficient emergency management, resulting in a valuable addition to the body of knowledge in the area of emergency management.

- The paper examines [13] how emerging technologies have enabled AI and machine learning to be deployed at the edge of the network. For high-velocity applications, simple models can be trained on the edge, and since they do not require high computational power, they can be run on local devices, making them close to the source of the data, enabling far superior scaling along with better data privacy. In particular, the paper contributes to the emerging framework of Federated Learning (FL) which offers a distributed machine learning approach for constructing a global model by learning from a number of decentralized edge clients. Though FL provides various advantageous features, such as improving privacy, it also results in challenges, especially, the computational complexity caused by heterogeneous devices. The unique nature of most IoT devices has computational constraints, unreliable connections, or different operating systems which all pose challenges for the effective implementation of FL. The focus is on breathtaking FL techniques, especially for edge devices that have limitations on computational ability and provide the most commonly used FL architectures that could facilitate the exchange of learning between clients and servers. The authors cover important concepts such as system architecture models, application use cases, privacy and security issues, and resource management- approaches. The paper also highlights critical issues that emerge due to the computational requirements of edge devices, including hardware heterogeneity, communication overhead, and constraints on device resources. This paper contributes to the increasing body of literature on FL for edge devices, offering a thorough overview of the state-of-the-art and potential applications and limitations of this emerging paradigm.
- This paper presents [14] an innovative Breast Cancer Di- agnosies method based on Deep Neural Networks (DNNs), a problem that prevails as one public health challenge worldwide. In this study, an iterative approach of collaborative learning is used where a breast cancer detection model with high precision is built using Federated Learning (FL). Utilizing FL, the framework allows multiple healthcare organizations to contribute local data while maintaining strong patient privacy and data security. Based on optimized feature selection, the proposed model performs exceptionally well, with an accuracy of 97.54%, precision of 96.5%, and recall of 98.0%. Moreover, data augmentation approaches play a crucial role in reducing loss and improving the overall performance of the model. Among the highlight results of the study is the F1-Score of 97%, which is a robust measure of the efficacy of the model employed. This study represents a landmark advancement in breast cancer screening with the promise of enhanced patient outcomes due to more accurate and robust detection. Breast cancer detection with FL: the transformative potential of collaborative learning Moreover, the paper outlines how breast cancer detection with FL has the potential to change the game when it comes to early detection. This research represents a significant advancement in the early detection and treatment of breast cancer, allowing a global patient population to benefit from these results by leveraging privacy-preserving techniques and diverse data sources.
- In view of security and privacy concerns, smart cities play a critical role, particularly in healthcare. As more Internet of Things (IoT)devices are deployed, user data has become an important property to support intelligent healthcare solutions [15]. In such a complex infrastructure where networks and applications have merged, it is essential to preserve the confidentiality and protection of this data. Data up to October 2023 is used to train on Blockchain federated-based architecture in a smart healthcare environment. The framework

implements Blockchain-based IoT cloud platforms that provide strong security and privacy to users' data. Federated Learning, a distinct variant of machine learning, is being employed to facilitate scalable healthcare applications without requiring users to send personal data to the cloud, thus protecting privacy. The paper further discusses how Federated Learning helps in building a secure environment in Smartt cities and its various applications, where it can be used for improving data security, and privacy scalability in modern healthcare solutions. This study marks a substantial step forward in the field of privacy-preserving technologies for smart cities, suggesting a secure and decentralized framework for managing healthcare data.

- In their paper [16], the authors introduced a novel, intelligent intrusion detection (IID) model based on deep learning techniques that combine Federated Learning (FL) with Long Short-Term Memory (LSTM) networks (FL- LSTM). Conventional deep learning-based IID methods relate to the training of the model on central servers, which cannot train the model with power due to the limit on a single user's server and going against user privacy, as well as collecting datasets from multiple user servers. In response to these problems, this paper proposes a federated learning framework, where the first LSTM global model is initially deployed on all user servers. Each user then trains their personal model locally and uploads the model parameters to a central server. These parameters are aggregated to form an updated global model which the central server re-distributes to the user servers, repeating the process until the model is fully trained. The simulation results show that the proposed FL-LSTM approach outperforms traditional approaches, achieving superior accuracy and consistency in intrusion detection. More importantly, since no raw data leaves the end user, user privacy is protected.

- State-of-the-art AI techniques, such as Federated Learning (FL), operate on distributed data and allow on-device or edge training of models while minimizing the need to move data to a centralized server, which raises new threats to security and privacy [17]. FL has received attention as a promising innovation in AI, however, it is still in the very early stages and there is limited trust in adopting it due to unresolved security and privacy concerns. This work seeks to advance the FL research by properly defining, assessing, and documenting the implications of these concerns. Given that is typically applied in conditions where privacy and security are imperative, being aware of the risk factors is vital for creating a safe environment and directing future research. A detailed overview of FL's security and privacy aspects is provided in the paper, along with an illustrative description of the different types of approaches and implementation styles. It also explains the prevalent issues in FL, especially the security threats (e.g., communication bottlenecks, poisoning attacks, backdoor attacks, etc.) and privacy risks (e.g., inference-based attacks, etc.). This shows that privacy-specific threats are less than security- related threats in FL. However inference-based attacks can be highly damaging to privacy. They end the paper with the future work required to tackle these challenges and make (FL) more adjustable to realistic scenarios and thus pave the path for its mass adoption.

- The proposed study [18] investigates federated learning in HAR by mimicking a distributed environment where several institutes participate to build only local models and the data is not shared among participants. They assess the impact of different data distributions (IID, non-IID, independent, and non-independent) and different participating institutions. They apply majority voting to obtain improved classification accuracy and robustness using an ensemble of YOLOv8 models. With time-consuming data transfer and privacy concerns about different data set sharing, the movement of data sets brings inconvenient and costly disadvantages to the distributed learning system, at the same time, empirical results indicate that federated The summary of Federated Learning Methods and Contributions are described in Table 1.

Table 1 Summary of Federated Learning

Author	Methods	Merit	Remarks
Michalek et al. [12]	Federated Learning, CATA Proto-col, Emergency Management	Improved communication and model training for emergency systems	Introduces a new communication protocol for federated learning to enhance communication in critical emergency management systems.
Brecko et al. [13]	Federated Learning (FL), Edge AI, IoT Devices	Enables AI deployment at the edge with privacy preservation	Addresses computational complexity and resource constraints in IoT devices, providing a detailed overview of FL architectures for edge devices.
Almufareh et al. [14]	Federated Learning (FL), Deep Neural Networks (DNNs), Data Augmentation	High accuracy (97.54%), precision (96.5%), and recall (98.0%)	The framework allows privacy-preserving breast cancer detection using FL. Data augmentation improves performance, and the model achieves an F1-Score of 97%.
Singh et al. [15]	Federated Learning (FL), Blockchain, IoT Cloud Platforms	Strong security and privacy in healthcare systems	Blockchain federated architecture in a smart healthcare environment preserves data privacy while allowing secure data-sharing among healthcare providers.
Zhao et al. [16]	Federated Learning (FL), Long Short-Term Memory (LSTM) networks, Intelligent Intrusion Detection (IID)	Improves accuracy and consistency in intrusion detection	The FL-LSTM approach offers superior accuracy while maintaining user privacy by preventing raw data transfer.
Mothukuri et al. [17]	Federated Learning (FL)	Overview of security and privacy concerns in FL	Addresses challenges like communication bottlenecks, poisoning attacks, and privacy risks such as inference-based attacks in FL-based systems.
Adnan et al. [18]	Federated Learning (FL), YOLOv8, Ensemble Learning	Improves classification accuracy and robustness in Human Activity Recognition (HAR)	Federated learning combined with the YOLOv8 ensemble boosts privacy and scalability in online proctoring applications. The model generalizes well across external datasets.
Rahman et al. [19]	Federated Learning (FL), Artificial Intelligence (AI), Explainable AI (XAI)	Decentralized model training, privacy preservation	FL enables strong online proctoring without exposing sensitive data. Future research on improving security, fairness, and transparency in digital education.
Shahid et al. [20]	Federated Learning (FL), Network Bandwidth Optimization	Improves model performance with high device participation	Communication overhead and computational costs may become bottlenecks with multiple devices.
Kang et al. [21]	Reputation-based worker selection, Blockchain integration in FL	Ensures trustworthy model updates, improves transparency	Reputation-based worker selection mitigates adversarial attacks and enhances FL robustness.
Batool et al. [22]	FL Design Patterns, Architecture Design, Model Aggregation Strategies	Insights on trade-offs, scalability, and performance	Identifies challenges in communication Efficiency, statistical/system heterogeneity, and security/privacy in FL-based systems.
Li et al. [23]	FedProx, FL with heterogeneity	Improves robustness and convergence in heterogeneous environments	FedProx guarantees convergence and demonstrates improved accuracy over FedAvg in heterogeneous environments.
Avdiukhin et al. [24]	Asynchronous Local SGD, FL with non-synchronous updates	Reduces communication delay, improves scalability	Achieves similar convergence as synchronous methods with better practical impreventability.

- The high interest in the areas of Federated Learning (FL), Artificial Intelligence (AI), and Explainable Artificial intelligence (XAI) to secure and optimize the online examination monitoring system [19]. The centralized architecture against the classical proctoring systems where the raw data is sent to a centralized server for storage and then transferred to a storage raises privacy issues and can expose the system to security vulnerabilities. On the other hand, the incorporation of FL with AI forms a distributed architecture and it makes it possible to train models collectively across different institutions without sharing the actual data, preserving

privacy. This allows for strong online proctoring without ever exposing sensitive information. This paper provides an extensive review of FL and AI for HAR in online examinations. In doing so, they explained how federated learning (FL) can be applied to decentralize the model training paradigm, thus, allowing institutions to achieve such intelligent monitoring without exposing sensitive data. Moreover, addresses the importance of XAI adoption to enhance the transparency and reliability of AI-based proctoring systems. The work categorizes and investigates the different FL-based AI techniques utilized in securing online examinations, and pertinent factors affecting security such as privacy, scalability, as well as model performance in non-IID contexts.

- Federated Learning (FL) has been proposed [21] as a novel decentralized machine learning framework that enables the training of machine learning models across multiple devices while keeping the data localized and thus does not expose data to the central server. FL: Given a pool of mobile devices promising high-quality variable datasets, local datasets on each device can be leveraged (F254), accumulating valuable training data for ML device nodes(without sharing raw data across the network). These local updates are collected by a central aggregator for iterative refinement of a global model. Nonetheless, the security of FL is heavily dependent on the integrity and trustworthiness of the involved devices. A key challenge in FL is the existence of unreliable data, due to intentional adversarial attacks such as data poisoning or unintentional issues such as device energy constraints and network instability. Malicious or low-quality updates could substantially degrade the performance of the model and damage the integrity of the system. Last but not least, this problem can be solved by means of reputation-based worker selection, which has emerged as a significant strategy for reliable participation in FL. This paper provides a framework for reputation-based worker selection using consortium blockchain to form a decentralized and immutable reputation management system. With the implementation of blockchain, the approach improves transparency, accountability, and trust between the devices involved. However, the numerical analysis shows that the effective method can eliminate the contribution of unfairness, which is very effectively improving the robustness and reliability of FL tasks in mobile networks. This study shows the fundamental need for the management of trust that is inherent in FL and provides the key insight that using blockchain-integrated reputation mechanisms could be a promising approach to ensuring trustworthy model updates within distributed environments. Future studies can investigate optimizing computational efficiency and scalability for practical applications.
- Federated Learning (FL) [22] has arisen as a promising paradigm for dealing with decentralized data preserving privacy and security. While extensive works focus on the ML side of FL, the software architecture design of FL systems has received little attention. To bridge this gap, this paper presents a toolkit consisting of design patterns that provide reusable solutions to recurring architectural issues in FL. Study Approach — There are three primary fields of focus: FL Design Patterns – The Paper describes core design elements: architectures, frameworks, client selection protocols, personalization, and model aggregation strategies. This approach allows us to explore valuable insights into Trade-offs, Scalability, Performance, and Security implications of each design aspect to better understand how they impact FL systems. Challenges in FL Design and Implementation –The paper investigates core challenges in FL; namely communication efficiency, statistical and system heterogeneity, and security/privacy issues. It highlights the ongoing research works that are being done to mitigate these limitations for better performance and effective use of FL-based frameworks. Applications in Industrial Control Systems (ICS) – The paper describes how FL is currently being used in industrial automation and control systems, pointing out both advantages and disadvantages. The research highlights gap identification in this domain i.e., improved FL solutions are crucial to be

implemented in industrialized settings. This paper provides a holistic and comprehensive reference that discusses FL design patterns, challenges, and applications, it will be a remarkable piece of information and reference for the researchers, practitioners, and system designers working on FL-based solutions. The future research directions for enhancing system design for real-world scalability, improving the level of FL heterogeneity in simulated and actual environments, and fortifying security frameworks to support FL applications in industrial environments.

- Federated Learning (FL) [23] arises into a realm that lies within the barrier to traditional optimization, namely systems heteronomy (heterogeneousness of devices) as well as statistical heterogeneity (non-identical distributed data). To address these problems, this paper, proposes FedProx, a framework to further improve the robustness and convergence of FL in the presence of heterogeneities. FedProx is a re-parametrized and generalized version of the standard FL algorithm, FedAvg. Although its modifications to FedAvgare all minor, they have far-reaching theoretical and practical implications. Convergence Guarantees– A theoretical analysis proves that FedProx guarantees convergence. It allows for heterogeneous computation resource usage on devices, making it well-suited for real-world federated environments. Empirical Validation Then show that experimental results show that Fed- Prox converges more stable and accurately than FedAvg, especially in a very heterogeneous environment. The study demonstrates its effectiveness, reporting an average absolute test accuracy increase of 22%.
- Federated Learning (FL) refers [24] to the process of training a global model on decentralized data that lies within many heterogeneous clients. These clients usually experience slow and unreliable network connections, so synchronous communication is difficult. To tackle this, the paper investigates a case of local Stochastic Gradient Descent (SGD), where the clients update and pass messages to the central server asynchronously instead of synchronously. In particular, the main contributions of this work are: Asynchronous Local SGD Framework – Instead of requiring clients to synchronize at fixed intervals, clients update their local model independently and send update signals to the central server at different times, thus reducing communication delay. The paper shows that the asynchronous version of local SGD achieves similar convergence rates as the synchronous version, which have been held for smooth strongly convex and smooth nonconvex functions, even though update intervals differ.
- The suggested method improves the scalability and practicality of FL as it does not need tight synchronization across clients, which could be used for real-world scenarios where clients might randomly join or leave.

5. Future Direction of Federated Learning

- In recent years, FL research has been intensive and has made great advances to improve security, efficiency, and personalization. To ensure security and adaptability, techniques such as secure aggregation using homomorphic encryption, differential privacy, and personalized FL models have been proposed. Blockchain technology has also been proposed to ensure the transparency and reliability of FL systems.
- Ultimately, the future of FL research will involve the optimization of communication efficiency, improved robustness against attacks, and the development of adaptive federated learning models that can handle dynamic participation. FL is gaining popularity across industries, with ongoing research focusing on its challenges to position FL as a defect paradigm for privacy-preserving, distributed machine learning.
- Moreover, we suggest possible future research directions in terms of FL-supported AI applications in online education. The insights of the study can help in overcoming the existing

limitations and enhancing the efficacy of AI-based proctoring using FL and ensemble learning techniques. In closing, we present future avenues for improving federated AI systems in terms of security, fairness, and transparency for digital educational settings.

- Number of Participating Devices [20] in an FL environment, the higher the number of devices, the better the model performance due to training on diverse data.
- Yet, participating in multiple rounds of training simultaneously results in high communication overhead and computational costs, which may become a bottleneck.
- Network Bandwidth Even though FL reduces data transfer costs compared to traditional ML, it still requires sufficient communication bandwidth. Unreliable network conditions, fluctuations in upload/download speeds, and model update delays can interrupt the FL process and cause communication traffic bottlenecks.

References

[1] J. Wen, Z. Zhang, Y. Lan, Z. Cui, J. Cai, and W. Zhang, "A survey on federated learning: challenges and applications," International Journal of Machine Learning and Cybernetics, vol. 14, no. 2, pp. 513–535, 2023.

[2] L. Li, Y. Fan, M. Tse, and K.-Y. Lin, "A review of applications in federated learning," Computers & Industrial Engineering, vol. 149, p. 106854, 2020.

[3] P. M. Mammen, "Federated learning: Opportunities and challenges," arXiv preprint arXiv:2101.05428, 2021.

[4] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, "A survey on federated learning," Knowledge-Based Systems, vol. 216, p. 106775, 2021.

[5] A. Nilsson, S. Smith, G. Ulm, E. Gustavsson, and M. Jirstrand, "A per- formance evaluation of federated learning algorithms," in Proceedings of the second workshop on distributed infrastructures for deep learning, pp. 1–8, 2018.

[6] S. Banabilah, M. Aloqaily, E. Alsayed, N. Malik, and Y. Jararweh, "Federated learning review: Fundamentals, enabling technologies, and future applications," Information processing & management, vol. 59, no. 6, p. 103061, 2022.

[7] A. Z. Tan, H. Yu, L. Cui, and Q. Yang, "Towards personalized federated learning," IEEE transactions on neural networks and learning systems, vol. 34, no. 12, pp. 9587–9603, 2022.

[8] M. Shaheen, M. S. Farooq, T. Umer, and B.-S. Kim, "Applications of federated learning; taxonomy, challenges, and research trends," Elec- tronics, vol. 11, no. 4, p. 670, 2022.

[9] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. Cummings, et al., "Advances and open problems in federated learning," Foundations and trends® in machine learning, vol. 14, no. 1–2, pp. 1–210, 2021.

[10] W. Zellinger, V. Wieser, M. Kumar, D. Brunner, N. Shepeleva, R. Ga´lvez, J. Langer, L. Fischer, and B. Moser, "Beyond federated learning: On confidentiality-critical machine learning applications in industry," Procedia Computer Science, vol. 180, pp. 734–743, 2021.

[11] J. Xu, B. S. Glicksberg, C. Su, P. Walker, J. Bian, and F. Wang, "Federated learning for healthcare informatics," Journal of healthcare informatics research, vol. 5, pp. 1–19, 2021.

[12] J. Michalek, V. Oujezsky, M. Holik, and V. Skorpil, "A proposal for a federated learning protocol for mobile and management systems," Applied Sciences, vol. 14, no. 1, p. 101, 2023.
[13] A. Brecko, E. Kajati, J. Koziorek, and I. Zolotova, "Federated learning for edge computing: A survey," Applied Sciences, vol. 12, no. 18,p. 9124, 2022.
[14] M. F. Almufareh, N. Tariq, M. Humayun, and B. Almas, "A federated learning approach to breast cancer prediction in a collaborative learning framework," in Healthcare, vol. 11, p. 3185, MDPI, 2023.
[15] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, and B. Yoon, "A framework for privacy-preservation of iot healthcare data using federated learning and blockchain technology," Future Generation Computer Systems, vol. 129, pp. 380–388, 2022.
[16] R. Zhao, Y. Yin, Y. Shi, and Z. Xue, "Intelligent intrusion detection based on federated learning aided long short-term memory," Physical Communication, vol. 42, p. 101157, 2020.
[17] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, "A survey on security and privacy of federated learning," Future Generation Computer Systems, vol. 115, pp. 619–640, 2021.
[18] M. Adnan, S. Kalra, J. C. Cresswell, G. W. Taylor, and H. R. Tizhoosh, "Federated learning and differential privacy for medical image analysis," Scientific reports, vol. 12, no. 1, p. 1953, 2022.
[19] A. Rahman, M. S. Hossain, G. Muhammad, D. Kundu, T. Debnath, M. Rahman, M. S. I. Khan, P. Tiwari, and S. S. Band, "Federated learning-based ai approaches in smart healthcare: concepts, taxonomies, challenges and open issues," Cluster computing, vol. 26, no. 4, pp. 2271–2311, 2023.
[20] O. Shahid, S. Pouriyeh, R. M. Parizi, Q. Z. Sheng, G. Srivastava, and L. Zhao, "Communication efficiency in federated learning: Achieve- ments and challenges," arXiv preprint arXiv:2107.10996, 2021.
[21] J. Kang, Z. Xiong, D. Niyato, Y. Zou, Y. Zhang, and M. Guizani "Reliable federated learning for mobile networks," IEEE Wireless Com- munications, vol. 27, no. 2, pp. 72–80, 2020.
[22] H. Batool, J. Xu, A. U. Rehman, and H. Hamam, "Design pattern and challenges of federated learning with applications in industrial control system,"
[23] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, "Federated optimization in heterogeneous networks," Proceedings of Machine learning and systems, vol. 2, pp. 429–450, 2020.
[24] D. Avdiukhin and S. Kasiviswanathan, "Federated learning under arbi- trary communication patterns," in International Conference on Machine Learning, pp. 425–435, PMLR, 2021.