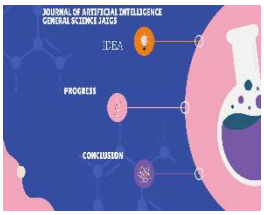
Vol.3, Issue 01, March 2024
Journal of Artificial Intelligence General Science JAIGS



Constructing Executing and Overcoming Challenges in Distributed AI Systems: A Study of Federated Learning Framework

José Gabriel Carrasco Ramírez

Lawer graduated at Universidad Católica Andrés Bello. Caracas. Venezuela. / CEO, Quarks Advantage. Jersey City, United States. / Director at Goya Foods Corp., S.A. Caracas. Venezuela

*Corresponding Author: José Gabriel Carrasco Ramírez

ARTICLEINFO
Article History:
Received: 05.03.2024
Accepted: 10.03.2024
Online: 02.04.2024
Keyword: *Federated Learning, Decentralized AI Systems, Architectural Design, Implementation Approaches, Data Privacy Preservation, Communication Optimization, Model Aggregation Techniques, Security Concerns.*

ABSTRACT

Federated learning stands out as a promising approach within the realm of distributed artificial intelligence (AI) systems, facilitating collaborative model training across decentralized devices while safeguarding data privacy. This study presents a thorough investigation into federated learning architecture, covering its foundational design principles, implementation methodologies, and the significant challenges encountered in distributed AI systems. We delve into the fundamental mechanisms underpinning federated learning, elucidating its merits in diverse environments and its prospective applications across various domains. Additionally, we scrutinize the technical complexities associated with deploying federated learning systems, including considerations such as communication efficiency, model aggregation techniques, and security protocols. By amalgamating insights gleaned from recent research endeavors and practical deployments, this study furnishes valuable guidance for both researchers and practitioners aiming to harness federated learning for the development of scalable and privacy-preserving AI solutions.

Introduction:

The surge in data-generating devices and the growing need for privacy-centric AI solutions have propelled federated learning to the forefront of distributed artificial intelligence (AI) exploration. Traditional centralized machine learning methods often encounter significant hurdles in handling sensitive data, as data aggregation raises concerns about privacy violations and regulatory compliance. Federated learning offers a compelling alternative by facilitating model training directly on decentralized devices while maintaining raw data locality, effectively addressing privacy concerns while upholding model performance.

This article offers a comprehensive analysis of federated learning architecture, covering its design, implementation, and challenges within distributed AI systems. We commence by elucidating the fundamental principles of federated learning, emphasizing its advantages in heterogeneous environments where data sources exhibit diversity and geographical dispersion. Through federated learning, organizations can unlock insights from data silos without compromising data privacy, rendering it particularly attractive in sectors such as healthcare, finance, and IoT.

Furthermore, we delve into the intricacies of implementing federated learning systems, exploring various strategies for orchestrating model training across a network of edge devices, mobile phones, or IoT sensors. This includes examining techniques for streamlined communication, robust model aggregation, and adaptive learning algorithms tailored to the decentralized nature of federated environments.

Despite its promise, federated learning also presents several challenges, spanning from communication overheads and heterogeneity in device capabilities to security vulnerabilities and algorithmic biases. Throughout this article, we endeavor to address these challenges and provide insights into mitigating their impact on the efficacy and dependability of federated learning systems.

By amalgamating insights from recent research advancements and practical implementations, this paper serves as a valuable guide for researchers, developers, and practitioners keen on harnessing the potential of federated learning to construct scalable, privacy-preserving AI solutions in distributed settings.

Objectives

1. Exploring Federated Learning Architecture: This paper aims to delve into the foundational principles and structural components of federated learning, elucidating how decentralized model training can be orchestrated across a network of devices while safeguarding data privacy.

2. Investigating Implementation Strategies: We aim to analyze various implementation strategies and techniques employed in federated learning systems, encompassing communication optimization, model aggregation methods, and adaptive learning algorithms tailored to distributed environments.

3. Addressing Challenges in Distributed AI Systems: This paper endeavors to identify and tackle key challenges encountered in federated learning and distributed AI systems, such as communication overheads, heterogeneity in device capabilities, security vulnerabilities, and algorithmic biases, providing insights into effective mitigation strategies.

Review of Relevant Literature:

Federated Learning (FL) architectures within distributed AI systems strive to safeguard privacy by aggregating locally trained models without external raw data sharing. Challenges encompass accountability, fairness, communication costs, and non-IID data distribution. Innovative solutions are proposed by researchers to tackle these challenges. For instance, a blockchain-based architecture enhances accountability and fairness [1] [2]. Moreover, in-cluster training and gradient scarification techniques bolster communication efficiency and performance, particularly with Non-IID data, as evidenced by the FedOES approach [3]. It's also imperative to grasp Quantum Federated Learning (QFL), with ongoing research centering on novel frameworks, applications, and critical design factors [4] [5]. These advancements contribute significantly to shaping more resilient and efficient federated learning systems within distributed AI environments.

Background:

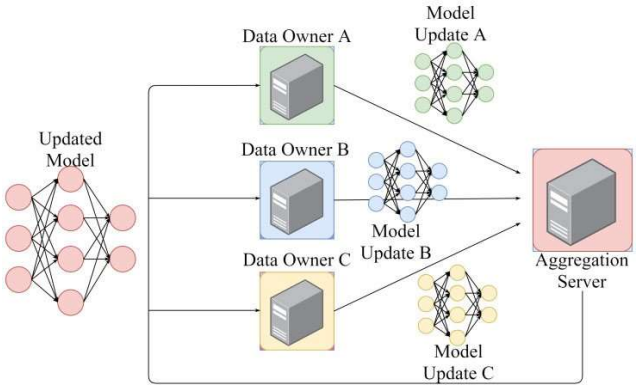
In recent years, the field of machine learning (ML) and deep learning (DL) has witnessed remarkable growth, largely driven by the vast availability of data. However, numerous application domains lack centralized repositories of adequately labeled and comprehensive data, such as medical image analysis for doctors' diagnoses. The creation of such datasets is often time-consuming, labor-intensive, and reliant on domain expertise, resulting in the emergence of data silos within individual organizations. While some organizations manage to accumulate high-quality datasets, they are often small in scale, impeding the effectiveness of DL applications that necessitate extensive, fully labeled data.

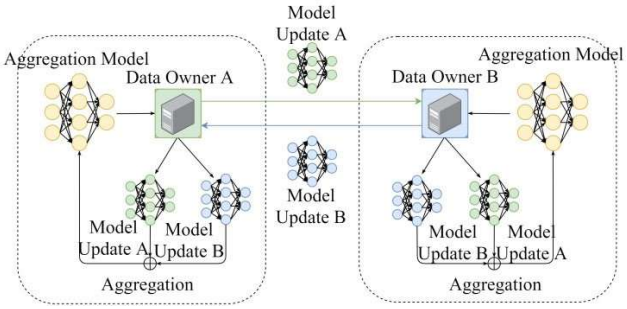
Traditionally, ML models were constructed using data collected in centralized locations. However, concerns regarding data ownership, confidentiality, user privacy, and evolving data management regulations like the General Data Protection Regulation (GDPR) require private, secure, efficient, and equitable distributed model training methodologies. Federated learning (FL) addresses these concerns by permitting separate model training on local data distributed across various devices or organizations. Local model updates are subsequently aggregated to form a global model, ensuring the privacy of individual data.

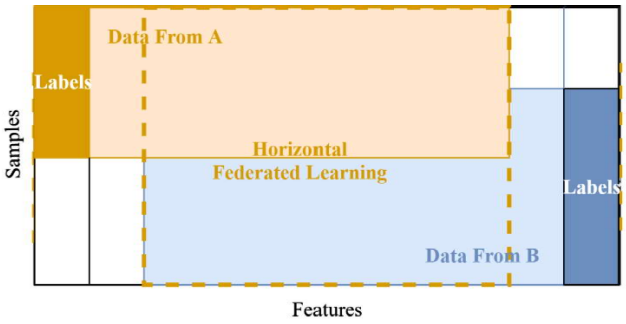
Initially introduced by researchers at Google for updating language models in keyboard systems, FL entails constructing a joint model using data from different sites without sharing raw data. The joint model is encrypted and shared among participants to uphold privacy, resulting in a performance approximation of an ideal model trained with centralized data. Despite potential accuracy losses due to added security measures, FL offers significant privacy and security benefits, often outweighing the drawbacks, especially in sensitive application domains.

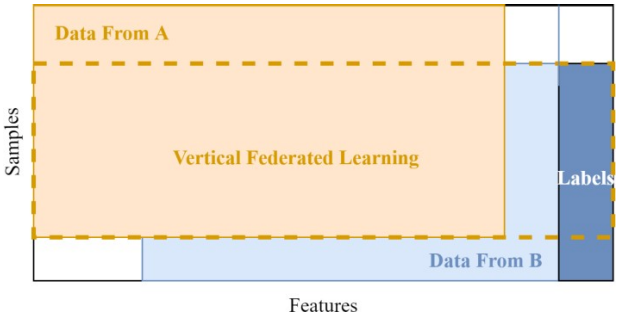
FL architectures typically adhere to either the client-server or peer-to-peer model. In the client-server model, a coordinator aggregates model parameters using federated averaging (FedAvg). Each participating client receives an initial model, trains locally, and sends updates to the coordinator for aggregation. This process repeats until convergence. While the client-server architecture minimizes communication overhead, the peer-to-peer model enhances security by facilitating direct client communication. However, the peer-to-peer model requires more computational resources for encryption and decryption.

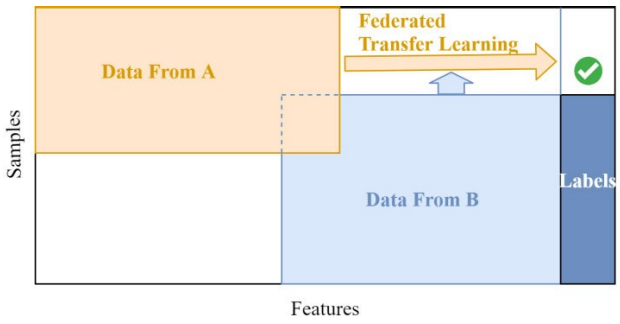
In summary, FL presents a promising approach to address data privacy concerns while enabling collaborative model training in distributed environments. Its adoption holds significant potential for improving model quality and security across various application domains.











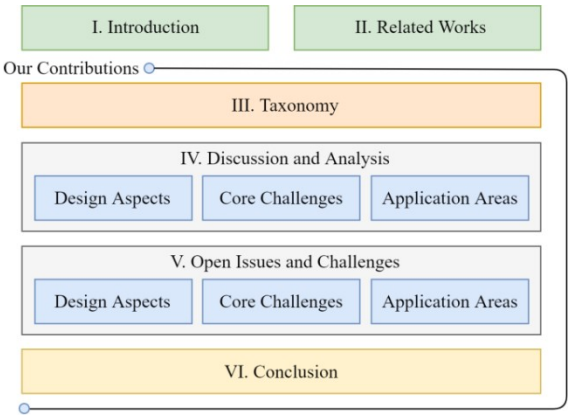
Federated Learning (FL) encompasses various methodologies, including horizontal FL (HFL), vertical FL (VFL), and federated transfer learning (FTL). In HFL, alignment occurs in data features across participants, while in VFL, alignment is in data samples rather than features. However, both HFL and VFL may not be effective in highly heterogeneous data scenarios. In such cases, FTL offers a solution by transferring learned knowledge from a source domain to a target domain, inspired by transfer learning principles.

Yet, the discussed architectures and FL categories represent only a fraction of FL research. Numerous research thrusts explore novel architectures, data partitioning schemes, and aggregation techniques. Efforts are also underway to address core challenges in FL such as privacy, security, communication costs, system and statistical heterogeneity, and personalization techniques. Each application area of FL presents unique challenges and considerations.

While significant research has already been conducted in FL, various survey papers have summarized different focus areas. This study aims to review existing surveys covering various domains and focus areas in FL research. We delve into core challenges such as privacy, security, communication costs, system and statistical heterogeneity, architecture, and aggregation algorithm designs, each of which varies by domain and specific use case.

The motivation behind this paper lies in reviewing the current literature and summarizing state-of-the-art approaches developed to address these challenges. We also aim to identify gaps in existing FL surveys and fill them by surveying the latest developments in all aforementioned FL research areas. Our review offers a holistic examination of challenges, applications, and design factors, outlining promising future research directions.

We thoroughly investigate contemporary FL survey papers, classify FL research into broad categories of design aspects, challenges, and application areas, and discuss open issues and challenges in FL research. The remainder of this paper is organized as follows: Section II discusses related studies, Section III illustrates the taxonomy of survey papers, Section IV provides a discussion and analysis of topics under each category, Section V discusses open issues and challenges, and finally, Section VI concludes the paper.



Related Work

In this section, we undertake an investigation and analysis of contemporary survey papers in the field. The reviewed papers, along with their summaries and focuses, are detailed in Table 1.

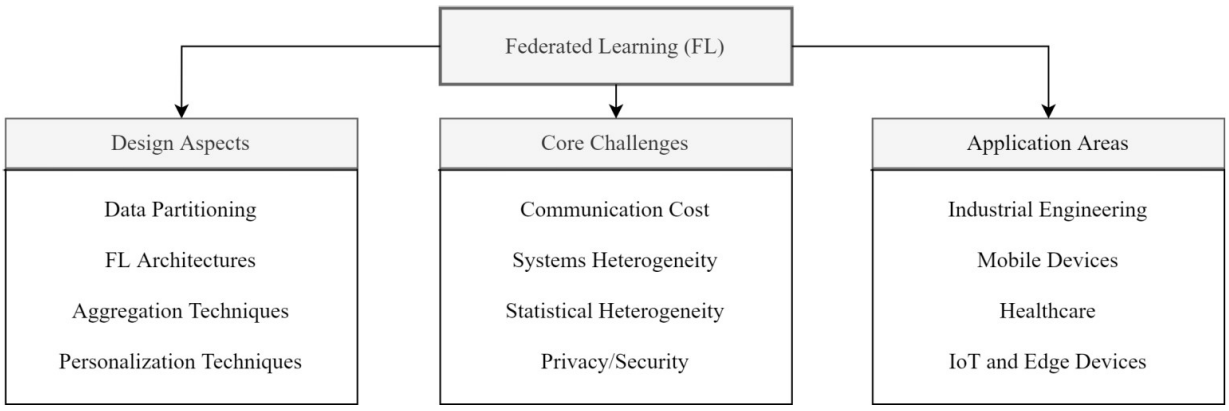
Li, Sahu et al. [3] examined the distinctions between federated learning (FL) and standard distributed machine learning (ML). They explored FL's unique characteristics, challenges, current methodologies, and future prospects. Although the paper did not concentrate on any specific domain, it addressed approaches tackling four core challenges: expensive communication, systems heterogeneity, statistical heterogeneity, and privacy/security. Local updating [1], [4] emerged as an approach to reduce the number of communication rounds. Conversely, compression schemes [5] aimed to diminish message sizes during communication rounds. Moreover, decentralized training [6], [7] alleviated the central server's communication burden. To tackle systems heterogeneity, asynchronous communication [8]–[10] was employed to minimize stragglers, while active sampling selected or influenced participating devices based on their system resources and overheads, with fault tolerance [11]–[16] disregarding failed devices through algorithmic redundancy. Addressing statistical heterogeneity, methods such as meta-learning and multitask learning were utilized to model heterogeneous data, adapting the selection

between global and device-specific models, and leveraging transfer learning for personalization. Additionally, convergence guarantees for non-independent and identically distributed (non-IID) data [4], [10], [17], [18] were investigated. Finally, this survey encompassed secure multiparty computation (SMC) [19], [20], and differential privacy (DP) [21]–[24] approaches.

Authors in [25] directed their focus towards mobile edge networks, identifying core challenges including expensive communication, systems heterogeneity, and privacy/security. To address communication cost challenges, they explored various approaches such as model compression [26], [27], importance-based updating for selective gradients [28], or local model updates [29], with a specific focus on edge and end computation. Methods to mitigate systems heterogeneity encompassed active sampling based on computation capabilities [33], data characteristics [34], and resource consumption [35] and allocation [36], [37].

TABLE 1. Summary table of survey papers and main focus.

Survey Paper	Summary	Main Focus
Li, Sahu, *et al.* [3]	Discusses the unique characteristics and challenges of FL, provides details of current approaches, outlines directions of future work.	Challenges
Lim *et al.* [25]	Highlights challenges of FL implementation and existing solutions and presents applications of FL for mobile edge network optimization.	Mobile edge networks
Briggs *et al.* [57]	Focusing on IoT, covers works related to FL challenges and privacy preserving methods, identify the strengths and weaknesses of different methods applied to FL, and outlines future directions.	IoT, privacy/security
Li, Wen, *et al.* [58]	Categorizes FL systems according to six different aspects to facilitate and guide the design of FL systems, provides case studies and future research opportunities.	FL systems
Li, Fan, *et al.* [59]	Illustrates the evolution of FL and reviews existing applications of FL in industrial engineering, mobile devices and healthcare.	Applications
Kurupathi, Maass [60]	Highlights existing privacy techniques and proposes applications of FL in industries.	Privacy/security, applications
Yang *et al.* [61]	Introduces a secure FL framework, which includes horizontal FL, vertical FL and federated transfer learning, and proposes building data networks among organizations based on federated mechanisms.	Architecture, applications
Xu *et al.* [62]	Provides a review for FL technologies mainly for biomedicine, and discusses the challenges, issues and potential of FL in healthcare.	Healthcare
Kulkarni *et al.* [63]	Highlights the need for personalization in FL and surveys research on the topic.	Personalization
Lyu *et al.* [64]	Introduces taxonomy of threat models and major attacks on FL, highlighting intuitions, techniques and assumptions adopted by different attacks and discusses future research directions.	Threat models and attack types
Aledhari *et al.* [65]	Provides a thorough summary of relevant protocols, platforms, challenges and real-life uses cases of FL.	Platforms, protocols, applications
Mothukuri *et al.* [66]	Provides a detailed study of security and privacy, and presents current approaches, challenges and future directions in FL.	Privacy/security



Discussion and Analysis

In this section, we undertake a review and discussion of the design aspects, core challenges, and application areas to offer a comprehensive summary of the following subtopics: data partitioning, FL architectures, aggregation techniques, personalization techniques, communication cost, systems heterogeneity, statistical heterogeneity, privacy/security, and application areas.

Design aspects

Data partitioning

Data utilized for training in FL exhibits non-identical characteristics due to its distribution across various devices. The dataset's sample space comprises all instances, while the feature space encompasses different attributes. For instance, two hospitals may possess records of different patient sets (sample space) and diverse information about each patient in their Electronic Health Records (EHR) (feature space). FL systems (FLSs) categorically fall into horizontal FL (HFL), vertical FL (VFL), and hybrid FL based on how data are allocated across multiple devices in terms of sample and feature spaces.

Horizontal FL (HFL): This scenario occurs when datasets share the same feature space but differ in sample space. HFL is commonly employed in cross-device scenarios where individual users aim to enhance their model's performance on a task. It's characterized by horizontal partitioning, where local data overlap in the feature space, allowing each user to train their local models using a duplicate model architecture. For example, regional branches of an organization may possess different user groups but share the same feature spaces. Notably, research by McMahan et al. [1] falls within the horizontal partitioning paradigm, where individual users on the Android platform update model parameters locally, contributing to centralized model training. Additionally, to address finite labeled entities, hierarchical

heterogeneous HFL frameworks have been proposed, allowing adaptation of each user multiple times as the target domain.

Vertical FL (VFL): This scenario arises when datasets across institutions share similar sample spaces but have dissimilar feature spaces. In VFL, participants possess homogeneous data but differ in feature space, necessitating privacy-preserving methods for model training. VFL aggregates distinct features while preserving privacy, ultimately constructing a model by combining data from multiple parties. Approaches such as linear regression have been proposed for vertically partitioned data, along with secure models like k-means, association rule mining, decision trees, and naive Bayesian classifiers. VFL systems typically perform entity alignment to combine common samples from different institutions, followed by encryption for collaborative model training.

In the subsequent sections, we continue to explore various aspects of federated learning, including architectures, challenges, and application domains.

Federated Transfer Learning (FTL)

FTL finds utility in situations where two datasets vary not only in sample but also in feature space. Initially proposed in [79], FTL enhances existing FL systems and extends beyond the scope of conventional FL algorithms. Its application has garnered significant attention across various industries, notably in healthcare [121]. FTL facilitates the sharing of diverse treatment and diagnosis information among hospitals to address a range of diseases. Transfer learning, a fundamental concept underlying FTL, aims to establish a common representation of features from disparate parties, requiring both parties to compute prediction results independently. Consequently, transfer learning techniques can be applied to the entire feature and sample space within a federated environment. To uphold privacy, FTL leverages encryption and approximation techniques, ensuring that sensitive data and models remain locally preserved [122]. Efforts to enhance FTL include Sharma et al.'s integration of secret sharing technology [123]. Furthermore, works by [124], [125] introduce the FedHealth model, which leverages FL to collect data from various institutions and deliver tailored healthcare services through transfer learning.

Each data partitioning paradigm presents its own set of advantages and limitations. For instance, two distinct clinics or hospitals can securely exchange data based on their respective needs in terms of instances or features required. While one clinic may possess millions of patient records with specialized information (e.g., oncology), another clinic, albeit newer, may have fewer records but diverse patient

information. In such cases, the first clinic could benefit from VFL, while the second could leverage HFL. Ultimately, FTL enables healthcare providers to offer more personalized care by leveraging data from users' wearable devices for personal fitness.

Federated Learning (FL) architectures

Federated Learning (FL) architectures depict the integration of various components to establish an FL environment. Two prevalent architectures in FL are the client-server and peer-to-peer architectures.

Client-Server Architecture:

In the client-server architecture, depicted earlier in Fig. 1, a central server initiates a global model shared with clients for training on their local datasets. Post local training, trained models from involved clients are gathered by the server. The server then aggregates the models' parameters to construct a global model, disseminating it to all clients. This architecture, also known as centralized FL architecture, sees the server coordinating the continuous learning process. Unlike conventional client-server setups where the server hosts and trains a model on shared data, in FL, the server operates solely on locally received models from clients, synchronously or asynchronously. The primary advantage of this architecture lies in its reduced communication overhead. Google's development of Gboard for Android, a virtual keyboard, utilized this architecture. Presently, nearly all FL implementations adopt the client-server architecture.

Peer-to-Peer Architecture:

In the peer-to-peer architecture, illustrated in Fig. 2, the concept of a central server for model aggregations, as seen in the client-server architecture, is absent. Instead, algorithms ensure security and reliability in the absence of a central server. Each participant in the FL environment possesses its own model, refining it by leveraging information obtained from neighboring participants. In this adopted peer-to-peer topology, a protocol, facilitated by a central authority, guides the network during training rounds. This architecture offers enhanced security as participating clients communicate directly without a third-party coordinator. However, it necessitates increased computation for message encryption and decryption.

The aggregation algorithm is pivotal in federated learning (FL)

The aggregation algorithm is pivotal in federated learning (FL), dictating how the global model is amalgamated from local model updates contributed by all participating clients during each training

round. Particularly crucial in horizontal FL (HFL) scenarios employing a centralized architecture, various popular aggregation algorithms are compared in Table 3 and summarized below.

FedAvg Algorithm: Proposed by Google, FedAvg operates on a stochastic gradient descent (SGD) optimization algorithm, ideally suited for HFL with a client-server architecture. Here, the server initializes the training process by disseminating global model parameters to a randomly selected group of clients. These clients then execute multiple epochs of SGD on their local datasets, training the global model, and subsequently share their locally trained models with the server. The server then computes the weighted average of all local models to generate a new global model. Despite its widespread success, FedAvg encounters convergence issues in certain settings, attributed to factors such as client drifting and the absence of an adaptive learning rate.

Scaffold: This algorithm tackles client drifting issues by employing a variance reduction technique in its local update. It estimates the update direction of both the server model and each client and measures client drifting using the difference, which is then utilized for local updates. This strategy effectively addresses client heterogeneity and reduces communication rounds during model convergence.

Adaptive Federated Optimization: Proposed by Google's research team, this approach introduces adaptability in server optimization, enhancing server optimization by incorporating adaptive learning rates informed by previous iterations. Clients minimize loss using local data over multiple training epochs, followed by server-based gradient-based optimization on the average of client model updates. While it incorporates adaptive learning rates in server optimization without increasing client storage or communication costs, it doesn't completely eliminate the effects of client heterogeneity. Nonetheless, it's particularly effective for moderate, naturally occurring heterogeneity, especially in cross-device settings.

Fed Boost: FedBoost is a communication-efficient FL algorithm based on ensemble learning techniques. It trains an ensemble of pretrained base predictors through FL, reducing both server-client and client-server communication costs without relying on gradient or model compression. Besides communication efficiency, FedBoost offers computational speedups, convergence guarantees, privacy, and optimal solutions for density estimation tasks, with language modeling as a special case.

FedProx: Addressing the inherent challenges of FL, FedProx deals with system and statistical heterogeneity by offering a reparametrized and generalized version of FedAvg. It allows partial work tolerance based on resource availability, accepting variable amounts of local updates from resource-

constrained devices for aggregation. Additionally, FedProx introduces a proximal term in a device's local solver objective to mitigate the impact of varying local updates.

FedMA: FedMA introduces FL into modern network architectures for deep learning. It performs matching and averaging layer-wise across convolutional layers, hidden states of long short-term memory networks, and fully connected layer neurons based on feature similarity to construct the shared global model at the server. FedMA exhibits robustness in handling client heterogeneity and outperforms FedProx and FedAvg within a few training rounds.

Open Issues and Challenges

Several open issues and challenges persist within the realm of federated learning (FL) [169]. Balancing accuracy, privacy, communication cost, and personalization levels is crucial when designing an FL system, with considerations often varying based on specific use cases or application areas. This section delves into some open issues concerning design aspects, core challenges, and application domains.

Design Aspects

1) Data Partitioning and FL Architectures:

Beyond the primary data partitioning schemes and FL architectures discussed herein, novel variations in FL architectures have emerged. For instance, PerFit a cloud-based platform, offers flexible selection of personalized FL approaches, catering to IoT applications. Another noteworthy architecture, FedHealth utilizes the Federated Transfer Learning (FTL) framework for wearable healthcare, facilitating the construction of personalized models for enhanced healthcare services. Future research endeavors could concentrate on developing FL architecture schemes tailored to meet the specific requirements of diverse industries and application domains.

2) Aggregation Techniques:

Facilitating developers in implementing FL solutions, toolkits featuring standardized and preconfigured aggregation algorithms suitable for distinct application areas and use cases could be invaluable. Analogous to AutoML solutions, such a toolkit for FL has the potential to lower the entry barrier for non-specialist developers.

3) Personalization Techniques:

Incorporating appropriate user and context features into the shared global model presents an alternative to device-specific personalization. For example, organizing filter orders in applications like

Snapchat based on user features such as browsing history, age, gender, preferences, and usage patterns. Consequently, developing architectures adept at effectively accommodating such user and context features for various tasks remains an open challenge. Moreover, bridging the gap between the accuracy of personalized and global models, as observed in underscores the significance of personalization techniques as a vital research area in FL. Nonetheless, comprehensive metrics to evaluate the effectiveness of personalized approaches have yet to be formulated. While Wang et al. examined the conditions conducive to yielding desirable models through personalization, further research is warranted to develop holistic metrics for assessing personalized approach performance.

Core Challenges

1) Communication:

In federated learning (FL), a trade-off exists between communication costs and accuracy. Unlike conventional machine learning (ML) benchmarks, FL benchmarks typically lack a restriction criterion on communication. Introducing communication budgets as a constraint in communication-focused FL benchmarks could be beneficial. For instance, studies like and have explored one-shot or few-shot communication schemes in FL, aiming to maximize performance within fixed rounds of communication. However, these methods require thorough evaluation and analysis in FL settings characterized by high network heterogeneity. In cross-device FL, asynchronous communication schemes are common, where only a few devices are active during each iteration. Investigating the consequences of such schemes, where device activity is event-driven, warrants further analysis.

2) Systems Heterogeneity:

Addressing systems heterogeneity in FL has been attempted through various algorithms [33], [35]. However, inconsistent wireless connectivity may lead to many participating devices dropping out during training. Future research could focus on designing FL algorithms that exhibit greater robustness, even when a significant number of devices experience connectivity issues. Recent efforts like the introduction of a proximal term in the optimization objective [4] have aimed to incorporate partial solutions from stragglers rather than entirely discarding them. Additionally, approaches like those proposed in [173] tackle device heterogeneity by selecting quantized models at different levels based on device-specific analyses conducted by the FL server.

3) Statistical Heterogeneity:

Eichner et al. proposed a pluralistic solution to mitigate data heterogeneity, considering variations in device characteristics between day and night. Further research avenues could explore similar methods to address diurnal variations at more granular times of day or during different days of the week. For

instance, in a federated network operating within a commercial neighborhood, data characteristics during weekdays might significantly differ from those on weekends. Investigating the effectiveness of pluralistic solutions in such scenarios warrants exploration. Additionally, further analysis could be conducted on block-cyclic data in nonconvex settings, employing methods such as parallel SGD, beyond the convex objectives and sequential SGD studied by [99].

4) Privacy/Security:

While device-specific privacy concerns have been extensively studied, finer privacy requirements at the sample level remain a promising research area. Techniques like the sample-specific privacy guarantee developed by Li et al. [174] trade off privacy for higher accuracy. Hybrid methods, addressing both sample- and device-level privacy requirements, could be explored. For instance, using sample-specific privacy for certain data subsets based on specific category levels or date ranges while employing device-specific privacy for the rest.

5) Ablation Analysis:

Evaluation in an FL system is often more complex than traditional ML and DL systems. A holistic industrial system necessitates considering various aspects such as privacy, accuracy/loss, communication rounds, and heterogeneity while building FL solutions. Developing a standard platform for facilitating comprehensive ablation analysis of different parts of an FL system is imperative for advancing research in this field.

Application Areas

Federated learning (FL) has predominantly found applications in supervised learning problems. However, future research endeavors can explore addressing challenges encountered when applying FL in domains requiring data exploration, unsupervised, semi-supervised, and reinforcement learning.

The challenges inherent in implementing FL solutions across various application domains have not been extensively explored. Existing studies have primarily focused on training FL models, overlooking domain-specific challenges. In addition to the core challenges delineated in this paper, it's imperative to consider issues pertinent to specific industries or application domains. For instance, domains like mobile edge networks may prioritize the emphasis on energy-efficient communication methods to a significant extent.

Conclusion

Federated Learning (FL) presents a collaborative approach for organizations to train prediction models without the need to share their sensitive data. This methodology has garnered significant interest from both industry and academia, offering solutions to challenges like data collection and privacy, particularly in sectors such as healthcare.

The escalating interest in FL prompted us to conduct a comprehensive review of contemporary survey papers on FL. We categorized FL into various topics encompassing design aspects, core challenges, and application domains. Through meticulous investigation and analysis of these survey papers, we provided an extensive overview of each FL topic. Lastly, we outlined potential avenues for future research.

This study is anticipated to serve as a valuable resource for upcoming researchers in FL and related fields, aiding them in delineating the scope of their work and fostering advancements in this burgeoning field.

References:

[1]. Rehan, H. (2024). Revolutionizing America's Cloud Computing the Pivotal Role of AI in Driving Innovation and Security. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 189-208. DOI: https://doi.org/10.60087/jaigs.v2i1.p208

[2]. Rehan, H. (2024). AI-Driven Cloud Security: The Future of Safeguarding Sensitive Data in the Digital Age. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 47-66. DOI: https://doi.org/10.60087/jaigs.v1i1.p66

[3]. Li, Z., Huang, Y., Zhu, M., Zhang, J., Chang, J., & Liu, H. (2024). Feature Manipulation for DDPM based Change Detection. *arXiv preprint arXiv:2403.15943*.

https://doi.org/10.48550/arXiv.2403.15943

[4]. Ramírez, J. G. C. (2023). Incorporating Information Architecture (ia), Enterprise Engineering (ee) and Artificial Intelligence (ai) to Improve Business Plans for Small Businesses in the United

States. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(1), 115-127. **DOI:** https://doi.org/10.60087/jklst.vol2.n1.p127

[5]. Ramírez, J. G. C. (2024). AI in Healthcare: Revolutionizing Patient Care with Predictive Analytics and Decision Support Systems. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 31-37. **DOI:** https://doi.org/10.60087/jaigs.v1i1.p37

[6]. Ramírez, J. G. C. (2024). Natural Language Processing Advancements: Breaking Barriers in Human-Computer Interaction. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *3*(1), 31-39. **DOI:** https://doi.org/10.60087/jaigs.v3i1.63

[7]. Ramírez, J. G. C., & mafiqul Islam, M. (2024). Application of Artificial Intelligence in Practical Scenarios. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 14-19. **DOI:** https://doi.org/10.60087/jaigs.v2i1.41

[8]. Ramírez, J. G. C., & Islam, M. M. (2024). Utilizing Artificial Intelligence in Real-World Applications. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 14-19.

DOI: https://doi.org/10.60087/jaigs.v2i1.p19

[9]. Ramírez, J. G. C., Islam, M. M., & Even, A. I. H. (2024). Machine Learning Applications in Healthcare: Current Trends and Future Prospects. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1). **DOI:** https://doi.org/10.60087/jaigs.v1i1.33

[10]. RAMIREZ, J. G. C. (2023). How Mobile Applications can improve Small Business Development. *Eigenpub Review of Science and Technology*, *7*(1), 291-305. **https://studies.eigenpub.com/index.php/erst/article/view/55**

[11]. RAMIREZ, J. G. C. (2023). From Autonomy to Accountability: Envisioning AI's Legal Personhood. *Applied Research in Artificial Intelligence and Cloud Computing*, *6*(9), 1-16. https://researchberg.com/index.php/araic/article/view/183

[12]. Ramírez, J. G. C., Hassan, M., & Kamal, M. (2022). Applications of Artificial Intelligence Models for Computational Flow Dynamics and Droplet Microfluidics. *Journal of Sustainable Technologies and Infrastructure Planning*, *6*(12). https://publications.dlpress.org/index.php/JSTIP/article/view/70

[13]. Ramírez, J. G. C. (2022). Struggling Small Business in the US. The next challenge to economic recovery. *International Journal of Business Intelligence and Big Data Analytics*, *5*(1), 81-91. https://research.tensorgate.org/index.php/IJBIBDA/article/view/99

[14]. Ramírez, J. G. C. (2021). Vibration Analysis with AI: Physics-Informed Neural Network Approach for Vortex-Induced Vibration. *International Journal of Responsible Artificial Intelligence*, *11*(3). https://neuralslate.com/index.php/Journal-of-Responsible-AI/article/view/77

[15]. Shuford, J. (2024). Interdisciplinary Perspectives: Fusing Artificial Intelligence with Environmental Science for Sustainable Solutions. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 1-12. **DOI:** https://doi.org/10.60087/jaigs.v1i1.p12

[16]. Islam, M. M. (2024). Exploring Ethical Dimensions in AI: Navigating Bias and Fairness in the Field. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 13-17. **DOI:** https://doi.org/10.60087/jaigs.v1i1.p18

[17]. Khan, M. R. (2024). Advances in Architectures for Deep Learning: A Thorough Examination of Present Trends. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 24-30. **DOI:** https://doi.org/10.60087/jaigs.v1i1.p30

[18]. Shuford, J., & Islam, M. M. (2024). Exploring the Latest Trends in Artificial Intelligence Technology: A Comprehensive Review. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1). **DOI:** https://doi.org/10.60087/jaigs.v2i1.p13

[19]. Islam, M. M. (2024). Exploring the Applications of Artificial Intelligence across Various Industries. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 20-25. **DOI:** https://doi.org/10.60087/jaigs.v2i1.p25

[20]. Akter, S. (2024). Investigating State-of-the-Art Frontiers in Artificial Intelligence: A Synopsis of Trends and Innovations. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 25-30. **DOI:** https://doi.org/10.60087/jaigs.v2i1.p30

[21]. Rana, S. (2024). Exploring the Advancements and Ramifications of Artificial Intelligence. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 30-35. **DOI:** https://doi.org/10.60087/jaigs.v2i1.p35

[22]. Sarker, M. (2024). Revolutionizing Healthcare: The Role of Machine Learning in the Health Sector. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 35-48.

DOI: https://doi.org/10.60087/jaigs.v2i1.p47

[23]. Akter, S. (2024). Harnessing Technology for Environmental Sustainability: Utilizing AI to Tackle Global Ecological Challenges. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 49-57. **DOI:** https://doi.org/10.60087/jaigs.v2i1.p57

[24]. Padmanaban, H. (2024). Revolutionizing Regulatory Reporting through AI/ML: Approaches for Enhanced Compliance and Efficiency. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 57-69. **DOI:** https://doi.org/10.60087/jaigs.v2i1.p69

[25]. Padmanaban, H. (2024). Navigating the Role of Reference Data in Financial Data Analysis: Addressing Challenges and Seizing Opportunities. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 69-78. **DOI:** https://doi.org/10.60087/jaigs.v2i1.p78

[26]. Camacho, N. G. (2024). Unlocking the Potential of AI/ML in DevSecOps: Effective Strategies and Optimal Practices. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 79-89. **DOI:** https://doi.org/10.60087/jaigs.v2i1.p89

[27]. PC, H. P., & Sharma, Y. K. (2024). Developing a Cognitive Learning and Intelligent Data Analysis-Based Framework for Early Disease Detection and Prevention in Younger Adults with Fatigue. *Optimized Predictive Models in Health Care Using Machine Learning*, 273. https://books.google.com.bd/books?hl=en&lr=&id=gtXzEAAAQBAJ&oi=fnd&pg=PA273&dq=Developing+a+Cognitive+Learning+and+Intelligent+Data+Analysis-Based+Framework+for+Early+Disease+Detection+and+Prevention+in+Younger+Adults+with+Fatigue&ots=wKUZk_Q0IG&sig=WDlXjvDmc77Q7lvXW9MxIh9Iz-Q&redir_esc=y#v=onepage&q=Developing%20a%20Cognitive%20Learning%20and%20Intelligent%20Data%20Analysis-Based%20Framework%20for%20Early%20Disease%20Detection%20and%20Prevention%20in%20Younger%20Adults%20with%20Fatigue&f=false

[28]. Padmanaban, H. (2024). Quantum Computing and AI in the Cloud. *Journal of Computational Intelligence and Robotics*, *4*(1), 14–32. Retrieved from https://thesciencebrigade.com/jcir/article/view/116

[29]. Sharma, Y. K., & Harish, P. (2018). Critical study of software models used cloud application development. *International Journal of Engineering & Technology, E-ISSN*, 514-518. https://www.researchgate.net/profile/Harish-Padmanaban-2/publication/377572317_Critical_study_of_software_models_used_cloud_application_development/links/65ad55d7ee1e1951fbd79df6/Critical-study-of-software-models-used-cloud-application-development.pdf

[30]. Padmanaban, P. H., & Sharma, Y. K. (2019). Implication of Artificial Intelligence in Software Development Life Cycle: A state of the art review. *vol*, *6*, 93-98. https://www.researchgate.net/profile/Harish-Padmanaban-2/publication/377572222_Implication_of_Artificial_Intelligence_in_Software_Development_Life_Cycle_A_state_of_the_art_review/links/65ad54e5bf5b00662e333553/Implication-of-Artificial-Intelligence-in-Software-Development-Life-Cycle-A-state-of-the-art-review.pdf

[31]. Harish Padmanaban, P. C., & Sharma, Y. K. (2024). Optimizing the Identification and Utilization of Open Parking Spaces Through Advanced Machine Learning. *Advances in Aerial Sensing and Imaging*, 267-294. **https://doi.org/10.1002/9781394175512.ch12**

[32]. PC, H. P., Mohammed, A., & RAHIM, N. A. (2023). *U.S. Patent No. 11,762,755*. Washington, DC: U.S. Patent and Trademark Office. https://patents.google.com/patent/US20230385176A1/en

[33]. Padmanaban, H. (2023). Navigating the intricacies of regulations: Leveraging AI/ML for Accurate Reporting. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(3), 401-412. DOI: https://doi.org/10.60087/jklst.vol2.n3.p412

[34]. PC, H. P. Compare and analysis of existing software development lifecycle models to develop a new model using computational intelligence. https://shodhganga.inflibnet.ac.in/handle/10603/487443

[35]. Camacho, N. G. (2024). Unlocking the Potential of AI/ML in DevSecOps: Effective Strategies and Optimal Practices. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 79-89. DOI: https://doi.org/10.60087/jaigs.v2i1.p89

[36]. Camacho, N. G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *3*(1), 143-154.

DOI: https://doi.org/10.60087/jaigs.v3i1.75

[37]. Islam, M. S., Ahsan, M. S., Rahman, M. K., & AminTanvir, F. (2023). Advancements in Battery Technology for Electric Vehicles: A Comprehensive Analysis of Recent Developments. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *2*(02), 01-28.

https://doi.org/10.62304/jieet.v2i02.63

[38]. Ahsan, M. S., Tanvir, F. A., Rahman, M. K., Ahmed, M., & Islam, M. S. (2023). Integration of Electric Vehicles (EVs) with Electrical Grid and Impact on Smart Charging. *International Journal of Multidisciplinary Sciences and Arts*, *2*(2), 225-234.

https://doi.org/10.47709/ijmdsa.v2i2.3322

[39]. Rahman, M. K., Tanvir, F. A., Islam, M. S., Ahsan, M. S., & Ahmed, M. (2024). Design and Implementation of Low-Cost Electric Vehicles (Evs) Supercharger: A Comprehensive Review. *arXiv preprint arXiv:2402.15728*.

https://doi.org/10.48550/arXiv.2402.15728

[40]. Latif, M. A., Afshan, N., Mushtaq, Z., Khan, N. A., Irfan, M., Nowakowski, G., ... & Telenyk, S. (2023). Enhanced classification of coffee leaf biotic stress by synergizing feature concatenation and dimensionality reduction. *IEEE Access*.
DOI: https://doi.org/10.1109/ACCESS.2023.3314590

[42]. Irfan, M., Mushtaq, Z., Khan, N. A., Mursal, S. N. F., Rahman, S., Magzoub, M. A., ... & Abbas, G. (2023). A Scalo gram-based CNN ensemble method with density-aware smote oversampling for improving bearing fault diagnosis. *IEEE Access*, *11*, 127783-127799.
DOI: https://doi.org/10.1109/ACCESS.2023.3332243

[43]. Irfan, M., Mushtaq, Z., Khan, N. A., Althobiani, F., Mursal, S. N. F., Rahman, S., ... & Khan, I. (2023). Improving Bearing Fault Identification by Using Novel Hybrid Involution-Convolution Feature Extraction with Adversarial Noise Injection in Conditional GANs. *IEEE Access*.

DOI: https://doi.org/10.1109/ACCESS.2023.3326367

[44]. Rahman, S., Mursal, S. N. F., Latif, M. A., Mushtaq, Z., Irfan, M., & Waqar, A. (2023, November). Enhancing Network Intrusion Detection Using Effective Stacking of Ensemble Classifiers With Multi-Pronged Feature Selection Technique. In *2023 2nd International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (ETECTE)* (pp. 1-6). IEEE.

DOI: https://doi.org/10.1109/ETECTE59617.2023.10396717

[45]. Latif, M. A., Mushtaq, Z., Arif, S., Rehman, S., Qureshi, M. F., Samee, N. A., ... & Al-masni, M. A. Improving Thyroid Disorder Diagnosis via Ensemble Stacking and Bidirectional Feature Selection.
https://doi.org/10.32604/cmc.2024.047621

[46]. Ara, A., & Mifa, A. F. (2024). INTEGRATING ARTIFICIAL INTELLIGENCE AND BIG DATA IN MOBILE HEALTH: A SYSTEMATIC REVIEW OF INNOVATIONS AND CHALLENGES IN HEALTHCARE SYSTEMS. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *3*(01), 01-16.

DOI: https://doi.org/10.62304/jbedpm.v3i01.70

[47]. Bappy, M. A., & Ahmed, M. (2023). ASSESSMENT OF DATA COLLECTION TECHNIQUES IN MANUFACTURING AND MECHANICAL ENGINEERING THROUGH MACHINE LEARNING MODELS. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *2*(04), 15-26.
DOI: https://doi.org/10.62304/jbedpm.v2i04.67

[48]. Bappy, M. A. (2024). Exploring the Integration of Informed Machine Learning in Engineering Applications: A Comprehensive Review. *American Journal of Science and Learning for Development*, *3*(2), 11-21.
DOI: https://doi.org/10.51699/ajsld.v3i2.3459

[49]. Uddin, M. N., Bappy, M. A., Rab, M. F., Znidi, F., & Morsy, M. (2024). Recent Progress on Synthesis of 3D Graphene, Properties, and Emerging Applications.
DOI: https://doi.org/10.5772/intechopen.114168

[50]. Hossain, M. I., Bappy, M. A., & Sathi, M. A. (2023). WATER QUALITY MODELLING AND ASSESSMENT OF THE BURIGANGA RIVER USING QUAL2K. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *2*(03), 01-11.
DOI: https://doi.org/10.62304/jieet.v2i03.64