Federated Learning: State-of-the-Art, Challenges and Research Opportunities

Ton That Tam Dinh, Manh Cuong Ho, Ayalneh Bitew Wondmagegn, Juyoung Kim, and Sungrae Cho

School of Computer Science and Engineering, Chung-Ang University, Seoul, South Korea,

Email: {tttdinh, hmcuong, ayalneh, jykim}@uclab.re.kr, srcho@cau.ac.kr

***Abstract*—Federated Learning (FL) is an emerging paradigm in machine learning that enables collaborative model training without centralizing data, thereby addressing privacy and security concerns. Unlike traditional centralized approaches, FL keeps data on local devices and only exchanges model updates, making it highly relevant in the era of strict data governance regulations. This survey provides a comprehensive overview of FL, covering its foundational concepts, related works, and major categories including horizontal, vertical, and transfer learning. We highlight practical applications across healthcare, finance, mobile devices, IoT, autonomous systems, and wireless communications. Furthermore, we examine the challenges faced by FL, such as data heterogeneity, system scalability, communication efficiency, and security vulnerabilities. We also explore solutions proposed in recent literature, ranging from differential privacy and secure aggregation to personalization and hierarchical architectures. The survey discusses future research directions that integrate FL with edge computing, blockchain, and next-generation wireless networks. By synthesizing these insights, we emphasize the transformative potential of FL in shaping decentralized, privacy-preserving artificial intelligence.**

***Index Terms*—Federated Learning, Distributed Machine Learning, Privacy-Preserving AI, Edge Intelligence, Internet of Things, Mobile Edge Computing, Wireless Communications, Blockchain, Healthcare Applications, Financial Applications.**

I. Introduction

In recent years, the rapid growth of data-driven applications has highlighted the tension between the need for powerful machine learning (ML) models and the protection of user privacy. Traditional centralized ML approaches require collecting and aggregating raw data into a single server, which introduces significant concerns regarding data ownership, confidentiality, and regulatory compliance. Federated Learning has emerged as a compelling solution to these challenges by enabling decentralized model training across multiple clients while ensuring that data remains local to each participant [1] . Instead of transferring raw data, FL relies on exchanging model parameters or gradients, which are then aggregated into a global model at a central server or coordinator.

The concept of Federated Learning was first introduced by Google in the context of mobile devices [2] . Smartphones and other edge devices continuously generate valuable data from user interactions, but uploading sensitive information such as typed text, health records, or voice samples to the cloud raises privacy risks. FL addresses this issue by training local models directly on-device, and only transmitting updates that reflect learned knowledge. This approach provides not only privacy benefits but also reduces communication overhead, since updates are typically smaller than raw datasets. Moreover, FL aligns with emerging regulatory frameworks such as the European Union's General Data Protection Regulation (GDPR) and the U.S. Health Insurance Portability and Accountability Act (HIPAA), which impose strict constraints on data sharing and storage [3].

Another driver of FL adoption is the increasing importance of edge computing. With the proliferation of Internet of Things (IoT) devices, autonomous vehicles, wearable sensors, and smart city infrastructure, vast amounts of data are being generated at the network edge [4]. Transmitting this data to cloud servers not only introduces latency but also consumes significant bandwidth and energy. FL offers a scalable alternative by leveraging distributed computational resources at the edge. This paradigm shift aligns with the broader vision of distributed artificial intelligence, where learning happens closer to where data is produced.

Beyond privacy and efficiency, FL also democratizes access to AI development. Organizations or individuals with limited data resources can collaborate in training powerful models without relinquishing control over their datasets. This enables multi-institutional collaborations, such as hospitals jointly developing medical diagnosis models, or financial institutions building fraud detection systems, while keeping proprietary or sensitive data secure [5]. By combining knowledge from diverse sources, FL also has the potential to improve model generalization and reduce bias.

Despite its advantages, FL is not without limitations. Challenges such as system heterogeneity, statistical non-independence of local datasets, and potential vulnerabilities to adversarial attacks make the design of robust FL systems complex [6], [7]. These challenges have sparked significant research interest from communities spanning machine learning, cryptography, networking, and distributed systems. Consequently, FL is now recognized as a multidisciplinary field with broad applications ranging from healthcare and finance to wireless communications and smart environments.

In summary, FL represents a paradigm shift in how models are trained and deployed. It reconciles the competing demands of data privacy, efficiency, and scalability, while also enabling

collaborative intelligence across distributed environments. As data generation continues to accelerate, and concerns about security and fairness intensify, FL is poised to become a cornerstone of next-generation machine learning systems.

II. Related Work

A. Definition of Federated Learning

Federated Learning (FL) is a decentralized machine learning paradigm that enables multiple clients or organizations to collaboratively train a shared global model without exchanging raw data [2], [3], [8], [9], [10]. In contrast to conventional centralized learning, where data must be collected and stored in a central server, FL ensures that data remains local to each participant while only transmitting model parameters or gradient updates. These updates are then aggregated, typically by a central server, to produce an improved global model. This approach provides significant advantages in terms of data privacy, communication efficiency, and compliance with regulatory frameworks such as GDPR and HIPAA . Formally, FL can be defined as an optimization problem over distributed datasets. Consider K clients, each with a local dataset $\mathcal{D}_k$ of size n_k. The objective of FL is to minimize a global loss function:

$$\min_{w} \; F(w) = \sum_{k=1}^{K} \frac{n_k}{n} F_k(w),$$

where $F_k(w)$ denotes the local loss function of client k, $n = \sum_{k=1}^{K} n_k$ is the total number of samples across all clients, and w represents the global model parameters. The most widely used algorithm, Federated Averaging (FedAvg), computes local updates on each client and averages them at the server to update the global model [2].

B. The Development of Federated Learning

The concept of Federated Learning was first popularized by Google in 2016, when researchers proposed a decentralized framework for training machine learning models directly on mobile devices [1]. This early effort emerged from the need to improve on-device services, such as predictive keyboards and voice assistants, without transferring sensitive user data to cloud servers. The subsequent introduction of the Federated Averaging (FedAvg) algorithm in 2017 [2] marked a turning point, establishing a simple yet powerful method for aggregating local model updates into a global model. FedAvg became the baseline for most subsequent FL research, laying the foundation for both theoretical analysis and practical deployment.

Following these initial contributions, the field rapidly expanded. Early research primarily addressed communication bottlenecks, proposing techniques such as update compression, quantization, and sparsification to reduce bandwidth usage [11]. In parallel, privacy-preserving mechanisms, including differential privacy [12] and secure aggregation protocols [13], were introduced to strengthen confidentiality guarantees. These advances positioned FL as a promising solution for applications in healthcare, finance, and IoT systems, where data sensitivity is a major concern.

From 2018 onward, the research community began to investigate the unique challenges of FL in heterogeneous environments. Studies revealed that non-IID (non-independent and identically distributed) data across clients could degrade convergence and model accuracy [6]. This motivated the development of personalized FL frameworks [14] and robust aggregation strategies to mitigate the effects of heterogeneity. At the same time, researchers distinguished between cross-device FL, involving millions of unreliable clients such as smartphones, and cross-silo FL, involving fewer but more reliable institutions [7]. This categorization clarified the scope of FL and guided algorithmic design.

In recent years, FL has evolved into a multidisciplinary research field, integrating ideas from cryptography, distributed systems, wireless communications, and edge computing. Applications have expanded to autonomous vehicles, smart cities, and next-generation 6G networks [15]. Meanwhile, large-scale open-source frameworks such as TensorFlow Federated, PySyft, and FATE have accelerated experimentation and industrial adoption [16]. Current research directions emphasize robustness against adversarial attacks, fairness across clients, energy-efficient training, and integration with blockchain for decentralized trust [17].

Overall, the development of FL reflects a trajectory from a practical solution for mobile devices to a broader paradigm for decentralized artificial intelligence. It has transformed from a niche topic into one of the most dynamic research areas in machine learning, shaping the future of privacy-preserving and distributed intelligence.

Privacy preservation is another major research direction. Although FL avoids centralizing raw data, studies demonstrated that model gradients could still leak sensitive information. To counter this, researchers integrated differential privacy [12] and secure aggregation protocols [13], ensuring stronger guarantees against inference attacks. Alongside these efforts, cryptographic methods like homomorphic encryption and secure multiparty computation further reinforced the robustness of FL systems. These privacy-preserving enhancements have been particularly critical in sensitive domains such as healthcare and finance, where compliance with regulations like GDPR and HIPAA is essential [3].

Another active line of work investigates the impact of statistical heterogeneity, where data across clients is non-IID and highly imbalanced. This issue has been shown to significantly degrade the convergence and generalization of federated models [6]. To address this, researchers have explored optimization strategies, robust aggregation rules, and personalized federated learning approaches that allow models to adapt to local client distributions [14]. Recent studies also differentiate between cross-device FL, involving millions of unreliable participants, and cross-silo FL, where fewer but more stable organizations collaborate [7]. This categorization has shaped much of the algorithmic development in the field.

In addition, numerous open-source frameworks have been

developed to support both research and deployment. Examples include TensorFlow Federated, PySyft, and FATE, each providing tools for secure aggregation, simulation environments, and deployment pipelines for real-world use cases [16]. These platforms have accelerated experimentation and facilitated collaboration between academia and industry.

Overall, related works on FL demonstrate the field's rapid evolution and multidisciplinary nature. From distributed optimization and cryptographic techniques to systems design and regulatory compliance, FL research has expanded into a wide ecosystem. This breadth not only underscores the versatility of FL but also highlights the need for continued exploration of its theoretical foundations, practical implementations, and long-term societal implications.

III. Categories of Federated Learning

Federated Learning can be categorized in several ways depending on how data is distributed across participants, how collaboration is organized, and how aggregation is performed. One of the most common taxonomies divides FL into *horizontal*, *vertical*, and *transfer* learning settings [18]. In Horizontal Federated Learning (HFL), participants share the same feature space but hold different sets of samples. For example, hospitals in different regions may each possess patient medical records with identical attributes (e.g., age, blood pressure, and diagnosis labels), but for different individuals. By pooling knowledge from these distributed datasets, HFL improves generalization while ensuring patient privacy [5].

In contrast, Vertical Federated Learning (VFL) arises when organizations have data about the same set of entities but with disjoint feature spaces. For instance, a bank may store financial transaction data about customers, while an e-commerce platform records their purchasing history. Combining these heterogeneous features through secure protocols enables richer predictive modeling while respecting organizational boundaries. VFL often requires entity alignment techniques to identify overlapping users across datasets, which introduces additional complexity.

A third category, Federated Transfer Learning (FTL), applies when both the sample space and the feature space overlap only partially [32]. This is common in scenarios where institutions operate in different domains but still benefit from transferring learned representations. FTL leverages transfer learning techniques to bridge gaps between domains, enabling knowledge sharing even when direct data compatibility is limited. Such flexibility is critical for real-world collaborations, where data heterogeneity is the norm.

Another perspective on categorization distinguishes between cross-device and cross-silo federated learning [7]. Cross-device FL involves a massive number of unreliable participants, such as smartphones or IoT devices, contributing intermittently with limited computational and communication capacity. In contrast, cross-silo FL typically includes fewer but more reliable organizations, such as hospitals, banks, or universities, which provide stable infrastructure and more consistent participation. These two paradigms raise different research challenges: scalability and resource constraints in cross-device settings, versus coordination and trust in cross-silo settings.

Finally, FL systems can also be classified by their synchronization strategy. In synchronous FL, the server waits for all selected clients to upload updates before aggregation, which ensures consistency but suffers from straggler effects. Asynchronous FL relaxes this requirement, allowing faster updates at the cost of potential staleness in model parameters [33]. Hybrid approaches that combine centralized aggregation with peer-to-peer learning have also been proposed, providing resilience against failures and improving scalability.

Overall, the various categories of FL reflect the adaptability of the paradigm to diverse data distributions, organizational contexts, and system requirements. Understanding these distinctions is critical for designing algorithms and frameworks that align with the specific characteristics of an application domain.

IV. Applications

Federated Learning has demonstrated significant potential across diverse domains where privacy, data sovereignty, and distributed collaboration are essential. One of the earliest and most widely deployed applications of FL is in the domain of mobile devices. Google has applied FL to train on-device models for next-word prediction in Gboard, enabling improvements in keyboard suggestions without collecting sensitive user data [2]. Similarly, FL has been leveraged in speech recognition, personalization of virtual assistants, and recommender systems, where training on-device interactions helps tailor services to individual preferences without centralized data aggregation.

A. Healthcare

Healthcare is one of the most promising domains for Federated Learning, as it involves highly sensitive patient data that cannot be freely shared across institutions due to privacy regulations such as HIPAA and GDPR. FL enables multiple hospitals, research centers, and pharmaceutical companies to collaboratively train models for tasks such as disease diagnosis, medical image segmentation, and patient risk prediction while keeping patient records local. For example, Sheller et al. [5] demonstrated that multi-institutional FL could achieve competitive performance in brain tumor segmentation without centralizing medical images. Similarly, Li et al. [34] applied FL for privacy-preserving radiology image analysis, showing that models trained across diverse institutions are more robust and generalizable. Beyond imaging, FL has been applied in electronic health records for predicting patient outcomes, in genomics for collaborative gene-disease association studies, and in drug discovery for accelerating pharmaceutical research. By enabling cross-institutional collaborations, FL not only safeguards privacy but also enhances model accuracy by leveraging diverse datasets. This paradigm has the potential to overcome data silos in healthcare and facilitate large-scale, privacy-preserving precision medicine.

TABLE I
SUMMARY OF KEY PAPERS IN FEDERATED LEARNING

Ref	Year	Key Idea
[1]	2016	The concept of Federated Learning (FL) was first introduced, accompanied by a communication-efficient method for distributed optimization.
[2]	2017	Researchers proposed the Federated Averaging (FedAvg) algorithm, which enabled the first large-scale deployment of FL on mobile devices, most notably Google Gboard.
[14]	2017	The MOCHA framework was introduced to extend FL into multi-task settings, allowing clients to address related yet distinct tasks.
[6]	2018	A study investigated the impact of non-IID data on FL convergence, demonstrating that FedAvg performs poorly under such heterogeneity.
[18]	2018	A study defined the fundamental concepts of FL and outlined applications in finance, healthcare, and IoT, while also providing a roadmap for future adoption.
[19]	2019	A system-level architecture for large-scale FL was developed, introducing secure aggregation protocols and fault-tolerant mechanisms.
[20]	2019	A survey presented a detailed account of the main challenges and open research opportunities in the field of FL.
[21]	2021	The PySyft framework was released as an open-source library supporting privacy-preserving FL through tools such as encrypted computation and differential privacy.
[22]	2021	Research on communication-efficient FL in wireless networks examined approaches such as over-the-air computation and optimized resource allocation.
[23]	2022	A survey reviewed FL applications across healthcare, IoT, and finance, while identifying key open challenges.
[24]	2022	A study analyzed the role of FL in emerging 6G wireless networks, emphasizing its applications in edge intelligence and ultra-reliable low-latency communications.
[25]	2023	A comprehensive review was published on heterogeneous FL, addressing challenges related to non-IID data distributions, device diversity, and model mismatch.
[26]	2024	A survey on decentralized FL examined peer-to-peer coordination, security risks, and blockchain-based privacy mechanisms.
[27]	2024	A systematic study proposed a taxonomy of FL pipelines, covering methods, optimization strategies, and applications.
[28]	2024	A survey addressed FL system design and functional models, focusing on aggregation techniques, client selection, and incentive mechanisms.
[29]	2024	Starlit, a privacy-preserving FL framework, was proposed to enhance fraud detection in financial systems.
[30]	2025	A survey on privacy-preserving FL was published, reviewing techniques such as differential privacy, homomorphic encryption, and secure aggregation.
[31]	2025	Research on FL for IoT networks highlighted challenges in communication efficiency, energy consumption, and device heterogeneity.

B. Financial Sector

In the financial sector [35], institutions such as banks and insurance companies apply FL to train fraud detection models, anti-money laundering systems, and credit scoring algorithms. These applications require collaboration among multiple organizations that cannot share raw data due to competitive and legal constraints. FL provides a secure mechanism for collective intelligence, allowing institutions to build more reliable models while preserving confidentiality.

C. Iot and Smart Cities

IoT and smart cities represent another domain where FL is highly relevant [36]. Smart sensors and devices deployed across cities generate massive amounts of data related to traffic, pollution, and energy consumption. FL enables distributed training of predictive models for traffic congestion management, smart grid optimization, and anomaly detection in real time [37]. Similarly, autonomous vehicles can collaboratively improve driving policies, navigation strategies, and object detection systems without exchanging raw sensor data, thus reducing latency and protecting user privacy [38].

D. Wireless Communications

Wireless communications has recently become a critical application domain for Federated Learning, especially with the rise of 5G and the development of 6G networks. Modern wireless systems generate massive volumes of distributed data from base stations, access points, mobile devices, and IoT sensors, which makes centralized training impractical due to bandwidth, latency, and privacy concerns [39], [40] . FL offers a scalable alternative by enabling distributed model training directly at the edge of the network, where data is generated, thereby reducing communication overhead and enhancing data privacy [15].

One major application of FL in wireless communications is spectrum allocation. By training models collaboratively across base stations, FL enables dynamic and efficient spectrum sharing while minimizing interference. In addition, interference management can be enhanced through federated training of predictive models that anticipate network congestion and adjust parameters accordingly. Another promising area is resource allocation, where FL can optimize power control, channel selection, and scheduling policies based on real-time distributed data. These solutions improve both spectrum efficiency and user experience.

In mobility management, FL is being explored for handover

prediction and trajectory forecasting. By allowing base stations to share only model updates, FL enables seamless connectivity while protecting user location privacy. Similarly, in device-to-device (D2D) communication, FL supports collaborative learning of adaptive transmission strategies, making networks more resilient to changing environments. At the same time, FL can be applied to wireless security, where intrusion detection systems are trained collaboratively across distributed nodes without centralizing sensitive traffic data.

The integration of FL with Mobile Edge Computing (MEC) further strengthens its role in wireless systems by empowering edge servers to participate in model training, thus reducing latency and enabling near real-time decision-making. Moreover, FL has potential in federated analytics for wireless systems, where global insights such as usage patterns and performance metrics are derived without raw data exchange. With the growing importance of decentralized, intelligent, and adaptive communication infrastructures, FL is expected to be a cornerstone of 6G networks, enabling autonomous, privacy-preserving, and resource-efficient wireless communications.

V. Challenges and Future Works

While Federated Learning has made substantial progress, it still faces numerous challenges that hinder its widespread adoption. A fundamental issue is statistical heterogeneity. Data across clients is often non-IID, imbalanced, or skewed due to local preferences, environments, or user behaviors. This heterogeneity can significantly degrade model convergence and generalization [6]. Addressing non-IID data remains an open research problem, with solutions ranging from personalized FL approaches [14] to robust aggregation rules and meta-learning techniques.

Another challenge is system heterogeneity. Clients vary widely in computational power, memory, and network connectivity, especially in cross-device FL. Some devices may act as stragglers, slowing down global training, while others may drop out entirely. Designing adaptive algorithms that account for device heterogeneity and intermittent participation remains critical [7]. Similarly, communication efficiency is a bottleneck: transmitting large model updates from thousands or millions of devices to a central server is resource-intensive. Compression techniques, quantization, and gradient sparsification have been proposed to mitigate this issue [11].

Privacy and security also remain pressing concerns. Although FL does not share raw data, gradients can still leak sensitive information. Attacks such as membership inference, gradient inversion, and model reconstruction threaten user confidentiality. Defenses based on differential privacy [12] and secure aggregation [13] have been proposed, but these often come at the cost of reduced accuracy or increased computational burden. Moreover, FL is vulnerable to poisoning and backdoor attacks, where adversarial clients inject malicious updates to manipulate the global model [17]. Building robust and trustworthy aggregation mechanisms is therefore essential.

In summary, the challenges of FL span technical, security, and societal dimensions. Addressing these issues will require interdisciplinary collaboration across machine learning, distributed systems, cryptography, and policy-making. The solutions developed in these directions will ultimately determine the scalability, robustness, and ethical deployment of FL in the coming years.

VI. Conclusion

Federated Learning has emerged as a transformative paradigm that fundamentally redefines how machine learning models are trained and deployed. By decoupling data collection from model development, Federated Learning addresses growing concerns regarding privacy, security, and regulatory compliance, while simultaneously unlocking opportunities for collaborative intelligence across distributed environments. This paradigm shift is particularly timely, as organizations and individuals increasingly recognize the importance of protecting data sovereignty in the era of big data. The survey has outlined the key categories of Federated Learning, including horizontal, vertical, and transfer learning, as well as cross-device and cross-silo settings. Each category introduces unique challenges and opportunities, reflecting the flexibility of Federated Learning in adapting to diverse application domains. From mobile services and healthcare to finance, IoT, and next-generation communication systems, Federated Learning has demonstrated its utility across a wide spectrum of industries, offering both theoretical elegance and practical impact.

Looking forward, several promising research directions are emerging. Personalized Federated Learning offers the potential to tailor models to individual client needs while retaining the benefits of collaboration. Hybrid and hierarchical Federated Learning frameworks may enhance scalability and robustness, especially in environments with unreliable participants. The convergence of Federated Learning with enabling technologies such as edge computing, blockchain, and 6G networks points toward a future where distributed intelligence becomes an integral component of digital infrastructure.

In conclusion, Federated Learning stands at the intersection of technical innovation and ethical responsibility. It represents not just an alternative to centralized learning, but a broader rethinking of how knowledge can be co-created in a privacy-preserving, secure, and decentralized manner. By continuing to address its challenges and harness its opportunities, Federated Learning has the potential to serve as a cornerstone for the next generation of artificial intelligence systems, fostering a more trustworthy, inclusive, and sustainable AI ecosystem.

ACKNOWLEDGMENT

This work was supported by the IITP (Institute of Information & Communications Technology Planning & Evaluation) - ITRC (Information Technology Research Center) (IITP-2026-RS-2022-00156353, 50% / IITP-2026-RS-2024-00436887, 50%) grants funded by the Korea government (Ministry of Science and ICT).

REFERENCES

[1] J. Konečnỳ, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," *arXiv preprint arXiv:1610.05492*, 2016.

[2] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Artificial intelligence and statistics*. PMLR, 2017, pp. 1273–1282.

[3] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," *A practical guide, 1st ed., Cham: Springer International Publishing*, vol. 10, no. 3152676, pp. 10–5555, 2017.

[4] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, 2017.

[5] M. J. Sheller, B. Edwards, G. A. Reina, J. Martin, S. Pati, A. Kotrotsou, M. Milchenko, W. Xu, D. Marcus, R. R. Colen *et al.*, "Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data," *Scientific reports*, vol. 10, no. 1, p. 12598, 2020.

[6] Y. Zhao, M. Li, L. Lai, N. Suda, D. Civin, and V. Chandra, "Federated learning with non-iid data," *arXiv preprint arXiv:1806.00582*, 2018.

[7] 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.

[8] M. C. Ho, A. T. Tran, D. Lee, J. Paek, W. Noh, and S. Cho, "A ddpg-based energy efficient federated learning algorithm with swipt and mc-noma," *ICT Express*, vol. 10, no. 3, pp. 600–607, 2024.

[9] J. Park and J. Ko, "Fedhm: Practical federated learning for heterogeneous model deployments," *ICT Express*, vol. 10, no. 2, pp. 387–392, 2024.

[10] S.-J. Lee and I.-G. Lee, "Lightweight federated learning-based intrusion detection system for industrial internet of things," *ICT Express*, 2025.

[11] F. Sattler, S. Wiedemann, K.-R. Müller, and W. Samek, "Robust and communication-efficient federated learning from non-iid data," *IEEE transactions on neural networks and learning systems*, vol. 31, no. 9, pp. 3400–3413, 2019.

[12] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 308–318.

[13] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth, "Practical secure aggregation for privacy-preserving machine learning," in *proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1175–1191.

[14] V. Smith, C.-K. Chiang, M. Sanjabi, and A. S. Talwalkar, "Federated multi-task learning," *Advances in neural information processing systems*, vol. 30, 2017.

[15] S. Niknam, H. S. Dhillon, and J. H. Reed, "Federated learning for wireless communications: Motivation, opportunities, and challenges," *IEEE Communications Magazine*, vol. 58, no. 6, pp. 46–51, 2020.

[16] T. Ryffel, A. Trask, M. Dahl, B. Wagner, J. Mancuso, D. Rueckert, and J. Passerat-Palmbach, "A generic framework for privacy preserving deep learning," *arXiv preprint arXiv:1811.04017*, 2018.

[17] E. Bagdasaryan, A. Veit, Y. Hua, D. Estrin, and V. Shmatikov, "How to backdoor federated learning," in *International conference on artificial intelligence and statistics*. PMLR, 2020, pp. 2938–2948.

[18] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 10, no. 2, pp. 1–19, 2019.

[19] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. Kiddon, J. Konečnỳ, S. Mazzocchi, B. McMahan *et al.*, "Towards federated learning at scale: System design," *Proceedings of machine learning and systems*, vol. 1, pp. 374–388, 2019.

[20] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE signal processing magazine*, vol. 37, no. 3, pp. 50–60, 2020.

[21] A. Ziller, A. Trask, A. Lopardo, B. Szymkow, B. Wagner, E. Bluemke, J.-M. Nounahon, J. Passerat-Palmbach, K. Prakash, N. Rose *et al.*, "Pysyft: A library for easy federated learning," in *Federated learning systems: Towards next-generation AI*. Springer, 2021, pp. 111–139.

[22] Z. Qin, G. Y. Li, and H. Ye, "Federated learning and wireless communications," *IEEE Wireless Communications*, vol. 28, no. 5, pp. 134–140, 2021.

[23] S. Bharati, M. R. H. Mondal, P. Podder, and V. S. Prasath, "Federated learning: Applications, challenges and future directions," *International Journal of Hybrid Intelligent Systems*, vol. 18, no. 1-2, pp. 19–35, 2022.

[24] Z. Yang, M. Chen, K.-K. Wong, H. V. Poor, and S. Cui, "Federated learning for 6g: Applications, challenges, and opportunities," *Engineering*, vol. 8, pp. 33–41, 2022.

[25] M. Ye, X. Fang, B. Du, P. C. Yuen, and D. Tao, "Heterogeneous federated learning: State-of-the-art and research challenges," *ACM Computing Surveys*, vol. 56, no. 3, pp. 1–44, 2023.

[26] E. Hallaji, R. Razavi-Far, M. Saif, B. Wang, and Q. Yang, "Decentralized federated learning: A survey on security and privacy," *IEEE Transactions on Big Data*, vol. 10, no. 2, pp. 194–213, 2024.

[27] B. Liu, N. Lv, Y. Guo, and Y. Li, "Recent advances on federated learning: A systematic survey," *Neurocomputing*, vol. 597, p. 128019, 2024.

[28] J. Ayeelyan, S. Utomo, A. Rouniyar, H.-C. Hsu, and P.-A. Hsiung, "Federated learning design and functional models: Survey," *Artificial Intelligence Review*, vol. 58, no. 1, p. 21, 2024.

[29] A. Abadi, B. Doyle, F. Gini, K. Guinamard, S. K. Murakonda, J. Liddell, P. Mellor, S. J. Murdoch, M. Naseri, H. Page *et al.*, "Starlit: Privacy-preserving federated learning to enhance financial fraud detection," *Cryptology ePrint Archive*, 2024.

[30] N. Jahan, R. Rahman, and M. Wang, "Federated learning: a survey on privacy-preserving collaborative intelligence," *arXiv preprint arXiv:2504.17703*, 2025.

[31] E. Dritsas and M. Trigka, "Federated learning for iot: A survey of techniques, challenges, and applications," *Journal of Sensor and Actuator Networks*, vol. 14, no. 1, p. 9, 2025.

[32] Y. Chen, X. Qin, J. Wang, C. Yu, and W. Gao, "Fedhealth: A federated transfer learning framework for wearable healthcare," *IEEE Intelligent Systems*, vol. 35, no. 4, pp. 83–93, 2020.

[33] A. Lalitha, O. C. Kilinc, T. Javidi, and F. Koushanfar, "Peer-to-peer federated learning on graphs," *arXiv preprint arXiv:1901.11173*, 2019.

[34] W. Li, F. Milletarì, D. Xu, N. Rieke, J. Hancox, W. Zhu, M. Baust, Y. Cheng, S. Ourselin, M. J. Cardoso *et al.*, "Privacy-preserving federated brain tumour segmentation," in *International workshop on machine learning in medical imaging*. Springer, 2019, pp. 133–141.

[35] P. Chatterjee, D. Das, and D. B. Rawat, "Federated learning empowered recommendation model for financial consumer services," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 2508–2516, 2023.

[36] B. Qolomany, K. Ahmad, A. Al-Fuqaha, and J. Qadir, "Particle swarm optimized federated learning for industrial iot and smart city services," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*. IEEE, 2020, pp. 1–6.

[37] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, and C. Miao, "Federated learning in mobile edge networks: A comprehensive survey," *IEEE communications surveys & tutorials*, vol. 22, no. 3, pp. 2031–2063, 2020.

[38] S. R. Pokhrel and J. Choi, "Federated learning with blockchain for autonomous vehicles: Analysis and design challenges," *IEEE Transactions on Communications*, vol. 68, no. 8, pp. 4734–4746, 2020.

[39] D.-T. Hua, Q. T. Do, N.-N. Dao, and S. Cho, "On sum-rate maximization in downlink uav-aided rsma systems," *ICT Express*, vol. 10, no. 1, pp. 15–21, 2024.

[40] S. H. Gardner, T.-M. Hoang, W. Na, N.-N. Dao, and S. Cho, "Metaverse meets distributed machine learning: A contemporary review on the development with privacy-preserving concerns," *ICT Express*, 2025.