Review
JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)
Vol.33 ; No.2 | 2025

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Exploring the Impact of Federated Learning on the Development of Modern Systems: A Review

Sura Jasim Mohammed[1]
College of Information Technology, University of Babylon, sura.phd2018@uobabylon.edu.iq, Babel, Hilla, Iraq.
Safa Saad Abbas[2]
College of Information Technology, University of Babylon, safa.abbas@uobabylon.edu.iq, Babel, Hilla, Iraq.
Fryal Jassim Abd Al-Razaq[3]
College of Information Technology, University of Babylon, fryal.jassim@uobabylon.edu.iq, Babel, Hilla, Iraq.

استكشاف تأثير التعلم الفيدرالي على تطوير الأنظمة الحديثة: مراجعة

سرى جاسم محمد[1]
كلية تكنلوجيا المعلومات ، جامعه بابل ، قسم البرمجيات ، sura.phd2018@uobabylon.edu.iq، بابل ، الحله ، العراق
صفا سعد عباس [2]
كلية تكنلوجيا المعلومات ، جامعه بابل ، قسم البرمجيات ، safa.abbas@uobabylon.edu.iq ، بابل ، الحله ، العراق
فريال جاسم عبد الرزاق [3]
كلية تكنلوجيا المعلومات ، جامعه بابل ، قسم البرمجيات ، fryal.jassim@uobabylon.edu.iq، بابل ، الحله ، العراق

Accepted: 3/6/2025 **Published:** 30/6/2025

ABSTRACT

Federated Learning (FL) represents a transformative advancement in Artificial Intelligence that enables decentralized model training across multiple institutions or devices without transferring raw data. This paradigm is particularly significant for sectors such as healthcare, where privacy, security, and compliance are paramount. This review explores the core principles of FL, its architectural framework, and key differentiators such as horizontal and vertical FL, while examining its major applications across domains including healthcare, finance, mobile systems, and robotics. Through a critical analysis of recent studies, the paper highlights FL's potential to enhance data privacy, mitigate bias from heterogeneous datasets, resist cybersecurity threats, and optimize communication efficiency. It also addresses the limitations that challenge FL's broader adoption, such as high computational costs, vulnerability to adversarial attacks, and data inconsistency across nodes. The findings suggest that FL has the potential to reshape the future of AI by enabling collaborative intelligence without compromising data confidentiality. The paper concludes by outlining future directions for FL research, including adaptive aggregation, secure federated algorithms, and energy-efficient frameworks to enable scalable, ethical, and privacy-aware AI systems.

Keywords: Federated Learning, Privacy Preservation, Healthcare AI, Data Security, Decentralized Systems.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

INTRODUCTION

The industrial sector comes in as one of the most critical areas when it comes to improving productivity, streamlining operations, and driving technological advancements. In recent years, industries have rapidly entered the era of a thoroughgoing digital transformation applied to processes in the supply chain, predictive maintenance, product development, and customer services, as well as improved resource organization due to IT application, allowing more efficient management and increasing organizational effectiveness to push growth and innovation further.[1]

Interest around data analytics is growing because of the greater availability of more diverse data emerging from different avenues like consumer feedback, processes taking place in manufacturing plants, and activities involving logistics. Although a huge amount of data is collected, integration typically remains complicated within multilayered industrial systems, and so also does fragmentation.[2] Big data analytics imbibed into AI has increasingly come to depend on intelligence, along with the emergence of several applications that leverage it predictively to maintain production optimization, predict demands, and sometimes even more functions.[3] Machine learning, a branch of artificial intelligence, has proven to play a significant role in enhancing business processes from instantly and effectively extracting stored insights to escalate real-time decision making.[4]

At present, Federated Learning (FL) is a relatively new technique that has come up in the field of data analytics within the circles of machine learning but under some conditions of data privacy. It makes room for model training over decentralized data sources in manufacturing shops, storehouses, or even in personal mobile devices without the necessity of sharing the raw data.[5] Instead, the model shares updates with a central server, which aggregates them, keeping sensitive data local and reducing the security breach surface. The adoption of Federated Learning in various industries may promise to optimize the use of big data, improving service quality while maintaining strict privacy regulations.[6]

This review will explore the applications and benefits of Federated Learning across different industries, demonstrating its potential to enhance productivity and security in real-world systems while respecting privacy. [7]

The remaining sections of this review are organized as follows: Section 2, will discuss federated learning and its main components, followed by Section 3, will highlight applications of federated learning in healthcare. Section 4, will review the major literature on federated learning, followed by Section 5 which includes the main conclusions and possible future works.

The most related works

This section covers the latest studies and research on the subject of federated learning. These studies indicate that federated learning has become a vital technology in many fields, as it enables collaborative learning between devices or organizations without directly sharing data, which enhances privacy and reduces security risks. By reviewing these studies, the importance of federated learning can be extracted from several main aspects:

1. Enhancing data privacy in medical applications

In the ref [8] develops an AI model for accurately interpreting cardiac CT scans under a federated learning scenario, with a particular focus on addressing the unique challenges of partially labeled data that hinder the full potential of decentralized data. This is accomplished by applying a semi-supervised approach, which involves a first stage of specialized CNNs to generate initial predictions on unlabeled data based on label type, and a second stage of transformer training. These predictions are delivered through dedicated headers for each label to enable simultaneous learning of all partial labels. This work applies the method to the largest labeled dataset, comprising 8,104 patient cases from eight hospitals. The results show that the proposed model outperforms traditional UNet models in terms of prediction accuracy and generalization ability. The study recommends the adoption of this framework in medical applications where labels are scarce, and the availability of source code and model weights supports future studies in cardiac image analysis.

In [9] researchers described a privacy-preserving federated learning framework for early detection of Alzheimer's disease, which enables collaborative training of models among different medical institutions without actual sharing of raw patient data. The study used neuroimaging features and employed a privacy-preserving architecture for maintaining the confiden-tiality of the data with high diagnostic accuracy. The model has competitive perfor-mance across several sites. This demonstrates the feasibility of using the pro-posed solution in real-world clinical deployment. Still, the major problems are the distribution of heterogeneous data and the performance disparity in low-resource settings.

2. Improving Model Performance and Reducing Bias from Heterogeneous Data

In [10] tries to address the issues of data heterogeneity and long-tailed distributions in a FL environment. The major objective of this new framework was to improve model performance across different clients while not compromising data privacy. The components of MuPFL are Biased Activation Value Dropout (BAVD), responsible for checking overfitting and speeding up training; Adaptive Cluster-based Model Update (ACMU) producing good local model refi nements and assuring coherent aggregation on the global level; and finally, the third one is the Prior Knowledge-assisted Classifier Fine-tuning (PKCF) enhancing the classification accuracy for a skewed local dataset. The performed real-world dataset evaluations gave a general superiority for the proposed method over existing FL methods up to 7.39% in some cases for accuracy and an 80% reduction in training time. Strengths of the framework are effective personalization of models, strengths of the framework are effective personalization of models, strengths of the framework are effective personalization of models, strengths of the framework are effective personalization of models, strengths of the framework are effective personalization of models, strengths of the framework are effective personalization of models, strengths of the framework are effective personalization of models, strengths of the framework

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

are effective personalization of models, strengths of the framework are effective personalization of models, strengths of the framework are effective personalization of models, strengths of the framework are effective personalization of models, strengths of the framework are effective personalization of models, strengths of the framework are effective personalization of models.

The study of ref. [11] did propose an adaptive aggregation weight strategy, termed FedAAW, which adjusts the influence of each client's model during aggregation beyond traditional size-based weighting. This is in an effort to improve federated learning (FL) performance on non-IID data. The paper further describes a theoretical formulation that minimizes the convergence upper bound in heterogeneous data settings, thus guiding the optimal assignment of aggregation weights. All these things, using four benchmark datasets, proved to make FedAAW outperform the state-of-the-art in terms of both the rate of convergence and the final accuracy, up to 37.32% increase in test performance. Strong points of the proposed approach comprise theoretical grounding, easy integration with existing FL methods, and improved performance in dealing with data heterogeneity. Where the proposed methodology falls is that it may require careful tuning. This can be a drawback in highly dynamic edge environments.

3. Improving Cybersecurity and Resilience Against Attacks

In their systematic literature review [12], the concept is developing secured federated learning (FL) systems by integrating intrusion detection systems (IDS) that are based on neural network (NN) models alongside feature engineering techniques and privacy-preserving methods. In a body of 88 works available from 2021 up to October 2024, to be thoroughly analyzed for all such applications, and more the treatment of advanced NNs—like CNNs, RNNs, DNNs, and hybrid models—in the malicious client detection process in FL environments, this review has updated knowledge. Indeed, in the review, mainly general CNNs, RNNs, and DNNs are found to further enhance the accuracy and computational efficiency of such detection with FL environments, also integral and hybrid models proposed. Another study is conducted to assess privacy-preserving models, like differential privacy and federated averaging, in the condition of keeping information confidential. Findings indicate that better results in the discovery of reduced false alarms in attacks over privileged FL system settings, the two feature engineering and NNs must join hands. The review has also identified challenges. Like; lack in generalizability of feature engineering methods across diverse datasets and need more robust privacy-preserving mechanisms to counter against sophisticated attacks.

In ref.[13] put forward DarkFed, a data-free backdoor attack on federated learning that does not rely on real client data, but instead, it uses some synthetic 'shadow' datasets and emulated fake clients to generate malicious updates that look like benign updates. The method was highly effective and stealthy, achieving strong attack success rates even under a limited attacker presence. High usability of the framework in a very practical environment for low attacker presence and its power to bypass defenses without any reduction in overall model performance makes the framework strong, subject to shadow dataset quality and precise optimization for indistinguishability of malicious updates.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

The study of ref.[14] also discusses FedMUA as a new attack framework that attacks the integrity of FL models through the federated unlearning process. This work focuses on a detailed exploration of how malicious clients could use unlearning requests to systematically induce misclassifications in the global model, hence degrading other clients' data predictions. The attack methodology is based on two steps: first, finding data on which some specific samples have a marked influence, and secondly, generating malicious unlearning requests to remove the influence of these samples. Experimental results provided that the initiation of merely 0.3% malicious unlearning requests can enable FedMUA to attack with up to an 80% success rate, therefore indicating a very high current FL system vulnerability. The paper is strong in that it unearths an FL attack vector that has not been considered before and goes further to propose a defense mechanism against such threats. Some limitations of the study are the assumed threat model, not comprehensive in all possible real-world scenarios, and the required further evaluation of the effectiveness of the proffered defense across a diversity of FL applications.

4. Reduce resource consumption and improve communication efficiency

Ref. [15] introduced an intelligent aggregation approach for federated learning (FL) that demonstrates strong resilience against attacks while preserving data privacy. The proposed method incorporates a training mechanism that updates information from anomalous clients, enabling unsupervised handling of adversarial behaviors. This approach was implemented in a realistic federated environment and evaluated using multiple datasets. The results revealed a clear trade-off between maintaining model accuracy under attack and outperforming existing defense strategies. A key strength of this method lies in its ability to effectively balance robustness and latency, making it a scalable and applicable solution for highly sensitive domains. However, the approach may encounter limitations when generalized to significantly different attack patterns or data domains, highlighting the need for broader validation in future research.

5. Addressing the economic and environmental challenges associated with AI

Ref. [16] highlights the social implications of federated learning (FL), a collaborative, crowd-sourced approach that prioritizes privacy preservation when compared to more centralized alternatives in traditional artificial intelligence systems. The paper assesses FL's potential to mitigate some of the negative consequences of large-scale AI, particularly concerning economic centralization, environmental costs, and data privacy threats. In a very recent study, it was noted that while FL holds promise for enabling more equitable and sustainable AI development, it remains in its early stages. Significant challenges persist—especially in relation to data leakage and the high communication overhead—which must be addressed before FL can be widely adopted. Although FL aligns with ethical AI principles and user privacy safeguards, practical barriers remain, stemming from both the immature state of the technology and the inherent complexity of the system.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Federated learning emerges as an innovative approach that can achieve an ideal balance between privacy, performance, and security. With its ability to operate in heterogeneous environments while maintaining data decentralization, it is revolutionizing the medical, industrial, and cybersecurity fields. As research continues to develop adaptive protection and performance technologies, FL will be the cornerstone of future AI systems, driving its wider adoption. Table 2 shows summary of related works.

Table 2. Summary of related works.

No.	Ref	Focus Area	Objective & Methodology	Key Findings	Strengths	Limitations
1	[8]	Data Privacy in Healthcare	Developed FL framework for cardiac CT imaging using semi-supervised CNNs and knowledge distillation with SWIN-UNETR on 8,104 scans from 8 hospitals.	Outperformed UNet; strong generalization in low-label scenarios.	Innovative architecture; privacy preserved; effective on external data.	High computational cost; sensitive to data heterogeneity.
2	[9]	Data Privacy in Healthcare	Proposed secure FL for Alzheimer's detection using neuroimaging and privacy-preserving methods.	Maintained high accuracy across institutions.	Data confidentiality ensured; real-world deployment ready.	Struggles with heterogeneous data and low-resource settings.
3	[10]	Model Performance & Bias	Introduced MuPFL combining BAVD, ACMU, and PKCF to handle data heterogeneity and long-tailed distributions.	Accuracy ↑ 7.39%, training time ↓ 80%.	Personalized learning, balanced skewed data, efficient.	Multi-stage design increases complexity.
4	[11]	Model Performance & Bias	Proposed FedAAW for adaptive aggregation beyond data-size weighting.	Test performance ↑ 37.32%; fast convergence.	Theoretically grounded, low communication overhead.	Requires tuning in dynamic edge settings.
5	[12]	Cybersecurity	Reviewed 88 studies using NNs and feature engineering in FL-based IDS.	NN + FE improve attack detection and privacy.	Covers privacy and performance integration.	Limited generalizability across datasets.
6	[13]	Cybersecurity	Presented DarkFed: backdoor attack using synthetic shadow data and fake clients.	Stealthy attack; high success with minimal presence.	Realistic attacker simulation; avoids model degradation.	Depends on shadow data quality; needs precise tuning.
7	[14]	Cybersecurity	Introduced FedMUA exploiting unlearning to trigger misclassifications.	Attack success rate up to 80% from only 0.3% of clients.	Exposes overlooked threat vector; proposes countermeasures.	Assumes specific threat model; needs broader validation.
8	[15]	Resource Optimization	Proposed anomaly-based aggregation for adversarial robustness.	Preserves accuracy in presence of malicious updates.	Scalable, practical balance of privacy and robustness.	May not generalize across all attack/data patterns.
9	[16]	Economic & Environmental Impact	Assessed FL's societal benefits and ethical implications.	FL reduces monopolization and carbon footprint.	Aligns with ethical AI; preserves user rights.	Faces adoption barriers: complexity, communication load.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Federated Learning (FL) has emerged as a transformative paradigm in artificial intelligence, enabling collaborative model training without the need to share sensitive data among participants. Recent studies highlight FL's strong potential across various domains, particularly in medical applications where it enhances diagnostic accuracy while preserving patient privacy. It also demonstrates effectiveness in addressing data heterogeneity (non-IID data) through adaptive aggregation strategies that improve model fairness and performance. On the security front, research has revealed critical vulnerabilities such as unlearning-based and data-free backdoor attacks, leading to the development of robust defense mechanisms that maintain both model integrity and communication efficiency. Furthermore, some studies have explored the societal and economic dimensions of FL, emphasizing its role in reducing data monopolies and environmental impact compared to centralized AI systems. Despite these advancements, FL still faces significant challenges, including system complexity, high communication costs, and limited generalizability in certain scenarios. Therefore, the future of FL hinges on achieving a careful balance between privacy, performance, security, and real-world applicability.

FEDERATED LEARNING

Google researchers presented a federated learning approach in the year 2016 [17], that enabled devices to train models locally without the need to send raw data to a central server. Federated learning is decentralized, thus, multiple organizations or even multiple devices can work together and train machine learning models without actually sharing the private data involved here. Data goes neither to nor via a central server [18]. The present study unites the participants in training models locally on data that is highly diverse, not explicitly, but implicitly, bound up by the users who help eliminate errors, thus improving model accuracy. The exchange of model parameters among devices does not involve sharing raw data, which provides more security. These updates are incorporated into a shared global model, which is then fed back to uplift the performance of local models [19]. The structure of federated learning is presented in Fig. (1) [20].

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

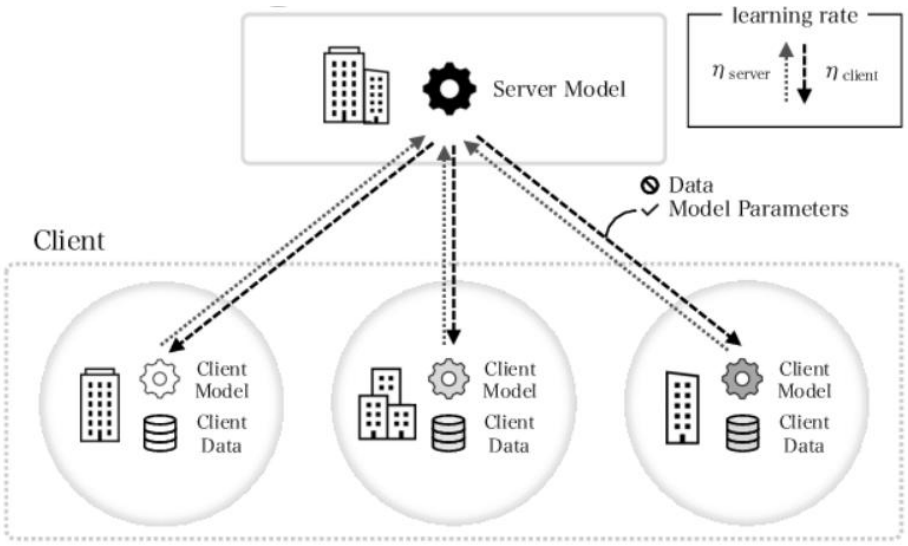

Figure 1: Structure of federated learning. [20]

Federated learning models are updated using Distributed Stochastic Gradient Descent (SGD), where the model update is computed locally on each machine and only the updates are sent to the central server. The updates can be mathematically represented as follows[21]:

1. **Local gradient computation** for each data owner **i**:

$$g_i = \nabla L(w_t, D_i)$$

Where:

- **$L(w_t, D_i)$)** is the loss function at model weight **w_t** and local dataset **D_i.**

2. **Global model aggregation at the central server**:

$$_{t+1}w = {}_{t}w - {}_{i}\eta \sum_{i=1}^{N} p_i g$$

Where:

η is the learning rate.

P_i represents the weight of each client based on its data proportion.

The classification of federated learning is horizontal as shown in figure2 and vertical FL. The former shares data on the same entities but different samples, while the latter shares data on the same entities but different features. Another distinction would be cross-silo vs. cross-device FL,

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

which allows for the introduction of much less reliable devices within resource-rich organizations. These methods increase the implementation of FL into healthcare, finance, or mobile computing, but with data privacy and security guaranteed.

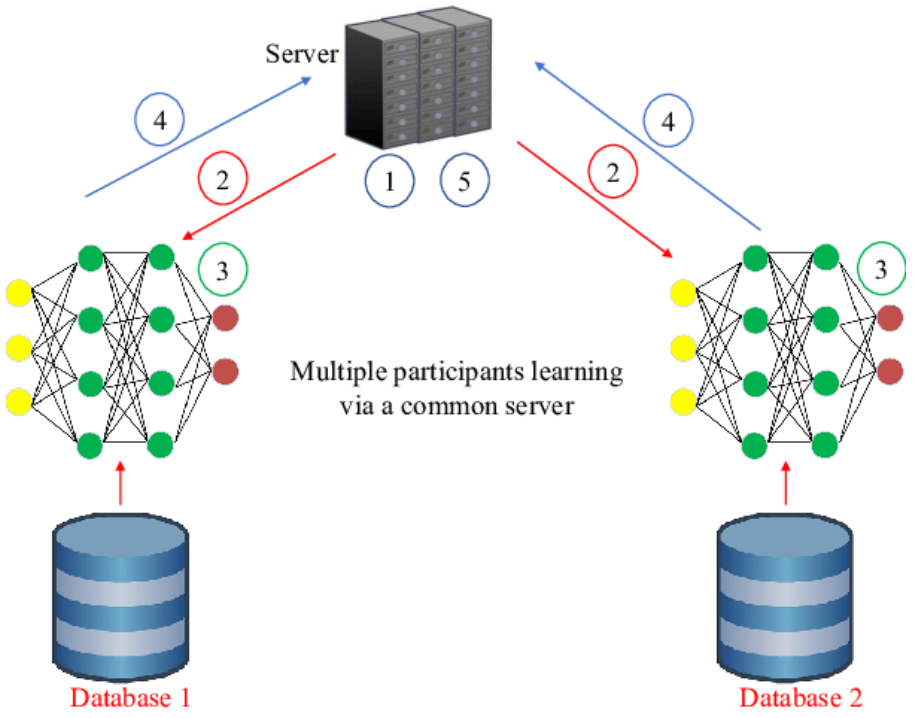

Figure 2: Federated Learning System (Horizontal) [22].

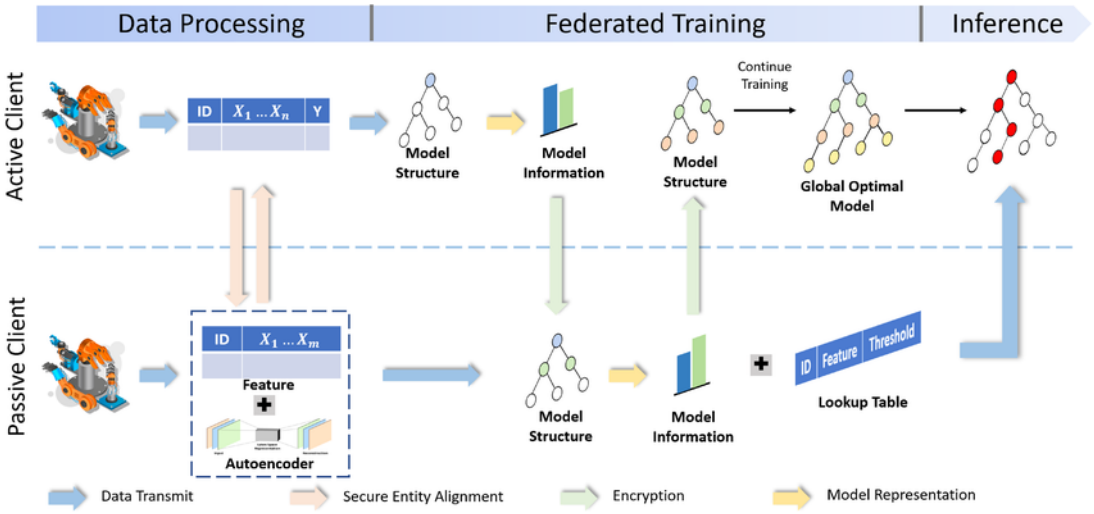

Figure 3: Federated Learning System (Horizontal) [23].

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Characteristics of Federated Learning

Federated learning is a branch of distributed machine learning that primarily focuses on data privacy protection. It also leverages distributed systems that facilitate collaboration among multiple nodes connected via a network, with a central server managing operations and coordinating interactions between these nodes. The key characteristics of federated learning include [24]:

- **Collaboration between multiple organizations:** Initially developed by Google as a distributed machine learning technique, federated learning enables organizations to build a global model while keeping their data in its original locations. Over time, the concept has expanded to encompass all decentralized machine learning techniques that ensure privacy .
- **Asymmetric data distribution:** Data is widely spread across numerous edge devices, and the data available on each device may be significantly smaller than the total number of devices.
- **Decentralization:** While not entirely decentralized in a technical sense, federated learning does not rely on a single control center. All nodes contribute to the central model without any of them acting as the primary control hub. Instead, parameter servers function as central coordinators that distribute data and facilitate cooperation between participants.
- **Equality among nodes:** All participants in federated learning have equal access to resources and opportunities. However, nodes with larger datasets exert a greater influence on improving the global model.

Federated Learning applications

Federated learning advances AI development across lifecycles by enabling decentralized training and maintaining privacy and security across different data sources. Table 1 shows the most important applications that use federated hashing techniques:

Table 1. Most federated Learning applications

Application Area	Description
Smart Retail	Federated learning can provide personalized services such as product recommendation and sales services by aggregating data features like user purchasing power, personal preference, and product characteristics, which are distributed among different departments or enterprises[25].
Multi-Party Database Querying in Finance	In a financial application, federated learning can be used to detect multi-party borrowing between banks, ensuring that user lists remain encrypted and private. This is particularly important for preventing financial system collapses due to fraudulent activities[25].
Healthcare	Federated learning revolutionizes medical AI and healthcare insurance by enabling institutions to collaborate on AI model training without sharing sensitive patient data. This improves privacy, security, data diversity,

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

	scalability, and regulatory compliance (e.g., HIPAA, GDPR). It is particularly beneficial for sharing medical data across hospitals and research centers to improve diagnostic accuracy. Examples: MedPerf is an open-source platform that enables federated evaluation of AI models across multiple hospitals, ensuring diagnostic accuracy without compromising patient confidentiality[25, 26].
Mobile Applications	Federated learning is applied in the mobile AI application for next-word prediction, face detection, and speech recognition. This ensures privacy, as well as personalized models with reduced bandwidth usage while also offering benefits, such as proof against the attacker, since the data remains on the device. Real-Life Example: Google uses federated learning in the "Hey Google" detection part of Google Assistant. The models are fully trained on the device based on real user utterances without the need for raw audio data leaving the device. This maintains privacy for the user[27].
Robotics	Robotics involves the use of machine learning in perception, decision-making, and control, from simple tasks to complex navigation. Applications demand continuous learning and adaptability, but centralized training faces data movement, privacy, and communication issues in a multi-robot system. Federated learning enables robots to collaborate in improving their models while keeping their data localized, explicit, and thus efficient in multi-robot navigation under bandwidth limitations. The robots learn from their local experiences and share only the updates of the essential elements of the model with each other. A Real-life Example: The FLDDPG strategy does swarm robotics for Federated Learning-based Deep Reinforcement Learning on low communication bandwidth; generalizes well across environments and actual robots while baseline methods show diminishing capabilities with bandwidth limitations[27].

Table1 provides applications of federated learning techniques across industries thus, mitigating concerns about privacy and security of data because sensitive data remains local and only model updates are exchanged rather than raw data. It further improves the work between different sectors, such as finance, healthcare, and robotics, in improving AI models without compromising privacy. The process also saves time because one does not have to carry data from one area to another and saves bandwidth and computing resources while maintaining high model performance. The applications herein place federated learning within the frame of a revolutionized industry with personal systems that are less harmful and free from privacy invasion.

CONCLUSION

The federated learning (FL) framework excels at handling unlabeled datasets, exploiting security vulnerabilities, and enhancing model generalization on heterogeneous data. However, it still faces significant challenges, such as communication costs, security threats (such as poisoning and backdoor attacks), and practical deployment in real-world settings is difficult due to computational limitations and privacy risks.

.

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Conflict of interests.

There are non-conflicts of interest.

References

[1] J. Xu, B. S. Glicksberg, C. Su, et al., "Federated learning for healthcare informatics," *Journal of Healthcare Informatics Research*, vol. 5, no. 1, pp. 1–19, 2021. doi: 10.1007/s41666-020-00082-4.

[2] G. Muhammad, F. Alshehri, F. Karray, A. El Saddik, M. Alsulaiman, and T. H. Falk, "A comprehensive survey on multimodal medical signals fusion for smart healthcare systems," *Information Fusion*, vol. 76, pp. 355–375, 2021.

[3] R. T. Adek and M. Ula, "A Survey on the Accuracy of Machine Learning Techniques for Intrusion and Anomaly Detection on Public Data Sets," *in Proc. Int. Conf. Data Sci. Artif. Intell. Bus. Anal. (DATABIA)*, 2020, pp. 19–27. doi: 10.1109/DATABIA50434.2020.9190436.

[4] M. Batta, "Machine Learning Algorithms - A Review," Int. J. Sci. Res., p. 7, 2020.

[5] M. Alruwaili, M. H. Siddiqi, M. Idris, S. Alruwaili, A. S. Alanazi, and F. Khan, "Advancing Disability Healthcare Solutions Through Privacy-Preserving Federated Learning With Theme Framework," *Expert Systems*, vol. 42, no. 1, e13807, 2025.

[6] S. Khan, M. Khan, M. A. Khan, L. Wang, and K. Wu, "Advancing Medical Innovation through Blockchain-Secured Federated Learning for Smart Health," *IEEE J. Biomed. Health Inform*., 2025.

[7] E. Dritsas and M. Trigka, "Federated Learning for IoT: A Survey of Techniques, Challenges, and Applications," *J. Sensor Actuator Netw*., vol. 14, no. 1, p. 9, 2025.

[8] M. Tölle, P. Garthe, C. Scherer, J. M. Seliger, A. Leha, N. Krüger, et al., "Real world federated learning with a knowledge distilled transformer for cardiac CT imaging," *npj Digital Medicine*, vol. 8, no. 1, p. 88, 2025.

[9] A. Mitrovska, P. Safari, K. Ritter, B. Shariati, and J. K. Fischer, "Secure federated learning for Alzheimer's disease detection," Front. *Aging Neurosci*., vol. 16, p. 1324032, 2024.

[10] R. Zhang, Y. Chen, C. Wu, and F. Wang, "Multi-level personalized federated learning on heterogeneous and long-tailed data," *IEEE Trans. Mobile Comput*., 2024.

[11] X. Li, Y. Gao, Y. Deng, and X. Jiang, "Federated Learning With Adaptive Aggregation Weights for Non-IID Data in Edge Networks," *IEEE Trans. Cogn. Commun. Netw*., 2025.

[12] N. Latif, W. Ma, and H. B. Ahmad, "Advancements in securing federated learning with IDS: a comprehensive review of neural networks and feature engineering techniques for malicious client detection," *Artif. Intell. Rev*., vol. 58, no. 3, p. 91, 2025.

[13] M. Li, W. Wan, Y. Ning, S. Hu, L. Xue, L. Y. Zhang, and Y. Wang, "Darkfed: A data-free backdoor attack in federated learning," arXiv preprint arXiv:2405.03299, 2024.

[14] J. Chen, Z. Lin, W. Lin, W. Shi, X. Yin, and D. Wang, "FedMUA: Exploring the Vulnerabilities of Federated Learning to Malicious Unlearning Attacks," *IEEE Trans. Inf. Forensics Secur*., 2025.

[15] F. Shi, W. Lin, C. Peng, C. Zhong, D. Wang, and M. Cheng, "Dynamic Client Selection for Over-the-Air Federated Learning Network," *IEEE Internet Things* J., 2025.

[16] M. Zeybek, "Classification of UAV Point Clouds By Random Forest Machine Learning Algorithm," *Turkish J. Eng*., 2021. doi: 10.31127/tuje.669566.

[17] J. Curl and X. Xie, "Societal impacts and opportunities of federated learning," *Chin. J. Sociol*., 2025. doi: 10.1177/2057150X251314299.

[18] B. Yurdem, M. Kuzlu, M. K. Gullu, F. O. Catak, and M. Tabassum, "Federated learning: Overview, strategies, applications, tools and future directions," *Heliyon*, 2024.

[19] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, et al., "Advances and open problems in federated learning," *Found. Trends Mach. Learn.*, vol. 14, no. 1–2, pp. 1–210, 2021.

[20] C. Dilmegani and S. Ermut, "Federated learning: 5 use cases & real-life examples in 2025," *AIMultiple*, Feb. 18, 2025. [Online]. Available: https://research.aimultiple.com/federated-learning/

[21] H. Yamamoto, D. Wang, G. K. Rajbahadur, M. Kondo, Y. Kamei, and N. Ubayashi, "Towards Privacy Preserving Cross Project Defect Prediction with Federated Learning," in Proc. IEEE Int. Conf. Softw. Anal. Evol. Reengineering (SANER), Macao, 2023, pp. 485–496. doi: 10.1109/SANER56733.2023.00052.

[22] 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.

[23] Z. Li, V. Sharma, and S. P. Mohanty, "Preserving Data Privacy via Federated Learning: Challenges and Solutions," *IEEE Consum. Electron. Mag.*, vol. 9, no. 3, pp. 8–16, May 2020. doi: 10.1109/MCE.2019.2959108.

[24] L. Xia, et al., "Privacy-preserving gradient boosting tree: Vertical federated learning for collaborative bearing fault diagnosis," IET Collab. Intell. Manuf., vol. 4, no. 3, pp. 208–219, 2022.

[25] K. Zhang, Y. Chen, et al., "A privacy-preserving multi-task learning framework for face detection, landmark localization, pose estimation, and gender recognition," *Frontiers in Neurorobotics*, vol. 13, p. 112, 2020.

[26] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y. C. Liang, Q. Yang, et al., "Federated learning in mobile edge networks: *A comprehensive survey," IEEE Commun. Surv. Tutor.*, vol. 22, no. 3, pp. 2031–2063, 2020.

[27] M. Babar, B. Qureshi, and A. Koubaa, "Investigating the impact of data heterogeneity on the performance of federated learning algorithm using medical imaging," *PLOS ONE*, vol. 19, no. 5, e0302539, 2024.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com