International Journal of Basic and Applied Sciences, 14 (8) (2025) 710-716

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/2ybenf06
Research paper

Federated Learning Architectures for Distributed Financial Institutions: Challenges and Optimizations

Saravanan Thirumazhisai Prabhagaran *

Anna University, Chennai, Tamil Nadu, India
**Corresponding author E-mail: saravanan.prabhagaran@gmail.com*

Abstract

Data privacy and regulatory compliance are also crucial threats to the centralized machine learning practice in the digital financial environment. Federated Learning (FL) provides a referral-free solution that enables several financial units to collaborate in training machine learning models without sharing sensitive customer data. The paper investigates the architecture design, system issues, and performance enhancements of FL in distributed financial settings. By conducting a thorough analysis of communication restrictions, data heterogeneity, and security flaws, the paper identifies obstacles to the smooth implementation of FL. Other emerging technologies in the privacy-preserving methods, adaptive optimization algorithms, and hierarchical architectures relate specifically to the area of financial applications that are evaluated in the paper. Moreover, it presents new governance regimes and practical applications, underscoring the relevance of FL in fraud detection and credit rating assessment, as well as in investment approaches. The insights introduced not only demonstrate the viability of FL in the financial sphere but also outline a path towards the creation of safe, scalable, and regulatory-compliant AI ecosystems. Grounding technology in collaboration between institutions and legal frameworks, federated learning is one of the core infrastructures of the new era of safe, intelligent financial systems.

Keywords: *Federated Learning; Financial Institutions; Data Privacy; Distributed Ai; Regulatory Compliance.*

1. Introduction

As compliance and privacy rules continue to cement financial data privacy under mounting challenges, the opportunities conjured by the federated learning (FL) architecture, which has the capacity to maintain data locality and yet facilitate collaborative machine learning, are beginning to shift into the gears of distributed financial organizations. Coming with conventional decentralized data aggregation raises a lot of questions about privacy violation, regulatory violation, and security of data, especially in such areas as banking and finance, where data sensitivity is valued supremely [1] [2]. The decentralization of the training process by federated learning solves these problems by enabling various institutions to assist in improving the model without exchanging raw data. Data decoupling ensures that data acquisition is independent of model training, providing a realistic solution that is compliant with contemporary legislative frameworks such as GDPR and the CCPA [3] [4].

The importance of such a paradigm, such as FL, is of particular concern in the global and distributed financial systems, which are made up of many members, such as banks, insurance companies, investment firms, and fintech startups, producing huge amounts of heterogeneous and proprietary data. FL-based coordinated learning not only protects privacy but also has the potential to improve model generalizability across different market situations and user demographics [5] [6]. The benefit is critical in financial settings where judgments must often rely on subtle and dynamic trends in consumer transactions, market trends, and fraudulent instances. Nevertheless, deploying FL in such a dispersed and compliance-heavy business is quite problematic. Such difficulties range from data and model disparity to communication incompetence, management of trust between stakeholders, and robustness of the system against adversarial attack [7] [8]. Thus, it is crucial to understand these complexities to formulate FL architectures that suit financial ecosystems. The paper discusses these challenges in detail, in addition to recommending architectural and algorithmic optimizations to make FL more feasible as the solution to distributed financial institutions.

With the shift in the discussion towards the technical design of federated learning systems in the financial contexts, one will need to learn how these systems are designed and implemented to work with the realities of modern financial organizations. To support this systematic review of the applicability of federated learning to distributed financial ecosystems, the following three research questions are used to organize the present review.

- What federated learning architectures can be best applied to the deployment in a diversity of heterogeneous financial institutions with stringent privacy, security, and regulatory restrictions?
- What are the technical, organizational, and legal constraints that restrict the practical use of federated learning in the financial sector?
- What optimization techniques, governance, and privacy-protective approaches may make federated learning systems, used in finance, scalable, trustful, and regulated?

In addressing these questions, the present paper makes three main contributions.

1) It provides a structured summary of federated learning systems that are contextualized with respect to distributed financial institutions and constraints of their operations.
2) It gives an in-depth study of issues of multidimensional implementation, such as data heterogeneity, communication overhead, adversarial security risk, inter-institutional trust, and regulatory fragmentation.
3) It summarises state-of-the-art optimization strategies, collaborative governance models, and new real-world financial application scenarios to sketch possible ways to practical production scale and privacy-preserving financial intelligence.

Together, all of these efforts will close the gap between theoretical federated learning research and its secure, compliant implementation in current financial infrastructures.

2. Review Methodology

The current research will follow a systematic narrative review approach to investigate the architectures of federated learning (FL) and its applicability to distributed financial institutions. The literature of interest was identified by searching major academic databases, including IEEE Xplore, SpringerLink, ScienceDirect, ACM Digital Library, and Google Scholar, with publications from 2018 to 2025 considered to reflect current trends in privacy-preserving distributed machine learning. The search keywords included: federated learning, financial systems, privacy-preserving AI, secure aggregation, regulatory compliance, and distributed analytics. The criteria used to include studies were that they had to deal with FL architectures, optimization strategies, governance mechanisms or real-world financial implementation, with purely theoretical studies lacking financial deployment being excluded. The chosen literature was further thematically analyzed in terms of architectural design, implementation issues, optimization strategies, compliance systems, and practiced case studies to derive the existing knowledge and research gaps in the context of secure and scalable financial AI ecosystems.

Based on the above structured review methodology, the synthesized literature forms the basis of investigating the architectural implementation of federated learning in real-life financial settings. It is necessary to understand such architectural paradigms, since the success of federated learning in finance cannot be attributed solely to theoretical privacy guarantees but also to the functionality of distributed training systems, communication networks, and models of institutional involvement. In this respect, the next section will give a comprehensive discussion of federated learning architectures in financial institutions, their decentralized training processes, their client-server coordination schemes, as well as their convergence dynamics in regulation-bounded financial ecosystems.

3. Federated Learning Architectures in Financial Institutions

A federated learning system architecture of the financial application is generally focused on a decentralized model training paradigm. Under normal FL conditions, a central server launches a universal model shared with voting client nodes, which are financial entities such as banks or insurance companies. Such clients would then locally train the model using their data and share the updated model (not raw data) with the server, which would pool all of them to update the global model [9] [10]. This process repeats after a few communication rounds until the worldwide model converges to the intended degree of precision.

Financial institutions impose special demands and limitations on this model. By way of example, institutions may have different data structures, customer trends, and regulatory requirements. Consequently, client data is highly non-independent and identically distributed (non-IID), which has a major impact on the model's convergence and performance [11] [12]. This discrepancy places exceptional obligations on the FL frameworks, i.e., to address heterogeneity in statistics while ensuring client fairness and model accuracy. In addition, the architectures should be cost-effective in terms of communication and resource constraints, given the large volume and velocity of financial data. A number of Federations have been discussed to meet these requirements, such as hierarchical FL, wherein a group of so-called intermediary aggregators is inserted between clients and the central server to minimize latency and bandwidth usage [13] [14]. Cross-silo FL would suit banks and other large financial institutions and presupposes fewer, but more stable, customers, with increased computing power and connection quality, enabling the training of more sophisticated learning systems, including deep neural networks, in a collaborative manner [15]. Another important architectural factor is security. Cyber threats often target financial systems; therefore, the FL implementation should employ advanced cryptographic protocols, such as secure aggregation, differential privacy, and homomorphic encryption, to ensure the confidentiality and integrity of model updates [16] [17]. Also, identity management and access control planes are required to prevent model poisoning or inference attacks by compromised clients. These architectural requirements point to the conclusion that the passive utilization of a ready-made FL solution is not enough. It is critical to customize architecture according to client heterogeneity, communication infrastructure, and regulatory requirements to enable practical deployment of such architecture in financial fields. Having established the architectural foundations of federated learning, the paper now delves deeper into the key challenges that arise when implementing these frameworks within real-world financial institutions.

Combined, these architectural aspects show that federated learning in financial institutions is not only a decentralized technical architecture but a sophisticated socio-technical infrastructure that has to be influenced by data heterogeneity, communication limitations, security conditions and regulatory supervision. Although the presented architectural solutions, including hierarchical, cross-silo, and privacy-focused federated designs, offer practical development directions, their feasibility will ultimately be determined by their ability to withstand the operational realities of distributed financial ecosystems. In its turn, it leads to the need to analyze the practical issues that arise in the course of practical implementation in a more detailed manner. The next section thus changes the discussion of designing architecture to the critical examination of the technical, organizational, and regulatory constraints imposed to limit large-scale implementation of federated learning in financial systems.

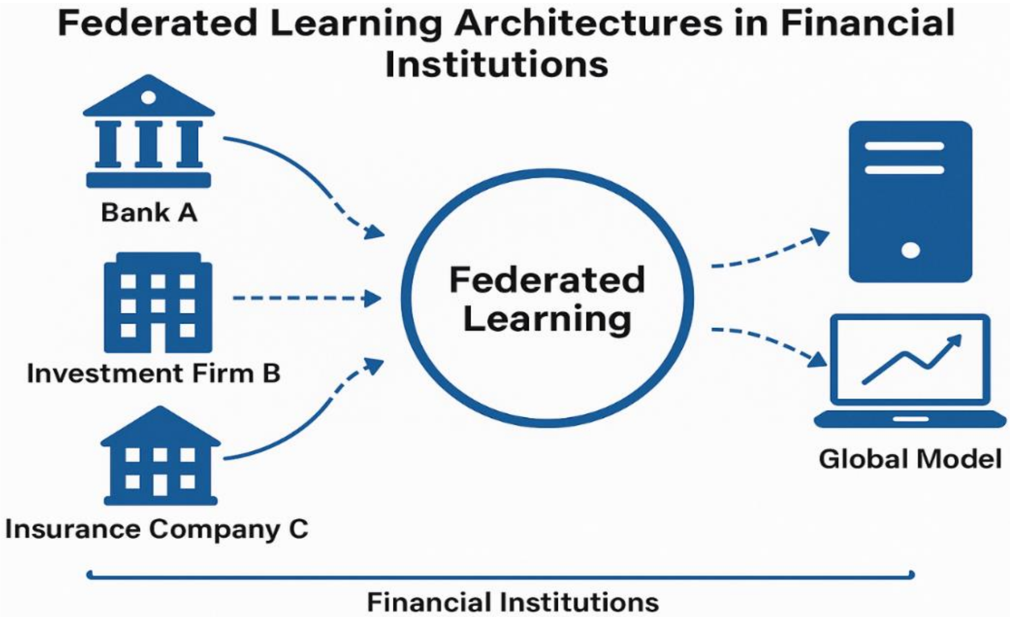

Fig. 1: Diagram Illustrating A Federated Learning Architecture Among Financial Institutions, Where Banks, Investment Firms, and Insurance Companies Collaboratively Train A Shared Global Model without Sharing Raw Data.

4. Challenges in Federated Learning for Financial Systems

Building on the architectural description, it is also necessary to critically examine the associated challenges that prevent the implementation of federated learning across distributed institutions in the financial domain. These problems occupy technical, organizational, and regulatory planes of consideration and require a joint solution in order to make FL an effective real-life paradigm in the field of finance. Data heterogeneity is one of the leading technical issues. Financial institutions operate in various markets, serve different customer populations, and use different internal data processing systems. This leads to non-IID data distributions across FL clients, so that each participant's dataset may exhibit distinct statistical properties. This causes a training algorithm to be unstable during convergence and introduces biases that can drastically affect performance in the global model [18] [19]. For example, FL training of fraud detection models could perform poorly in banks with customer profiles that are not common, due to bias introduced by more prevalent contributors to the data. The other challenge to address is the communication bottleneck, a characteristic of FL architectures. As opposed to a centralized learning setting, FL necessitates sending model parameters at every training iteration. Since models, such as deep neural networks, may be enormous, such communications may not only be costly in bandwidth but also unacceptable when a large number of clients in various geographical regions need to be involved [20] [21]. Besides, random connectivity and variations in network latency across financial parties will complicate synchronization further and result in the loss of clients or stragglers, slowing global updates.

There is still a threat to security and privacy, regardless of what FL claims about decentralized learning. Poisoning attacks allow malicious participants to upload degraded gradients to degrade the performance of the global model or even introduce a specific vulnerability [22] [23]. Conversely, introductions of inference attacks might also exploit the updates of a shared model to derive sensitive data. Solutions such as differential privacy and secure multiparty computation have been suggested, but usually at the cost of a trade-off between utility and privacy, either in terms of computational overhead or model accuracy [24]. Compliance with regulations is a particular challenge in the financial industry. All jurisdictions have the right to set their rules on how data is to be protected, and one would therefore not be able, at the same time uphold all rules imposed, in a non-trivial way, to implement all FL. For example, metadata, system logs, and other auxiliary communication systems, though they do not share any significant data, might contain sensitive or personally identifying information (PII) that is subject to regulation [25]. Financial institutions are therefore required to implement stringent risk controls and establish effective governance structures to regulate them. Trust among participants is more organisational than personally driven. Within a federated ecosystem, institutions are forced to collaborate with others they neither know nor trust, nor understand their internal data quality processes. Such distrust may lead to an unwillingness to contribute resources or to align on common goals. Moreover, institutions may face competition, which slows participation toward complete coverage, or participation may be strategic as institutions aim to reap all the benefits of the global model at the expense of contributions [26] [27].

There is also the issue of system robustness. Since financial services are mission-critical, FL systems must tolerate node failures, adversarial inputs, and infrastructure failures. High availability and fault tolerance of a distributed learning system are more complicated than in a centralized setting. It has advanced orchestration procedures, operational monitoring, and dynamic resource management systems to prevent interruptions that could affect service delivery [28]. Besides these operational and technical limitations, assessing federated models poses a dilemma. Systems Performance measures in federated domains. In a federated setting where model utility can differ significantly across clients, traditional machine learning metrics cannot be used to measure performance. Thus, new equity-sensitive assessment plans are required to ensure that the benefits of FL are fairly distributed and that service quality is not degraded for minority clients [29]. Such obstacles highlight the disparity between the theoretical capabilities of federated learning and its implementation in the financial ecosystem. Nevertheless, a lot of these limitations can actually be addressed by making suitable optimizations. The next part presents a discussion of the main architectural and algorithmic improvements that can enhance the effectiveness, efficiency, and robustness of FL systems, specifically in the financial community.

The conceptual and algorithmic issues stated leave aside the multi-dimensional set of operational risks inherent to federated learning applied to financial systems. Table 1 gives a systematic description of such risks in four domains: technical, legal, organizational, and reputational, though it identifies the vulnerabilities that can develop during deployment.

Table 1: Categorization of Operational Risks in Federated Learning for Financial Institutions

Risk Category	Specific Risk	Potential Impact	Mitigation Strategy
Technical	Model divergence from non-IID data	Degraded model performance across minority institutions	Adaptive optimizers (e.g., FedProx), personalized FL
Legal	Incomplete compliance with regional data laws	Financial penalties, litigation, operational halt	Regulatory sandbox trials, automated compliance auditing
Organizational	Misalignment in participation incentives	Low-quality contributions or free-riding behavior	Weighted aggregation, governance via smart contracts
Reputational	Perceived data leakage through metadata sharing	Loss of client trust, negative media attention	Secure multiparty computation, differential privacy layers

5. Optimizations and Solutions for Financial FL Systems

In order to convert the federated learning technology into a usable solution to be deployed in financial ecosystems, various optimizations are required: the focus is on communication, security, model architecture, and system design. Such improvements are not only necessary to enhance the models but also to make them scalable and compliant with regulatory requirements in production environments. Efficient communication is one of the essential optimizations in FL. Pruning, quantization, and smartification models are used to greatly decrease transmitted updates by transmitting only essential components of gradients or compressed model parameters. This reduces bandwidth use by a significant margin while maintaining the necessary dynamics of learning [30]. Specifically, by making the federated optimization strategies asynchronous, the clients can perform the updates to the global model without relying on all peers, therefore alleviating the effects of stragglers and network fluctuation.

The common FedAvg, however, is nevertheless vulnerable to heterogeneous data settings. Adaptive algorithms such as FedProx and Scaffold insert a regularization term and control variates, correspondingly, to adjust to client drift and maintain stable convergence in non-IID conditions [19]. Through these improvements, there is a better chance of realizing fair learning, especially by small institutions where accumulated data cannot relate to larger financial entities. Optimization of security is also essential. Secure aggregation protocols can be incorporated so that the server can compute global updates without accessing individual model gradients, thereby preserving data privacy, even when using untrusted intermediaries. Even though homomorphic encryption and differential privacy can provide a mathematical guarantee against data leakage, they are computationally intensive. Therefore, cross-platform privacy-preserving frameworks that dynamically assign cryptographic resources based on data sensitivity and risk profile have become popular [22] [24]. To enhance system robustness, architectural redundancies can be implemented, e.g., through hierarchical or cross-device FL arrangements. Hierarchical FL also enables regional aggregators to do intermediate fusions of the models, where latency is reduced, and fault tolerance is guaranteed by localizing the failures to the regional pipeline. Moreover, in order to minimize the likelihood of collusion or random defaulter, the system could be made less vulnerable to the possibility of such an occurrence by client sampling mechanisms that assure the diversity and redundancy of participation. In the context of trust and governance, blockchain-based audit layers have been proposed to maintain immutable records of who attended and what changes were made to the model. These are capable of promoting transparency and conflict resolution among multi-party co-operations. Smart contracts can also auto-enforce compliance by dynamically limiting usage or participation according to legal thresholds and organizational policies set up in advance [26].

Concerning model architecture, vertically partitioned and modular structures are especially relevant when various institutions have different feature sets for the same users. Vertical Federated Learning (VFL) enables collaborative learning among such institutions without exchanging information, making it particularly applicable to joint risk scoring, fraud detection, and other sensitive financial analytics activities [15]. Also, attention-based architectures and federated multi-task learning approaches can enable the modelling of client-specific behavioural patterns whilst maintaining the overall quality of global models. Moreover, performance-monitoring mechanisms tailored to federated learning environments can be used to track training dynamics, detect anomalies, and assess system health in real time. These features cannot be compromised in production-level financial services, where operational failures are completely unacceptable, and systems must always deliver high-quality services and adhere to strict regulations. By combining these architectural and operational optimizations, federated learning can become a solid base for smart and privacy-conscious financial analytics. Nevertheless, the sustainability and institutional internalization of such technically optimized systems in the long term is not only due to sustained innovation but also due to the need to have coordinated governance formations, compliance enforcement, and mutually-trusted systems among participating financial institutions. The latter institutional component is the subject of the next section of the work, which analyses models of collaborative governance and regulatory compliance in federated finance.

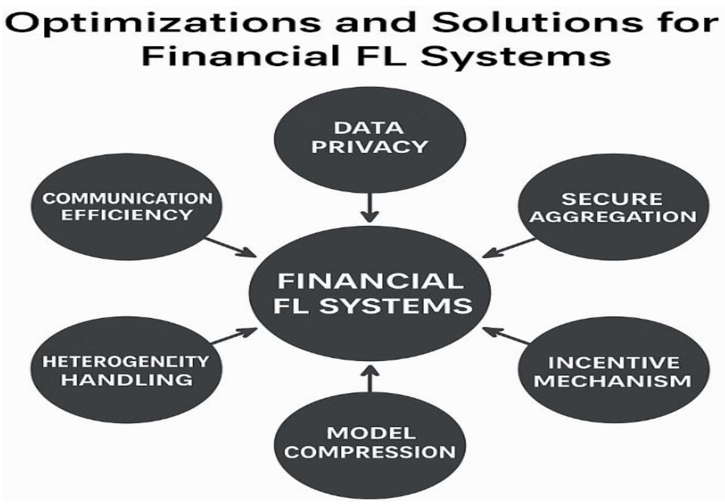

Fig. 2: Circular Diagram Illustrating Key Optimizations and Solutions in Financial Federated Learning (FL) Systems, Including Privacy, Efficiency, and Model Management Strategies.

6. Collaborative Governance and Compliance Models in Federated Finance

Federated learning is increasingly becoming a reality, and an effective collaborative governance model ensures it is implemented effectively, especially in heavily regulated industries like finance. Although the technical implementation can be used to guarantee the safe transfer of the parameters of the model and safeguard the sensitive client data, legal and organizational structures of these interactions should also be clear and exposed. A common compliance and trust framework should be institutionalized in distributed financial ecosystems where several financial institutions develop the models in a decentralized manner with no central authority in place to avoid legal, moral, and operational conflicts [25 - 27]. Federated learning demands that all parties involved have to agree with one another on data ownership, model ownership, liability procedures, and breach mitigation plans. To deal with this complexity, formalized contracts, regulatory sandboxes, and automation tools of compliance have become the subject of interest. The regulatory sandboxes, specifically, provide a well-regulated space to test the FL deployment and fail-safe to follow national and international set standards and policies like the GDPR, Basel III, and CCPA [3] [4] [25]. These frameworks also allow regulators to serve as observers or validators, ensuring real-time control without impeding innovation in the federated ecosystem [24] [25].

Collaborative governance may also be enhanced by smart contracts running on blockchain infrastructure. They can set rules of participation, compliance limits, and performance benchmarks, leaving little need for manual guidance or legal action [26]. Furthermore, to update FL models, third-party auditors can be integrated into the FL lifecycle to audit the integrity of model updates and ensure that privacy assurances are maintained throughout the training rounds [28]. New work has also considered the concept of federating governance, which can enable its decentralization to have participants vote on specific model changes or policies to include clients using weighted consensus algorithms. These mechanisms promote democratic input and minimize the control over the global model by larger institutions, which are likely to discriminate against others [27]. Also, immutable logging of training iterations provides audit trails, enabling traceability and accountability that support legal discovery and other internal risk reviews [29].

Although there are still no international benchmarks for FL in finance. With the increased cross-border work, harmonization of the laws on data protection is a necessity. Global, federated finance compliance might facilitate compliance by participating institutions with the most demanding law of their home jurisdiction, thereby easing cross-border legal integration and reducing deployment complexity. Such collaborative governance approaches not only address regulatory concerns but also create the context for more scalable and sustainable FL systems in the financial sector. Since trust and compliance will be institutionalized with the help of shared governance, FL would be a pillar of financial innovation and resilience.

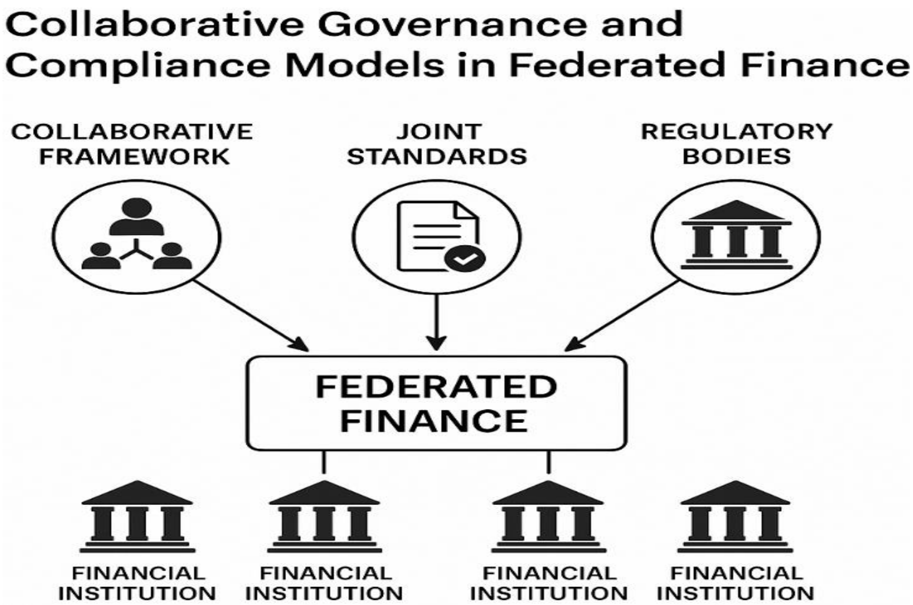

Fig. 3: Diagram Depicting Collaborative Governance and Compliance Models in Federated Finance, Highlighting the Integration of Frameworks, Standards, and Regulatory Bodies to Guide Financial Institutions.

7. Real-world Case Studies and Applications of Federated Learning in Finance

In order to convert the theoretical advantages of federated learning into financial gain, a number of financial organizations and consortia started pilot FL projects in the real world. These case studies provide vital insights into the possibilities and constraints of implementing FL to scale in real-world financial domains. Fraud detection is one of the most notable fields of application. Given that fraud patterns are common across institutions, a model trained via FL can be highly effective at improving detection accuracy, while still allowing banks to retain ownership of customer information. In the real world, FL-enhanced fraud models have proved superior to siloed models in recall, response time, and false positives [5] [6] [10]. Such systems are also being implemented in a consortium-based system where a group of banks works together to establish a common fraud intelligence network.

Credit scoring has also proven a good candidate for FL adoption, especially in underserved or thin-file customer segments. Aggregated credit profiles provide a results-based indication of financial conduct in situations where consumers are connected to multiple financial mechanisms, including banks, microfinance institutions, and digital wallets. Vertical Federated Learning (VFL) enables this by allowing entities to train models on partitioned features, enabling more accurate credit decisions with strong data privacy [15] [30]. Portfolio optimization and market prediction using federated learning have also become an application of these companies to investment management firms. The FL models generally can generalize across various economies since they are pools of different geographies and market conditions, with their views on the same views. The additional benefits of these models are that they are more robust and less prone to overfitting than traditional, locally trained models [20].

Besides the operational enhancements, these implementations have also established best practices for deployment architecture, client selection, and performance measurement. For example, dynamic client sampling reduced model drift and enabled fast convergence in highly variable environments [19] [30]. On the same lines, the application of performance-weighted aggregation, where clients' contributions are weighted by data quality or past performance, has helped strike the right balance between model fairness and efficiency. Nonetheless, obstacles to success still exist despite such achievements. Practical applications still struggle with unstable internet connections, limited client access, and regulatory opposition to metadata disclosure. However, based on the case studies trend, it may be concluded that with planning and optimization, it is possible to bring federated learning into production in mission-critical financial implementations. These case studies can guide broader adoption of FL in the financial industry by demonstrating successful implementations and outlining key considerations in practice. They further offer empirical support for the theoretical issues discussed in the preceding sections, hence making the research meet practice.
To supplement the story about practical applications, Table 2 provides a comparative study of pilot FL projects in finance on the scope of application, involved entities, technical setup, and reported results. This developmental case demonstrates the viability and scalability of FL in production financial systems.

Table 2: Comparative Overview of Real-World FL Implementations in Finance

Use Case	Participants	FL Type	Model Type	Reported Benefit
Fraud Detection	Consortium of 5 retail banks	Cross-silo FL	LSTM with attention	18% increase in early fraud detection accuracy
Credit Scoring	Bank + Microfinance provider	Vertical FL (VFL)	Logistic Regression	25% improvement for thin-file customers
AML (Anti-Money Laundering)	Global investment firms	Cross-silo FL	Graph Neural Networks	Enhanced anomaly identification across networks
Portfolio Optimization	Hedge funds in different regions	Hybrid FL (cross-silo + VFL)	Reinforcement Learning	Reduced model overfitting and improved returns

8. Conclusion and Future Outlook

Federated learning offers a first-of-its-kind opportunity to leverage the collective intelligence of distributed financial institutions while maintaining data sovereignty and privacy. Its learning capacity over decentralized sensitive information without central amalgamation fits hand in glove with priorities of trust, compliance, and security of operations within the financial sector. Nonetheless, its implementation is not that easy. As mentioned, in the area of finance, FL systems will have to deal with data heterogeneity, communication overhead, security threats, trust dynamics, and regulatory issues. The future of FL in finance is based on the emergence of new optimization methods that better fit financial infrastructures, as well as on partnership decisions that assure reliability and responsibility between institutions. New technologies such as blockchain, secure multiparty computation, and vertical FL architectures have significant potential to improve the existing shortcomings. We shall also consider the institutional readiness in terms of technical and organizational aspects that will be important to integrate FL into the mainstream.
The future will see further development of modular and composable FL ecosystems with financial institutions able to plug in to federated infrastructures as they wish, with standardized protocols, interoperable components, and real-time governance systems. These innovations will not only translate into tomorrow, opening new ways of doing financial intelligence, but will also reset the data collaboration paradigm within regulated businesses. Even when federated learning in finance finally becomes the technology of choice, it may still be a form of structural rethinking, as it forces institutions to rethink their interactions in terms of collaboration, competition, and compliance in a highly digital, data-heavy world.

References

[1] Matschinske, J., Späth, J., Bakhtiari, M., Probul, N., Kazemi Majdabadi, M. M., Nasirigerdeh, R., ... & Baumbach, J. (2023). The FeatureCloud platform for federated learning in biomedicine: unified approach. *Journal of Medical Internet Research*, 25, e42621. https://doi.org/10.2196/42621.
[2] Moshawrab, M., Adda, M., Bouzouane, A., Ibrahim, H., & Raad, A. (2023). Reviewing federated learning aggregation algorithms, strategies, contributions, limitations, and future perspectives. *Electronics*, 12(10), 2287. https://doi.org/10.3390/electronics12102287.
[3] Chen, X., Ji, J., Luo, C., Liao, W., & Li, P. (2018, December). When machine learning meets blockchain: A decentralized, privacy-preserving, and secure design. In *2018 IEEE International Conference on Big Data (Big Data)* (pp. 1178-1187). IEEE. https://doi.org/10.1109/BigData.2018.8622598.
[4] Gill, M., & Singh, D. (2021). A comprehensive study of simulation frameworks and research directions in fog computing. *Computer Science Review*, 40, 100391. https://doi.org/10.1016/j.cosrev.2021.100391.
[5] Long, G., Tan, Y., Jiang, J., & Zhang, C. (2020). Federated learning for open banking. In *Federated Learning: Privacy and Incentive* (pp. 240-254). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-63076-8_17.
[6] Yang, W., Zhang, Y., Ye, K., Li, L., & Xu, C. Z. (2019). FFD: A federated learning based method for credit card fraud detection. In *Big Data–BigData 2019: 8th International Congress* (pp. 18-32). Springer International Publishing. https://doi.org/10.1007/978-3-030-23551-2_2.
[7] Tang, Y., Liu, J., & Chen, W. (2021). Exchange, adopt, evolve: Modeling the spreading of opinions through cognition and interaction in a social network. *Information Sciences*, 551, 1-22. https://doi.org/10.1016/j.ins.2020.11.043.
[8] Zhang, Y., Zeng, D., Luo, J., Xu, Z., & King, I. (2023, April). A survey of trustworthy federated learning with perspectives on security, robustness and privacy. In *Companion Proceedings of the ACM Web Conference 2023* (pp. 1167-1176). https://doi.org/10.1145/3543873.3587681.
[9] Zhuang, W., Chen, C., & Lyu, L. (2023). When foundation model meets federated learning: Motivations, challenges, and future directions. *arXiv preprint arXiv:2306.15546*.
[10] Lee, C. M., Fernández, J. D., Menci, S. P., Rieger, A., & Fridgen, G. (2023, January). Federated learning for credit risk assessment. In *HICSS* (pp. 386-395). https://doi.org/10.24251/HICSS.2023.048.
[11] Labati, R. D., Piuri, V., Rundo, F., & Scotti, F. (2022). Photoplethysmographic biometrics: A comprehensive survey. *Pattern Recognition Letters*, 156, 119-125. https://doi.org/10.1016/j.patrec.2022.03.006.
[12] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine*, 37(3), 50-60. https://doi.org/10.1109/MSP.2020.2975749.
[13] Lim, W. Y. B., Ng, J. S., Xiong, Z., Jin, J., Zhang, Y., Niyato, D., ... & Miao, C. (2021). Decentralized edge intelligence: A dynamic resource allocation framework for hierarchical federated learning. *IEEE Transactions on Parallel and Distributed Systems*, 33(3), 536-550. https://doi.org/10.1109/TPDS.2021.3096076.

[14] Jiang, L. (2021). A fast and accurate circle detection algorithm based on random sampling. *Future Generation Computer Systems*, 123, 245-256. https://doi.org/10.1016/j.future.2021.05.010.
[15] Zhang, H., Zou, Y., Yin, H., Yu, D., & Cheng, X. (2024). CCM-FL: Covert communication mechanisms for federated learning in crowd sensing IoT. *Digital Communications and Networks*, 10(3), 597-608. https://doi.org/10.1016/j.dcan.2023.02.013.
[16] Campos, P., Hernández-Solana, Á., & Valdovinos-Bardají, A. (2020). Analysis of hidden node problem in LTE networks deployed in unlicensed spectrum. *Computer Networks*, 177, 107280. https://doi.org/10.1016/j.comnet.2020.107280.
[17] Liu, T., Wang, Z., He, H., Shi, W., Lin, L., An, R., & Li, C. (2023). Efficient and secure federated learning for financial applications. *Applied Sciences*, 13(10), 5877. https://doi.org/10.3390/app13105877.
[18] Jimeno, J., Roy, M., & Tortora, C. (2021). Clustering mixed-type data: A benchmark study on KAMILA and k-prototypes. In *Data Analysis and Rationality in a Complex World 16* (pp. 83-91). Springer International Publishing. https://doi.org/10.1007/978-3-030-60104-1_10.
[19] Leevi, E. (2025). *Model Distillation in Federated Learning for Human Action Recognition*.
[20] Xue, J., Qu, Z., Xu, J., Liu, Y., & Lu, Z. (2023). Bandwidth allocation for federated learning with wireless providers and cost constraints. *IEEE Transactions on Mobile Computing*, 23(6), 7470-7482. https://doi.org/10.1109/TMC.2023.3335258.
[21] Zhang, P., Gan, P., Kumar, N., Hsu, C. H., Shen, S., & Li, S. (2022). RKD-VNE: Virtual network embedding algorithm assisted by resource knowledge description and deep reinforcement learning in IIoT scenario. *Future Generation Computer Systems*, 135, 426-437. https://doi.org/10.1016/j.future.2022.05.008.
[22] Sikandar, H. S., Waheed, H., Tahir, S., Malik, S. U., & Rafique, W. (2023). A detailed survey on federated learning attacks and defenses. *Electronics*, 12(2), 260. https://doi.org/10.3390/electronics12020260.
[23] Chen, C., Liu, J., Tan, H., Li, X., Wang, K. I. K., Li, P., ... & Dou, D. (2025). Trustworthy federated learning: privacy, security, and beyond. *Knowledge and Information Systems*, 67(3), 2321-2356. https://doi.org/10.1007/s10115-024-02285-2.
[24] Ali, F., & Khusro, S. (2021). Content and link-structure perspective of ranking webpages: A review. *Computer Science Review*, 40, 100397. https://doi.org/10.1016/j.cosrev.2021.100397.
[25] Balakrishnan, A. (2024). Leveraging artificial intelligence for enhancing regulatory compliance in the financial sector. *International Journal of Computer Trends and Technology*.
[26] Javed, A. R., Hassan, M. A., Shahzad, F., Ahmed, W., Singh, S., Baker, T., & Gadekallu, T. R. (2022). Integration of blockchain technology and federated learning in vehicular (IoT) networks: A comprehensive survey. *Sensors*, 22(12), 4394. https://doi.org/10.3390/s22124394.
[27] Knol, W. J. H. (2025). *Strategic AI Deployment in Decentralized Organizations, Balancing Central Oversight with Local Flexibility* (Master's thesis, University of Twente).
[28] Pillutla, K., Kakade, S. M., & Harchaoui, Z. (2022). Robust aggregation for federated learning. *IEEE Transactions on Signal Processing*, 70, 1142-1154. https://doi.org/10.1109/TSP.2022.3153135.
[29] Das, S., Donini, M., Gelman, J., Haas, K., Hardt, M., Katzman, J., ... & Zafar, B. (2021). Fairness measures for machine learning in finance. https://doi.org/10.3905/jfds.2021.1.075.
[30] Shahid, O., Pouriyeh, S., Parizi, R. M., Sheng, Q. Z., Srivastava, G., & Zhao, L. (2021). Communication efficiency in federated learning: Achievements and challenges. *arXiv preprint arXiv:2107.10996*. https://doi.org/10.3390/app12188980.