Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Federated Intelligence in Financial Ecosystems: A Privacy-Preserving AI Framework for Cross-Border Risk Analysis

Sreenivasulu Gajula
Independent Researcher, USA

ARTICLE INFO

Received: 10 Aug 2025
Revised: 15 Sept 2025
Accepted: 24 Sept 2025

ABSTRACT

Federated Learning Cross-Buster represents a transformative paradigm for financial risk analysis, which enables institutions to train the training machine learning models cooperatively, maintaining data sovereignty and regulatory compliance in many courts. The architecture addresses the fundamental stress between analytical sophistication and privacy protection, which allows distributed client nodes to undergo local model training on the dataset, and shares only encrypted model parameters rather than raw financial data. This structure naturally satisfies the data localization requirements imposed by rules such as GDPR and PIPL, while facilitating the conclusion of credits, fraud detection, market risk analysis, and the necessary refined pattern recognition for operational risk management. Differential privacy mechanisms and safe aggregation protocols provide mathematical guarantees against attacks, estimate attacks, and model toxicity, although implementation challenges arise from data inequality in institutions, lack of communication efficiency in international networks, and model clarity in regulatory contexts. Algorithm innovation production, including non-IID data distribution, gradient compression technology for bandwidth adaptation, and federated learning to handle blockchain-based audit trails for governance, shows the practical feasibility of federated intelligence in innovation production financial systems. The convergence of privacy-conservation calculation, distributed adaptation, and regulatory technology establishes federated learning as an essential infrastructure for the next generation of financial risk management in the rapidly connected global markets.

Keywords: Federated Learning, Financial Risk Management, Privacy-Preserving Machine Learning, Cross-Border Compliance, Distributed Artificial Intelligence

1. Introduction

Although the globalization of financial markets has opened up hitherto unheard-of chances for capital flows and economic development, it has also presented difficult problems in regulatory compliance and risk management. Financial institutions with operations across several countries have the conflicting need of doing a thorough risk assessment while adhering to ever stricter data protection legislation, such as strict data protection rules like the California Consumer Privacy Act (CCPA) in the European Union and the General Data Protection Regulation (GDPR)in the United States. Conventional centralized machine learning techniques that demand gathering sensitive financial information in one location have become impractical in this regulatory scene, with under GDPR, non-compliance carries fines of up to 4% of annual worldwide turnover. Effective risk models need varied datasets across many geographic and regulatory boundaries, yet modern privacy policies explicitly forbid the unrestrained centralization and transfer of such highly classified data.

Emerging as a transformational paradigm, federated learning tackles this basic conflict between analytical complexity and privacy preservation. Federated learning lets several parties cooperate in training

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

machine learning models while preserving data ownership, unlike conventional machine learning architectures that demand data centralization. Every participating school trains the model on its own local database and shares only model parameters or gradient updates instead of actual data. Research by Konečný et al. It has been demonstrated that structured updates and sketched updates can reduce communication costs by two orders of magnitude compared to baseline federated optimization, with structured updates achieving compression ratios between 100:1 and 1000:1 through the use of random rotation, quantization, and subscription techniques [1]. Their empirical analysis on deep neural networks has shown that learning time can be reduced by up to 99% with a 99% reduction in communication bandwidth through the strategic application of gradient sparsification, where only the most significant 1% of gradient values are transmitted during each training round, thereby addressing both the practical constraints of cross-border network communication in financial systems and the cost of communication. This approach naturally aligns with the principle of data minimization underlying contemporary privacy law while facilitating the cross-border collaboration necessary for comprehensive risk assessment.

The financial sector presents unique requirements for federated learning implementation. The heterogeneity of data sources, varying regulatory frameworks across jurisdictions, and the critical need for model interpretability in compliance contexts distinguish financial applications from other federated learning domains. Yang et al. provide a comprehensive taxonomy demonstrating that federated learning architectures can be classified into horizontal federated learning, where institutions share the same feature space but different sample spaces, vertical federated learning, where participants possess different feature spaces for overlapping samples, and federated transfer learning for scenarios with minimal overlap in both features and samples [2]. Their analysis of real-world implementations in financial services reveals that horizontal federated learning configurations, most applicable to multi-branch banking networks and international payment consortia, can achieve model convergence with communication rounds reduced to between 50 and 200 iterations compared to thousands required in traditional distributed learning approaches. Moreover, the adversarial nature of financial fraud and the sophistication of money laundering operations demand robust security mechanisms that extend beyond basic privacy guarantees. This article examines the theoretical foundations, architectural considerations, and practical implementations of federated learning frameworks specifically designed for cross-border financial risk analysis, with particular attention to privacy preservation and regulatory compliance mechanisms.

Strategy	Compression Method	Architecture Type	Bandwidth Impact
Structured Updates	Random rotations with quantization	Horizontal federated learning	Two orders of magnitude reduction
Sketched Updates	Gradient sparsification	Vertical federated learning	Minimal transmission requirements
Communication Round Optimization	Strategic parameter exchange timing	Multi-branch networks	Substantially reduced iterations
Federated Learning Taxonomy	Feature and sample space classification	Horizontal, vertical, transfer variants	Application-specific optimization

Table I: Communication Efficiency Strategies in Federated Learning [1][2]

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2. Architectural Foundations of Federated Financial Intelligence

The architecture of federated learning systems for financial ecosystems must accommodate the structural complexities inherent in multi-jurisdictional operations. At its core, the framework consists of distributed client nodes representing individual financial institutions or regional branches, a central aggregation server responsible for coordinating model updates, and secure communication channels that ensure confidentiality and integrity during parameter exchange. Each client node maintains complete control over its local data repository, which may include transaction records, customer profiles, credit histories, and market data specific to its operational jurisdiction. McMahan et al. introduced the Federated Averaging algorithm as a foundational approach to distributed optimization, demonstrating through extensive empirical evaluation that models trained on datasets partitioned across multiple clients can achieve convergence comparable to centralized training [3]. Their experiments on the MNIST dataset with 100 clients showed that FedAvg achieved 99% test accuracy after 1,200 communication rounds when clients performed five local epochs of training with batch size 10, compared to baseline federated stochastic gradient descent requiring significantly more rounds, illustrating the computational efficiency gains achievable through increased local computation before parameter aggregation in financial network architectures.

The model training process follows an iterative protocol wherein the central server initializes a global model and distributes it to participating clients. Each client then performs local training using its proprietary dataset, computing gradient updates or model parameters through standard optimization algorithms such as stochastic gradient descent. Critically, only these computed parameters—not the underlying data—traverse the network to the aggregation server. The server employs aggregation algorithms, most commonly federated averaging, to synthesize the local updates into an improved global model, which is subsequently redistributed to clients for the next training iteration. McMahan et al. demonstrated that when only a fraction of clients participate in each round, specifically 10% random sampling from a population of 1,000 clients, the algorithm maintains robust convergence properties while reducing coordination complexity [3]. Their analysis on convolutional neural networks for image classification revealed that client learning rates between 0.01 and 0.1, combined with appropriately tuned momentum parameters around 0.9, enable stable convergence even under highly non-IID data distributions where each client possesses data from only two distinct classes, a scenario directly analogous to financial institutions specializing in particular market segments or geographical regions with distinct customer demographics and transaction patterns.

However, the naive implementation of this protocol reveals vulnerabilities that are particularly concerning in financial contexts. Gradient updates, while not raw data, can leak sensitive information through various inference attacks. Differential privacy mechanisms address this concern by introducing carefully calibrated noise into the shared parameters, providing mathematical guarantees that individual data points cannot be reconstructed from model updates. Geyer et al. present a rigorous framework for client-level differential privacy in federated learning, establishing that privacy guarantees can be achieved through moment accountant methods with noise calibration based on the sensitivity of gradient computations [4]. Their theoretical analysis demonstrates that for deep neural networks with a gradient clipping threshold C equals 4.0 and a noise multiplier sigma equals 0.004, training for 3,000 rounds with sampling probability 0.01 achieves epsilon equals 8.0 differential privacy guarantee, while maintaining model accuracy degradation of less than 2% compared to non-private baselines on standard benchmarks. The implementation of differential privacy in federated financial systems requires balancing the privacy budget—measured by the epsilon parameter—against model utility, a trade-off that becomes more complex when dealing with the high-dimensional feature spaces typical of financial risk models. Geyer et al. further established that increasing the number of participating clients from 100 to 1,000 while

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

maintaining a constant privacy budget allows for proportionally stronger privacy protection per individual client, with privacy guarantees improving by factors corresponding to the square root of client population size [4]. These findings indicate that large-scale financial consortia comprising hundreds of institutions can achieve robust privacy protection while maintaining predictive accuracy sufficient for credit scoring, fraud detection, and risk assessment applications where model AUC scores above 0.85 represent commercially viable performance thresholds.

Component	Configuration	Privacy Mechanism	Performance Impact
Client Sampling	Random selection per round	Privacy amplification	Maintained convergence
Local Training	Multiple epochs before transmission	Client-level aggregation	Reduced communication frequency
Gradient Clipping	Threshold bounding	Sensitivity control	Minimal accuracy degradation
Privacy Budget	Epsilon parameter management	Moment accountant methods	Stronger guarantees at scale

Table II: Federated Averaging and Differential Privacy Integration [3][4]

3. Cross-Jurisdictional Compliance and Regulatory Alignment

The regulatory landscape that controls borders across financial data analysis presents a maze challenge that the federated learning framework must navigate with accuracy. Different jurisdictions apply different requirements about data localization, border transfer sanctions, and consent mechanisms. The GDPR, for instance, restricts the transfer of personal data outside the European Economic Area unless adequate safeguards are in place, while China's Personal Information Protection Law (PIPL) mandates localization of critical data within Chinese territory. Federated learning's architecture inherently addresses many of these concerns by eliminating the need for data transfer, yet the movement of model parameters and the collaborative nature of training still require careful legal analysis. Hard et al. demonstrated the practical viability of federated learning for privacy-sensitive applications through their implementation of Gboard mobile keyboard prediction, where models were trained across millions of devices without centralizing user typing data [5]. Their system processed over 1.5 million user contributions per training round, with each device performing between 3 and 10 local epochs on recently typed text before contributing encrypted model updates to the aggregation server, achieving word prediction accuracy improvements of 13.0% in recall at rank three and 8.6% in recall at rank one compared to server-trained baselines, while maintaining strict user-level differential privacy with epsilon values between 2.7 and 6.5 computed using Rényi differential privacy accounting with order alpha equals 32.

Regulatory compliance in the Federated Financial System extends beyond data security to include sector-specific requirements. Anti-money laundering regulations mandate suspicious activity reporting and customer due diligence processes that rely on pattern recognition in transactions. The Bank Secrecy Act in the United States and the Fourth Anti-Money Laundering Directive in the European Union impose obligations that require sophisticated analytical capabilities, yet these must be achieved without creating centralized databases that violate privacy principles. Federated learning enables financial institutions to collectively improve their AML detection models by learning from distributed transaction patterns while maintaining the confidentiality of individual customer information. Hard et al. established that federated optimization with secure aggregation protocols introduces computational overhead of approximately 30-

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

50% compared to non-private federated training, yet this overhead remains acceptable given that their production system successfully trained recurrent neural network models with 1.4 million parameters across heterogeneous device populations where only 5-10% of selected clients completed each training round due to connectivity constraints and device availability [5]. Their empirical results showed that client sampling strategies selecting between 50 and 500 devices per round from pools of tens of thousands of eligible participants maintained convergence properties while distributing privacy risk across the client population, with the total privacy budget consumed over 500 to 2,000 training rounds remaining within acceptable thresholds for applications handling sensitive personal information subject to regulatory oversight.

System Aspect	Technology	Governance Mechanism	Compliance Feature
Distributed Processing	Device-level training	User-level privacy control	GDPR consent alignment
Secure Aggregation	Encrypted transmission	Smart contract enforcement	Purpose limitation
Audit Trail	Blockchain recording	Immutable timestamps	Regulatory accountability
Participant Management	Dynamic sampling	Permissioned ledger access	Cross-jurisdictional verification

Table III: Production-Scale Implementation and Governance [5][6]

4. Risk Analysis Applications in Multi-Tenant Financial Systems

Financial risk analysis benefits from federated learning's practical application in a number of spheres, each with distinct operational difficulties and technical requirements. Credit risk assessment is one example. The potential of a federated approach in situations where information asymmetry usually obstructs proper risk pricing. Banks working in different regions have insightful views on how privacy issues and competitive dynamics limit direct data sharing; federated learning lets these organizations train credit ratings together. Borrower behavior in their region. Models combining several geographical and demographic trends improve prediction accuracy while preserving data sovereignty. Lee et al. provide an exhaustive study of federated learning. Difficulties showing statistical heterogeneity among patients—that is, where data distribution differs significantly between participating institutions—may lower convergence rates by ten to 100 times. Relative to centralized learning environments [7]. Their empirical evaluations on non-IID partitions of standard datasets showed that when data is partitioned by class with only 2 classes per client out of 10 total classes, standard Federated Averaging required 5,000 communication rounds to achieve 80% test accuracy compared to 500 rounds for IID partitions, illustrating the profound impact of data heterogeneity on federated credit scoring models where regional banks may specialize in distinct borrower segments with divergent risk profiles, necessitating algorithmic innovations such as FedProx which introduces proximal terms with mu values typically between 0.001 and 1.0 to limit divergence between local and global models.

Market risk analysis benefits particularly from federated learning's capacity to synthesize perspectives across disparate trading venues and geographical markets. Systemic risk calls for analytical systems capable of spotting weaknesses and linkages free from centralized repositories of sensitive trading data. Early-warning models trained by central banks and regulatory authorities that make use of transaction

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

data from several institutions help to identify developing systemic weaknesses while honoring the privacy of personal trading approaches and positions. Li et al. documented that system heterogeneity, encompassing variations in storage, computational, and communication capabilities across participating devices, introduces significant practical challenges with their experiments showing that stragglers—the slowest 10% of clients—can increase wall-clock training time by factors of 3 to 5 compared to scenarios where all clients complete local training within similar timeframes [7]. Their proposed asynchronous federated optimization approaches allow faster clients to contribute more frequently, with weighted averaging schemes that discount contributions from stale model versions by factors proportional to staleness, maintaining convergence guarantees while reducing total training time by 40-60% in heterogeneous financial networks where some institutions operate high-performance computing clusters while others rely on standard server infrastructure with computational capacity differences spanning two orders of magnitude.

Fraud detection represents perhaps the most compelling application domain for federated financial intelligence. The sophistication of modern financial fraud necessitates continuous model updating to counter evolving attack vectors. However, the effectiveness of fraud detection depends critically on the diversity and volume of training data. Liu et al. present a secure federated transfer learning framework specifically designed for financial applications, demonstrating through experiments on cross-bank fraud detection that their system achieved AUC scores of 0.891 when training gradient boosting models across simulated banking consortia comprising 5 to 10 participating institutions [8]. Their architecture incorporated homomorphic encryption for secure gradient aggregation with Paillier cryptosystem using 2048-bit keys, introducing computational overhead of approximately 100 to 200 times compared to plaintext operations, yet achieving total training completion within 8 to 12 hours for models with 500 trees and maximum depth of 6, processing datasets containing 100,000 to 500,000 transaction records per institution with fraud prevalence rates between 0.1% and 0.8%, representative of real-world payment card fraud scenarios.

Operational risk management similarly benefits from federated learning's collaborative paradigm. Liu et al. demonstrated that their framework maintained differential privacy guarantees with epsilon equals 5.0 through Gaussian noise addition calibrated to gradient L2 sensitivity bounds of 1.0, achieving model accuracy within 3-5% of non-private baselines while providing provable protection against model inversion attacks [8].

Risk Domain	Heterogeneity Source	Training Solution	Security Method
Credit Scoring	Divergent demographics	FedProx regularization	Homomorphic encryption
Systemic Risk	Market condition variations	Asynchronous optimization	Byzantine-robust aggregation
Fraud Detection	Geographical attack patterns	Secure gradient boosting	Differential privacy
Operational Risk	Institution-specific failures	Weighted averaging	Cryptographic key protection

Table IV: Heterogeneity in Financial Risk Applications [7][8]

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5. Technical Challenges and Emerging Solutions

Despite its theoretical elegance and regulatory advantages, the practical implementation of federated learning in financial ecosystems confronts substantial technical challenges. Data heterogeneity across participating institutions poses perhaps the most fundamental obstacle. Financial institutions operate with different data schemas, feature definitions, and labeling conventions—a circumstance termed non-IID (non-independent and identically distributed) data in machine learning literature. This heterogeneity can cause model divergence during federated training, where local updates pull the global model in conflicting directions, ultimately degrading performance below that of models trained on homogeneous centralized data. Li et al. demonstrate through extensive empirical analysis that data heterogeneity fundamentally impacts federated learning convergence, with experiments showing that FedAvg accuracy on CIFAR-10 degraded from 83.5% under IID conditions to 67.2% when data was partitioned by a Dirichlet distribution with concentration parameter alpha equals 0.5, representing moderate heterogeneity comparable to financial institutions serving demographically distinct customer bases [9]. Their proposed FedProx algorithm, which adds a proximal term to the local objective function with hyperparameter mu typically set between 0.01 and 1.0, demonstrated robustness to heterogeneity by limiting divergence between local and global models, achieving 78.4% accuracy on the same heterogeneous partition, recovering approximately 75% of the performance loss while requiring only marginal increases in communication rounds from 200 to 240 iterations, making it particularly suitable for credit risk models where regional banks exhibit statistical heterogeneity quantified by Earth Mover's Distance values between 0.4 and 0.9 across participant data distributions.

Several algorithmic innovations address this challenge through personalized federated learning approaches that allow each institution to maintain institution-specific model components while sharing generalizable layers with the federation. Li et al. established that system heterogeneity, where participating devices exhibit varying computational capabilities and network connectivity, introduces additional complexities with their measurements showing that in mobile device deployments, computation times for a single training epoch varied by factors of 5 to 10 across device types, while network upload times ranged from seconds to minutes depending on connection quality [9]. Their asynchronous federated optimization framework addressed these challenges by allowing faster clients to contribute more frequently, implementing weighted averaging schemes where contributions from models with staleness tau rounds are weighted by factors of (1 - 0.01tau), effectively discounting stale updates while maintaining convergence guarantees that bound the suboptimality gap to values proportional to staleness variance, critical for international financial consortia where institutions in developed markets operate data centers with computational throughput measured in teraflops while emerging market participants may rely on infrastructure with capacities one to two orders of magnitude lower.

Communication efficiency emerges as another critical constraint, particularly when federated learning extends across continents with varying network infrastructure quality. Gradient compression techniques reduce communication overhead by transmitting only the most significant parameter updates through methods such as top-k selection or random sparsification. Bonawitz et al. present a practical secure aggregation protocol enabling privacy-preserving federated learning at scale, demonstrating that their system successfully aggregated model updates from 1,000 to 10,000 clients with dropout tolerance supporting up to 50% client failures while maintaining cryptographic security guarantees [10]. Their implementation using double-masking with pairwise keys and threshold secret sharing achieved computational overhead of approximately 1.8 seconds per client for models containing 1.2 million parameters on commodity server hardware with 16 CPU cores, representing less than 10% of total round time when local training required 20-30 seconds per client, making secure aggregation practically viable

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

for financial fraud detection models with parameter counts ranging from 500,000 to 5 million that update on daily or weekly schedules.

The challenge of model poisoning attacks assumes particular gravity in financial contexts. Bonawitz et al. established that their protocol provides information-theoretic security, ensuring the server learns only the aggregate sum without accessing individual contributions, maintaining security even when up to one-third of participants behave maliciously, with formal proofs demonstrating that adversaries observing network traffic gain negligible information beyond what is revealed by the final aggregated model [10].

Conclusion

Federated learning establishes a foundational architecture for privacy-preserving artificial intelligence in global financial ecosystems, reconciling the inherent contradiction between comprehensive cross-border risk analysis and stringent data protection regulations that govern contemporary financial markets. The framework's capacity to enable collaborative model training without data centralization directly addresses regulatory requirements spanning multiple jurisdictions while delivering predictive performance approaching that of centralized alternatives across credit scoring, fraud detection, systemic risk identification, and operational risk quantification domains. Technical implementations incorporating differential privacy guarantees, secure multi-party computation protocols, and Byzantine-strong aggregation mechanisms demonstrate both the cryptographic hardness and computational feasibility required for production deployment in adversarial financial environments where model integrity and data confidentiality represent non-negotiable requirements. The persistent challenges of statistical and system heterogeneity across participating institutions, communication overhead in transcontinental network architectures, and imperatives for model interpretability in regulatory contexts drive algorithmic innovation in personalized federated learning, asynchronous optimization, and interpretable artificial intelligence techniques adapted to distributed settings. Emerging governance frameworks that leverage blockchain technology for immutable audit trails and smart contracts for automated compliance enforcement provide regulators with unprecedented transparency into collaborative training processes, while preserving the competitive confidentiality required for voluntary participation in federated consortia. The demonstrated convergence properties of algorithms such as FedProx and FedAVG under realistic non-IID data distributions, coupled with practical secure aggregation protocols capable of handling dropout rates and managing computational heterogeneity across thousands of participants, validate the operational readiness of federated learning for mission-critical financial applications. As regulatory frameworks are evolving toward greater emphasis on data minimization and purpose limitation principles, and as financial institutions face increasingly sophisticated fraud vectors and systemic vulnerabilities requiring collective intelligence, federal learning shifts from theoretical innovation to the necessary infrastructure, enabling both regulatory compliance and competitive advantage in interconnected global markets. The trajectory toward ubiquitous adoption depends critically on standardization efforts encompassing communication protocols, privacy accounting methods, and governance structures that facilitate interoperability across heterogeneous institutional technology stacks while maintaining the security properties and performance characteristics validated in controlled implementations. The integration of federated learning with complementary privacy-enhancing technologies, including trusted execution environments, zero-knowledge proofs, and quantum-resistant cryptographic protocols, positions the framework to address emerging threats while scaling to accommodate the data volumes, participant populations, and computational demands characteristic of global financial networks processing trillions of transactions annually across hundreds of jurisdictions with divergent regulatory philosophies and enforcement mechanisms.

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

References

[1] Jakub Konečný, et al., "Federated learning: Strategies for improving communication efficiency," arXiv, 2017. [Online]. Available: https://arxiv.org/abs/1610.05492
[2] Qiang Yang, et al., "Federated machine learning: Concept and applications," ACM Digital Library, 2019. [Online]. Available: https://dl.acm.org/doi/10.1145/3298981
[3] H. Brendan McMahan, et al., "Communication-efficient learning of deep networks from decentralized data," arXiv, 2023. [Online]. Available: https://arxiv.org/abs/1602.05629
[4] Robin Geyer, et al., "Differentially private federated learning: A client-level perspective," 2017. [Online]. Available: https://www.researchgate.net/publication/321963259_Differentially_Private_Federated_Learning_A_Client_Level_Perspective
[5] Andrew Hard, et al., "Federated learning for mobile keyboard prediction," arXiv, 2019. [Online]. Available: https://arxiv.org/abs/1811.03604
[6] Stacey Truex, et al., "A Hybrid Approach to Privacy-Preserving Federated Learning," Springer Nature Link, 2019. [Online]. Available: https://link.springer.com/article/10.1007/s00287-019-01205-x
[7] Tian Li, et al., "Federated learning: Challenges, methods, and future directions," IEEE, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9084352
[8] Yang Liu, et al., "A secure federated transfer learning framework," IEEE, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9076003
[9] Peter Kairouz, et al., "Advances and Open Problems in Federated Learning," IEEE, [Online]. Available: https://ieeexplore.ieee.org/document/9464278
[10] Keith Bonawitz et al., "Practical secure aggregation for privacy-preserving machine learning," ACM Digital Library,[Online]. Available: https://dl.acm.org/doi/10.1145/3133956.3133982