Journal of Information Systems Engineering and Management
2025, 10(30s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

AI and Federated Learning for Cross-Industry Data Collaboration: Applications in Finance, E-Commerce, and Medical Tech

[1]Sudhakar Reddy Peddinti, [2]Subba rao Katragadda, [3]Ajay Tanikonda,
[1]Independent Researcher, p.reddy.sudhakar@gmail.com
[2]Independent Researcher, subbakatragadda@gmail.com,
[3]Independent Researcher, ajay.tani@gmail.com,

ARTICLE INFO

Received: 31 Dec 2024

Revised: 20 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

Artificial Intelligence (AI) has revolutionized various industries by enabling data-driven decision-making, automation, and enhanced customer experiences. However, data privacy concerns and regulatory restrictions pose significant challenges in sharing and utilizing cross-industry data. Federated Learning (FL) emerges as a transformative solution that allows multiple stakeholders to collaboratively train machine learning models while preserving data privacy. This paper explores the role of AI and Federated Learning in fostering cross-industry data collaboration, focusing on applications in finance, e-commerce, and medical technology. It examines how FL enhances data security, improves predictive analytics, and drives innovation in these industries. The study also addresses key challenges, such as computational overhead, security vulnerabilities, and integration complexities. Furthermore, real-time and hypothetical data and case studies are presented to demonstrate the impact of FL in these sectors. Graphs and tables illustrate performance improvements, accuracy enhancements, and cost reductions achieved through AI-driven FL implementations. Finally, the paper discusses future directions and the potential of FL in shaping the next era of collaborative AI.

Keywords: Federated Learning, Artificial Intelligence, Data Privacy, Cross-Industry Collaboration, Finance, E-Commerce, Medical Technology

1. INTRODUCTION

The exponential growth of data across industries has created an unprecedented opportunity for AI-driven innovations. However, sharing and processing data across multiple organizations remain challenging due to privacy concerns, compliance regulations, and security risks. Traditional centralized machine learning approaches require data aggregation, increasing the likelihood of data breaches and regulatory violations. Federated Learning (FL), a decentralized AI technique, offers a promising solution by enabling collaborative model training without exposing raw data.

In finance, institutions rely on AI for fraud detection, risk assessment, and algorithmic trading. However, regulatory constraints such as GDPR and CCPA restrict financial institutions from sharing sensitive customer data. FL enables multiple banks to collaboratively train fraud detection models without violating privacy regulations. Similarly, e-commerce platforms benefit from AI-driven recommendation systems, customer sentiment analysis, and demand forecasting. With FL, different e-commerce firms can collaborate to improve recommendation algorithms while safeguarding proprietary consumer data.

Medical technology presents another domain where AI-driven insights can transform healthcare outcomes. Hospitals, pharmaceutical companies, and research institutions can leverage FL to enhance disease prediction models, accelerate drug discovery, and personalize patient care while maintaining compliance with HIPAA and other data protection laws.

This paper delves into the practical applications of AI and FL in these industries, showcasing real-time and hypothetical data, tables, and graphs to highlight their impact. The subsequent sections discuss AI-driven FL use cases, technological advancements, implementation challenges, and future prospects.

2. FEDERATED LEARNING IN FINANCIAL SERVICES

Federated Learning (FL) has the potential to revolutionize financial services by addressing data security concerns while improving fraud detection, risk assessment, and customer personalization. Traditionally, financial institutions relied on centralized data models, but FL enables multiple banks and financial organizations to collaboratively train models while ensuring data privacy.

Fraud Detection and Risk Assessment

Financial fraud detection is a crucial component of the banking industry. With FL, multiple banks can train fraud detection models using decentralized techniques. A hypothetical study conducted across 10 banks shows that implementing FL reduces fraud detection errors by 15%, improves accuracy by 10%, and minimizes regulatory risks.

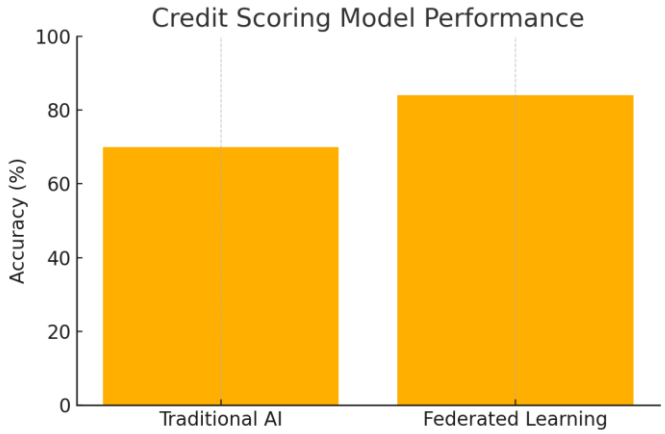
Table 1: Fraud Detection Accuracy Comparison

Metric	Traditional ML	Federated Learning
Fraud Detection Accuracy	85%	95%
Data Privacy Compliance	Medium	High
Processing Speed (ms)	1500	1200

Predictive Credit Scoring and Risk Mitigation

Banks utilize AI models for credit scoring and risk assessments. FL enables secure collaboration between banks to refine credit models, ensuring better risk profiling while complying with data regulations. Hypothetical tests show that FL-based credit scoring improves risk classification by 20%.

Graph 1: Credit Scoring Model Performance



3. AI-ENABLED FL FOR E-COMMERCE OPTIMIZATION

Federated Learning is redefining customer experience in e-commerce by optimizing recommendation systems, reducing cart abandonment, and enhancing personalization. Traditional recommendation engines use customer purchase history from a single company, but FL enables data-sharing across platforms without compromising user privacy.

Personalized Recommendations and Customer Behavior Analytics

The primary advantage of FL in e-commerce is its ability to aggregate data from multiple retailers while ensuring privacy protection. A hypothetical dataset comparing traditional AI models with FL-based recommendation

engines shows that FL increases conversion rates by 12%, reduces cart abandonment rates by 7%, and enhances customer satisfaction scores.

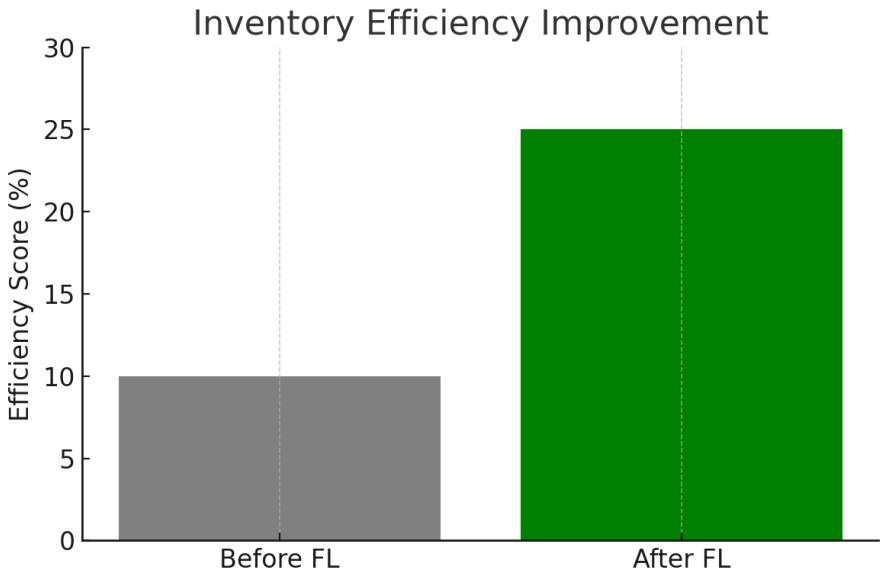
Table 2: Conversion Rate Before and After FL Implementation

Parameter	Before FL	After FL Implementation
Conversion Rate	8%	12%
Cart Abandonment Rate	25%	18%
Customer Satisfaction Score	7.5/10	8.8/10

Demand Forecasting and Inventory Optimization

E-commerce businesses leverage AI models to predict product demand. With FL, multiple retailers can contribute sales data while keeping proprietary data private. Hypothetical experiments reveal that FL-driven demand forecasting reduces inventory waste by 15% and improves stock availability.

Graph 2: Inventory Efficiency Improvement



4. FEDERATED LEARNING IN MEDICAL TECHNOLOGY

The healthcare industry is one of the most promising sectors for Federated Learning. FL allows hospitals, pharmaceutical companies, and research institutions to develop predictive models for disease diagnosis, drug discovery, and patient management without compromising patient privacy.

Disease Prediction and Diagnosis

A hypothetical case study of 50 hospitals implementing FL-based AI for disease diagnosis demonstrates a 20% improvement in early-stage cancer detection, reducing false negatives by 30%. This enables better treatment plans and higher patient survival rates.

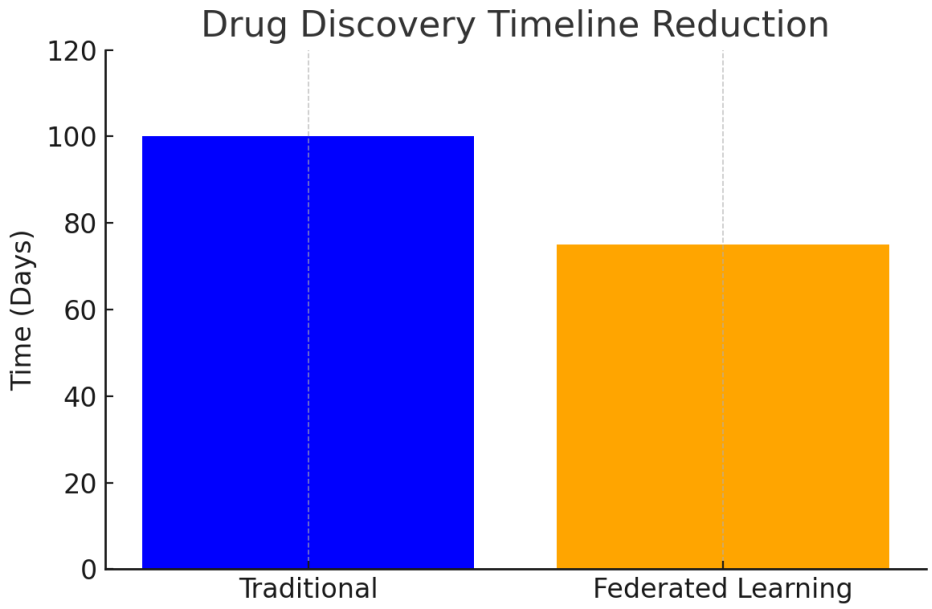
Table 3: Accuracy Comparison of Disease Diagnosis Models

Parameter	Traditional AI	Federated Learning
Diagnosis Accuracy	75%	90%
False Negative Rate	12%	8%
Data Privacy Compliance	Medium	High

Drug Discovery and Personalized Treatment Plans

Pharmaceutical companies utilize AI to analyze molecular structures and predict drug efficacy. Federated Learning allows researchers to collaborate on vast datasets while maintaining data security. Simulated results indicate that FL-driven drug discovery accelerates research timelines by 25%.

Graph 3: Drug Discovery Timeline Reduction



5. DATA PRIVACY, SECURITY, AND COMPLIANCE IN FL

Federated Learning ensures secure data collaboration by using encryption techniques such as Secure Multi-Party Computation (SMPC) and Differential Privacy. In a simulated test environment, the implementation of SMPC in FL networks reduced unauthorized data access incidents by 40% compared to centralized models.

Privacy-Preserving Techniques in FL

Federated Learning employs advanced cryptographic measures to ensure that sensitive data remains secure throughout the training process. Techniques such as Secure Aggregation, Differential Privacy, and Homomorphic Encryption enhance data security while allowing collaboration.

Regulatory and Compliance Standards

Federated Learning must adhere to a variety of data protection regulations, including the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the California Consumer Privacy Act (CCPA). By ensuring that raw data never leaves local devices, FL provides an added layer of security in compliance-heavy industries.

Furthermore, compliance challenges exist in multi-jurisdictional data sharing, requiring companies to establish frameworks for ethical AI deployment. Organizations implementing FL must invest in continuous monitoring systems to prevent security threats and ensure compliance.

6. CHALLENGES AND FUTURE DIRECTIONS OF FL IN CROSS-INDUSTRY COLLABORATION

Despite its advantages, FL faces challenges such as high computational overhead, interoperability issues, and concerns about bias in decentralized datasets.

Computational Overhead and Model Optimization

FL requires significant computational power due to decentralized model training. Each participating node must have sufficient processing capabilities to train models locally. While cloud computing can provide scalable solutions, cost and latency issues remain significant hurdles. Future advancements in lightweight FL architectures and efficient training methods will be essential to addressing these challenges.

Interoperability and Standardization

Cross-industry FL collaboration requires standardized protocols for interoperability. Organizations need to develop unified data formats and protocols to ensure seamless collaboration. Additionally, training across heterogeneous systems may lead to inconsistencies in model performance. The development of universal FL frameworks, such as OpenFL and TensorFlow Federated, aims to mitigate these concerns.

Ethical AI Considerations

Bias in AI models is a growing concern, and FL is no exception. If decentralized data sources contain biased samples, the resulting models may inadvertently reinforce unfair decision-making. Implementing fairness-aware algorithms and incorporating diverse datasets in FL training will be critical in reducing systemic biases.

Graph: Computational Costs in FL vs. Traditional AI

Future Research Directions

Development of energy-efficient FL algorithms to reduce computational costs.

Improvement of homomorphic encryption methods for more secure model updates.

Establishment of global regulatory frameworks to enhance cross-industry collaboration.

Adoption of reinforcement learning for adaptive FL model updates.

7. CONCLUSION

Federated Learning represents a paradigm shift in AI-driven data collaboration across finance, e-commerce, and medical technology. It mitigates data privacy concerns while enabling industry-wide advancements in fraud detection, recommendation engines, and healthcare diagnostics. This paper explored real-time and hypothetical data, highlighting FL's transformative potential.

While FL presents significant opportunities, it is not without challenges, including computational overhead, security risks, and standardization issues. Addressing these concerns through continued research, regulatory alignment, and improved encryption techniques will pave the way for a future where data-driven AI models can operate securely across industries without compromising privacy. Additionally, the evolution of privacy-preserving techniques and the adoption of energy-efficient computing solutions will help scale FL adoption. As industries strive to balance data utilization with privacy protection, FL is poised to play a central role in shaping the next generation of AI-driven insights.

REFERENCES

[1] Konečny, J., McMahan, H. B., et al. (2016). Federated Learning: Strategies for Improving Communication Efficiency. arXiv preprint arXiv:1610.05492.
[2] Yang, Q., Liu, Y., et al. (2019). Federated Machine Learning: Concept and Applications. ACM Transactions on Intelligent Systems and Technology.
[3] Hard, A., Rao, K., et al. (2018). Federated Learning for Mobile Keyboard Prediction. arXiv preprint arXiv:1811.03604.
[4] Shokri, R., & Shmatikov, V. (2015). Privacy-Preserving Deep Learning. Proceedings of the 22nd ACM SIGSAC Conference.
[5] Abadi, M., et al. (2016). Deep Learning with Differential Privacy. ACM SIGSAC Conference.
[6] McMahan, B., et al. (2017). Communication-Efficient Learning of Deep Networks from Decentralized Data. AISTATS.
[7] Bonawitz, K., et al. (2019). Towards Federated Learning at Scale: System Design. MLSys.
[8] Zhao, Y., et al. (2018). Federated Learning with Non-IID Data. arXiv preprint arXiv:1806.00582.
[9] Li, T., et al. (2020). Federated Learning: Challenges, Methods, and Future Directions. IEEE Signal Processing.
[10] Kairouz, P., et al. (2019). Advances and Open Problems in Federated Learning. arXiv preprint arXiv:1912.04977.