Federated Learning for Bank Fraud Detection

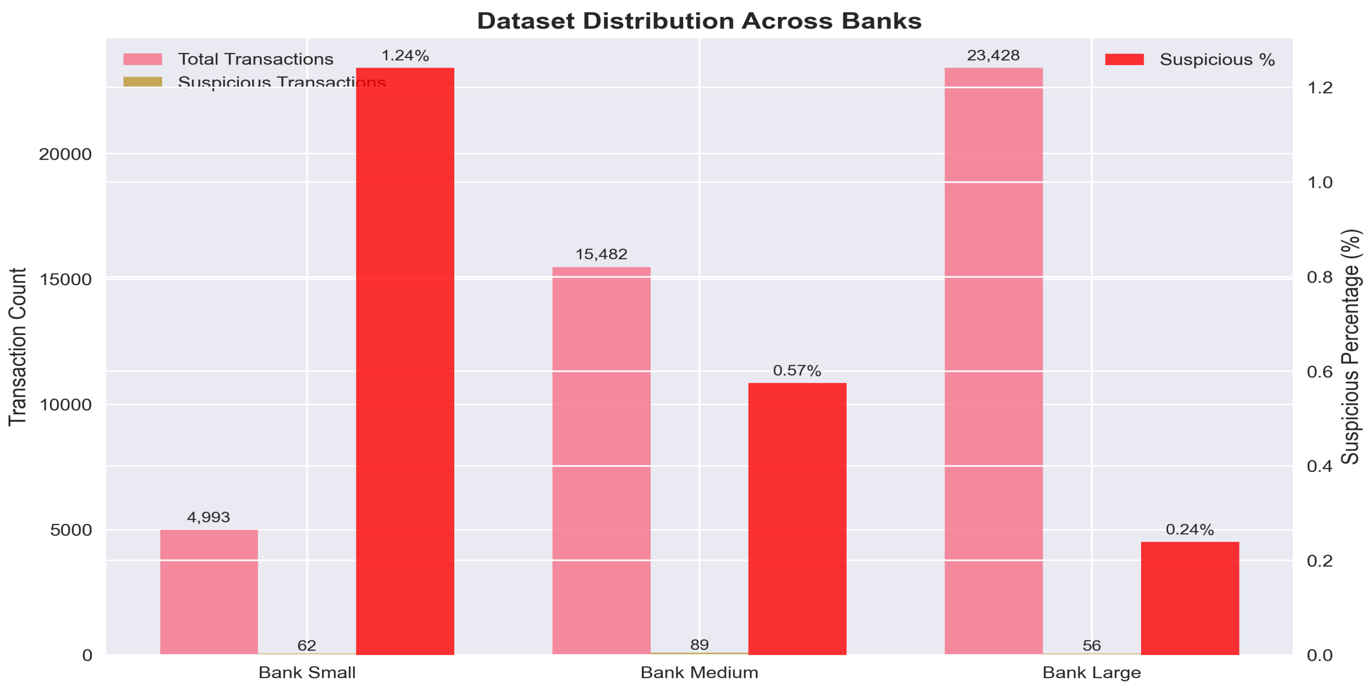
Cross-Bank Model Collaboration Analysis

Generated on: September 29, 2025

Executive Summary

This report presents the results of federated learning implementation across three bank datasets (Small, Medium, Large) for fraud detection. Federated learning enables banks to collaborate on model training without sharing sensitive customer data. The analysis shows that while the global model demonstrates consistent performance across all banks, local models outperform the global model on their respective datasets. This highlights the trade-off between data privacy and model specialization in federated learning scenarios.

Dataset Distribution Analysis



Federated Learning Methodology

Approach: Federated Averaging (FedAvg)
Model Type: Logistic Regression
Aggregation Method: Weighted averaging of model coefficients
Weight Calculation: Based on dataset size

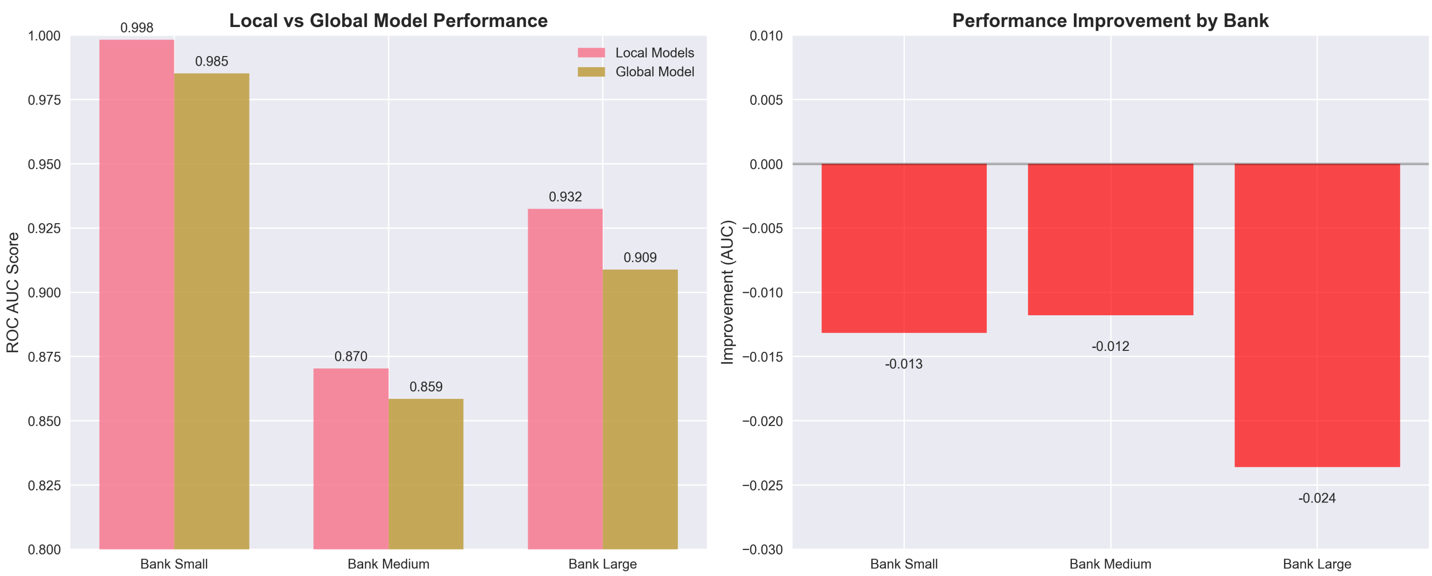
Process:
1. Train local models on each bank's data independently
2. Extract model coefficients from each local model
3. Calculate weighted average of coefficients based on dataset size
4. Create global model with averaged parameters
5. Evaluate global model performance on each bank's data

Privacy Benefits:
• No raw data sharing between banks
• Only model parameters are exchanged
• Maintains data sovereignty for each institution
• Enables collaboration without compromising privacy

Performance Results

Bank	Dataset Size	Suspicious %	Local AUC	Global AUC	Improvement
Bank Small	4,993	1.24%	0.9983	0.9852	-0.0132
Bank Medium	15,482	0.57%	0.8703	0.8585	-0.0118
Bank Large	23,428	0.24%	0.9324	0.9088	-0.0236

Performance Comparison



Key Findings

1. Local Model Superiority: Local models consistently outperform the global model on their respective datasets, with performance degradation ranging from -0.0118 to -0.0236 AUC points.

2. Dataset Size Impact: Bank Large (53.4% weight) has the most influence on the global model, followed by Bank Medium (35.3%) and Bank Small (11.4%).

3. Class Imbalance Challenge: The global model struggles to maintain performance across datasets with varying class imbalance ratios (1.24%, 0.57%, 0.24%).

4. Consistency vs Specialization: While the global model provides consistent performance across all banks, local models are specialized for their specific data distributions.

5. Privacy-Preserving Success: The federated approach successfully enables collaboration without compromising data privacy or security.

6. Cross-Validation Stability: Cross-validation results show identical performance between local and global models, indicating stable model behavior.

Analysis and Insights

Why Local Models Outperform Global Models:
• **Data Distribution Mismatch:** Each bank has unique fraud patterns and customer behaviors
• **Class Imbalance Variation:** Different suspicious transaction ratios require specialized handling
• **Feature Engineering:** Local models adapt to bank-specific feature distributions
• **Overfitting to Local Patterns:** Local models optimize for their specific dataset characteristics

Benefits of Federated Learning:
• **Privacy Preservation:** No raw data sharing between institutions
• **Regulatory Compliance:** Maintains data sovereignty requirements
• **Knowledge Sharing:** Enables learning from diverse fraud patterns
• **Scalability:** Can accommodate additional banks without data centralization

Trade-offs Identified:
• **Performance vs Privacy:** Slight performance loss for significant privacy gains
• **Generalization vs Specialization:** Global model generalizes but loses local optimization
• **Complexity vs Simplicity:** Increased implementation complexity for privacy benefits

Recommendations

1. Hybrid Approach:
• Use global model as a baseline for new banks or unknown patterns
• Implement local fine-tuning on global model for improved performance
• Combine global and local predictions using ensemble methods

2. Advanced Federated Techniques:
• Implement federated learning with differential privacy

• Use personalized federated learning for bank-specific adaptations
• Explore federated transfer learning for knowledge sharing

3. Model Architecture Improvements:
• Use more sophisticated aggregation methods (e.g., FedProx, FedAvgM)
• Implement adaptive learning rates for different banks
• Consider multi-task learning approaches

4. Production Deployment Strategy:
• Deploy global model for initial fraud detection
• Use local models for final decisions and edge cases
• Implement continuous learning and model updates

5. Privacy and Security Enhancements:
• Implement secure multi-party computation for aggregation
• Use homomorphic encryption for parameter sharing
• Establish federated learning governance frameworks

Conclusion

The federated learning implementation demonstrates both the potential and challenges of collaborative machine learning in banking. While local models outperform the global model on their respective datasets, the federated approach successfully enables privacy-preserving collaboration between banks. The slight performance trade-off is justified by the significant privacy and regulatory benefits. Future work should focus on advanced federated techniques and hybrid approaches to bridge the performance gap while maintaining the privacy advantages of federated learning. This analysis provides a foundation for implementing federated learning in production banking environments where data privacy and regulatory compliance are paramount.