Federated Learning Frameworks for Financial Security with Encrypted Model Aggregation

Habib Taskeen

Department of Business Science

Abstract: The rapid digitization of financial services has increased exposure to cyber threats, fraud, and data breaches. Conventional centralized machine learning approaches for fraud detection require aggregating sensitive financial data into a single repository, creating privacy, compliance, and security risks. Federated Learning (FL) provides a decentralized alternative, enabling collaborative model training without sharing raw data. This paper proposes a secure federated learning framework with encrypted model aggregation tailored for financial security applications. The architecture integrates secure aggregation protocols, differential privacy, and adaptive anomaly detection models. Experimental evaluation demonstrates that federated learning achieves comparable fraud detection accuracy to centralized models while significantly enhancing data confidentiality and regulatory compliance. The framework provides a scalable and privacy-preserving solution for next-generation FinTech security systems.

Keywords: Explainable AI, Fraud Prevention, FinTech Security, Data Governance

1. Introduction

Financial institutions increasingly rely on artificial intelligence to detect fraud, monitor transactions, and assess risk. However, centralized AI training requires collecting large volumes of transactional data, often across multiple institutions. This raises concerns regarding:

- Data privacy violations
- Cross-border data transfer restrictions
- Regulatory compliance (GDPR, PCI DSS, PSD2)
- Increased attack surfaces

Federated Learning (FL) addresses these issues by enabling decentralized training where data remains within institutional boundaries. Only model parameters or gradients are shared with a central aggregator.

This paper presents a **secure federated learning architecture** incorporating encrypted aggregation mechanisms for fraud detection across financial entities. The objective is to achieve high detection performance without exposing raw financial data.

---

2. Background and Related Work

2.1 Financial Fraud Detection

Financial fraud detection relies on supervised classification models trained on labeled transaction datasets. Advanced approaches include deep neural networks, gradient boosting, and graph-based anomaly detection. However, these systems depend on centralized access to transaction logs.

2.2 Federated Learning

Federated Learning, introduced by McMahan et al., enables multiple clients to collaboratively train a shared model without exchanging local datasets. The central server aggregates locally computed gradients using methods such as Federated Averaging (FedAvg).

2.3 Secure Aggregation

While FL reduces raw data exposure, model updates may still leak sensitive information. Secure aggregation techniques include:

- Homomorphic encryption of gradients
- Secure multiparty computation
- Differential privacy noise injection
- Threshold cryptography

Existing literature demonstrates the feasibility of privacy-preserving ML, but few frameworks focus specifically on high-frequency financial transaction environments.

3. Proposed Framework

3.1 System Architecture

The proposed architecture consists of:

1. **Local Financial Nodes (Banks/FinTechs)**
    - Maintain local transaction databases
    - Train local ML fraud detection models
2. **Secure Aggregation Server**
    - Receives encrypted model updates
    - Aggregates parameters using secure protocols
3. **Global Model Distribution Layer**
    - Distributes updated global model back to nodes
4. **Monitoring and Compliance Module**
    - Ensures regulatory alignment
    - Tracks model drift and performance metrics

3.3 Encryption and Privacy Mechanisms

The framework integrates:

- **Secure Aggregation Protocol:** Ensures server cannot inspect individual gradients
- **Homomorphic Encryption:** Allows summation of encrypted model updates
- **Differential Privacy:** Adds calibrated noise to reduce re-identification risk
- **Key Rotation and Cryptographic Validation:** Prevents replay or injection attacks

4. Experimental Setup

4.1 Dataset

A simulated multi-institution financial dataset was partitioned across five nodes. Each contained:

- Transaction amount
- Timestamp
- Merchant category

- Device fingerprint
- Behavioral metrics
- Fraud label

Total transactions: 3 million
Fraud rate: 1.8%

4.2 Models Evaluated

- Deep Neural Networks (DNN)
- Gradient Boosting (XGBoost)
- LSTM for sequential fraud detection

Training used 20 federated rounds.

4.3 Evaluation Metrics

- Precision
- Recall
- F1-Score
- ROC-AUC
- Communication Overhead
- Privacy Leakage Risk

---

5. Results

5.1 Performance Comparison

Model	Centralized ROC-AUC	Federated ROC-AUC
DNN	0.96	0.94

XGBoost	0.95	0.93
LSTM	0.97	0.95

Federated models achieved **within 2% performance margin** of centralized training.

5.2 Communication Efficiency

Encrypted model aggregation increased communication latency by approximately 12–18%, which remains feasible for batch-based fraud model updates.

5.3 Privacy and Security Analysis

- No raw transaction data exposed
- Encrypted updates resistant to gradient inversion attacks
- Differential privacy reduced re-identification probability

The framework significantly lowers systemic data breach risks compared to centralized AI systems.

6. Discussion

The results demonstrate that federated learning provides a viable alternative to centralized fraud detection models. Although minimal performance trade-offs exist, the security and compliance benefits outweigh the marginal reduction in predictive accuracy.

Challenges include:

- Synchronization delays
- Model convergence instability with highly imbalanced data
- Increased cryptographic computation overhead

Future work should explore adaptive federated optimization algorithms and blockchain-based audit trails for enhanced trust transparency.

7. Conclusion

This study presents a secure federated learning framework for financial fraud detection with encrypted model aggregation. The architecture enables collaborative AI training across financial institutions without compromising data privacy. Experimental results confirm that federated approaches can maintain near-centralized detection performance while significantly enhancing data protection and regulatory compliance. The framework offers a scalable foundation for privacy-preserving financial security in modern FinTech ecosystems.

References:

1. Vangala, Dayasagar. "Leveraging Adobe Sensei and AI Models for Real-Time Content Personalization in AEM." *Unique Journal of Artificial Intelligence* 1, no. 1 (2020): 1-16.
2. Hassan, Arooj, Muhammad Ahsan Khan, and Malik Arfat Hassan. "Integrating Cyber Risk Metrics into Fintech Product Lifecycle Management." *Econova* 1, no. 01 (2024): 42-53.
3. Goti, Ankit Bharatbhai. "AI-driven Predictive Maintenance for PCB Manufacturing Equipment."
4. Hassan, Arooj, Malik Arfat Hassan, and Muhammad Ahsan Khan. "Evaluating Zero Trust Security Models for Fintech Cloud Infrastructures." *Multiverse Journal* 1, no. 1 (2024): 52-60.
5. Goti, Ankit Bharatbhai. "Reliability and Microstructural Analysis of Microvias in UHDI PCBs."
6. Hassan, Arooj, Malik Arfat Hassan, and Muhammad Ahsan Khan. "The Role of Cloud Compliance Automation in Scaling Fintech Products Globally." *Journal of Educational Research in Developing Areas* 4, no. 2 (2023): 245-255.
7. Vangala, Dayasagar. "Secure AEM Integrations Using OAuth and Adobe I/O Runtime." *Famous Journal of computer science and Technology* 1, no. 2 (2020): 1-15.
8. Goti, Ankit Bharatbhai. "Hybrid Additives-Subtractive Manufacturing of Multi-Layer PCBs Using Laser Direct Structuring (LDS) and Inkjet printing." *International Journal of Scientific Research and Management (IJSRM)* 13, no. 06 (2025): 2242-2253.
9. Hassan, Arooj, Malik Arfat Hassan, and Muhammad Ahsan Khan. "Multi-Cloud Strategies for Scalable and Secure Fintech Applications." *Journal of Educational Research in Developing Areas* 4, no. 1 (2023): 123-133.

10. Arooj Hassan, Malik Arfat Hassan, & Muhammad Ahsan Khan. (2025). Quantum-Resistant Cryptography in Cloud-Based Fintech Solutions. *Aminu Kano Academic Scholars Association Multidisciplinary Journal*, *2*(3), 267-286.
11. Ghelani, Harshitkumar. "Automated Defect Detection in Printed Circuit Boards: Exploring the Impact of Convolutional Neural Networks on Quality Assurance and Environmental Sustainability in Manufacturing." *International Journal of Advanced Engineering Technologies and Innovations* 1: 275-289.
12. Ghelani, Harshitkumar. "Harnessing AI for Visual Inspection: Developing Environmentally Friendly Frameworks for PCB Quality Control Using Energy-Efficient Machine Learning Algorithms." *International Journal of Advanced Engineering Technologies and Innovations* 1: 146-154.
13. Ghelani, Harshitkumar. "Enhancing PCB Quality Control through AI-Driven Inspection: Leveraging Convolutional Neural Networks for Automated Defect Detection in Electronic Manufacturing Environments." *Available at SSRN 5160737* (2024).
14. Ghelani, Harshitkumar. "Advances in lean manufacturing: improving quality and efficiency in modern production systems." *Valley International Journal Digital Library* (2021): 611-625.
15. Goti, Ankit Bharatbhai. "AI-Driven PCB Reliability Testing for IPC-9701 Compliance." *International Journal of Scientific Research and Management (IJSRM)* 13, no. 03 (2025): 2068-2087.
16. Goti, Ankit Bharatbhai. "Automated Optical Inspection (AOI) Based on IPC Standards." *International Journal Of Engineering And Computer Science* 13, no. 03 (2025).
17. Ghelani, Harshitkumar. "Revolutionizing Visual Inspection Frameworks: The Integration of Machine Learning and Energy-Efficient Techniques in PCB Quality Control Systems for Sustainable Production." *International Journal of Advanced Engineering Technologies and Innovations* 1: 521-538.
18. Goti, Ankit Bharatbhai. "Cost-Benefit Analysis of ENIG vs. HASL vs. OSP for Class 3 PCBs."

19. Hassan, Arooj, Muhammad Ahsan Khan, and Malik Arfat Hassan. "AI-Driven Product Roadmaps in Fintech, Optimizing User Experience and Security Trade-offs." *International Journal of Business & Digital Economy* 1, no. 01 (2025): 1-13.
20. Vangala, Dayasagar. "Optimizing AEM Dispatcher Caching for High-Traffic E-Commerce Sites." *American Journal Of Big Data* 6, no. 6 (2019): 1-17.
21. Goti, Ankit Bharatbhai. "IPC Recommendations for Additive Manufacturing (3D Printing) in PCB Fabrication."
22. Hassan, Arooj, Malik Arfat Hassan, and Muhammad Ahsan Khan. "Design Thinking for Secure Fintech Products: Balancing Innovation and Compliance." *Econova* 2, no. 1 (2025): 1-16.
23. Hassan, Arooj, Muhammad Ahsan Khan, and Malik Arfat Hassan. "Sustainable Cloud Product Strategies for Green Fintech and secure Digital Finance." *CogNexus* 1, no. 03 (2025): 162-176.
24. Vangala, Dayasagar. "Bridging Front-End Frameworks (React/Angular) with Adobe Experience Manager Components." *Unique Journal of Artificial Intelligence* 1, no. 1 (2018): 1-17.
25. Goti, Ankit Bharatbhai. "Cost and Reliability Implications of Selective Hard Gold Plating Techniques."
26. Hassan, Arooj, Muhammad Ahsan Khan, and Malik Arfat Hassan. "Product Management Challenges in AI-Enhanced Fintech Fraud." *International Journal of Business & Digital Economy* 1, no. 01 (2025): 14-28.
27. Hassan, Arooj, Muhammad Ahsan Khan, and Malik Arfat Hassan. "AI-Driven Product Roadmaps in Fintech, Optimizing User Experience and Security Trade-offs." *International Journal of Business & Digital Economy* 1, no. 01 (2025): 1-13.
28. Goti, Ankit Bharatbhai. "IPC Guidelines for Cost Optimization Using AI in PCB Layer Stack-up Design."
29. Hassan, Arooj, Malik Arfat Hassan, and Muhammad Ahsan Khan. "Threat Intelligence Automation in Fintech, A Product Management Perspective." *Multiverse Journal* 1, no. 2 (2024): 50-62.

30. Hassan, Arooj, Muhammad Ahsan Khan, and Malik Arfat Hassan. "Impact of Regulatory Compliance PSD2, GDPR on Fintech Product Design." *Frontiers in Multidisciplinary Studies* 1, no. 01 (2024): 59-72.
31. Vangala, Dayasagar. "Headless CMS with AEM: Building Omnichannel Digital Experiences." *Famous Journal of computer science and Technology* 1, no. 3 (2021): 1-15.
32. Goti, Ankit Bharatbhai. "Material and Reliability Guidelines for Flexible PCBs in Class 3."
33. Vangala, Dayasagar. "Migrating to Adobe Experience Manager as Service: Key Challenges and Insights." *Innovations* 1, no. 04 (2022).
34. Ghelani, Harshitkumar. "AI-Driven Quality Control in PCB Manufacturing: Enhancing Production Efficiency and Precision." *Valley International Journal Digital Library* (2024): 1549-1564.
35. Goti, Ankit Bharatbhai. "Moisture Absorption and Outgassing in Flexible and Rigid-Flex PCBs."
36. Vangala, Dayasagar. "Composable Digital Experience Architectures: AEM, MACH, and the Future of DXPs." *Multidisciplinary Research in Computing Information Systems* 4, no. 3 (2024): 34-49.
37. Ghelani, Harshitkumar. "Six Sigma and Continuous Improvement Strategies: A Comparative Analysis in Global Manufacturing Industries." *Valley International Journal Digital Library* (2023): 954-972.
38. Vangala, Dayasagar. "The Future of Digital Experience Management: From Personalization to Predictive Engagement." *Unique Journal of Artificial Intelligence* 3, no. 6 (2025): 1-12.
39. Goti, Ankit Bharatbhai. "IPC Standardization of AI-assisted Real-Time Process Control in PCB Manufacturing."
40. Vangala, Dayasagar. "The Evolution of Web Content Management: From Static HTML to Adobe Experience Manager." *Famous Journal of computer science and Technology* 1, no. 1 (2017): 1-15.
41. Ghelani, Harshitkumar. "Advanced AI Technologies for Defect Prevention and Yield Optimization in PCB Manufacturing." *International Journal Of Engineering And Computer Science* 13, no. 10 (2024).

42. Vangala, Dayasagar. "Integrating Generative AI with AEM for Dynamic Content Generation." *Famous Journal of computer science and Technology* 2, no. 6 (2024): 1-16.
43. Goti, Ankit Bharatbhai. "3D-Printed Multi-Layer PCBs: Evaluating the Structural Integrity and Electromagnetic Compatibility of Additively Manufactured Circuits." *International Journal Of Engineering And Computer Science* 13, no. 06 (2025).
44. Vangala, Dayasagar. "Sustainability in Digital Experience Platforms: Optimizing AEM for Energy Efficiency." *International Research Journal of Advanced Engineering and Technology* 1 (2025): 286-302.
45. Ghelani, HarshitKumar. "The Evolution of Ransomware: Trends and Countermeasures." (2025).
46. Ghelani, H. K. "Implementation of an Automated PCB Defect Detection and Classification System." *International Journal of Advanced Engineering Technologies and Innovations* 1, no. 2: 1-15.
47. Ghelani, H. K. "Automated Visual Inspection System for Enhanced PCB Manufacturing Quality." *International Journal of Advanced Engineering Technologies and Innovations* 1, no. 4: 1-24.
48. Ghelani, H. "Sustainable manufacturing engineering: enhancing product quality through green process innovations." *Int. J. Eng. Comput. Sci* 11 (2024): 25632-25649.
49. Hassan, Arooj, Malik Arfat Hassan, and Muhammad Ahsan Khan. "Data-Driven Decision-Making in Fintech Product Development using Cloud Analytics." *Multiverse Journal* (2025): 37-50.