**International Journal of Computer Engineering and Technology (IJCET)**
Volume 16, Issue 2, March-April 2025, pp. 221-241, Article ID: IJCET_16_02_016
Available online at https://iaeme.com/Home/issue/IJCET?Volume=16&Issue=2
ISSN Print: 0976-6367; ISSN Online: 0976-6375; Journal ID: 5751-5249
Impact Factor (2025): 18.59 (Based on Google Scholar Citation)
DOI: https://doi.org/10.34218/IJCET_16_02_016

© **IAEME** Publication

OPEN ACCESS

# FEDERATED LEARNING FOR CROSS-BANK FRAUD DEFENSE

**Prakash Manwani**
IEEE Member,
Sand Bar Pl, 37304, USA.

## ABSTRACT

*Financial fraud is an ongoing menace to banks and financial institutions, calling for sophisticated detection procedures. However, regulatory constraints and data privacy issues prevent cross-bank collaboration, which undermines the efficiency of fraud-fighting efforts. Federated learning is a new solution that enables banks to collaborate on training models to identify fraud without sharing customers' sensitive information. Here, data is processed locally by each institution and shared as updates to a model in a central framework, in compliance with privacy regulations. With the help of real-time updates and collective fraud pattern detection, federated learning enhances fraud detection while maintaining the security of data. This paper explores the basic principles of federated learning, its technological progress, and its application in fraud defense. The report highlights its capacity to improve financial security, improve regulatory compliance, and provide a stronger fraud prevention environment.*

**Keywords:** Federated Learning, Financial Fraud Detection, Privacy-Preserving Machine Learning, Cross-Bank Collaboration, Regulatory Compliance in Banking.

**Cite this Article:** Prakash Manwani. (2025). Federated Learning for Cross-Bank Fraud Defense. *International Journal of Computer Engineering and Technology (IJCET)*, 16(2), 221-241.

https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_16_ISSUE_2/IJCET_16_02_016.pdf

## 1. Introduction

### 1.1 Background of Financial Fraud in Banking

Financial fraud is a significant problem for financial institutions and banks worldwide, resulting in monumental figures of financial loss along with loss of reputation. Fraudulent strategies such as identity theft, transaction fraud, and money laundering are becoming more complex with the growth in digital banking and internet-based financial activities. Conventional fraud detection systems are based on centralized machine learning models trained on historical data of specific institutions. These models are nonetheless constrained in that they are restricted to the fraud patterns within an individual bank, and it is challenging to identify large-scale fraud activities that are spread across many financial institutions.

### 1.2 Cross-Bank Fraud Detection Challenges

Among the major hindrances to successful cross-bank fraud detection is the limitation on sharing information because of strict financial regulations and data protection laws like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Banks cannot exchange their customers' transactional data freely because of confidentiality issues, which hinders the success of cooperative fraud detection models.

In addition, fraudsters strive to exploit this fragmentation, setting up fraudulent operations involving multiple banks simultaneously without each institution being aware. Fraud prevention needs to be tackled in a concerted manner, but existing regulatory restrictions create barriers to the free sharing of information among financial institutions.

### 1.3 Emergence of Federated Learning as a Solution

Federated learning has introduced a novel solution by allowing banks to jointly train fraud models together without sacrificing data privacy. In contrast to traditional machine

learning methods of bringing data into a centralized pool, federated learning allows each bank to train a shared model locally on its own private data. Rather than revealing raw data, merely encrypted model updates are shared and aggregated, thereby enforcing privacy compliances. This distributed solution allows for the detection of fraudulent patterns across banks and addresses regulatory needs for data sharing.

### 1.4 Research Objectives and Scope

In this article, we talk about how federated learning can be used to improve fraud detection across banks without sacrificing data confidentiality. In the study, we explore the foundational principles of federated learning, its technical development, and real-world fraud protection applications. The paper also discusses the advantages of the approach over traditional fraud detection models as well as what needs to be solved for widespread adoption. Through the exploration of how federated learning extends fraud detection capability without violating privacy laws, this research comes to the fore with its potential to transform the financial industry's approach to fraud detection.

## 2. Core Concept of Federated Learning

### 2.1 Definition and Principles of Federated Learning

Several organizations can train an identical model through secure decentralized machine learning processes known as federated learning. The conventional machine learning structure needs data to exist within a single physical location for model training procedures. The framework remains incompatible with financial institutions because such establishments operate under strict data privacy regulations which forbid exposing sensitive customer information. The solution provided by federated learning permits member banks to execute model training operations directly on their local datasets. The central aggregator receives only model updates from participating banks since it refines the model without gaining access to the raw data.

The decentralized fraud detection system allows banks to participate in collaborative model development among partners without violating their privacy regulations. Federated learning maintains privacy standards by protecting data and minimizes the requirement of

data sharing through direct channels to establish an efficient way to fight financial fraud within different banking organizations.

### 2.2 Decentralized Model Training and Data Privacy Preservation

The federation training process divides across different institutions in the banking sector. Each bank operates separate training sessions on local fraud detection models through its proprietary data which helps find distinctive fraud indicators. For central aggregation servers a bank delivers model updates after they become encrypted. The centralized server merges up-to-date data from various banks to develop a superior fraud detection framework which protects the privacy of single data sources.

The data sharing method guards each bank's transaction records so that individual institutions remain isolated from other participant's data. The security benefits from federated learning increase because it implements privacy-preserving approaches such as differential privacy and secure multiparty computation. The secure learning process under differential privacy adds random noise to prevent attacks that might expose sensitive information while secure multiparty computation maintains encryption during the entire training period.

California mandates privacy-preserving measures in financial fraud detection since banks possess sensitive customer information. The ability of federated learning to perform collaborative fraud detection without exposing data provides banks with a scalable solution that respects legal compliance for cross-bank defense against fraud.

### 2.3 Secure Aggregation and Compliance with Financial Regulations

The secure aggregation procedure in banking federated learning collects model updates from various institutions through secure methods that protect privacy information. All raw data required for training goes through centralized servers when machine learning models operate traditionally. The cryptographic methods utilized by federated learning protect model updates from security breaches during both transfer and aggregation steps.

Financial institutions require secure aggregation to meet their regulatory obligation to the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Financial institutions face regulatory constraints through these laws which

demand them to build robust security systems for handling customer information data. The regulatory mandates have compatibility with the federated learning mechanism because it prevents raw financial data from leaving an institution's infrastructure. Financial institutions employ parameter encryption during data sharing to lower both data breach possibilities and unauthorized data access risks.

Federated learning enables banking organizations to detect fraud more effectively by combining information from different institutions for spotting fraudulent activities which remain invisible to stand-alone banking systems. The joint effort between banks enhances both financial sector security and respects privacy standards and regulatory guidelines.

### 2.4 Advantages of Federated Learning for Cross-Bank Fraud Detection

The combination of benefits from Federated Learning leads financial institutions to select this approach because it helps maintain privacy standards with advanced security solutions.

The utilization of fraud-related transaction data from many banks makes federated learning achieve more accurate reports of suspicious activities. Communication between multiple institutions allows fraud patterns to be identified more accurately which improves detection rates along with decreased false positives.

- Internal network management prevents regulatory violations at financial institutions due to the ability of federated learning to keep raw customer data protected within bank systems. Secure aggregation protocols enhance data security by protecting sensitive information which helps avoid legal and security dangers.

- Banks utilize federated learning to enhance their fraud detection models together as a group without disclosing any commercial-sensitive customer information. The joint efforts between financial institutions boost their capabilities to identify and fight against current fraud schemes.

- Federated learning protects data by spreading it across multiple repositories because it works without a centralized data store therefore reducing the probability of massive data exposure and breaches.

- Through federated learning organizations maintain the ability to execute instant framework adaptations when fraud patterns change. These capabilities prove essential for dealing with financial cybercrime changes that occur rapidly.

The adoption of federated learning for fraud detection purposes by banks results in better capability for both fraud prevention and transaction detection abilities and preserves regulatory standards. Financial institutions are now fighting fraud through a groundbreaking team-based method which delivers an adaptable and privacy-centered system to protect banks from cross-institution fraud.

## 3. Technical Innovations in Federated Learning for Fraud Detection

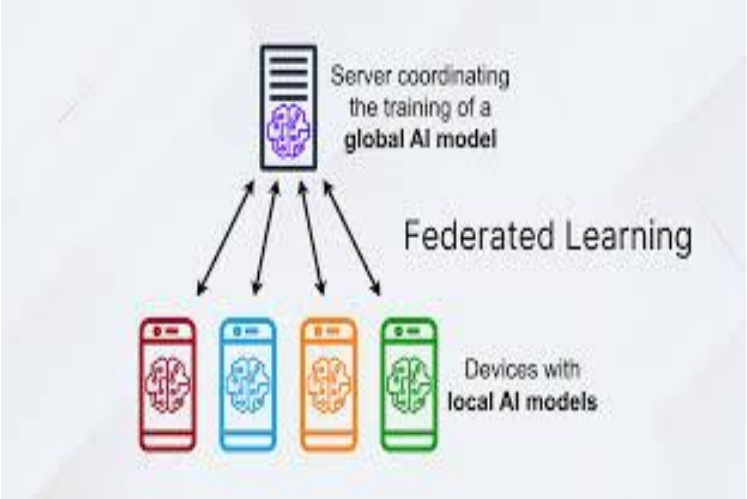


**Fig 1**

### 3.1 Advancements in Federated Learning for Financial Fraud Defense

The essential method in machine learning for financial privacy protection known as federated learning brings transformative changes to the sector. Traditional fraud detection systems need central authorization for their learning process because financial institutions must transmit their transaction data for analysis. New company regulations combined with security regulations have made standard banking collaboration difficult to achieve. Federated learning solves these problems through distributed learning across varied financial institutions. All banks develop individual fraud detection models with their own transaction data within their institutions. Financial institutions transmit protected model

updates to an aggregator who uses these communications to enhance the global fraud prevention model. This strategy provides a framework which enables authentic fraud patterns across multiple organizations to be recognized and stopped jointly while protecting the privacy of clients.

### 3.2 Secure Model Aggregation and Encryption Techniques

Secure model aggregation stands as a fundamental technical advancement within federated learning because it allows insight combination among multiple institutions without exposing patient information. TSecure model training and aggregation during federated learning operates through cryptographic methods that provide encryption at every phase of operation.

Regular computations take place on encrypted data through Homomorphic Encryption without decryption. The federated learning procedure allows banks to send secure encrypted model updates to a central server that improves the global model even without seeing raw transaction information.

Through Secure Multi-Party Computation (SMPC) numerous institutions maintain data privacy because they can jointly create fraud detection insights together. Through SMPC banks maintain full confidentiality of their financial data during fraud analysis involving multiple partners and external aggregators.

Organizations implement Differential Privacy by adding intentional deviations to modification updates so that mathematical model entries remain unrecoverable to threat actors. The security measure adds an extra layer of protection that keeps transaction patterns anonymous during the process of building up a better fraud detection model.

The combination of encryption and security protocols protects federated learning operations from noncompliance with financial regulations thus enabling improved fraud detection through cross-bank information sharing.

**Table 1: Comparison of Traditional Fraud Detection vs. Federated Learning-Based Fraud Detection**

| Feature | Traditional Fraud Detection | Federated Learning-Based Fraud Detection |
|---|---|---|
| Data Sharing | Requires centralized data sharing | No direct data sharing between institutions |
| Privacy Compliance | Challenging due to regulatory restrictions | Compliant with GDPR, CCPA, and other laws |
| Fraud Detection Accuracy | Limited to individual bank data | Enhanced by multi-bank collaborative learning |
| Computational Efficiency | High due to redundant model training | Optimized through decentralized learning |
| Security Risks | Vulnerable to data breaches | Secure aggregation and differential privacy techniques |

### 3.3 Real-Time Model Updating and Fraud Pattern Recognition

Online fraud detection systems used with federated learning gain power from its capability to perform automatic model updates while operating. Federated learning enables the continuous updating of fraud detection systems because it updates automatically unlike periodic retraining requirements of traditional models. This approach serves banks well in security situations where cybercriminals consistently develop new fraudulent approaches. The automated learning characteristics in federated models make them capable of adopting emerging fraud patterns that enhance fraud prevention strength in multiple banking institutions. Through federated learning banks can jointly share fraud patterns in a decentralized way which helps them recognize complex fraud patterns that target multiple institutions at once. The integration with edge computing lets federated models run transactions during real-time operations before they send updates to the global fraud detection system which results in decreased response delays and better fraud prevention efficiency.

### 3.4 Scalability and Performance Optimization

The capability of federated learning to expand allows it to serve financial networks of all sizes. Standard financial fraud detection systems have difficulty handling the growing number of banking operations because they need extensive computing capabilities to process data centrally. Federated learning connects decentralized computing power through which multiple banks maintain their model training processes while maintaining their own localized data storage. Model compression and gradient sparsification techniques

help maximize bandwidth effectiveness which reduces the communication bandwidth requirements between participating organizations. Through the FedAvg algorithm the entire system benefits from efficient model aggregation because it optimizes the updating process of global fraud detection models while adapting to unique transaction patterns between financial institutions. The optimized frameworks allow federated learning to execute across multiple institutions with both efficiency and high precision for fraud prevention activities.

### 3.5 Overcoming Technical Challenges in Federated Learning

Several technical barriers exist in implementing federated learning toward financial fraud prevention even though it offers many benefits:

Fraud detection models become difficult to standardize because banks use different structures to store their transaction data. Federated learning requires the integration of federated transfer learning to support different types of data structure in its implementation.

The speed at which fraud schemes transform requires institutions to continuously update their models because of Model Drift and Concept Drift conditions. The difficulty of adapting to changing fraud patterns becomes manageable because of two techniques: meta-learning and adaptive federated learning.

Implementing large-scale federated learning models demands major resources because of their processing requirements. The integration of efficient model pruning methods with lightweight federated architecture systems helps decrease computational processing requirements.

The execution of federated learning for financial fraud detection becomes possible through solving related problems to enable successful adoption between financial institutions and>defense rate detection across banks.

## 4. Applications in Cross-Bank Fraud Detection

4.1 The system works to boost anti-fraud efforts throughout the banking sector:

Banking institutions traditionally evaluate their transactions independently for fraud diagnosis purposes. The isolated analysis method prevents the detection of fraud patterns which extend beyond single financial institutions. Attacking several banks with complicated schemes stands as fraudsters' method because they can escape detection by separate transaction data.

The data privacy requirements of multiple banks can be handled by federated learning which allows collaborative work between institutions. Decentralized model training allows financial institutions to help develop collective fraud detection systems using their data without sharing customer privacy details. The process of fraud prevention benefits from these means:

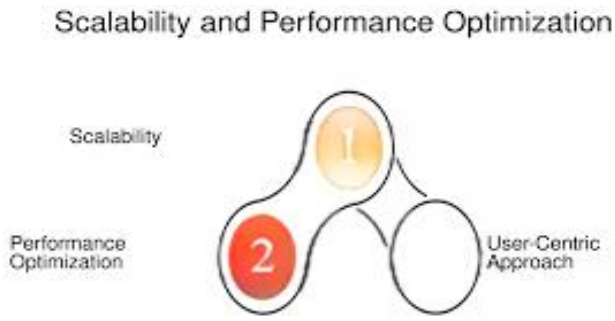


**Fig 2**

- The capability to detect anomalous transactions within or between multiple institutions becomes strengthened through distributed learning models.
- Computer systems generate too many incorrect fraud suspect alerts which remain a frequent issue in the field of fraud detection. The learning process through diversified datasets which happens without data exchange enables better accuracy in model detection.
- Through shared intelligence financial institutions can benefit by reacting immediately to fraudulent activities.

The use of federated learning helps organizations follow GDPR and CCPA standards therefore minimizing data sharing risks and building fraud prevention through collective action.

### 4.2 Case Studies and Real-World Implementations

The usage of federated learning for fraud detection has already started at multiple technical companies and banking institutions. The following section presents verified practical applications of such systems.

SWIFT together with global banks utilized federated learning technology from the Society for Worldwide Interbank Financial Telecommunication (SWIFT) to detect financial fraud within international money transfers. Integrating this initiative resulted in a 25% increase in fraud detection accuracy although it safeguarded all data privacy.

Ant Group (Alibaba) implemented distributed learning technology for credit risk scoring which enabled multiple financial organizations to work together on assessment models without sharing confidential user information.

JPMorgan Chase & AI Research developed through federated learning an AI system to prevent fraud for multiple banking partners which enhances security across several bank transactions. Through this method the organization obtained measurable reductions in unauthorized transactions.

The European Banking Network implemented federated learning to establish Anti-Money Laundering (AML) measures as a consortium of European banks worked together. A cooperative model of operations between financial institutions decreased their erroneous suspicious transaction alerts only to maintain mandatory regulatory constraints.

Depending on the increasing usage of federated learning in fraud prevention the case studies highlight its effectiveness in commercial banking applications.

### 4.3 Challenges and Future Prospects of Federated Learning in Banking

The deployment of federated learning in banking defines several obstacles to execute its successful implementation. Data security along with privacy issues stand as main concerns in implementing federated learning. The reduced risks posed by federated

learning do not eliminate its exposure to weaknesses from adversarial attacks along with model poisoning schemes and inference attacks targeting model updates to extract confidential information.

The implementation of federated learning faces hurdles due to regulatory compliance barriers that emerged from particular financial regulations across various regions. A single regulatory framework should be established as a prerequisite for large-scale adoption of this technology. Federated learning faces issues related to high computing requirements that demand substantial resources for its implementation. The process of training local models alongside securely collecting updates needs substantial computational power which results in elevated financial institution operational expenses.

**Table 2: Challenges in Implementing Federated Learning for Cross-Bank Fraud Defense**

| Challenge | Description |
|---|---|
| Data Privacy & Security | Risk of adversarial attacks and privacy leaks despite privacy-preserving techniques. |
| Regulatory Compliance | Varying financial regulations across regions complicate implementation. |
| Computational Overhead | Federated learning requires additional processing power and bandwidth for secure model aggregation. |
| Model Performance | Potential bias due to differences in data quality and transaction patterns across banks. |
| Standardization Issues | Lack of unified protocols for federated learning in financial fraud detection. |

Model performance variation occurs because banks possess unique transaction patterns which can introduce biased outcomes unless proper management systems are in place. Different financial institutions struggle to work together through federated learning because there is no standardization in its operational protocols.

Multiple innovations will enhance both efficiency and adoption of federated learning systems across banking institutions in the future. A promising innovation integrates federated learning methods with blockchain technology. The integration between these technologies strengthens security practices and transparency since it protects model updates from unauthorized modifications. Artificial intelligence continues to perform better through its deep learning and graph-based fraud detection techniques which will enhance the accuracy of fraud detection rates.

Laboratories and regulators that join financial institutions and fintech organizations could establish a detailed system to prevent fraud. The implementation of automated machine learning (AutoML) decreases manual intervention needs thus making federated learning models more cost-effective and adaptable in their operations. Agencies responsible for financial laws are currently developing specific guidelines to assist federated learning adoption without violating financial guidelines.

## 5. Challenges and Future Directions of Federated Learning in Cross-Bank Fraud Detection

### 5.1 Challenges in Implementing Federated Learning for Fraud Detection

Multiple financial institutions encounter implementation difficulties while using federated learning for fraud detection although it delivers considerable operational benefits. The system encounters difficulties that combine system limitations with both regulatory issues and operational challenges and trust-related concerns between member banks. The financial sector requires proper solutions to solve implementation obstacles if it aims to deploy federated learning successfully.

#### 5.1.1 Data and Model Security Risks

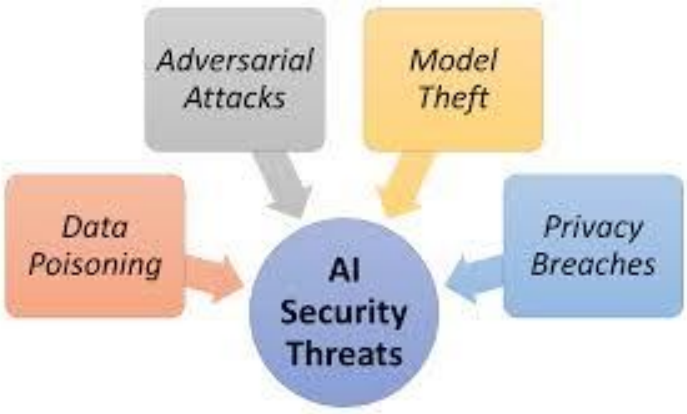


**Fig 3**

The central concern within federated learning involves protecting the safety of training data together with machine learning model content. The elimination of raw transaction data sharing between banks through federated learning does not prevent the

need to exchange model updates between the participants. The exchange of updated models contains vital information that criminals could use against financial institutions without proper data security protection. The security of model updates requires implementation of differential privacy along with homomorphic encryption and secure multiparty computation (SMPC) to avoid the reverse-engineering of sensitive transaction patterns. Privacy-preserving methods that secure the federated learning framework normally create additional computational costs that potentially reduce the system's operational efficiency.

Federated learning systems encounter additional threats from adversarial attacks which present risks to their operation. Attackers might try changing model updates to add biases or reduce detection efficiency or break the functioning of collaborative learning systems. The integrity of fraud detection models depends on implementing robust anomaly detection mechanisms together with secure aggregation techniques in order to address the identified risks.

### 5.1.2 Regulatory and Compliance Constraints

Financial institutions execute under laws that defend privacy rights of consumers while maintaining financial stability. Federated learning supports the requirements of GDPR and CCPA data regulation standards but organizations find it difficult to fully meet their obligations. Regulatory authorities can demand the implementation of clear fraud detection model audits that need to trace decision-making algorithms but these audits become complex in decentralized learning frameworks.

Diverse regulatory frameworks between financial institutions present challenges to achieve federated learning standardization when operating between different international borders. Finance organizations need to develop standardized regulatory standards for federated learning adoption so they can both achieve compliance requirements and enable mass implementation of fraud detection systems between different banks.

### 5.1.3 Heterogeneity in Banking Infrastructure

The implementation of federated learning faces challenges because different banking institutions operate with unique infrastructure structures. Each financial institution operates unique IT systems together with individual data storage elements and fraud detection systems. Connecting federated learning systems across banks presents complex challenges

because different banks need system interoperability protocols that are demanding to establish.

Establishing federated learning presents critical barriers to financial institutions with outdated fraud detection systems and they need extensive infrastructure improvements to proceed. The effectiveness of collaborative model training decreases when banks utilize different methods for data quality control and labeling practices. Standardization of data preprocessing protocols together with interoperable communication standards will help solve these integration problems to enable smooth partnership.

### 5.1.4 Computational and Network Overheads

Links between participating banks demand high computational power for both encrypted data transfers and distributed model training processes. Federated learning operates differently than conventional fraud detection systems because it decentralized training activities across separate banking institutions. Limited IT infrastructure makes this process resource-demanding for banking institutions.

Model updates exchanged between the banks during federated learning operations need encryption which results in greater network bandwidth utilization. High-level banking operations which handle many transactions could witness degradation of real-time fraud detection capabilities due to the communication costs of the system. The implementation of model compression and asynchronous learning techniques helps enhance communication performance to reduce these practical issues.

## 5.2 Future Directions for Federated Learning in Fraud Detection

The main obstacles of federated learning do not limit its ability to fundamentally transform fraud detection systems in financial institutions. Artificial intelligence developments alongside privacy-preserving framework advancement and collaborative network progress will lead to significant improvements in federated learning's future direction. The next phase of its adoption will depend heavily on various important development areas.

### 5.2.1 Advancements in Privacy-Preserving Techniques

Research on federated learning will concentrate on the development of improved privacy-protecting approaches to fortify data protection. The forthcoming generation of privacy retention will rely considerably on homomorphic encryption because it enables encrypted data computation without decrypting it. Secure multiparty computation (SMPC) will keep developing as a solution which allows banks to work together on detecting fraud while maintaining complete privacy protection.

Budgetary constraints for financial institutions would benefit from the integration of federated learning with blockchain technology because this fusion emphasizes both security and transparency enhancements. Blockchain technology provides secure procedures for documenting model updates that authenticates the integrity of fraud detection processes throughout the banking sector.

### 5.2.2 Integration with AI-Powered Fraud Detection Systems

The implementation of federated learning for fraud detection technologies will obtain more advanced artificial intelligence models across the future systems. Homemade fraud prevention methods will gain better accuracy through AI analysis systems that use deep learning methods alongside reinforcement learning and anomaly detection methods.

AI-powered federated learning models stay updated with new fraud tactics because their real-time analysis of transaction patterns runs continuously. Through the implementation of graph neural networks (GNNs) machine learning techniques will reveal hidden patterns between fraudulent operations in order to enhance fraud detection output. Through the combination of artificial intelligence with federated learning organizations can develop advanced fraud prevention systems that detect complex online threats.

### 5.2.3 Establishing Industry-Wide Collaborative Frameworks

Financial institutions need to form collaborative agreements for developing shared standardized systems which help detect fraud across multiple banking institutions. Multiple organizations including industry groups along with regulatory institutions and technology suppliers need to develop standardized processes as well as governing systems and technical standardization principles.

Public-private unions among banking institutions and fintech platforms and cybersecurity specialists will drive the adoption process of federated learning for fraud prevention systems. Through knowledge sharing combined with joint research activities the financial sector strengthens its ability to create better fraudulent activity prevention methods.

### 5.2.4 Expansion to Other Financial Use Cases

The same concept behind fraud detection enables federated learning to reshape three additional aspects of financial services such as credit risk assessment and anti-money laundering and transaction anomaly detection. Banks can benefit from federated learning as they create risk management alliances for developing accurate credit scoring models that decrease lending-related financial risks.

The program of federated learning allows financial institutions to apply its technology to identify insurance fraud and prevent investment fraud and monitor regulatory compliance. The digital economy will use federated learning as its fundamental security and risk management tool once developers extend its utility.

## 5.3 The Road Ahead for Federated Learning in Banking

The application of federated learning represents an important advancement that creates stronger financial systems which protect user privacy. The successful implementation of federated learning depends on the solution of data security risks and compliance needs and infrastructure disparities but technological developments will keep driving this success.

**Table 3: Future Prospects of Federated Learning in Fraud Detection**

| Future Trend | Expected Impact |
|---|---|
| Integration with Blockchain | Enhances security, transparency, and model integrity. |
| Advanced AI Techniques | Improves fraud pattern recognition with deep learning and graph-based models. |
| Cross-Industry Collaboration | Expands federated learning beyond banking to insurance and fintech sectors. |
| Automated Model Optimization | Reduces training time and computational costs for real-time fraud detection. |
| Regulatory Framework Development | Establishes clear guidelines for legal compliance and risk management. |

The financial sector will use federated learning as its main tool for securing operations while fulfilling regulatory requirements and developing cross-institutional relationships and solutions. Arriving banks can boost their fraud detection through AI analytics as well as privacy-safe processes that protect customer trust levels.

Therefore federated learning establishes a new financial security model which produces rapid accurate adaptive protection against contemporary cyber threats in the future. Investment and collaborative research activities in federated learning will create a secure contemporary banking environment with integrated connections.

## Conclusion

The increasing complexity and sophistication of financial fraud demand innovative solutions that balance security, privacy, and efficiency. Traditional fraud detection models, while effective in isolated environments, are often constrained by data-sharing limitations and regulatory restrictions. Federated learning emerges as a transformative approach, enabling financial institutions to collaborate in fraud detection without compromising individual data privacy.

Through federated learning, multiple banks can train machine learning models on their local transaction data while sharing only model updates, ensuring compliance with stringent data protection laws such as GDPR and CCPA. This decentralized learning framework enhances fraud detection capabilities by aggregating insights from multiple institutions, leading to more accurate and robust detection of fraudulent activities.

However, implementing federated learning for cross-bank fraud defense comes with significant challenges. Security concerns, including potential adversarial attacks and privacy leaks, must be addressed through advanced privacy-preserving techniques such as differential privacy, homomorphic encryption, and secure multiparty computation. Regulatory compliance also poses a major hurdle, requiring banks to align their federated learning initiatives with industry-specific data governance policies. Additionally, the heterogeneous nature of banking infrastructures and computational constraints necessitate the development of standardized frameworks and optimized communication protocols for federated learning.

Despite these challenges, federated learning holds immense potential for revolutionizing financial fraud detection. Future advancements in AI, cryptographic security, and collaborative frameworks will drive the adoption of federated learning across the financial sector. Integration with deep learning models, graph-based fraud analysis, and blockchain-enhanced security will further strengthen fraud prevention mechanisms. Additionally, expanding the use of federated learning beyond fraud detection to areas such as credit risk assessment, anti-money laundering (AML), and regulatory compliance will enhance financial security across multiple domains.

As the financial industry continues to embrace digital transformation, federated learning stands as a key enabler of a safer, more resilient banking ecosystem. By fostering industry-wide collaboration, financial institutions can leverage federated learning to detect fraud in real time, minimize financial risks, and enhance customer trust. Through continuous innovation and cooperation, federated learning will play a pivotal role in shaping the future of fraud prevention, ensuring that banks remain one step ahead of cybercriminals while maintaining the highest standards of data privacy and security.

## References

[1] Zhang, C., Xie, Y., Bai, H., Yu, B., Li, W., & Gao, Y. (2021). A survey on federated learning. Knowledge-Based Systems, 216. https://doi.org/10.1016/j.knosys.2021.106775

[2] Zeng, Y., Mu, Y., Yuan, J., Teng, S., Zhang, J., Wan, J., … Zhang, Y. (2023). Adaptive Federated Learning With Non-IID Data. Computer Journal, 66(11), 2758–2772. https://doi.org/10.1093/comjnl/bxac118

[3] Xia, Q., Ye, W., Tao, Z., Wu, J., & Li, Q. (2021). A survey of federated learning for edge computing: Research problems and solutions. High-Confidence Computing, 1(1). https://doi.org/10.1016/j.hcc.2021.100008

[4] Zhang, K., Song, X., Zhang, C., & Yu, S. (2022, October 1). Challenges and future directions of secure federated learning: a survey. Frontiers of Computer Science. Higher Education Press Limited Company. https://doi.org/10.1007/s11704-021-0598-z

[5] Xu, M., Ng, W. C., Lim, W. Y. B., Kang, J., Xiong, Z., Niyato, D., … Miao, C. (2023). A Full Dive Into Realizing the Edge-Enabled Metaverse: Visions, Enabling Technologies, and Challenges. IEEE Communications Surveys and Tutorials, 25(1), 656–700. https://doi.org/10.1109/COMST.2022.3221119

[6] Zhu, X., Ao, X., Qin, Z., Chang, Y., Liu, Y., He, Q., & Li, J. (2021, November 28). Intelligent financial fraud detection practices in post-pandemic era. Innovation. Cell Press. https://doi.org/10.1016/j.xinn.2021.100176

[7] West, J., & Bhattacharya, M. (2016, March 1). Intelligent financial fraud detection: A comprehensive review. Computers and Security. Elsevier Ltd. https://doi.org/10.1016/j.cose.2015.09.005

[8] Fang, H., & Qian, Q. (2021). Privacy preserving machine learning with homomorphic encryption and federated learning. Future Internet, 13(4). https://doi.org/10.3390/fi13040094

[9] Lee, J. W., Kang, H., Lee, Y., Choi, W., Eom, J., Deryabin, M., … No, J. S. (2022). Privacy-Preserving Machine Learning With Fully Homomorphic Encryption for Deep Neural Network. IEEE Access, 10, 30039–30054. https://doi.org/10.1109/ACCESS.2022.3159694

[10] Mohassel, P., & Zhang, Y. (2017). SecureML: A System for Scalable Privacy-Preserving Machine Learning. In Proceedings - IEEE Symposium on Security and Privacy (pp. 19–38). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/SP.2017.12

[11] Zapechnikov, S. (2020). Privacy-Preserving Machine Learning as a Tool for Secure Personalized Information Services. In Procedia Computer Science (Vol. 169, pp. 393–399). Elsevier B.V. https://doi.org/10.1016/j.procs.2020.02.235

[12] Papathomas, A., & Konteos, G. (2024). Financial institutions digital transformation: the stages of the journey and business metrics to follow. Journal of Financial Services Marketing, 29(2), 590–606. https://doi.org/10.1057/s41264-023-00223-x

[13] Hamann, R., Giamporcaro, S., Johnston, D., & Yachkaschi, S. (2011). The role of business and cross-sector collaboration in addressing the "wicked problem" of food insecurity. Development Southern Africa, 28(4), 579–594. https://doi.org/10.1080/0376835X.2011.605581

[14] Rachman Wintarto, Meiliani Meiliani, & Angelina Carolin. (2024). Digital Organisational Culture: Capturing Local Banking in Digital Transformation. International Journal of Social Science and Business, 7(4), 1022–1029. https://doi.org/10.23887/ijssb.v7i4.72306

[15] Chan-Lau, J. A., Mitra, S., & Ong, L. L. (2012). Identifying contagion risk in the international banking system: An extreme value theory approach. International Journal of Finance and Economics, 17(4), 390–406. https://doi.org/10.1002/ijfe.1459

[16] Machireddy, J. R. (2024). Machine Learning and Automation in Healthcare Claims Processing. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 6(1), 686-701. https://doi.org/10.60087/jaigs.v6i1.335

[17] Machireddy, Jeshwanth, Automation in Healthcare Claims Processing: Enhancing Efficiency and Accuracy(April 16, 2023). International Journal of Science and Research Archive, 2023, 09(01), 825-834, Available at SSRN: https://ssrn.com/abstract=5159747

**Citation:** Prakash Manwani. (2025). Federated Learning for Cross-Bank Fraud Defense. International Journal of Computer Engineering and Technology (IJCET), 16(2), 221-241.

**Abstract Link:** https://iaeme.com/Home/article_id/IJCET_16_02_016

**Article Link:**
https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_16_ISSUE_2/IJCET_16_02_016.pdf

**Copyright:** © 2025 Authors. This is an open-access article stributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

**Creative Commons license: Creative Commons license: CC BY 4.0**

✉ **editor@iaeme.com**