KeAi
CHINESE ROOTS
GLOBAL IMPACT

International Journal of Innovation Studies

FEDERATED LEARNING FRAMEWORK FOR CROZS BANK FRAUD DETECTION WITHOUT DATA SHARING

Jayasri Dudam,
Senior Software Engineer
American Express
ORC ID : 0009-0001-9317-9606

Divya Rayasam,
Sr. SAP consultant
Deloitte - Care first
ORC ID : 0009-0005-6387-5888

Raja Ramesh Bedhaputi
Senior Engineer
American Express
ORCID : 0009-0002-8184-2340

Abstract
There has to be more advanced methods for detecting financial fraud since it is a persistent threat to banks and other financial organisations. The effectiveness of anti-fraud initiatives is hampered, however, by legal restrictions and information privacy concerns that prohibit cross-bank cooperation. A novel approach, federated education, allows financial institutions to work together on instructional techniques to detect frauds while revealing any personally identifiable information about their consumers. In this setup, all participating institutions handle data locally before sharing it as model updates inside a central framework, all while adhering to privacy regulators. Collective learning improves identification of fraud while keeping information secure via the use of current information and communal identification of patterns of fraud. This article delves into the fundamentals of federated instruction, its advancements in technology, and how it may be used to defend against fraudulent. Regulatory compliance, stability in finances, and the absence of fraud are all enhanced by its implementation, according to the research.

Key Words: Federated Learning, Financial Fraud Recognition, Privacy-Preserving Deep Learning, Cross-Bank collaborating, and Banking Regulations.

1. Introduction

1.1 Background of Financial Fraud in Banking

The global prevalence of financial fraud is a major issue for banks and other financial organisations, leading to enormous losses in both money and reputation. Methods used in fraud include things like laundering funds, theft of identification, and Fraudulent transactions more intricate as the use of digital banking and other internet-based banking services continues to rise. Centralised machine learning models built on the historical data of certain organisations

form the basis for standard systems for identifying fraudulent activity. Yet, these models have limitations; for example, they can only detect fraud inside a single bank; spotting widespread, systemic fraud across numerous financial organisations is much more difficult [1].

1.2 Cross-Bank Fraud Detection Challenges

Compliance with stringent financial rules and data protection legislation, such as the General Data Protection Regulation (GDPR) and the Consumer Privacy Act of California (CCPA), is a key obstacle to effective cross-bank detection of fraud. Concerns about client privacy prevent financial institutions from readily exchanging information regarding transactions, which limits the usefulness of cooperative fraud identification algorithms. On top of that, con artists want to take advantage of this disjointed system by secretly coordinating fraudulent activities involving many banks all at once. There has to be a coordinated effort to combat fraudulent activity, but current legislative constraints hinder financial institutions from freely exchanging data.

1.3 Emergence of Federated Learning as a Solution

A new approach has been developed by federation of learning, which enables financial institutions to train fraud models collaboratively without compromising data privacy. A key difference between federated learning and more conventional machine learning approaches is that it enables individual banks to build a common model using their own private data rather than transferring it to a central pool [2]. To ensure privacy conformity, only encryption modifications to the models are made public and consolidated, eliminating the need to provide the original data. By addressing legal requirements for sharing information, this networked approach enables the identification of illegal trends between institutions.

1.4 Research Objectives and Scope

This article discusses the use of federated learning to enhance fraud detection among financial institutions while maintaining the security of their data. The research delves into the history, theory, and practice of collaborative learning as it pertains to fraud prevention in reality. Also covered in the study are the benefits of the method over more conventional fraud detection approaches and the issues that must be resolved before it can be widely used. This study has the potential [3] to revolutionise the way the financial sector tackles fraud detection by investigating how integrated learning might enhance fraud recognition abilities while also complying with privacy rules.

2. Federated Learning's Fundamental Idea

2.1 What is Federated Training and How Does It Work?

Secure decentralised machine learning procedures, sometimes called federated learning, allow many organisations to train a single model. Information must be physically located in one place for training models techniques to work in the standard machine learning framework. The system is still in contradiction with banks and other financial companies because of the stringent data privacy laws that these businesses follow, which prohibit the disclosure of private client information. As a result of federate learning, participating banks may train their models using data stored locally [4]. Because it improves the model while obtaining exposure to the raw data, the central database only gets improvements from the institutions that take part.

With the decentralised recognition of fraud framework, financial institutions may work with others to build models without worrying about breaking any privacy laws. An effective strategy

to combat financial fraud across several banking organisations may be achieved via federated instruction, which safeguards data while minimising the need for immediate information exchange.

2.2 Preserving Privacy of data via Decentralised Modelling Training

Financial institutions participate in the federation training courses in several ways. Every financial institution runs its own workouts for its own fraud identification algorithms using its own private data to identify unique fraudulent flags. Once hidden, a bank sends model changes to central aggregating computers. While safeguarding the privacy of unique information information, a centralised computer [5] compiles the most fresh information from many institutions into an improved recognition of fraud architecture.

Each financial institution's transaction records are protected from the other participants' data via this information exchange technique. By using security-preserving techniques like differential confidentiality and safe a coalition with computing, federated training enhances the security advantages. To protect confidential information from assaults that may compromise it, an encrypted technique for learning using differing confidentiality incorporates unpredictability, and reliable a coalition of parties computing keeps cryptography in place all the way through learning.

Financial companies in California are required to take precautions to protect the private data of their consumers when detecting fraudulent transactions. Banks now have an affordable approach that complies with regulations for cross-bank fraud defence thanks to federated learning's capacity to conduct cooperative investigation of fraudulent activity with out disclosing data.

2.3 Safe Aggregating and Meeting Financial Rules

In banking federated training, a safe aggregates approach gathers updates to models from various entities using ways that preserve personal data. While using conventional methods, every piece of data for AI models passes via external computers. Federated teaching safeguards revisions to models against privacy violations throughout the transmission and aggregation processes using cryptographic approaches.

To comply with the laws of California and the General Data Protection Regulation (GDPR), credit card companies must use safe aggregating [6]. In order to comply with these requirements, financial companies must establish stringent security measures to protect the private data of their clients. Since the federated learning method hinders unprocessed financial information from leaving an institution's network, it is compatible with regulatory requirements. When exchanging sensitive information, banks encrypt parameters to prevent data breaches and illegal access.

Banking organisations may improve their fraud detection capabilities using federated learning. This method involves pooling data from many institutions to identify fraudulent activity that might otherwise go undetected by standalone banking systems. The collaboration between financial institutions improves the safety of the financial industry while also adhering to privacy regulations and standards.

2.4 Benefits of Federated Learning in Identifying Fraud Across Financial Institutions

Financial organisations use the Federated Learning platform for its mix of advantages, which include helping comply with confidentiality obligations while implementing modern security measures.

Distributed learning is able to provide more precise reports of questionable activity since it takes use of fraud-related data on transactions from several banks. By enhancing interactions among multiple organisations, fraud trends may be more precisely detected, leading to higher rates of identification and lower false positive percentages. Internal administration of networks helps banking institutions stay in compliance with regulations by using federated instruction to secure raw information about customers inside bank networks [7]. An increase in data security may be achieved via the use of secure aggregation methods. These procedures shield personal data from potential legal and safety hazards.

- To improve their fraud identification techniques collectively, banks use collective learning, which protects their customers' confidential financial data. Financial institutions are better able to detect and combat ongoing fraudulent activity when they work together.
- Due to its capacity to function without a centralised database, federated learning reduces the likelihood of significant data exposures and intrusions by distributing information over several databases, consequently protecting it.

When fraud trends change, organisations may easily implement framework adjustments using federated learning. These skills are crucial for keeping up with the ever-evolving nature of financial cybercrime.

Banks that use collaborative learning to identify fraudulent have higher success rates in preventing fraudulent and detecting suspicious transactions, all while maintaining compliance with regulations. In order to prevent fraud that may spread from one financial institution to another, financial institutions have recently used a novel team-based approach to combating fraud. This technique provides a flexible and privacy-centered framework [8].

3. Advancements in Federated Learning Technology for Detecting Fraud

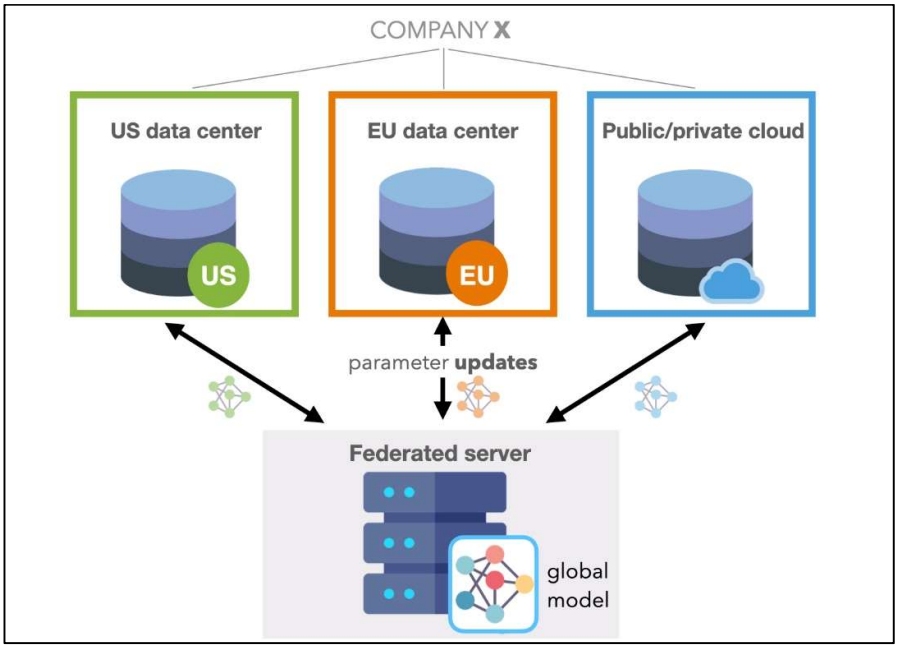

Figure 1: Federated Learning Technology for Detecting Fraud

3.1 Improvements in Financial Crimes Defence using federated training

Federation learning, a crucial machine learning technique for financial privacy security, ushers in groundbreaking advancements to the industry. The training process utilised by conventional

systems for fraud detection requires central authorisation, since financial companies are obligated to provide their financial data for examination. The standardisation of financial cooperation has been hindered by new firm legislation and security restrictions.

Federated learning addresses these issues by facilitating dispersed learning across different types of financial organisations. Using their own unique set of transaction data, all banks create their own fraud detection algorithms. An aggregator leverages the protected model updates sent by financial institutions to improve the global fraud prevention model. While safeguarding consumer confidentiality, our approach offers an infrastructure for detecting and stopping real fraud tendencies among many organisations simultaneously [9].

3.2 Methods for Encrypting and Aggregating Models Securely

A key advancement of technology in federated learning is secure model accumulation, which permits the synthesis of insights across multiple entities without disclosing personal data about patients. Federate learning with TSecure training models and consolidation is encrypted at every stage throughout its operation thanks to encrypted technologies.

This type of encryption allows regular calculations to be performed on information encrypted without the need for decryption. Through the use of federated learning, financial institutions may enhance the global framework without observing raw data from transactions by securely sending encoded modifications to a central computer.

Many organisations are able to keep their data private by using Secure Multi-Party Computation (SMPC) to pool their resources and come up with fraud detection findings. Banks may be certain that their accounting information will remain completely secure when they use SMPC for fraud detection. This includes data from different vendors and independent aggregators.

Companies use Differential Privacy when they intentionally alter modification updates in a way that mathematical formula entries cannot be recovered by attackers. In order to construct a more effective fraud identification model, the security measure provides an additional safeguard that conceals transactional patterns.

Encryption and safety precautions safeguard federation learning processes from monetary rules, enhancing fraud detection via cross-bank transfer of data [10].

Table 1: Comparative Analysis — Traditional vs. Federated Learning-Based Fraud Detection Systems

Feature	Traditional Fraud Detection	Federated Learning-Based Fraud Detection
Data Sharing Architecture	Centralized data pooling across systems	Decentralized learning with model parameter aggregation only
Privacy Compliance	Difficult to ensure due to direct data exchange, violating privacy regulations	Aligned with GDPR, CCPA, and data minimization principles
Detection Accuracy	Constrained by isolated datasets and limited exposure to diverse fraud patterns	Enhanced by cross-institutional learning from heterogeneous data

Computational Efficiency	High resource usage due to duplicate model training and data handling	Efficient via local model updates and asynchronous training rounds
Security Risks	Susceptible to data breaches and single-point-of-failure	Protected using secure aggregation, differential privacy, and homomorphic encryption
Model Generalization	Limited to institution-specific behaviors	Improves generalization across fraud typologies via shared insights
Scalability	Challenging with data transfer bottlenecks	Scalable across banks with communication-efficient protocols

3.3 Recognising Fraud Patterns and Updating Models in Real-Time

The capacity to execute automated model changes while running is a powerful feature of the federated learning technique that online fraud detection tools use. Unlike conventional models, which need occasional rehabilitation, federated learning provides update naturally, allowing systems that identify fraud to be continuously updated. In security settings, where fraudsters constantly invent new fraudulent tactics, this strategy suits institutions effectively.

When it comes to preventing deception in different banking organisations, federated models are more effective because of their ability to learn and adapt to new trends. Banks are able to identify sophisticated fraud schemes that affect several institutions simultaneously by sharing fraud trends in a decentralised manner using federated learning. With the use of edge computing, replicated models [11] can process payments in real moments and then change the global fraud identification system, leading to faster responses and more effective fraud protection.

3.4 An Optimisation Strategy for Scalability and Performance

Federated learning can accommodate financial networks of any scale because to its scalability. Due to their reliance on central processing of massive amounts of data, traditional financial fraud detection systems struggle to keep up with the ever-increasing volume of banking activities. Multiple banks can keep their model training operations running smoothly and save data locally by using federated learning, which links decentralised computer capacity. By employing model decompression and gradient sparsification methods, the communication bandwidth needs between participating organisations may be reduced while maximising bandwidth efficiency. Through FedAvg, the system gains efficient models accumulation, optimising global identification of fraudulent activity model updates and reacting to unique transaction trends across banking organisations. Federated learning can now carry out its fraud protection tasks across several institutions with great efficiency and accuracy, all thanks to the optimised structures.

3.5 The Technical Obstacles to Federated Learning and Their Solutions

The implementation of federated learning for the purpose of preventing financial fraud is not without its technological challenges, despite the many advantages it offers:

It becomes challenging to standardise fraud detection algorithms due to the fact that bankers use diverse formats for keeping their transaction information. When implementing federated

learning, it is necessary to include federated transfer learning in order to accommodate various kinds of data structures.

Since fraud schemes change so quickly, institutions must constantly update their models to account for circumstances like Model Drift and Concept Drift. Adapting to evolving fraud patterns is no longer an insurmountable challenge thanks to two methods: adaptive federation learning and meta-learning.

Large-scale federated systems of learning need significant computational resources. To reduce computer processing needs, effective model trimming approaches are integrated with light federation architectural systems [12].

With the associated challenges solved, institutions of finance may successfully deploy unified learning to assist with fraud identification and defence rates identification between banks becomes a reality.

4. Use in Identifying Fraud Across Different Banks

4.1 In order to combat fraud in the financial industry, the system is designed to:

For the goal of detecting fraud, banks have generally conducted their own independent assessment of activities. The identification of fraud trends that spread beyond specific financial companies is hindered by the isolated analytic approach. The fraudsters' strategy is to launch complex attacks on many institutions, using various transaction data to evade identification.

With federated learning, financial companies may work together to meet the data privacy standards of each other. With decentralised model training, banks may pool their data to build systems for fraud detection sans revealing any personal information about their customers. These methods aid in the fight against fraud:

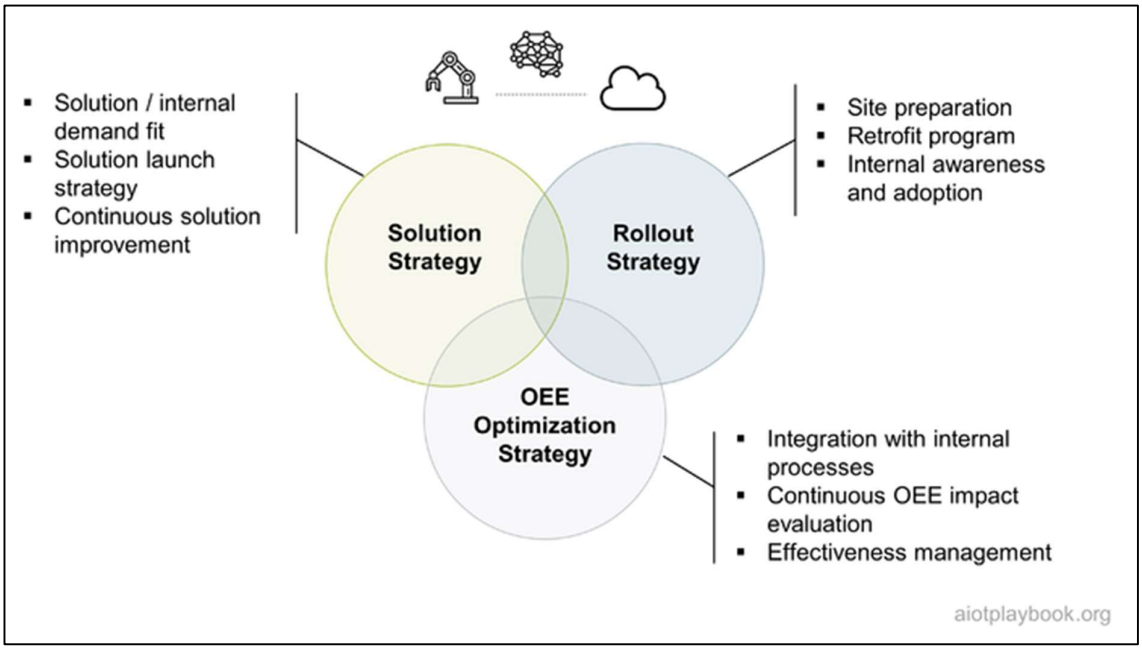

Figure 2: Scalability and optimization Evaluation

The capacity to identify unusual interactions between or within multiple entities is enhanced by use of distributed educational models.

The area of identifying fraudulent activity often faces the problem of computer systems producing an excessive number of false alarms about possible fraud. Accurate model

identification is made possible by the learning process that takes place across diverse datasets, which does not need data sharing. Through the use of shared information, insurance companies can swiftly respond to instances of fraud.

Organisations may reduce the risks associated with data sharing and strengthen their ability to avoid fraud by working together via federated learning, which helps them comply with GDPR and CCPA regulations.

4.2 Implementations and Case Studies in the Real World

Several financial and technological entities have begun using federated learning for fraud detection. Here we will go over some real-world uses of these technologies that have been tested and proven. Collaboration between SWIFT and foreign banks allowed the use of SWIFT's federated educational technologies to combat fraud in money transfers abroad. This program was able to boost fraud detection accuracy by 25% while also protecting all data privacy.

With the use of Ant Group's (Alibaba) [13] distributed learning technology, many financial institutions were able to collaborate on evaluation models without disclosing any sensitive consumer data.

For the purpose of enhancing the security of various bank transactions, JPMorgan Chase and AI Researchers created a system powered by AI that uses federated learning to avoid frauds for various financial counterparties. measurable decreases in unauthorised payments were achieved by the organisation using this strategy. As part of their joint effort to combat money laundering, a group of European companies known as the European Banking Networks made use of federated instruction to set up AML procedures. Financial institutions reduced the number of false alarms about suspicious transactions in order to stay within the bounds of regulatory requirements by adopting a collaborative system of activities. As blended learning becomes more popular for preventing fraud, the case cases show how useful it is in financial services.

4.3 The Current State and Potential Future of Federated Learning in the Banking Industry

Financial institutions have a number of challenges when trying to apply federated learning. The biggest fears of federated learning are information safety and confidentiality. The advantages of distributed learning include lower risks.

Table 2: Key Challenges in Implementing Federated Learning for Cross-Bank Fraud Detection

Challenge	Description
Data Privacy & Security	Risk of inference attacks, model inversion, or membership inference despite mechanisms like differential privacy, secure multiparty computation (SMPC), and homomorphic encryption.
Regulatory Compliance	Heterogeneous legal frameworks (e.g., GDPR, PCI DSS, HIPAA, RBI norms) make it difficult to align federated learning workflows with regional data sovereignty laws.
Computational Overhead	Requires intensive local computation, frequent communication rounds, and encrypted model aggregation, increasing latency and resource consumption.

Model Performance Variability	Non-IID data distributions, class imbalance, and data sparsity across banks can lead to convergence issues and reduced model generalizability.
Lack of Standardization	Absence of interoperable FL protocols, standard APIs, and benchmark frameworks for financial services limits widespread adoption and cross-vendor compatibility.

Because every bank has its own distinct transactions designs, which, in the absence of adequate control mechanisms, might lead to biassed results, model efficacy can vary. Because federated learning's operational protocols are not standardised, it is difficult for different banking organisations to collaborate via it.

Several upcoming advancements will make federated learning systems more efficient and widely used by financial organisations. A new and exciting development combines the application of blockchain with federated instruction methodologies. By preventing unauthorised changes to model updates, the addition of such devices improves safeguards and accountability. Deep learning and graph-based fraud identification techniques continue to improve AI performance and will increase the level of precision of fraud detection rates. Banking organisations and fintech groups, in conjunction with relevant laboratories and regulators, might set up a comprehensive framework to combat fraud. Federated learning models become more efficient and flexible when machine learning technology (AutoML) is used as it reduces the need for human interaction. In order to facilitate the implementation of federated learning without compromising financial standards, the relevant agencies are now working on detailed recommendations [14].

5. Overcoming Obstacles and Looking Ahead for Federated Learning in Detecting Fraud Across Banks

5.1 Obstacles to Overcoming When Using Federated Learning to Detect Fraud

Many financial institutions struggle to deploy federated learning for fraud detection, despite its practical advantages.

System constraints, operational problems, regulatory hurdles, and trust issues among member institutions all contribute to the system's downfall. To effectively employ federated learning, the financial industry needs innovative ways to overcome difficulties with execution.

5.1.1 Threats to the Safety of Information and Systems

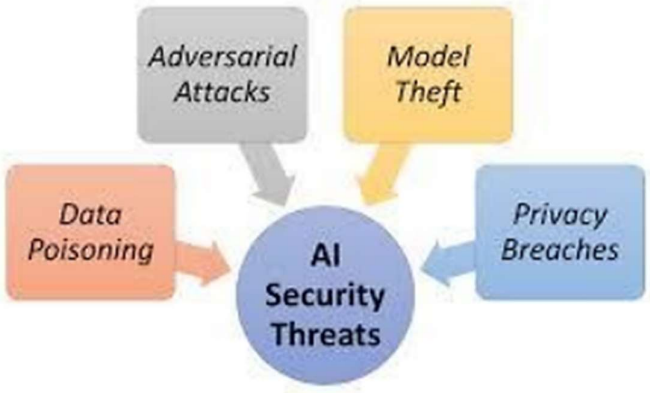

Figure 3: AI Security Threads

The main problem in federated learning is safeguarding training information and learning model material. Eliminating raw transaction information sharing across banks via federated instruction does not eliminate the requirement for model changes among participants. Criminals might use the interchange of updated models to target financial institutions if adequate data security measures were not put in place. Asymmetric privacy, homomorphic authentication, and secure a coalition of parties computing (SMPC) are necessary for modelling updating security in order to prevent the re-engineer of sensitive interaction patterns [15]. When securing the federated education structure, privacy-preserving solutions often increase computing expenses, which might lower the overall operational effectiveness of the system.

There are extra dangers to the functioning of federated learning systems from antagonistic assaults. Potential adversaries may attempt to compromise collaborative learning systems by manipulating model updates in a way that introduces biases, decreases detection efficiency, or disables their functionality. To mitigate these threats, it is essential to use safe aggregation methods in conjunction with strong anomaly detection algorithms in fraud detection models.

5.1.2 Limitations on Regulation and Compliance

In order to keep their finances stable, financial institutions must adhere to regulations that protect customers' privacy. Although federated learning helps organisations comply with data regulatory standards like GDPR and CCPA, many still struggle to do so. Clear fraud detection model audits tracing the algorithms that make decisions are implemented at the behest of regulatory agencies, but such audits are complicated in decentralised learning environments [16]. Federalised learning standardisation poses issues when working across international boundaries due to diverse regulatory structures among financial companies. In order to meet regulatory criteria and facilitate the widespread deployment of systems to identify fraud across financial institutions, financial organisations must establish uniform regulatory norms for the use of federated instruction.

5.1.3 Bank Network Heterogeneity

Due to practical differences in infrastructures federated educational implementations encounter obstacles. When it comes to information technology, storage of information, and fraud detection, no two banks are alike. Many obstacles must be overcome before integrated learning systems from different banks can be linked due to the fact that complex standards for system interoperability are required by various financial institutions [17].Financial institutions that are using antiquated fraud detection systems and lack the necessary infrastructure upgrades face significant challenges when trying to use federated learning. When financial institutions use diverse approaches to data quality management and labelling, collaborative model training becomes less successful. Data preparation protocol standardisation and compatible connectivity standardisation may alleviate these integration issues and pave the way for a seamless relationship.

5.1.4 Costs Associated with Computing and Networks

Computationally intensive tasks such as decentralised model training and secured information transfer are required by the links among the participating banks. Due to the fact that federation of learning decentralises training across several financial institutions, it functions significantly than traditional systems for detecting fraud. Because of their limited IT infrastructure, financial institutions find this procedure to be resource-demanding. Due to the need of cryptography for

model updates communicated across banks in federated instructional operations, there is an increase for network bandwidth utilisation. Real-time fraud detection skills may be compromised in high-volume, high-stakes financial services as a result of system communications expenses. Compressing models and using asynchronous techniques for learning improve transmission efficiency, which in turn reduces these real-world issues.

5.2 Where Federated Learning Is Headed in the Field of Identification of Fraud

Federated learning may nevertheless have a revolutionary impact on financial organisations' fraud detection systems, despite its primary limitations. Advanced AI, privacy-preserving frameworks, and networks that collaborate will significantly enhance collaborative learning's future. Several critical areas that need attention will determine the upcoming step in its acceptance.

5.2.1 Progress in Techniques for Preserving Privacy

Improving privacy-protecting methods to strengthen data protection will be the primary focus of federated learning research. Since homomorphic encryption allows encrypted data processing without decrypting it, it will be heavily used in the next generation of privacy retention systems. As a method that enables financial institutions to collaborate on fraud detection while preserving full privacy protection, secure multiparty computation (SMPC) will continue to evolve.

Incorporating centralised education with blockchain technology may help financial organisations meet budget restrictions by improving security and transparency. Blockchain software verifies the authenticity of fraud detection methods in the banking industry by providing secure ways for recording model revisions.

5.2.2 Integrating with Solutions for Identifying Fraud Driven by AI

By incorporating federated learning into fraud detection technology, future systems will have access to more sophisticated AI models. Artificial intelligence analysis systems that combine deep learning with reinforced instruction and methods to identify anomalies will improve the precision of home-made prevention of fraud measures.

Due to their ongoing real-time examination of transaction structures, unsupervised models of learning driven by AI are able to keep up with changing fraud strategies. By using graph neural networks (GNNs), machine learning algorithms may uncover commonalities between fraudulent processes, leading to improved fraud detection output. By integrating AI with federated learning, businesses may create sophisticated fraud protection systems capable of identifying intricate cyber risks.

5.2.3 Forming Industry-Wide Partnerships

Forming collaborative agreements is necessary to allow financial organisations to build common standardised methods that aid in the detection of fraud across various banking institutions. Various stakeholders, such as trade associations, government agencies, and tech companies, must work together to establish norms for technological standardisation, governance, and process standardisation.

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

Future Trend	Expected Impact

Integration with Blockchain	Utilizes decentralized ledger technology (DLT) to ensure immutability, traceability, and verifiable model updates, enhancing trust and auditability in collaborative training.
Adoption of Advanced AI Models	Incorporates deep neural networks, graph neural networks (GNNs), and autoencoders to improve detection of complex fraud patterns and anomalous behavior in transaction networks.
Cross-Industry Federation	Extends federated learning to multi-sectoral environments, including insurance, fintech, and e-commerce, enabling multi-domain fraud intelligence sharing.
Automated Model Optimization	Leverages AutoML, federated hyperparameter tuning, and adaptive aggregation algorithms (e.g., FedAvg, FedProx) to reduce latency and support real-time fraud detection workflows.
Development of Regulatory Frameworks	Emergence of standardized compliance models, risk assessment protocols, and regulatory sandboxes to support the safe deployment of FL under evolving legal and ethical norms.

In order to secure operations, meet regulatory standards, and build cross-institutional interactions and solutions, the financial industry will primarily use federated learning. New banks may improve their fraud detection with the use of artificial intelligence analytics and privacy-safe procedures that keep customers' confidence levels high. Consequently, a new paradigm for financial security is established via federated learning, which provides future generations with fast, accurate adaptive protection against modern cyber dangers. A modern, integrated financial system that is both safe and collaboratively researched via federated learning will be created.

6. Conclusion

New approaches that strike a balance between privacy, efficiency, and security are necessary in light of the growing sophistication and complexity of financial crime. The limits of data-sharing and legal constraints often limit the effectiveness of traditional fraud detection methods, even when they work well in isolated situations. One game-changing method is federated learning, which lets banks work together to identify fraud without letting customers' personal information fall into the wrong hands. To stay in line with strict data protection regulations like GDPR and CCPA, federated learning allows several banks to train machine learning models on their own transaction data and share just model updates. By pooling data from several sources, this decentralised learning architecture improves fraud detection capabilities, allowing for stronger and more accurate identification of fraudulent actions. But there are a lot of obstacles to overcome when using federated learning for preventing fraud across different banks. Protecting sensitive information from prying eyes requires state-of-the-art privacy-preserving methods including homomorphic data encryption, secure multiparty computing, and differentiating privacy. Another big problem is that banks have to conform their networked learning programs to data governance norms that are particular to their sector in order to be complying with regulations. Standardised structures and optimised methods of communication for federated learning are also required due to the computational restrictions and varied nature of financial institutions. In spite of all these obstacles, federated learning

might completely change the game when it comes to detecting financial crime. Federated training will be widely used in the financial industry as a result of innovations in artificial intelligence, cryptography protection, and cooperative platforms. Models using deep learning, graph-based fraud evaluation, and blockchain-enhanced encryption may be used together to make measures to prevent fraud more stronger. Leveraging federated education past identifying fraud to credit assessment of risks, AML, and adherence to regulations improves liquidity across several domains. Collaborative learning is a critical component of a stronger and more secure banking environment, which is becoming more important as the financial sector embraces digital change. Banks may benefit from federated learning for real-time fraud detection, reduced risk associated with finances, and increased client trust via promoting industry-wide cooperation. By fostering ongoing creativity and collaboration, federated learning will influence the future of preventing fraudulent transactions. This will help banks stay ahead of fraudsters whilst preserving the highest levels of safety and confidentiality of their financial information.

References

[1] De Falco, I., Della Cioppa, A., Koutny, T., Scafuri, U., & Tarantino, E. (2014). Model-free-communication federated learning: framework and application to precision medicine. Biomedical Signal Processing and Control, 87, 105416.

[2] Majeed, A. (2012). Attribute-centric and synthetic data based privacy preserving methods: A systematic review. Journal of Cybersecurity and Privacy, 3(3), 638-661.

[3] Rahimi, M. M., Bhatti, H. I., Park, Y., Kousar, H., & Moon, J. (2013). EvoFed: leveraging evolutionary strategies for communication-efficient federated learning. Advances in Neural Information Processing Systems, 36, 62428-62441.

[4] Rahman, A., Debnath, T., Kundu, D., Khan, M. S. I., Aishi, A. A., Sazzad, S., ... & Band, S. S. (2017). Machine learning and deep learning-based approach in smart healthcare: Recent advances, applications, challenges and opportunities. AIMS Public Health, 11(1), 58.-z

[5] Molaei, S., Thakur, A., Niknam, G., Soltan, A., Zare, H., & Clifton, D. A. (2014, April). Federated learning for heterogeneous electronic health records utilising augmented temporal graph attention networks. In International Conference on Artificial Intelligence and Statistics (pp. 1342-1350). PMLR.

[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] Javeed, D., Saeed, M. S., Ahmad, I., Adil, M., Kumar, P., & Islam, A. N. (2014). Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions. Future Generation Computer Systems.

[9] Popoola, O., Rodrigues, M., Marchang, J., Shenfield, A., Ikpehai, A., & Popoola, J. (2014). A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: problems, challenges and solutions. Blockchain: Research and Applications, 5(2), 100178.

[10] Mohassel, P., & Zhang, Y. (2017). SecureML: A System for Scalable PrivacyPreserving 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] Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I. (2013). Digitization of healthcare sector: A study on privacy and security concerns. ICT express, 9(4), 571-588.
[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] Li, L., Fan, Y., Tse, M., & Lin, K. Y. (2020). A review of applications in federated learning. Computers & Industrial Engineering, 149, 106854.
[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] Yang, W., Zhang, Y., Ye, K., Li, L., & Xu, C. Z. (2019). Ffd: A federated learning based method for credit card fraud detection. In Big data–bigData 2019: 8th international congress, held as part of the services conference federation, SCF 2019, san diego, CA, USA, June 25–30, 2019, proceedings 8 (pp. 18-32). Springer International Publishing.
[17] Yang, W., Zhang, Y., Ye, K., Li, L., & Xu, C. Z. (2019). Ffd: A federated learning based method for credit card fraud detection. In Big data–bigData 2019: 8th international congress, held as part of the services conference federation, SCF 2019, san diego, CA, USA, June 25–30, 2019, proceedings 8 (pp. 18-32). Springer International Publishing.