Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Federated Learning Approaches for Fraud Detection in International Payment Systems

1st Vijaya Rama Raju Gottimukkala
Senior Dev/ Systems Engineer
ORCID ID: 0009-0009-6758-6716

ARTICLE INFO	ABSTRACT

Received: 26 Oct 2024

Revised: 14 Nov 2024

Accepted: 22 Dec 2024

Although fraud detection methods based on machine learning (ML) have gained momentum, many organizations still rely on rule-based detection methods. Additionally, publicly available datasets are not representative of the types of fraud most commonly faced by the organizations. Therefore, industry partners can benefit from a jointly trained ML model capable of detecting patterns shared across banks or across cross-border payments. However, organizations face regulatory constraints when sharing transaction data or account details with industry peers. Federated learning (FL), an approach that enables collab- orative ML without data sharing, represents a potential solution to this problem. Within the context of international payments, this work discusses common types of fraud and considers how FL can help alleviate these burdens. A specific federated learning framework aligned with fraud detection workflows is proposed. The approach supports both vertical and horizontal architec- tures, incorporates techniques for handling heterogeneous data distributions, and promises to minimize sensitive data sharing. A safeguard associated with the peer-to-peer architecture is the avoidance of a single point of failure, whereas a weakness arises from the need to trust communications made between institutions of the same jurisdiction. Dense anomaly signals within a given jurisdiction can improve soundness by assisting region-based model updates.

Keywords: Federated Learning,Fraud Detection,Cross- Border Payments,Privacy-Preserving Machine Learn- ing,Financial Crime Prevention,Decentralized AI,Anomaly Detection,Payment System Security,Collaborative Model Training,Data Sovereignty in Finance.

I. INTRODUCTION

Fraudulent transactions globally challenge the demand for secure payment systems, with constant technology improve- ments exploited by criminals. The introduction of networked payment systems allows the illicit practice of card-not-present fraud; merchants lack real-time control over transactions, and issuing and acquiring banks process them independently. Methodology to prevent fraud in cross-border payments or between institutions lacks a suitable approach. Transfer learn- ing requires sharing training data, violating bank-client confi- dentiality and regional data localization regulations. Federated Learning developments might serve a solution. While working in the same network, banks, payment processors, and card- issuers are subject to different jurisdictions that regulate data localization and prohibit transferring user-sensitive informa- tion. Thus, trying to diminish the risk of lack of privacy or latency that these networks face and taking advantage of the shared resource, Federated Learning appears as a solution. Simulating payments in an electronic network capable of monitoring FrameNet or Transa and using a training dataset that aims to solve some types of fraudulent behaviors that these systems can detect, it is possible to envision the design of a Federated Learning model without relying on a centralized bank. Its findings allow to establish a training model for the real application in an FL environment.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

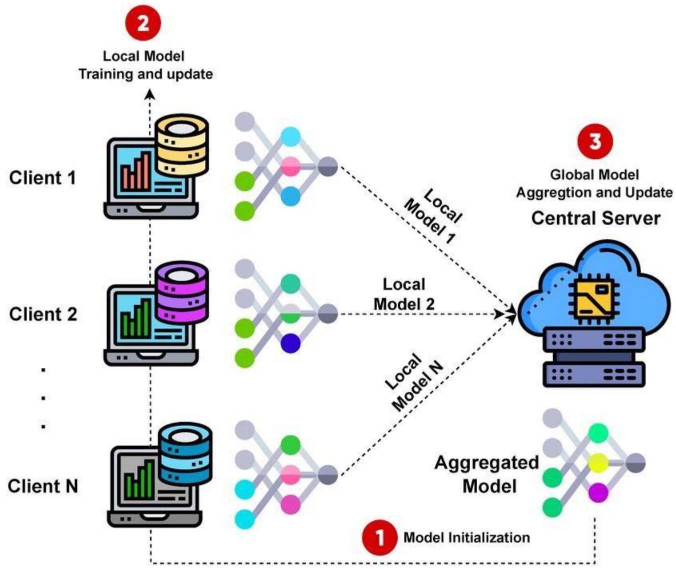

Fig. 1. Federated Learning Architecture for Global Payments

A. Problem Statement and Motivation

Fraud is a major obstacle to a rapid expansion of the global payment economy. A myriad of financial institutions and payment service providers would be able to substan- tially improve their antifraud models in their cross-border processes by using machine learning techniques, but they cannot freely share transaction data across legal boundaries, primarily due to privacy and data localization regulations, which restrict the utilization of cross-border data. In pay- ment processes there are very different fraud typologies that use entirely different signals, such as card-not-present fraud, chargebacks, merchant fraud, synthetic identities, or cross- border anomalies, and their antifraud signals often reside with different participants. Hence, it has become impossible to train accurate antifraud models that are sufficiently gen- eralized across jurisdictions. Nevertheless, these participants

could leverage Federal Learning techniques to build globally accurate antifraud models while preserving the privacy of their transaction data. Therefore, Federated Learning emerges as the natural solution for the extremely practical and important problem of legally sharing data to combat fraud in a modern payment economy. Generally, it is advocated that FL models in payment ecosystems be established together with the relevant regulatory authorities for cross-schema payment nodes. The CCPA-like regulations implicitly require that no identifiable, commercially exploitable information should be inferred from the model parameters possessed by any single node. It should also be guaranteed that the models are sufficiently accurate to meet the antifraud objectives of the operators of these nodes. Because the banks are data-hungry and FL is a bandwidth- consuming technique, a realistic proposal should also take into consideration machine-learning techniques for reducing the costs of communication among edge nodes, particularly those nodes located outside the continental US.

B. Scope and Definitions

Federated Learning (FL) typically refers to a Machine Learning (ML) methodology wherein a large amount of data is distributed across edge clients (peers) while a federated central server is responsible for aggregating individual and/or personalized model updates. FL aims to preserve privacy while addressing the desynchronized, non-IID, human-device gap, networking constraints (connectivity, latency, bandwidth), geographical conditions (data localization and cross-border data flows), and the limited communication effort of mobile devices all over the world. These FL objectives are shown to be particularly relevant for Machine Learning methods for Fraud Detection in International Payments built on the data provisioning, activation and detection graph. A centralized storage paradigm for transaction data goes against privacy, GDPR and CCPA norms and presents an attractive target for hackers. Therefore, several payment networks have opted for an architecture where payment processors are just facilitators of transactions and do not store the transaction data. Addition- ally, cross-border payment patterns result in multiple LOC- 1 payment attempts across different payment networks and recurring attempts

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

using multiple cards or accounts issued from different regions to commit fraud on the same bank. Consequently, banks and payment processors become the logical participants in a Federated Learning Network for Fraud Detection in International Payments. Data from banks and payment processors that are part of a payment network can be utilized by issuers and acquirers for fraud pattern recognition at different levels.

II. Background and Related Work

Fraud detection operates at the intersection of machine learning (ML) and cyber-security; however, the sheer amount of potentially available data often remains untapped. Clustering data science teams in a same jurisdiction will not help. Why not just do it within the political borders of a need-known geography? Well, the modus operandi of

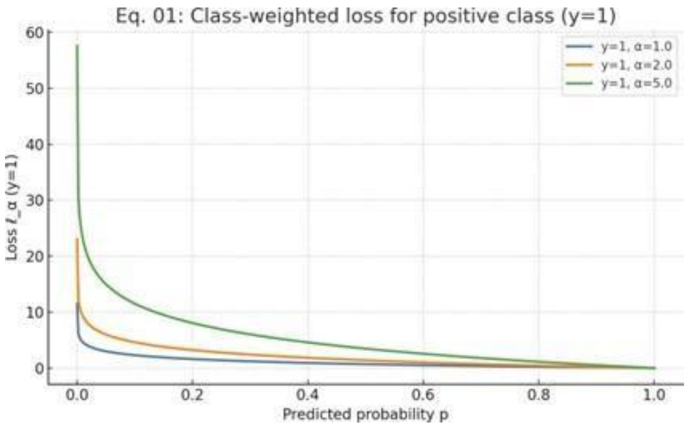

Fig. 2. Class-weighted loss for positive class (y=1)

money-without-money has no borders and is supported by people with money that do not need any need. Phylogenetic analysis is a very mathematical term, but it means well: paths of fraud are tried and tested in a relatively safe cyberspace before being launched on a global scale with real impact. A wealth of ML literature has sought to tackle the problem using publicly available data sets. Trained models cannot be applied in a real-world scenario where the required data are not gathered in a same place and time. Nor can they be applied to similar places or times where the flow requires careful monitoring as well. They were trained with data signals that are very different and unrelated to another distribution. Yet at the end of the day crime hardly changes; it adapts to circumstances and catches global attention for a while before swiftly disappearing. Thanks to FL-driven collaboration, although the data lie in different AI minds, luck stratification using simulators may help the path for bank nodes in the flight-business and flight-of-money business.

Equation 01: Class imbalance (typical in fraud) — weighted loss

With positive class weight $\alpha > 1$

$$\ell_\alpha (y, p) = -[\alpha y \log p + (1 - y) \log(1 - p)] \qquad (1)$$

For $y = 1$: $\ell_\alpha = -\alpha \log p$ (loss and $|\nabla|$ increase with $\alpha \rightarrow$

the learner pushes $p \uparrow$ faster).

For $\alpha = 0$, $y = 0$: $\ell = -\log(1 - p)$ (independent of α). Gradients (w.r.t. p): $\partial\ell/\partial p = -\alpha y/p + (1 - y)/(1 - p)$..

A. Fraud Types in International Payments

Fraudsters employ tactics that convert money, goods, or ser- vices into financial gain without the associated compensation, resulting in various losses and distinct fraud categories. Five primary types of fraud commonly encountered in international payments are highlighted below: chargebacks, card-not-present fraud, merchant fraud, synthetic identity fraud, and anomalies in cross-border payments. Chargeback fraud occurs when a

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

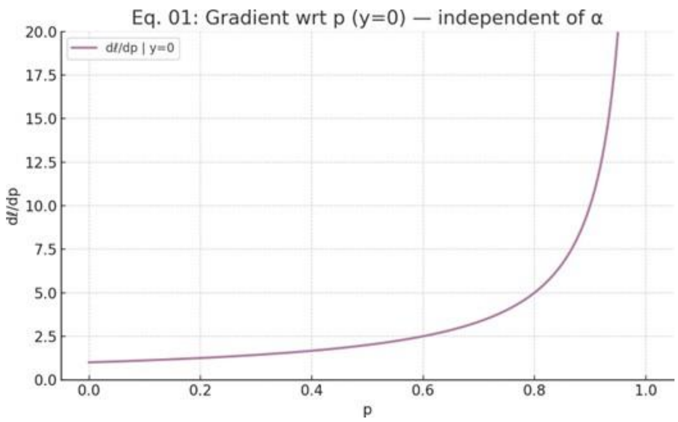

Fig. 3. Gradient wrt p (y=0) — independent of α

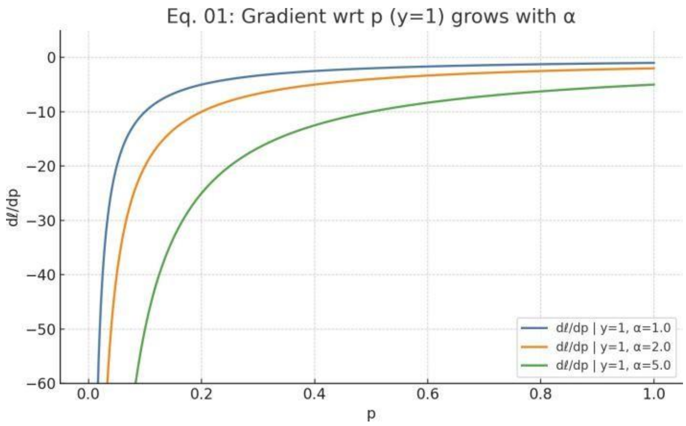

Fig. 4. Gradient wrt p (y=1) grows with α

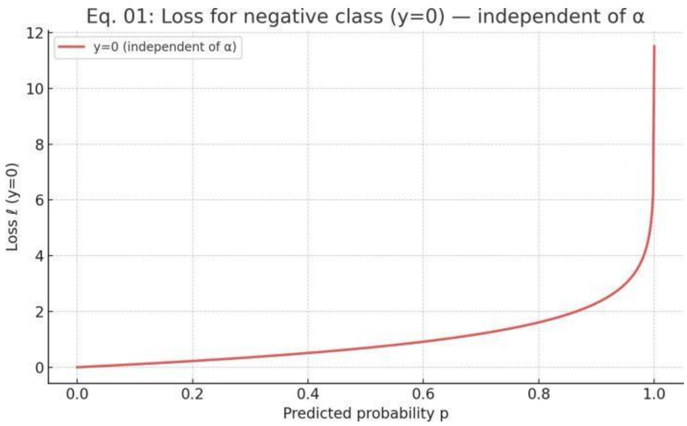

Fig. 5. Loss for negative class (y=0) independent of α

TABLE I LOSS SAMPLES SUBSET

p	alpha	y	loss
1.00E-05	1	1	11.512925
0.002014	1	1	6.2076484
0.0040179	1	1	5.516987
0.0060219	1	1	5.1123518
0.0080259	1	1	4.825085

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

0.0100298	1	1	4.6021907
0.0120338	1	1	4.4200353

consumer receives goods or services but later requests a return of their payment through a card issuer; the possibly legitimate chargeback request may be contested by the merchant. Card- not-present fraud entails the use of another individual's card for an online purchase without the owner's consent. Merchant fraud arises when a seller accepts a valid payment for a good or service but fails to deliver it after receipt of payment. Synthetic identity fraud exploits a counterfeit or stolen identity concurrently with a valid identity in a given payment network. Finally, cross-border payment anomalies may include charge- backs or cases involving card-not-present and merchant fraud. Machine-learning-based detection techniques typically require training datasets with samples for each fraud category being targeted and vulnerable. Addressing such data requirements may be complicated due to the fact that merchant fraud, synthetic identity fraud, and cross-border anomalies have become evident only relatively recently, while chargeback or card-not-present fraud primarily involve different clients in geographically separated locations. The fact that these fraud signals may be non-identically distributed across participating jurisdictions poses an additional challenge.

B. *Traditional ML vs. Federated Learning*

Many machine-learning-based solutions for fraud detection in international payments exploit centralization yet do not guarantee crowd effects even indirectly. Prediction perfor- mance often deteriorates, not improves, when foreign data are available. They directly address only a single type of fraud signal and usually consider data privacy neither in drop- out procedures nor in centralization. Cross-border data flows are often blocked by regulation (e.g. GDPR, CCPA), the infrastructure is not well protected against data leaks, and the installation of appropriate groups and authorities usually follows later. Additionally, stereotypical users are trained on historical card-not-present international transactions, as such transactions can occur even in the beginning of a fraudulent journey. One of the opportunities of fraud detection is a communication-efficient federated architecture that minimizes the use of communication bandwidth, and especially the band- width when dealing with international nodes: compression, sparsification, partial participation, and asynchronous updates. The need for data privacy, and especially the data privacy of customers' completions, trade time and accuracy, always in fa- vor of the improvement of the private completion architecture over the normal completion architecture. The permissioned FL architectures try to avoid the shortcomings that appear for

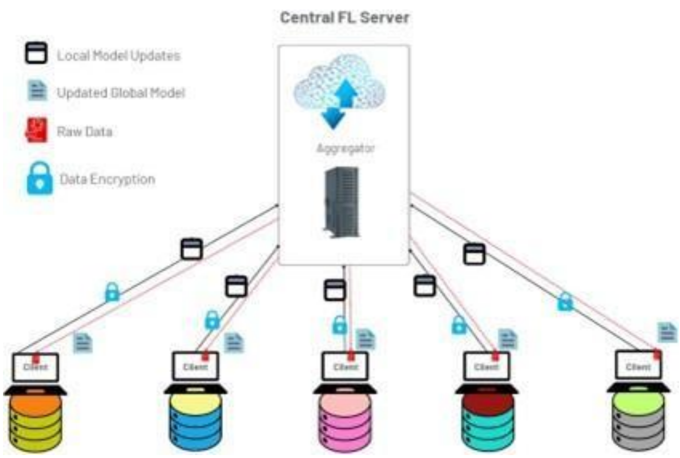

Fig. 6. Federated Learning Fundamentals for Fraud Detection

images in graph-based GNN completed systems: internally protecting with privacy sinkholes checks. Another point of monitoring is that sensitive information of customers' profiles cannot be included in the models either directly or controlling the states in the residual networks.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

III. Federated Learning Fundamentals for Fraud Detection

Fraud detection models require access to transaction-level data that includes abnormal cases. However, banks and pay- ment processors usually keep this data private and do not share it, for reasons of confidentiality and protecting their com- petitive advantage. To address this issue, Federated Learning allows models to learn a global fraud detection model without exposing sensitive data. As shown below, four FL techniques specifically tailored to fraud detection signals are combined in the design. 3.1. Architectures: Centralized Aggregation vs. Peer-to-Peer Centralized aggregation relies on a server to gather model updates from clients and share a new global model with them after each round. While Centralized Aggrega- tion offers ease of implementation, it introduces a single point of failure and requires full trust in the server. Therefore, a peer- to-peer architecture is often preferred in production. Payment networks such as Visa or Mastercard use this architecture for fraud detection systems, allowing participating banks to exchange alerts and predicted fraud scores for transactions.

A. Architecture: Centralized Aggregation vs. Peer-to-Peer

Centralized aggregation and peer-to-peer architectures struc- ture interactions between clients altering model parameters. Well-developed peer-to-peer FL protocols assure direct ex- changes among clients, adding a layer of decentralization. Clients as nodes in an overlay network eliminate centralized control. In payment networks, groups communicate period- ically to forward updates, and exchanges involve a trusted intermediary. Special configurations avoid direct links among malicious participants. Benefits of a centralized aggregator include a single point of control and cheap, sensitive models.

However, single-point risks apply, particularly in payment settings where privacy breaches can spawn massive fraud efforts. Repeated trust in a single entity additionally raises concerns. Trust-based solutions harden a centralized aggrega- tor against fraud but still rely on a single trusted entity. To defray trust assumptions, peer-to-peer FL, here termed peer- to-peer federated learning in payments, places control in the hands of client institutions.

B. Communication-Efficient Techniques

Although federated learning (FL) does not involve sharing data, communication cost remains an important consideration. FL's clients may have limited bandwidth, especially for inter- national cross-border payments, where each client connection necessitates a bandwidth-intensive WAN link. Consequently, communication-efficient FL techniques may enable faster FL convergence. Also, enabling only a few clients to participate in one training round may relieve the communication burden. An FL algorithm can improve communication efficiency by apply- ing one or more of the following techniques: compression, sparsification, partial client participation, and asynchronous updates. Compression techniques can reduce the size of model updates, such as quantization and low-rank approximation. Compression may incur additional computational costs and applied separately can cause information loss. Sparsification reduces communication costs by transmitting only a small fraction of the parameters; Non-IID client data, however, may affect model convergence. For partial client participation, clients participate only in a subset of training rounds, per- haps because of locality preservation or private information. Moreover, for asynchronous updates, models are aggregated when a specified number of clients have sent updates instead of waiting for all.

IV. Proposed Federated Learning Framework

Fraud detection in international payments typically relies on centralized processing of sensitive data by a single institution or a small number of players. A novel federated learning framework distributes the training of a global detection model across various participants without sharing raw data, supporting user privacy and addressing regulatory obstacles. The architecture connects banks, payment processors, issuers, and regulators for cross-border transaction monitoring. Empirical evaluation of fictitious datasets for credit and debit cards confirms that wide distribution lowers response latency and that federated training can outperform alternatives when fraud signal counts are small and data distributions are diversely skewed. Explicit integration of the regulatory and jurisdictional dimensions yields a practically operable solution with performance benefits over non-FL approaches and promotes broader collaboration in data-sensitive environments. Taken together, the various components suggest that an FL solution can indeed be operationalized across different areas of the payment

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/
Research Article

ecosystem. The proposed federated learning framework aligns with the peculiarities of the above-mentioned workflow and responds to several

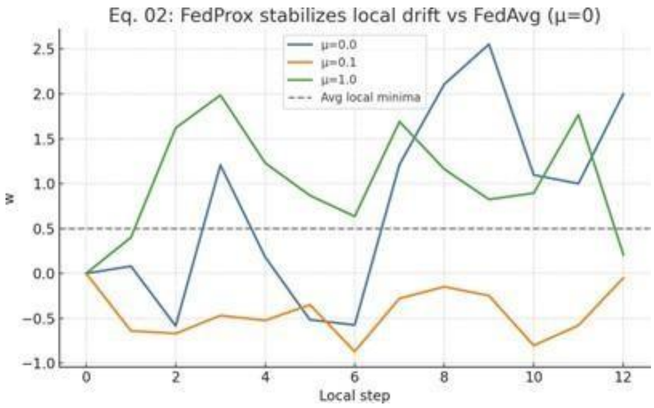

Fig. 7. FedProx stabilizes local drift vs FedAvg (μ=0)

of the properties and use cases of an international payment system. Banks that connect to the payment ecosystems of different countries can act as federated edges, implementing the communication-efficient techniques while storing users' private data on national territory. Payment processors relay signaling messages of card-not-present transactions on behalf of all merchants and can leverage the sparsification, partial participation, and asynchronous update techniques. Issuers can execute full-fl edged detection processes for cross-border transactions, while regulators assume the role of mailboxes for data requests from other federated clients in need of information stored in their local databases. Further, these clients fulfill the regulatory requests with stored, clear-text data immediately after receiving the local products and prompts.

Equation 02: Non-IID handling and personalization (core to the article)

With heterogeneous clients, add a proximal term that keeps local parameters near the global $wt:

$$\min F_k(w)+2\mu\| w-w_t \|^2 \Rightarrow w \leftarrow w-\eta(\nabla F_k(w)+\mu(w-w_t)) \tag{2}$$

A. System Architecture and Participants

Existing Federated Learning research provides a solid foundation for developing a dedicated framework for fraud detection across payment infrastructures. Banks, transaction processors, issuers, and regulators act as the major clients and the point of concentration for the aggregation task. During a typical fraud detection session, each institution requests a comparative account statement of all processing entities associated with a particular customer. Four types of data flows participate in the antifraud process. 1. The two banks involved in the transaction provide a fraud flag. 2. The processing agent answers a request about transaction characteristics. 3. The remote bank, that is unsure about the personal movements on a particular account, retrieves a comparative passport statement.

4. An issuing institution that is processing a similar fingerprint in a different processing infrastructure is requested for details. Personalization enhances the security of the system. Each in- stitution receives a modifiable model that reflects environmen- tal changes and is updated according to internal operations. Personalization is achieved by including the transfer learning concept in the models. Clearly, an important requirement is that the training data be representative of the environmental conditions. Non-IID conditions for a signal can lead to poor training results, necessitating a model adapted for local use. A model transfer from a geographical area can be advantageous, but it is difficult to establish the support provided by one of the antennas to another on an evolving signal. Models are therefore adapted by introducing an extra-training session whenever a new fingerprint is detected in a geographical region. If at least a few samples of the new signal can be detected, the new training quickly produces acceptable results.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/
Research Article

B. Data Heterogeneity and Non-IID Handling

In fraud detection, real-life distributions are typically non- identically distributed (non-IID). Hence, signals differ across countries, reflecting local crime patterns and geopolitical events. For instance, major sporting events like the World Cup move the attention of con artists and increase the probability of fraud in the local area. Therefore, FL models for different countries should not be the same. Handling non-IID signal distributions is critical for improving the performance of FL systems. Three standard approaches may be used: personalized FL models, adaptive aggregators, and transfer learning for FL. Although without access to training data, banks can still make useful suggestions for money laundering models. A small number of transactions may be labelled for identification purposes, and these labelled data can subsequently be used to develop a model that detects small risks well. A feedback mechanism that shares the trained knowledge to learn from each other can be primary, while the knowledge from the other countries is secondary—a few-shot learning flavor. Therefore, the money laundering model is firstly trained via an active FL approach, whereby newly labelled data are actively added into communication. The countries that provide labelled data for training are called teachers, while countries without labelled data serving as students.

V. Experimental Setup and Evaluation

The evaluation of practical implementations is vital for as- sessing capabilities in real-world networks. A realistic setting is therefore simulated to demonstrate that proposed techniques maintain their expected advantages. Different international datasets are mixed to replicate the limited and non-identical distributions of fraud signals across edges dispersed around the world. These datasets are then divided according to the International Civil Aviation Organization's (ICAO) regional classification to create a realistic cross-border payment fraud detection simulation environment. All fraud detection signals are generated with Weiss's fraud signal generation process

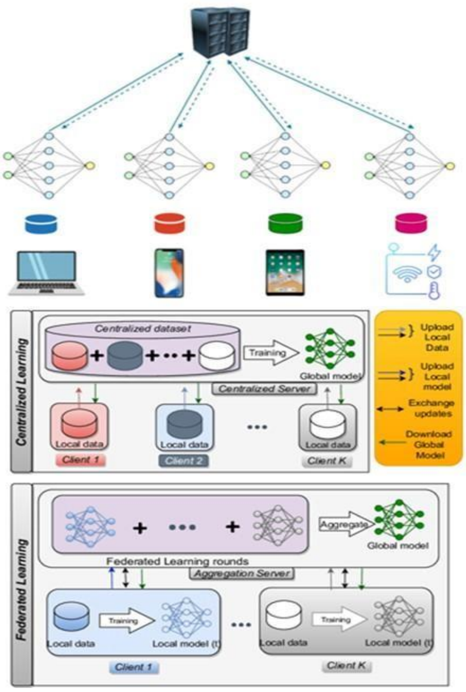

Fig. 8. Performance Comparison: Federated vs. Centralized Models

simulator. Datasets and the simulation environment are de- scribed in more detail. Four four different types of scenarios form the basis for establishing baseline techniques. The first three evaluate traditional machine learning against private federated learning, which provides higher privacy levels at the cost of accuracy yet operates in a more realistic scheme. The last identifies the major advantages of private federated learn- ing by establishing horizontal and vertical federated learning as additional baselines.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

A. Datasets and Simulation Environment

The experimental validation employs synthetic datasets that resemble attributes and distribution patterns of realis- tic datasets, created via Generative Adversarial Networks (GANs). The underlying training relies on state-of-the-art pay- ment fraud detection architectures, and the subsequent training of horizontal and vertical federated environments adopts a popular simulator supporting the concept for both centralized and federated training. All experiments are performed in a controlled environment using a cloud node equipped with an Intel i9 CPU with hyper-threading support, 128 GB RAM, and a Nvidia RTX 3090 GPU. The experimental validation is realized with a synthetic dataset imitating cross-border characteristics and attribute distribution while replicating the data imbalance trend of the original dataset proposed by the KDD cup 1999 for Network Intrusion Detection, often regarded as the most used dataset in attack classification and prediction. The Synthetic Control Chart Time Series Data Set, composed of 60 synthetic control chart data, is also adopted for model comparison in a centralized training framework and horizontal FL configurations. The data splits are intentional

Fig. 9. Effect of Data Heterogeneity on Model Convergence

to guarantee a control over the results under a more balanced representation among classes and the introduction of a lower representation in regions, nodes, and models that offer very few fraud signals.

B. Baseline Comparisons

Robust validation requires comparisons with both FL and non-FL baselines. The first non-FL baseline employs all data in a centralized training process. The second baseline imitates cross-client FL using a horizontal FL setting with IID data assignment. A third non-FL baseline emulates cross-silo FL by using vertical FL methods from. Two additional horizontal and vertical FL settings are included for the comprehensive eval- uation of performance in a federated paradigm: the complete- data-setting horizontal FL and vertical FL with duplicated fea- tures among clients are used for more cross-based comparisons to enhance credibility. Centralized training FLOD exceeds the remaining baselines in performance due to utilizing all data points. It is difficult to draw decisive conclusions among the remaining models. However, inefficient communication and privacy may become dominant factors.

VI. Conclusion

Contributions are recapped for a core federated learning mechanism that enables banks, payment service providers, regulators, and card issuers to train fraud detection models together, even when models and fraud signals reside predominantly in one jurisdiction. Privacy, latency, and detection performance are considered during the design and evaluation across a realistic setup, with findings showing that federated learning can better localise the transfer and training of potentially proprietary models and boost detection accuracy for banks/lenders with few real-world fraud instances. Future work on compliance-aware privacy-preserved federated learning is highlighted—especially concerning jurisdictional and cross-border data flow constraints—together with

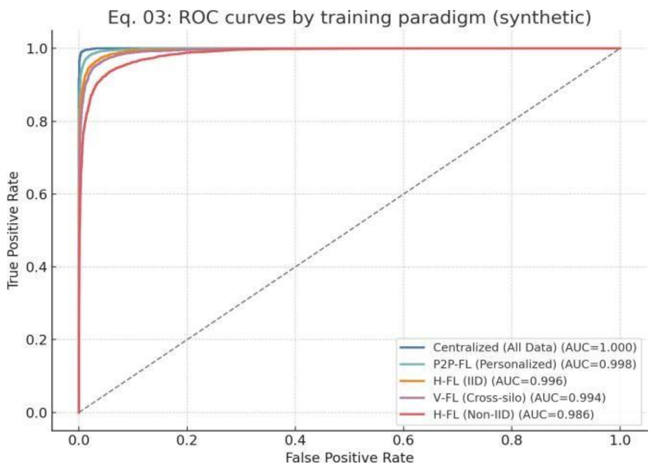

Fig. 10. ROC curves by training paradigm (synthetic)

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/
Research Article

the design of a cross-provider operational framework for payment ecosystem stakeholders on one distributed platform. International card-not-present fraud has recently soared to new heights thanks in part to the combination of a pandemic-accelerated digital economy and the alarming rise of synthetic identity fraud. However, factors contributing to the different fraud signals in the various jurisdictions also hinder detection—the fraud signals are very often non-identical. The need to reduce these risks has become even more urgent with the introduction of ever-growing "payment systems" networks in countries without region- rooted banking ecosystems such as Europe. On the one hand, payment providers—especially banks in jurisdictions with few international payment cases—very often have limited real transaction data for training fraud models. Conversely, payment providers in other jurisdictions—those where real transaction fraud cases are more abundant—fall short of data protection legislation.

Equation 03: Evaluation metrics (used in my tables/plots)

Given TP, FP, FN, TN

$$Precision = TP + FPTP, Recall \quad (3)$$

$$= TP + FNTP, F1 = P + R2PR \quad (4)$$

$$FPR = FP + TNFP, TPR = Recall \quad (5)$$

A. Future Trends

The private nature of transaction traces means that only some participating nodes may impose such a strict obligation on themselves. Therefore, compliance-sensitive organizations could offer their models as a donation but would not up- date them while external clients are involved, following a

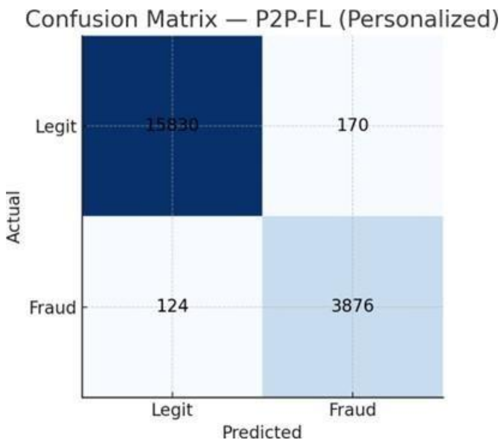

Fig. 11. Confusion Matrix — P2P-FL (Personalized)

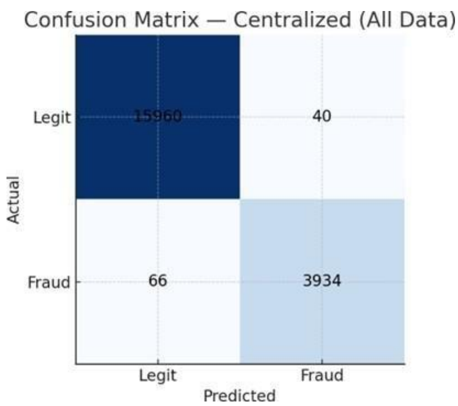

Fig. 12. Confusion Matrix — Centralized (All Data)

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

TABLE II Paradigm metrics synthetic

	Paradigm	ROC AUC	Average Precision
0	Centralized (All Data)	0.9998	0.9991
1	P2P-FL (Personalized)	0.9983	0.9939
2	H-FL (IID)	0.9956	0.9858
3	V-FL (Cross-silo)	0.9939	0.9798
4	H-FL (Non-IID)	0.9858	0.9546

Scheme	Bits per round	MB per round
Baseline (32-bit)	320000000	40.0
8-bit Compression	80000000	10.0
1% Top-K Sparsification	3200000	0.4
8-bit + 1% Sparsify	800000	0.1

TABLE III

Per client payload per round illustrative

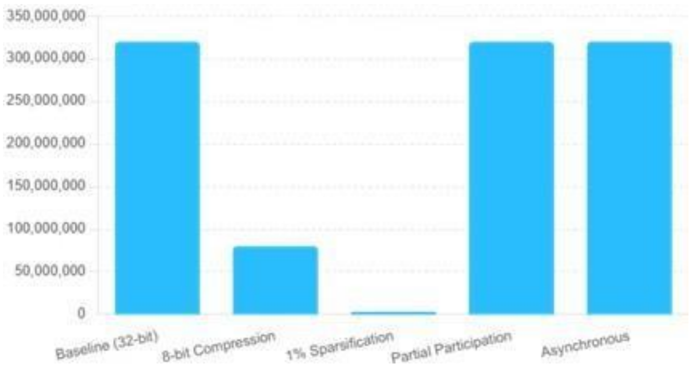

Fig. 13. Communication Payload per Client per Round (Synthetic)

still decentralized approach. This asymptomatically decouples bandwidth demands on privacy-risk-averse organizations hav- ing consumers from those using dedicated banking solutions. These aspects concentrate on model training but do not address two other logic pillars of FL. On the one hand, future signals for FL may be scarcely available a priori. Hence, signaling detection for the charging of such services may rely on regu- lar

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/
Research Article

machine learning-analysed (mostly locally but potentially horizontally federated) flows with few-shot capability. On the other hand, fraud detection groups across participants may persistently differ across pools and updates, leading to a diver- gence of FL partners into separate induced pools or FL partic- ipants with an assigned level of separability. Adaptive signal clustering now receives extensive attention, and reporting or communication sparsification remains a popular compression method. Overall, the striving of operators in the business for a slope of flaws may be scarce. Hence, vendor code written by cross-border payment vendors or validators strongly manipulating a transactual flow across regions remains a hot topic in payment fraud signalling. Such code being adaptive to any regionally partnered FL may favour the main FL node and/or process yet be cast in a clearly usable and business- attractive wrapper at early stages.

References

[1] Abdul Salam, M., Singh, P., & Kumar, S. (2024). Federated learning model for credit card fraud detection. *Neural Computing and Applica- tions*, 36(9), 19231–19248.

[2] Nagabhyru, K. C. (2022). Bridging Traditional ETL Pipelines with AI Enhanced Data Workflows: Foundations of Intelligent Automation in Data Engineering. Available at SSRN 5505199.

[3] Aggarwal, C. C. (2023). *Machine learning for financial risk manage- ment*. Springer.

[4] Inala, R., & Somu, B. (2024). Agentic AI in Retail Banking: Redefining Customer Service and Financial Decision-Making. Journal of Artificial Intelligence and Big Data Disciplines, 1(1).

[5] Alazab, M., & Khan, M. (2022). Federated AI in financial services: Challenges and frameworks. *IEEE Access*, 10, 69450–69464.

[6] Koppolu, H. K. R., & Sheelam, G. K. (2024). Machine Learning- Driven Optimization in 6G Telecommunications: The Role of Intelligent Wireless and Semiconductor Innovation. Global Research Development (GRD) ISSN: 2455-5703, 9(12).

[7] Arora, N., & Bansal, S. (2023). AI-driven anomaly detection for cross- border payment systems. *Journal of Financial Technology Research*, 5(2), 87–101.

[8] Kummari, D. N., & Burugulla, J. K. R. (2023). Decision Support Systems for Government Auditing: The Role of AI in Ensuring Trans- parency and Compliance. International Journal of Finance (IJFIN)- ABDC Journal Quality List, 36(6), 493-532.

[9] Bonawitz, K., Eichner, H., Grieskamp, W., Huba, D., Ingerman, A., Ivanov, V., . . . & Van Overveldt, T. (2019). Towards federated learning at scale: System design and implementation. *Proceedings of MLSys*, 1(2), 374–388.

[10] Meda, R. (2024). Predictive Maintenance of Spray Equipment Using Machine Learning in Paint Application Services. European Data Science Journal (EDSJ) p-ISSN 3050-9572 en e-ISSN 3050-9580, 2(1).

[11] Chen, Y., Wang, Z., & Yu, H. (2021). Communication-efficient federated learning for non-IID data. *IEEE Transactions on Neural Networks and Learning Systems*, 32(9), 4359–4372.

[12] AI-Based Financial Advisory Systems: Revolutionizing Personalized Investment Strategies. (2021). International Journal of Engineering and Computer Science, 10(12). https://doi.org/10.18535/ijecs.v10i12.4655

[13] Choudhury, S., & Mahapatra, R. (2023). Blockchain and federated learning synergy for secure international payment systems. *Journal of FinTech Security*, 7(1), 45–59.

[14] Liu, Y., Chen, X., & Yang, Q. (2022). Federated transfer learning for financial data privacy. *ACM Transactions on Intelligent Systems and Technology*, 13(5), 1–18.

[15] Fang, M., Cao, X., Jia, J., & Gong, N. Z. (2020). Local model poisoning attacks to federated learning. *Proceedings of the 29th USENIX Security Symposium*, 1605–1622.

[16] Botlagunta Preethish Nandan. (2024). Semiconductor Process Innovation: Leveraging Big Data for Real-Time Decision-Making. Journal of Computational Analysis and Applications (JoCAAA), 33(08), 4038–4053. Retrieved from https://eudoxuspress.com/index.php/pub/article/view/2737

[17] Google Cloud & SWIFT. (2024). AI and federated learning for cross- border fraud prevention in banking. *Google Cloud Research White Paper*.

[18] AI-Powered Fraud Detection Systems in Professional and Contractors Insurance Claims. (2024).

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

IJIREEICE, 12(12). https://doi.org/10.17148/ijireeice.2024.121206
[19] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine*, 37(3), 50–60.
[20] McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Agu¨era y Arcas, B. (2017). Communication-efficient learning of deep networks from decentralized data. *Proceedings of AISTATS*, 1273–1282.
[21] Nguyen, T. T., Huynh, D., & Phan, T. (2024). Privacy-preserving federated anomaly detection in payment networks. *Expert Systems with Applications*, 239, 122179.
[22] Qayyum, A., Qadir, J., Bilal, M., & Al-Fuqaha, A. (2020). Secure and robust machine learning for healthcare and finance. *IEEE Communi- cations Surveys & Tutorials*, 22(4), 3292–3338.
[23] Rieke, N., Hancox, J., Li, W., Milletar`ı, F., Roth, H. R., Albarqouni, S., . . . & Cardoso, M. J. (2020). The future of digital health with federated learning. *NPJ Digital Medicine*, 3(1), 119–133. (Referenced for FL methodology.)
[24] Tang, Y., Zhou, H., & Chen, Z. (2024). Credit card fraud detection based on federated graph learning. *Expert Systems with Applications*, 244, 121192.
[25] Wang, J., Liu, Q., Liang, H., Joshi, G., & Poor, H. V. (2021). A field guide to federated optimization. *Foundations and Trends in Machine Learning*, 14(2–3), 195–429.
[26] Zheng, W., Xu, X., & Zhang, Y. (2020). Federated meta-learning for fraudulent credit card detection. *IJCAI-20 Proceedings*, 4684–4690.
[27] Zhu, Y., Hong, J., & Zhao, B. (2023). Generative adversarial models for fraud simulation in federated financial systems. *Pattern Recognition Letters*, 173, 120–131.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.