Fighting Fraud with Federated Learning

Abstract

Fraudsters in the UK continuously adapt, shifting tactics as banks tighten fraud prevention measures. When one institution strengthens its defences—such as improving transaction monitoring or tightening KYC checks—criminals move to less secure providers, often targeting fintechs, smaller banks, or payment service providers with weaker controls. This cat-and-mouse game is particularly evident in APP fraud and money mule networks, where criminals use synthetic identities, social engineering, and cross-border transactions to evade detection.

In 2004, Jaywing addressed this challenge through its fraud data syndicate program, which brought together major banks to share application fraud data. This collaboration enabled Jaywing to develop effective fraud detection models. While the initiative was successful, evolving technology and regulations necessitated new solutions.

Federated learning is an emerging machine learning technique that allows institutions to train models collaboratively without sharing raw data. This decentralised approach is valuable in retail banking, where data privacy concerns and regulations limit cross-institutional fraud detection. By leveraging federated learning, banks can build more robust fraud prevention models while maintaining compliance with data protection laws.

Traditional fraud detection relies on centralised data, often limited to a single bank's transactions and behavioural patterns, restricting the detection of complex, multi-bank fraud schemes like mule networks and account takeovers. Federated learning addresses this by enabling banks to collaboratively train a shared fraud detection model without exposing sensitive customer data. Each institution processes its data locally, sharing only encrypted model updates rather than raw records.

How Federated Learning Enhances Fraud Detection:

1. Local model training – Each institution trains its fraud detection model using its own data.
2. Secure model aggregation – Only encrypted model updates are shared, not raw data.
3. Global model improvement – The aggregator refines the model using insights from all institutions.
4. Continuous learning – The cycle repeats, ensuring fraud detection evolves with new threats.

This privacy-preserving approach enables institutions to benefit from collective intelligence while remaining compliant with GDPR and data protection laws.

As fraud threats grow more sophisticated, financial institutions must embrace new ways to detect, share, and act on fraud intelligence while protecting customer data. Federated learning represents a major step forward in fraud prevention, allowing institutions to collaborate without compromising privacy.

Jaywing's market research confirms its potential as a practical solution to enhance fraud defences. We at Jaywing see federated learning as an innovative way to stay ahead of fraudsters.

Authors & Affiliations

Mr Ben Archer[1], Mr Peter Szocs[2]
[1]Jaywing, Solihull, United Kingdom. [2]Jaywing, Leeds, United Kingdom