inpher

New Approaches to Tackling Financial Crimes: Secure Data Collaboration With XOR

Successfully combating financial crime often requires sufficient data to derive insights using machine learning (ML) and artificial intelligence (AI).

Since many standalone institutions do not have enough data to obtain the unbiased insights needed, collaboration is crucial. Yet sensitive data is distributed across teams, organizations, and regulated jurisdictions. Leveraging that data in a way that meets institutions' privacy commitments and complies with regulations can be a formidable challenge.

With Inpher's encryption-in-use technologies, backed by mathematically proven data security, privacy, and residency, enterprise organizations can access a broader and deeper pool of data distributed across restricted silos and multiple parties.

The following four case studies illustrate how institutions that leverage Inpher can more effectively identify and combat financial crime.

BNY MELLON

FCA FINANCIAL CONDUCT AUTHORITY

Privacy-Enhancing Technologies PRIZE CHALLENGES

Microsoft Azure

BNY Mellon: Privacy-Preserving ML for Fraud Detection

Challenge

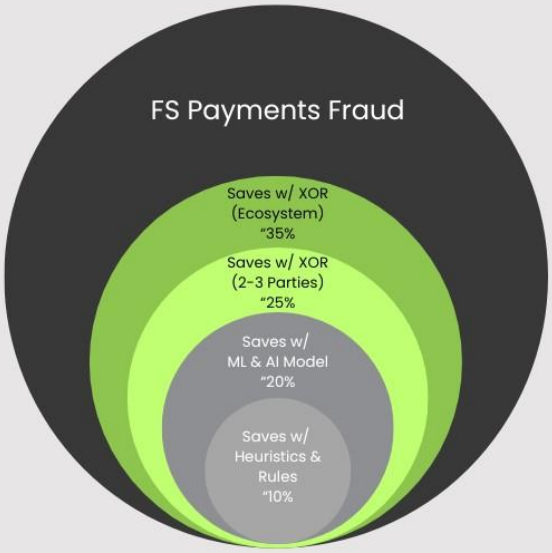
As one of the largest asset managers in the world, BNY Mellon must continually improve its ML-based fraud detection algorithms. Ideally, training data should be aggregated in one place, but this was stymied by jurisdictional barriers that prevent data from leaving the country of origin or being shared with competitors.

Solution

BNY Mellon began working with Inpher. Without sharing sensitive data across borders or jurisdictional silos, Inpher's technology enabled the stacking of data horizontally and vertically for training ML algorithms such as linear and logistic regression as well as XGBoost (XORBoost). The solution achieved a high level of precision, computing models identically as if they were computed in clear text. As a result, the number of false positives were reduced by 20% and the number of true positives were increased by 20%. The results reduce investigation workload and increase fraud detection efficiency.

Using AI to Defund Financial Fraud Crime

- Annual fraud losses across Financial Services in the billions
- Annual client losses in the 100s of millions
- Fraud instances are fairly constant over the months and therefore hard to predict
- Machine learning is a proven approach to finding hidden patterns
- Machine learning models using internal data have shown to reduce fraud by 20%
- With XOR, by adding data points that would otherwise not be available, the model improved by 20%



inpher

2019 FCA Global Anti-Money Laundering and Financial Crime TechSprint: Winner

In 2019, the U.K. Financial Conduct Authority (FCA) held a week-long TechSprint to explore better ways of increasing the detection and prevention rates of financial crime.

Challenge

Fraudsters split high volume transactions across several banks to avoid being detected by the institutions' anti-money laundering (AML) controls. As the intermediary banks cannot share data with each other without exposing sensitive client data, these transfers remain undetected.

Solution

Inpher emerged as a winner by using cryptographic privacy-enhancing technologies to aggregate adjacency matrices of different banks and to compute similarity scores in order to identify split transactions. The solution enables participating banks to detect transactions with the same originator and ultimate recipient even when intermediaries withdraw percentage commissions. As a result, banks can identify when they are harboring mule accounts that are used in ML schemes.

U.S.-U.K. PETs Prize Challenge, Phase 1: Winner

In 2022, the U.S. and U.K. governments collaborated on phase one of the PETs Prize Challenge to accelerate development and adoption of democracy-supporting privacy-enhancing technologies (PETs) using federated learning solutions.

Challenge

Inpher focused on Data Track A, improving AI-based fraud detection algorithms. While most data scientists would prefer that their training data be aggregated in one place for ease of operation, jurisdictional barriers mean ML-training data cannot leave the country or be shared with competitors.

Solution

Inpher emerged as one of three winners by proposing a federated architecture for data pooling, aggregation, and AI model training that preserves data input privacy and enables federated learning of AI algorithms without the use of trusted execution environments (TEEs). Leveraging some of the same techniques as in the BNY Mellon case study, the solution resulted in an increased performance of the models and improved fraud detection.

Microsoft Azure Confidential Computing and Inpher

In a detailed analysis, Inpher shares how its XOR software can be used in conjunction with trusted execution environment (TEE) hardware to help protect data during processing. The analysis explains how XOR advances the privacy preserving data sharing landscape for financial institutions that need to join and compute on disparate data sets.

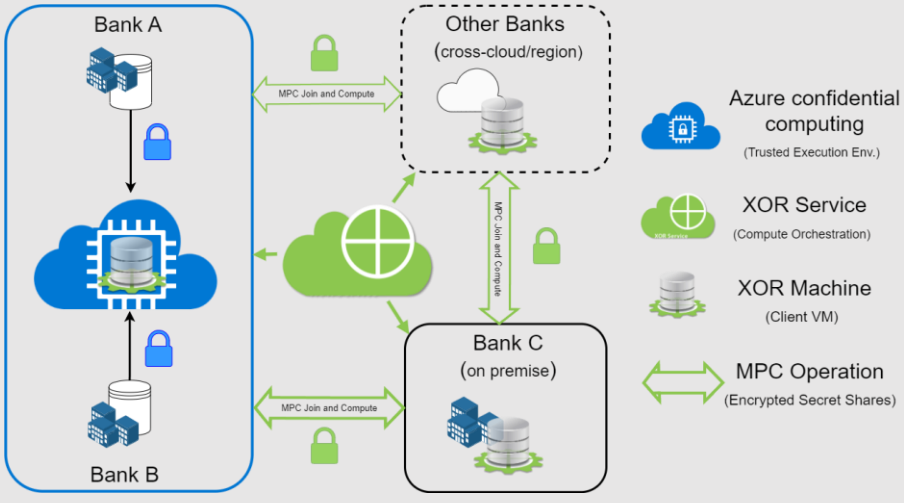
The use case involved provides a scenario where two banks have their private data on Azure, where one bank uses on-premise data policies. The goal is to run analytics, without sharing data directly, on features which will be used to target transactions similar to the ones that SWIFT communicates to its vast messaging network used to power most international money and security transfers.

Challenge

Improving the predictive power of their AI models requires aggregating data from more banks, yet currently the banks and the messaging platform can only access their own data. They would like to build a dedicated, infrastructure-agnostic platform for federated AI that can integrate diverse data in order to build better models and help banks better identify fraud–all in a privacy preserving way.

Solution

Microsoft confidential computing allows the banking network to incorporate features from banks that have agreed to share their data in the trusted environment. With the addition of Inpher's XOR Platform, the network can maximize data access by also incorporating features from banks that keep their data in their own trusted environments, on their own premises or cloud.



Inpher, Inc. is a New York-based, foremost leader in privacy-enhanced computation that empowers organizations to seamlessly adopt privacy-enhancing technologies. Inpher's award-winning platform revolutionizes secure collaboration across teams, borders by employing machine learning and AI that removes data barriers and siloes while delivering the highest level of trust and precision to even the most complex data collaboration initiatives. Founded by world-renowned cryptographers and engineers, Inpher has long been recognized as a leader in the fields of secure Multiparty Computation (MPC), Fully Homomorphic Encryption (FHE), and Federated Learning (FL), and other combinations of Privacy-preserving Technologies (PETs) and continue to deliver the fastest, high-precision privacy-preserving capabilities.

For more information on Inpher, please visit us at inpher.io and follow us on LinkedIn and Twitter for more information