Finding a Needle in a Haystack: A Machine Learning Framework for Anomaly Detection in Payment Systems

Ajit Desai[1], Anneke Kosse[2] and Jacob Sharples[1]

[1]Bank of Canada, [2]Bank for International Settlements

Objective & Data

Motivation: high-value payment systems (HVPSs) are **core** to national financial infrastructure.

→Safeguarding them requires real-time transaction monitoring, especially due to growing **cyber** threats targeting HVPS and its participants.

Problem: due to the substantial volume of HVPS transactions settled each day and the **scarcity** of anomalous payments to date, detecting anomalies resembles an attempt to find a **needle in a haystack**.

Solution: we use centralized & layered framework for anomaly detection using data-driven and nonlinear machine learning (ML) tools.

→The first layer **screens** typical payments, streamlining the subsequent **anomaly** detection task in the second layer.

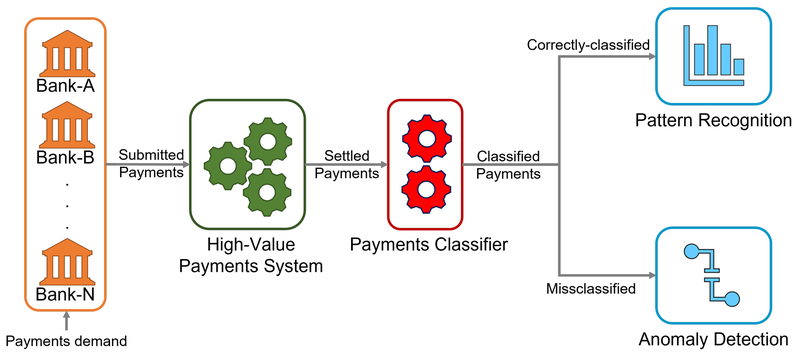
Payments data: transaction-level data from Canada's HVPS: we use clean data for training and a mix of clean & special days data for testing:

- Basic transaction features
- Liquidity features
- Intraday timing features
- Timestamp features

10	75M	25
Years	Payments	Features

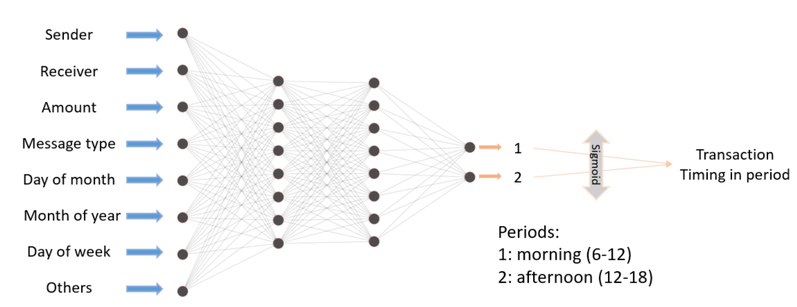
Methodology

Layered approach: a system-level **centralized** and **two-layer** approach to simplify pattern recognition and anomaly detection in HVPS.

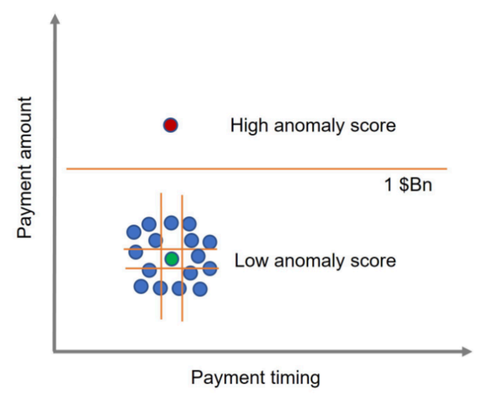


Layer 1 - classification: supervised ML algorithm to classify payments based on their submission time.

→ we use the **correctly** classified payments to study participants usual payment submission patterns.



Layer 2 - Anomaly detection: we use **only misclassified** payments in an unsupervised ML-based **isolation forest** (IF) model to identify and sort suspicious payments based on anomaly scores.



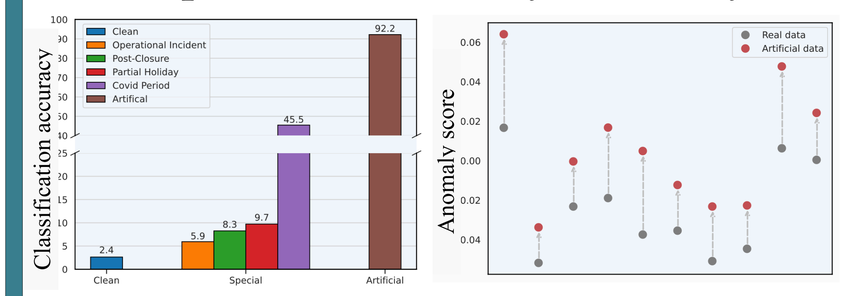
*Note: The opinions here are of the authors and do not necessarily reflect the ones of the Bank of Canada or the Bank for international settlements

Results

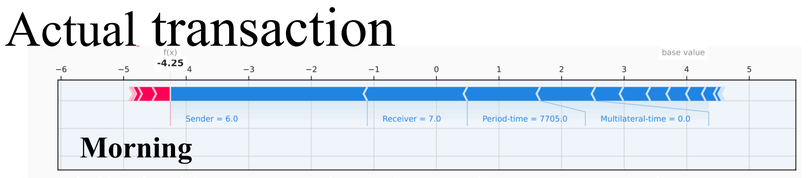
Key results:

- Basic transaction & intraday timing features play crucial role for both classification and anomaly detection.
- Models are relaying upon multilateral and bilateral payment coordination to learn patterns and detect anomalies.
- ML models from both layers can be interpreted to understand predictions.
- Approach is flexible to use for different types of HVPS and it can employ more ML tools to enhance robustness.

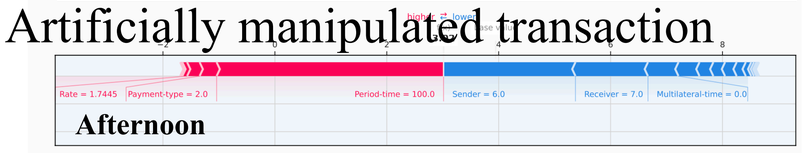
Model performance - Layer 1 & layer 2



Actual transaction



Artificially manipulated transaction



Low score (-4.25) → morning (more blue); and high score (3.02) → afternoon (more red)

Takeaways: Our centralized & layered framework, supported by advanced ML tools, offers a systematic approach for real-time transactions monitoring in HVPS.

→ It holds promise for safeguarding financial market infrastructure while remaining adaptable for broader payment system applications.