The 3-Tiered Approach to Fraud Detection

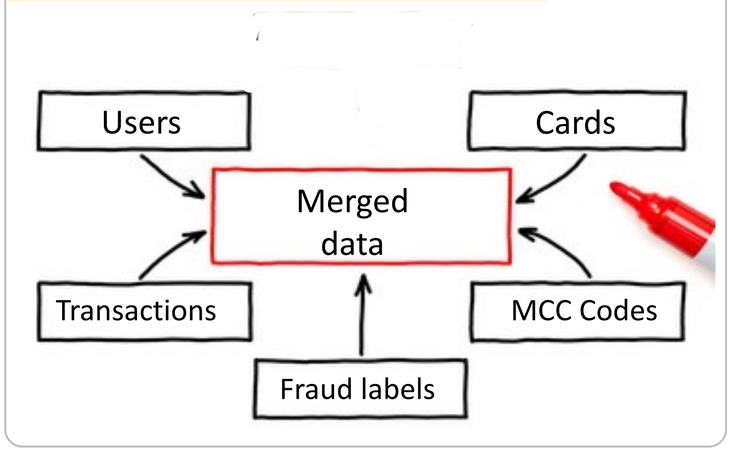
Itunuoluwa Olowoye | Eisha Imran Chaudhry | Juan Byju

UNIVERSITY OF CALGARY

Background

- Fraud detection is crucial in digital transactions, with over $10B lost to fraud annually.
- Traditional rule-based detection is not scalable due to evolving fraud tactics.
- Our hybrid approach combines Rule-Based, Anomaly Detection, and Classification methods to improve fraud detection.

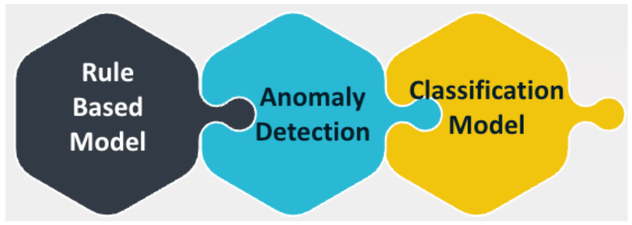
Datasets



Pipeline

Data Collection	Preprocessing	Exploratory Data Analysis	Model Training & Selection	Fraud Decision Making
Gather transaction data, user demographics, card details, and merchant categories to build a comprehensive fraud detection dataset.	Clean and normalize data, handling missing values, duplicates, and inconsistencies to ensure reliable model performance.	Identify fraud patterns, visualize transaction behaviors, and uncover key features that differentiate fraudulent from legitimate transactions.	Develop and compare rule-based, anomaly detection, and classification models to detect fraudulent transactions effectively.	Evaluate model accuracy, highlight key fraud indicators, and assess the hybrid system's ability to flag suspicious transactions in real-time.

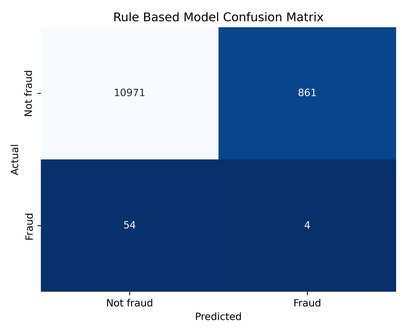
Modeling Approaches



Modeling Procedure

Rather than completely replace legacy systems or use only one machine learning method to detect fraud, our project provides a hybrid architecture to fraud detection systems, utilizing results from a rule-based system, a classification model, and an anomaly detection model.

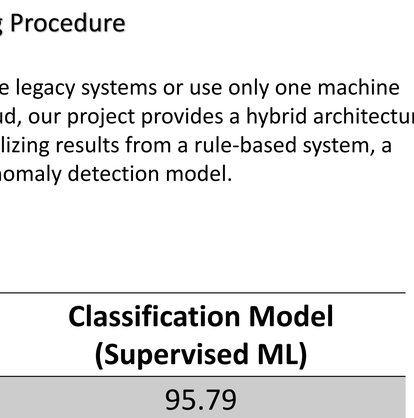
	Rule-based Model	Anomaly Detection Model (Unsupervised ML)	Classification Model (Supervised ML)
Accuracy	92.30	98.13	95.79
Recall	**6.90**	**55.17**	**89.96**
False alarms	7.28% ▲	1.66% ▼	4.18% ▼

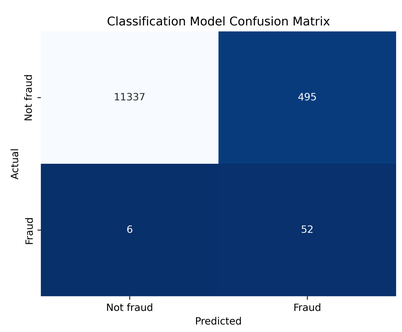


The rule-based model uses heuristic rules to detect fraud such as:

- High transaction amounts, in general (greater than 3 standard deviations from the user's average transaction amount)
- High transaction amounts with international merchants
- Transactions from unusual locations
- High-velocity transactions (numerous transactions in the span of one hour)
- High number of transactions during offload hours at night

The anomaly detection model identifies transaction patterns and detects transactions that deviate from the usual patterns. This model works best on an individual customer level. Existing customers will have individual baselines for their usual transaction patterns and deviations from these baselines are flagged. New customer transactions will be gauged based on a general baseline. Some form of generalization can be established using customer segments and baselines for each segment.



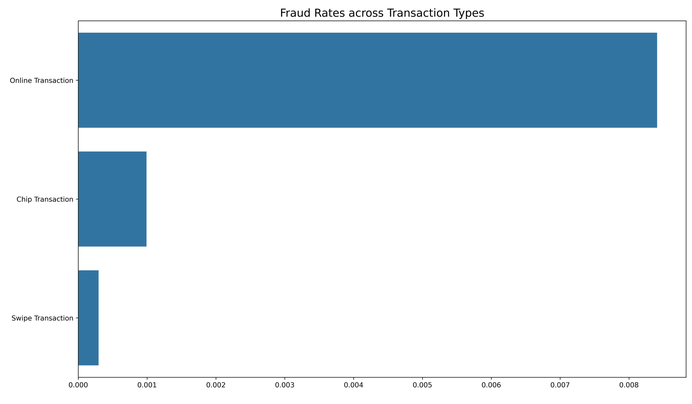


Classification models use supervised machine learning methods to detect fraud. They analyze large datasets to recognize patterns and relationships between different transaction features. As more data is collected, the models can be retrained to identify and learn from new fraudulent patterns.

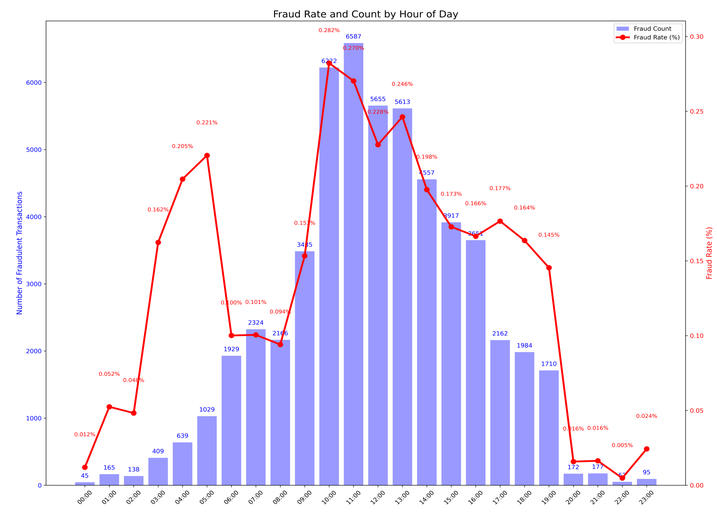
References: Karlsson, J. (2023, May 9). How to build a real-time fraud detection system. Tinybird. https://www.tinybird.co/blog-posts/how-to-build-a-real-time-fraud-detection-system

Exploratory Data Analysis

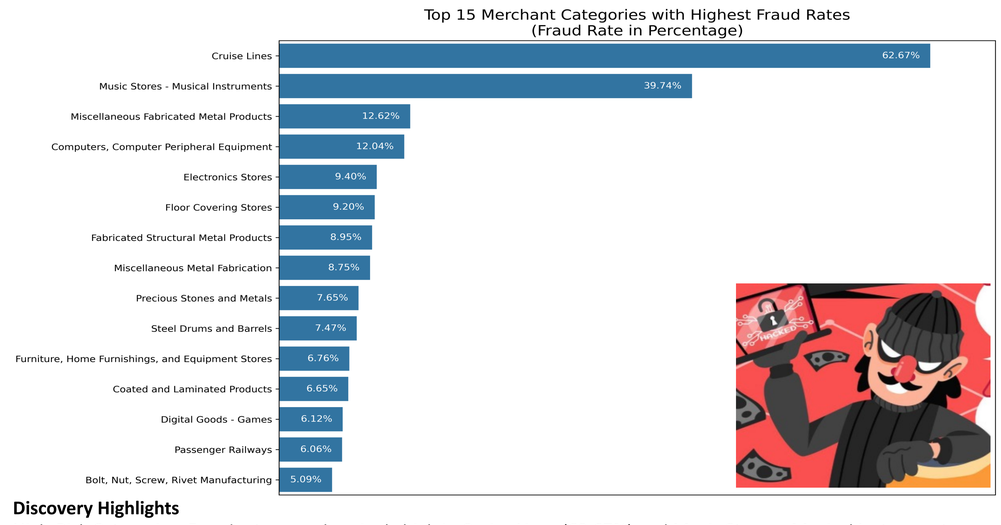
Goal: Uncover hidden fraud patterns, identify key risk factors, and gain insights into transaction behaviors to enhance model performance.



Discovery Highlights:
Fraud is more prevalent in online transactions, compared to Swipe and Chip Transactions



Discovery Highlights
Despite low transaction volume, the fraud rate is relatively high between 2 AM - 5 AM. This could indicate that fraudsters take advantage of reduced oversight during off-hours.



Discovery Highlights
High-Risk Categories: Fraud rates are alarmingly high in Cruise Lines (62.67%) and Music Stores - Musical Instruments (39.74%), suggesting targeted exploitation in these industries.
Technology & Retail Vulnerabilities: Fraud is also prevalent in Metal Fabrication (12.62%), Computer & Peripheral Equipment (12.04%), and Electronics Stores (9.40%), indicating potential weaknesses in digital transactions and high-value goods.
Lower-Risk Categories: Passenger Railways (6.06%) and Bolt, Nut & Screw Manufacturing (5.09%) have the lowest fraud rates, likely due to structured payment processes and lower incentives for fraudulent activity.

Summary

Key Findings

Rule-Based Model: High accuracy (92%) but low recall (7%), meaning it detects very few fraudulent cases. The false alarm rate (7%) indicates some legitimate transactions are incorrectly flagged.
Anomaly Detection Model (Unsupervised ML): Highest accuracy (98%) and improved recall (55%), effectively identifying fraud with minimal false alarms (2%). However, it still misses some fraudulent cases.
Classification Model (Supervised Learning): Balanced performance with high accuracy (96%) and the best recall (90%), making it the most effective in identifying fraudulent transactions while maintaining a low false alarm rate (4%).

Conclusion

No single model is perfect. A hybrid fraud detection system integrating rule-based, anomaly detection, and classification models offers a more robust and adaptive approach to combating fraud. This system enhances fraud prevention capabilities by leveraging machine learning to detect patterns, reduce false positives, and improve recall—ultimately providing better protection for businesses and consumers.

Impact & Future Work

Impact:
Our hybrid fraud detection system enhances fraud prevention by integrating rule-based, anomaly detection, and classification models, reducing false positives and improving detection accuracy. Businesses can proactively mitigate financial risks, safeguard customer transactions, and adapt to evolving fraud tactics more effectively than traditional methods.

Future Work:
To further enhance fraud detection, we plan to integrate our system into real-time transaction monitoring, allowing instant fraud detection and intervention. Additionally, we aim to incorporate adaptive learning techniques to continuously refine models based on new fraud patterns and expand the framework for diverse financial use cases.