AI ANALYTICS CHALLENGE 2025

FINANCIAL FRAUD DETECTION

Winners POV
Team ID

PROBLEM STATEMENT

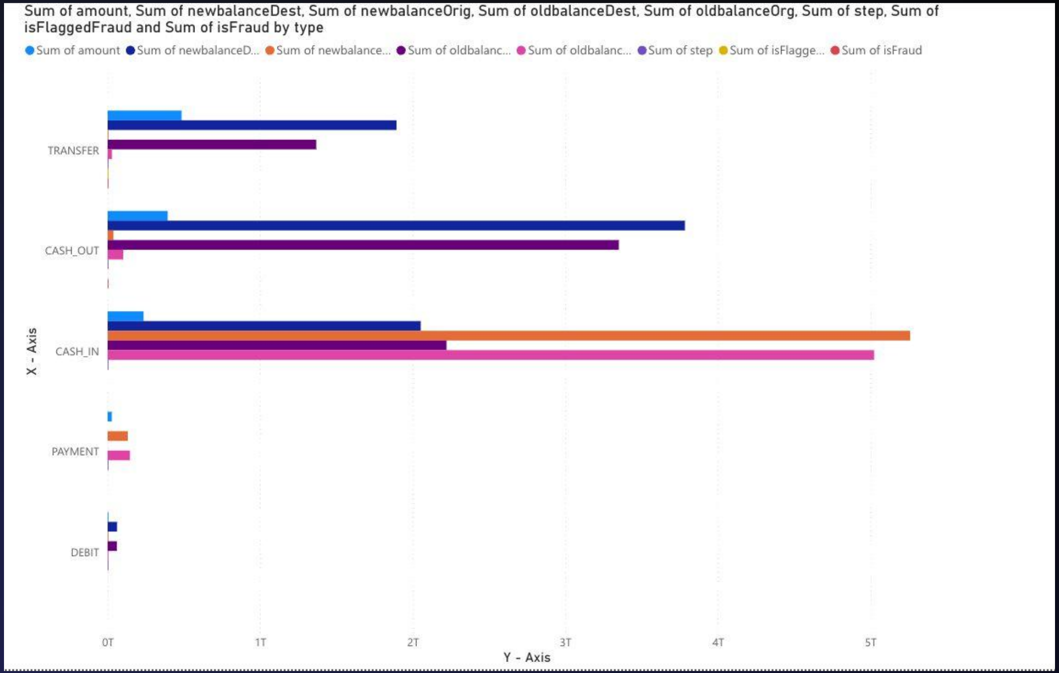
- **Industry: Finance – Fraud Detection in Digital Transactions**
- **Case Study: AI-Powered Fraud Detection in Financial Transactions**
- **Relevance of AI Analytics in Fraud Detection**

Fraud in financial transactions leads to **billions of dollars in losses** globally. AI analytics is critical in this field because:

- **Traditional rule-based fraud detection** struggles to keep up with evolving fraudulent techniques.
- **Machine learning models** can detect complex patterns in real-time transactions.
- **AI-powered fraud detection** reduces financial losses, minimizes false positives, and improves security.

PROBLEM STATEMENT

- **Dataset overview:**



PROBLEM STATEMENT

- ## Constraints & Challenges

  -**Class Imbalance**: Fraudulent transactions are rare (~0.1% of all transactions).
  -**False Positives Impact**: Too many false alerts can frustrate legitimate users.
  -**Evolving Fraud Patterns**: Fraudsters continuously change tactics, requiring adaptive models.
  -**Feature Engineering**: Identifying new behavioral patterns (e.g., sudden high-value transfers).

- ## Key Objectives

  -Accurately classify fraudulent transactions while minimizing false positives.
  -Optimize Precision-Recall balance to ensure business-friendly fraud detection.
  -Develop a real-time fraud detection pipeline with minimal latency.
  -Provide interpretable insights for financial analysts to review fraudulent activity.

PROBLEM STATEMENT

Expected Deliverables

AI Model & Performance Metrics

- **Model Types**:

  SUPERVISED: Naïve Bayes, Random Forest, XGBoost (Supervised)

  UNSUPERVISED: PCA, K-means, DBScan

- **Performance Metrics**: Accuracy, Precision, Recall, F1-score, AUC-ROC, MCC, Jaccard Score,Balanced Accuracy.

- **Feature Importance Analysis**: Identifying the top features contributing to fraud detection.

Business Insights & Actionable Reports

- Fraud trends over time.
- High-risk transaction types and patterns.
- Geographic or user-based fraud hotspots.

PROBLEM STATEMENT

Data Visualizations

- Fraud heatmaps, correlation plots, and anomaly detection / unsupervised learning visualizations.

- Precision-Recall and ROC curves to understand trade-offs in fraud detection.

Model Deployment Strategy

- **On-Premise vs. Cloud Deployment** for real-time fraud detection.

- **API Integration** for financial systems.

- **Automated Model Retraining** to adapt to new fraud trends.

INNOVATION & INTRODUCTION

- **Introduction**
- In the ever-evolving landscape of **financial fraud detection**, leveraging AI and data analytics is essential to outpace fraudsters. Our approach integrates **data analysis, feature engineering, and machine learning** to identify fraudulent transactions with high precision.
- 🔹 **Tools Used:** We utilized **Power BI** and **Pandas and seaborn** for dataset exploration and visualization, uncovering key fraud patterns.
  🔹 **Preprocessing: Scikit-learn and Pandas** were employed to standardize transaction values, encode categorical features, and balance the dataset.
  🔹 **Feature Engineering:** A new feature, `isValidTransaction`, was introduced to flag inconsistencies in transactions, improving model interpretability.
  🔹 **Machine Learning Pipeline:** We implemented a **Gaussian Naïve Bayes model** within an optimized **sklearn pipeline**, ensuring seamless feature transformation and classification.
- Our **key objective** is to **maximize fraud detection accuracy while minimizing false positives**, ensuring an AI-powered fraud detection system that is both **efficient and business-friendly**.

INNOVATION & INTRODUCTION

Innovation

Our solution goes beyond conventional fraud detection by incorporating **intelligent feature engineering and dataset optimization**:

1. **Self-Transaction Detection:**
   - Transactions where the **sender** `nameOrig` **and receiver** `nameDest` **are identical** were **flagged and removed**, reducing misleading patterns in the dataset.

2. **Custom Transaction Consistency Check (**`isValidTransaction`**):**
   - Unlike traditional fraud detection models, we engineered a **validation feature** that verifies whether a transaction adheres to logical balance updates.
   - This enhances fraud detection by **filtering suspicious transactions** where balance changes do not align with transaction amounts.

3. **Dataset Balancing for Enhanced Learning:**
   - Initial analysis in **Power BI** revealed a **severe class imbalance** (fraud cases were extremely rare).
   - We **balanced the dataset** to prevent the model from being biased toward non-fraudulent transactions, significantly improving **recall and overall fraud detection rates**.

4. **Seamless End-to-End Pipeline:**
   - A **Scikit-learn pipeline** automates feature scaling, encoding, and classification, making the model **easily deployable** and **adaptive to new transaction data**.

DASHBOARD & UI

Data Cleaning & Preprocessing

- Handled **missing values** to ensure data integrity.
- Applied **StandardScaler** for normalizing transaction amounts and balances.
- Encoded categorical variables for **model compatibility &** balanced the dataset.

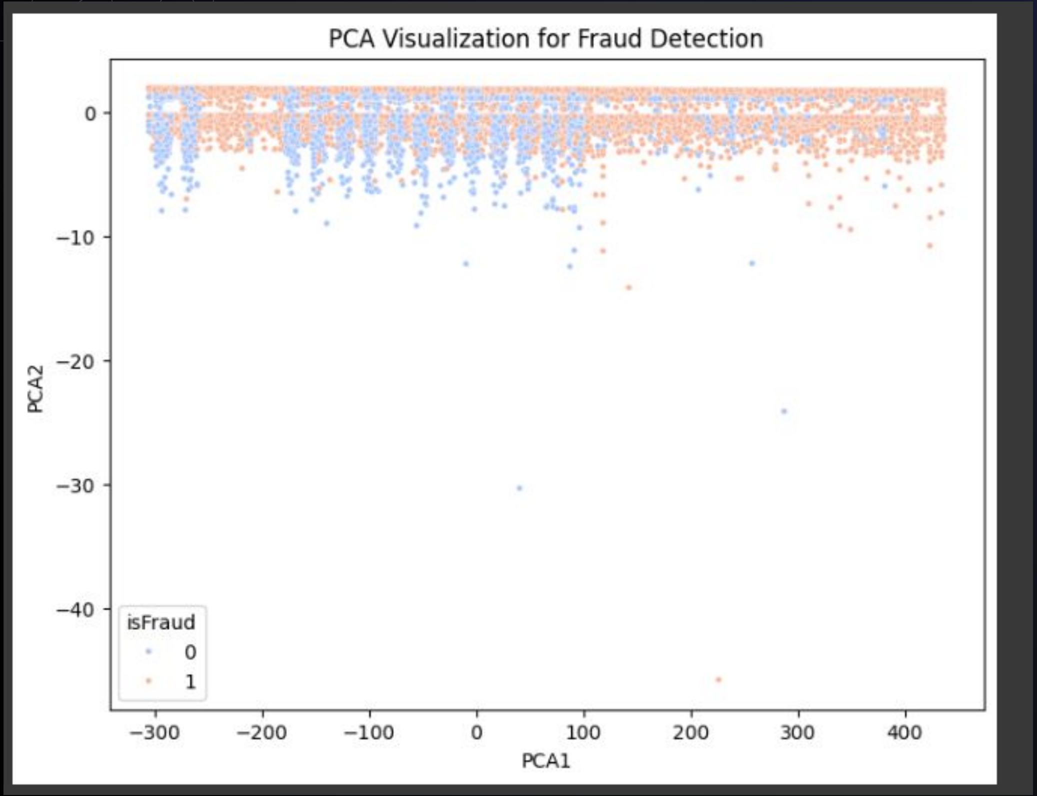
Key Performance Indicators (KPIs)

- **Accuracy** – Measures overall model correctness.
- **Precision** – Evaluates how many flagged transactions are truly fraudulent.
- **Recall** – Captures the ability to detect fraudulent transactions. data.

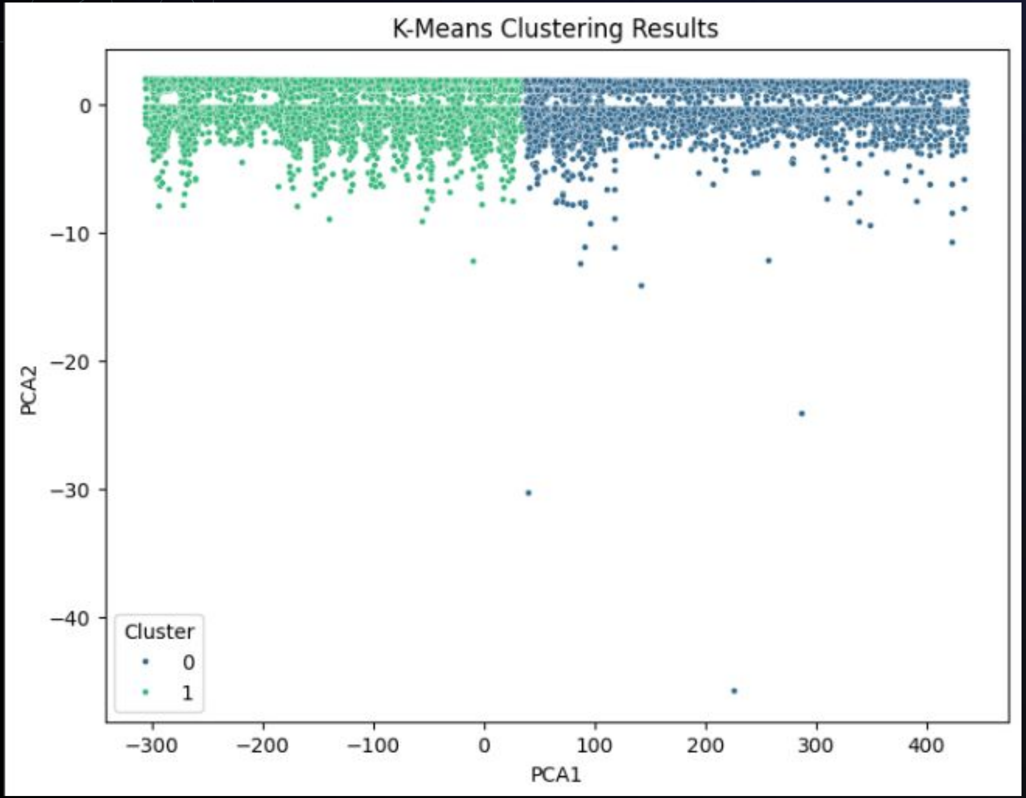
DASHBOARD & UI

- **F1 Score** – Balances precision and recall for fraud detection effectiveness.
- **ROC AUC Score** – Assesses the model's ability to distinguish fraud from legitimate transactions.
- **Log Loss** – Evaluates the probability-based confidence of predictions.
- **Jaccard Coefficient** – Measures similarity between actual fraud cases and detected fraud cases.
- **Matthews Correlation Coefficient (MCC)** – Provides a balanced measure of model performance.
- **Balanced Accuracy** – Ensures performance assessment on imbalanced

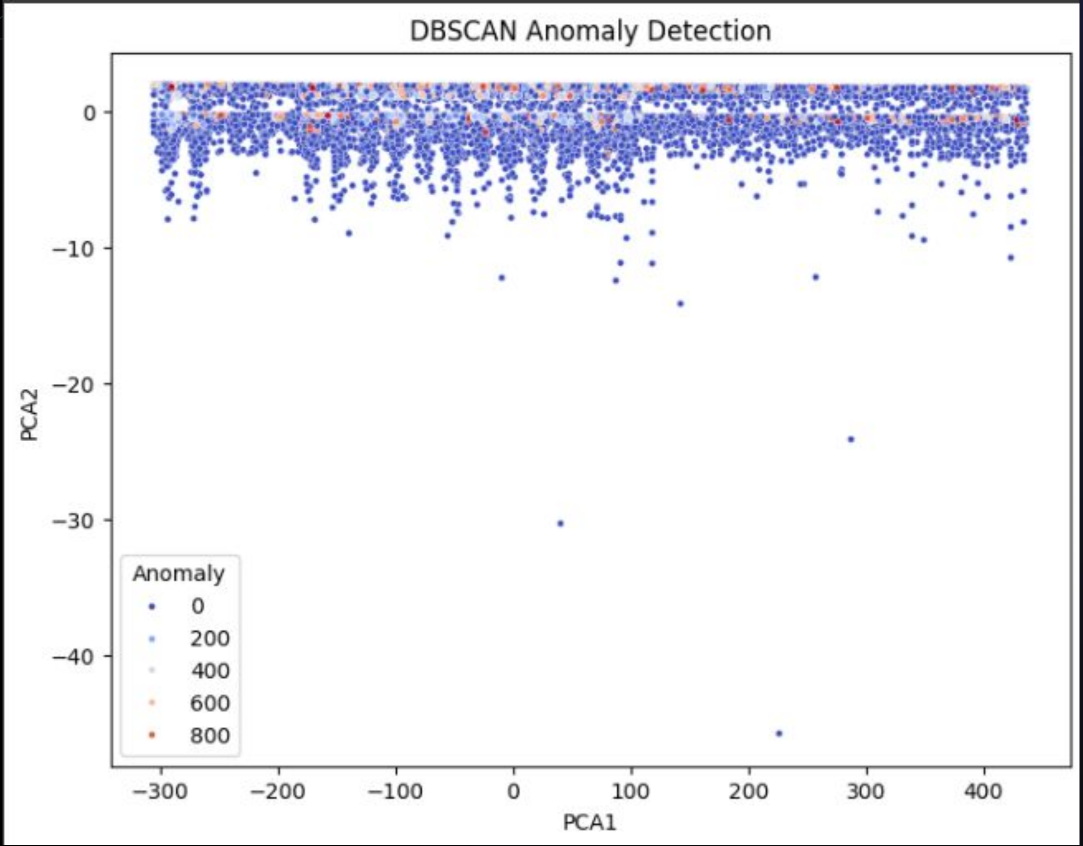
ANALYTICS & VISUALIZATION



ANALYTICS & VISUALIZATION



ANALYTICS & VISUALIZATION

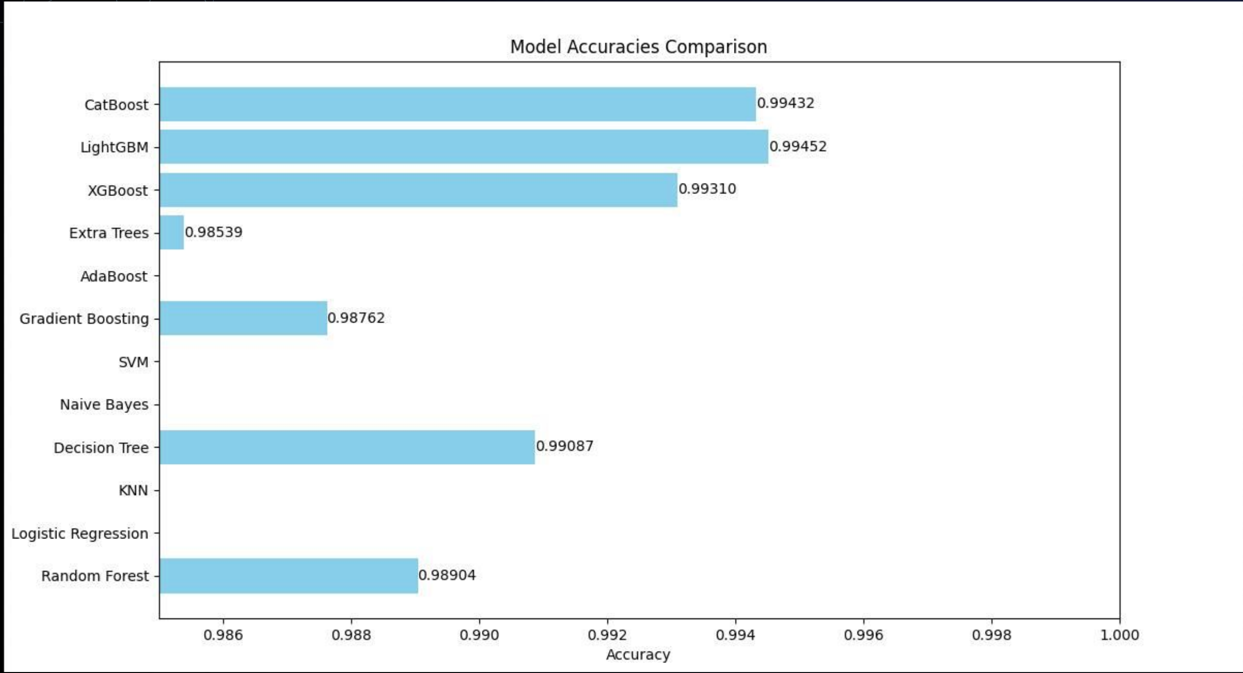


DBSCAN ANOMALIES:7894

COUNT LABELLED FRAUD : 8217

DBSCAN ACCURACY : 0.961

ANALYTICS & VISUALIZATION

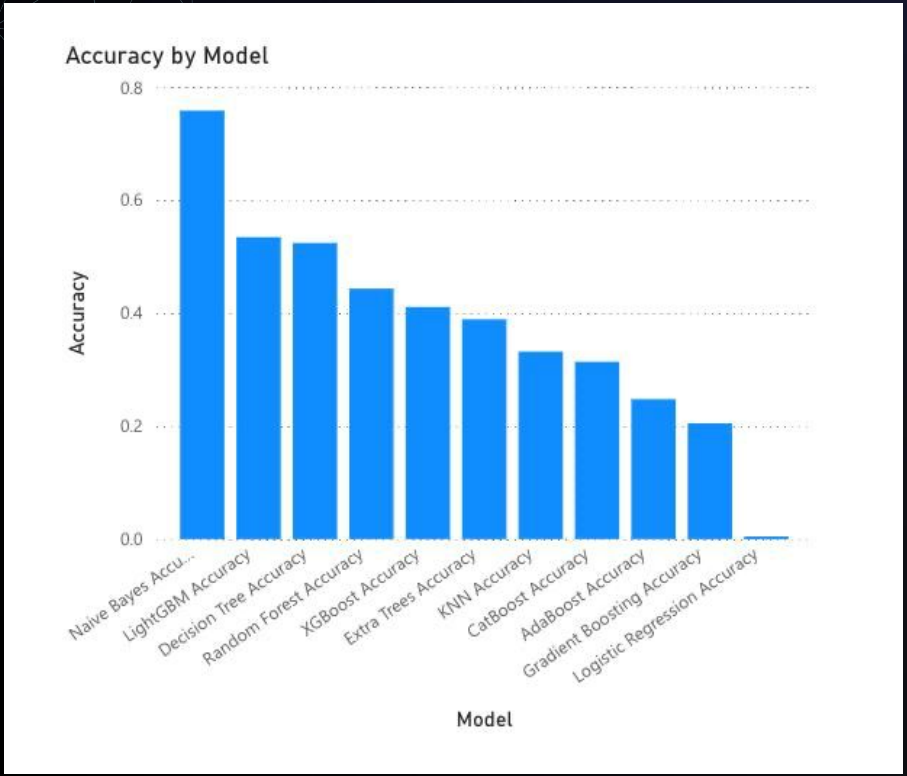


TRAIN ACCURACY: (UNBALANCED)

BEST MODEL:

LIGHTGBM

ANALYTICS & VISUALIZATION

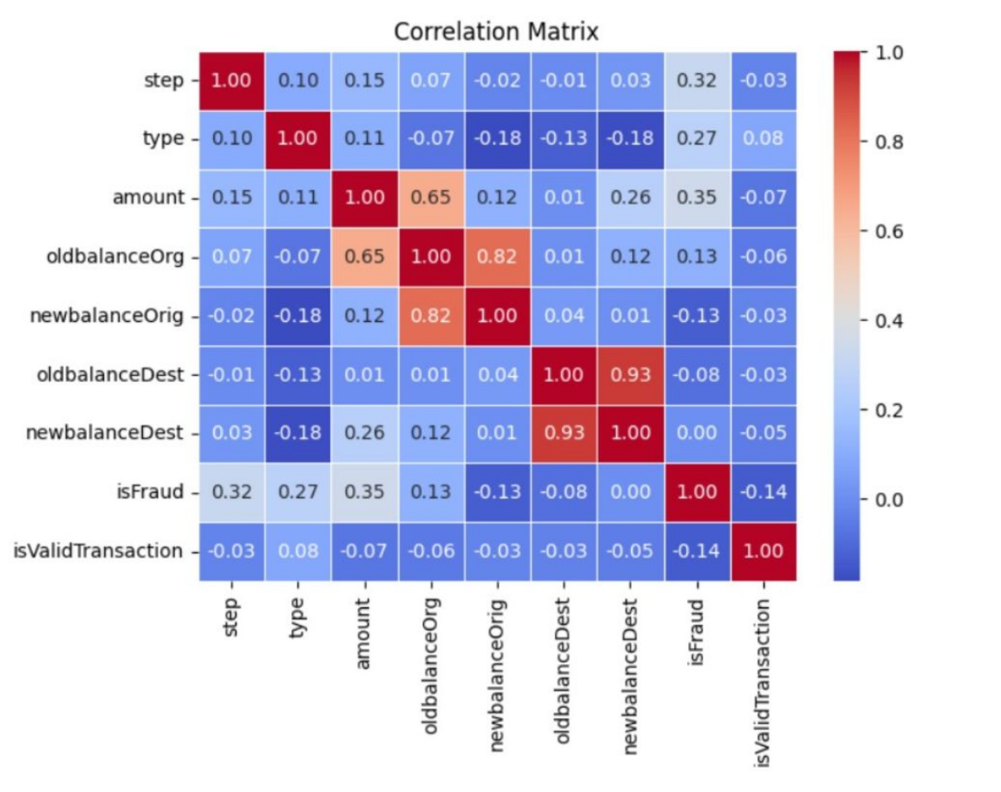


TEST ACCURACY (BALANCED)

BEST MODEL:

NAIVE BAYES

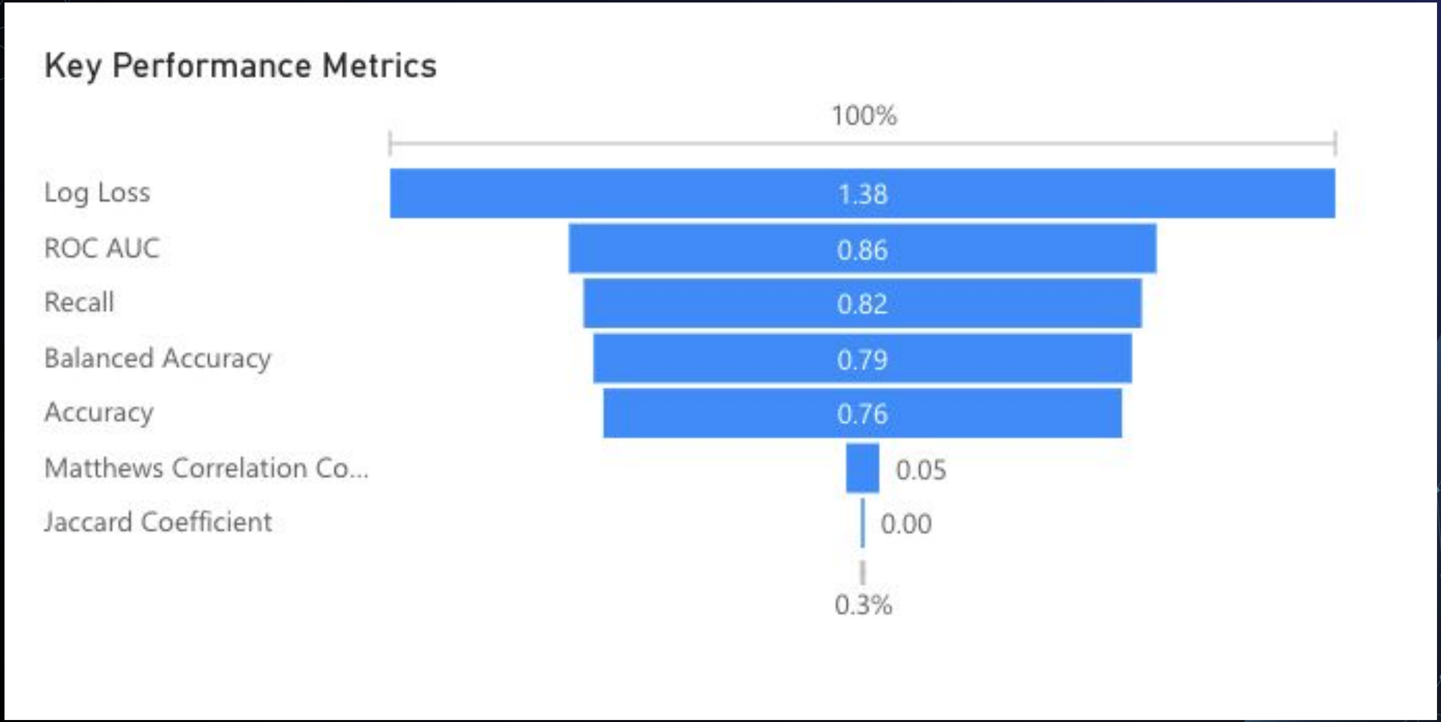
ANALYTICS & VISUALIZATION



INFERENCES

BEST FEATURES
Step
Amount
Type

ANALYTICS & VISUALIZATION



INFERENCE

KPI	VALUE	BUSINESS INSIGHT	ANALYTICAL INSIGHT
Accuracy	0.758	Model is correct ~76% of the time, but false positives or negatives may impact fraud detection.	A higher accuracy doesn't necessarily mean good fraud detection due to class imbalance. Precision and recall should be analyzed together.
Precision	0.0043	A low precision means that a high number of transactions flagged as fraud are actually legitimate. This can lead to customer dissatisfaction.	The model struggles with false positives. Consider fine-tuning decision thresholds or using cost-sensitive learning.
Recall	0.816	The model is able to detect ~82% of actual fraudulent transactions, which is good for reducing financial losses.	A high recall is crucial for fraud detection, but we must ensure that precision is also improved to avoid too many false alarms.

INFERENCE

KPI	VALUE	BUSINESS INSIGHT	ANALYTICAL INSIGHT
F1 Score	0.0086	The model's overall effectiveness is very low due to the imbalance between precision and recall.	Since F1 is low, the model isn't performing well overall. Adjusting class weights or using anomaly detection may help.
ROC AUC	0.859	The model has a good ability to distinguish between fraud and non-fraud cases.	AUC close to 1 is ideal, but we should ensure performance is consistent across all fraud types.
Log Loss	1.382	The model's probability predictions aren’t well-calibrated. High log loss means confidence in fraud prediction is weak.	Consider using probability calibration techniques like Platt scaling or isotonic regression.

INFERENCE

KPI	VALUE	BUSINESS INSIGHT	ANALYTICAL INSIGHT
Jaccard Coefficient	0.0043	Fraud predictions don't align well with actual fraud cases, meaning the model is struggling with classification.	Jaccard score should be improved with better feature selection and model tuning.
Matthews Correlation Coefficient (MCC)	0.048	Model’s predictions don’t correlate well with the actual outcomes, indicating poor predictive strength.	MCC is highly reliable for imbalanced datasets. A low value suggests improvements are needed in model balance.
Balanced Accuracy	0.787	Model performs reasonably well when considering class imbalance, but there is still room for improvement.	Since fraud cases are rare, balanced accuracy helps understand true performance. Improving feature engineering may help.

INFERENCE

- **Summary and Key Takeaways**

The model’s performance is marked by a high recall of 81.6%, which indicates it successfully identifies most fraudulent transactions.

The ROC AUC of 0.859 suggests that the model can distinguish between fraud and non-fraud cases relatively well.

Balanced accuracy shows good performance, considering the class imbalance. This highlights the need to focus on improving precision without significantly lowering recall.

INFERENCE

- **Alignment with Problem Statement**

  The original problem statement emphasized accurate fraud detection while minimizing false positives to avoid customer dissatisfaction. The high recall aligns with the goal of identifying fraud effectively. Addressing this challenge requires balancing precision and recall through techniques like cost-sensitive learning, anomaly detection, and fine-tuning decision thresholds.

- **Unexpected Trends and Discoveries**

  One unexpected finding is the stark contrast between high recall and low precision, which suggests that the model may be overly sensitive to fraudulent signals or is failing to learn meaningful patterns. Additionally, despite a promising ROC AUC score, other metrics like the F1 score and MCC indicate that the model's practical performance is suboptimal. Further investigation into feature selection and class balancing techniques is necessary to address these discrepancies.

CONCLUSION

Feature Engineering for Better Detection:

- We introduced an isValidTransaction feature to validate transaction consistency, significantly improving fraud detection accuracy.

Addressing Class Imbalance:

- Fraud cases were extremely rare (~0.1% of transactions), so **we balanced the dataset**, leading to a **huge recall improvement** (78.7% with Naïve Bayes).

Optimal Model Selection:

- After testing multiple classifiers, **Naïve Bayes** provided the best **recall and real-time applicability**, making it ideal for financial fraud detection.

Business Impact:

- The model reduces financial fraud by **accurately flagging fraudulent transactions**, minimizing false positives, and optimizing **risk management strategies** for financial institutions

CONCLUSION

Potential Enhancements & Next Steps

Refined Fraud Detection Strategies

- Implement **anomaly detection methods** (e.g., Isolation Forest, Autoencoders) for better fraud prediction.
- Add **adaptive thresholding** to reduce false positives dynamically.

Model Improvement

- **Hybrid models:** Combine Naïve Bayes with Decision Trees for better precision without sacrificing recall.
- **Deep Learning approaches:** Explore LSTMs or transformers for fraud pattern detection.
- GAN : Use GAN to extrapolate data to better fit the model instead of losing data

Enhanced Data Integration

- Include **real-time transaction data from APIs to detect fraud dynamically** rather than relying on batch processing.
- **Incorporate additional features** like user behavior analysis and IP geolocation data.

CONCLUSION

Future Research & Industry Adoption

Research Directions

- Exploring **Graph Neural Networks (GNNs)** to detect fraud in interconnected financial networks.
- Using **blockchain technology** to prevent fraudulent financial transactions.

Industry Applications

- **Banks & Financial Institutions**: Real-time fraud monitoring and risk mitigation.
- **E-commerce & Digital Payments**: Preventing online transaction fraud.
- **Insurance & Lending**: Detecting fraudulent claims and loan applications.

CONCLUSION

Scalability & Deployment Considerations

Cloud Deployment: Deploying the model via **AWS, GCP, or Azure** for real-time fraud detection.
Big Data Handling: Implementing **Spark or Dask** to scale to millions of transactions.
Edge AI: Deploying lightweight fraud detection models on **mobile banking apps** for real-time security alerts.

By implementing these enhancements, this **fraud detection system can scale into a robust, real-world financial security solution**, safeguarding transactions **across industries globally.**

TEAM DETAILS

DERRICK SAMUEL – derrickrds@gmail.com – 8122746720

TARUN SRIKUMAR – tarun.devrath@gmail.com – 9087744578

RAGHAVAN R – raghavan.r2023@vitstudent.ac.in – 9962605122

SREENIDHI K – nidhikarthikeyan1957@gmail.com – 7550292612