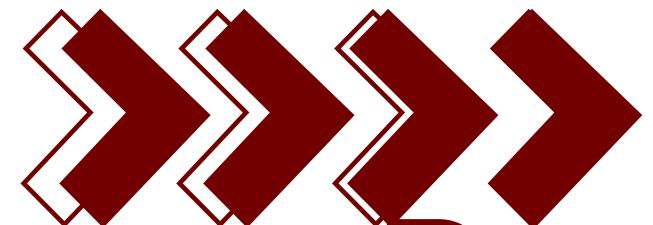


Fraud Detection

Kelompok 6:
2702213530 - Sandy Agatha Indra Lim
2702209483 - Vania Oriana Tanoto
2702279086 - Ricky Atha Ajie Alvianto



Background Review

Cybercrime banking fraud adalah kejahatan siber yang menargetkan sistem perbankan dan nasabah untuk mencuri uang atau data penting. Serangan dilakukan melalui internet, malware, atau penipuan sosial (social engineering). Bank Indonesia menyebutkan 3 modus utama:

- ◆ Skimming - Merekam data kartu di mesin ATM/EDC dengan alat tersembunyi.
 - ◆ Phishing - Menipu nasabah lewat email/situs palsu untuk mencuri data rahasia.
 - ◆ Malware - Software berbahaya yang mencuri data atau mengendalikan perangkat korban.
- 👉 Modus ini sering dikombinasikan.

Maka dari itu kami membuat sistem menggunakan Machine Learning untuk memprediksi Fraud dari beberapa faktor yang ada.





Literatur Review

Fraud Detection in Credit Card Transactions using HDBSCAN, UMAP, and SMOTE

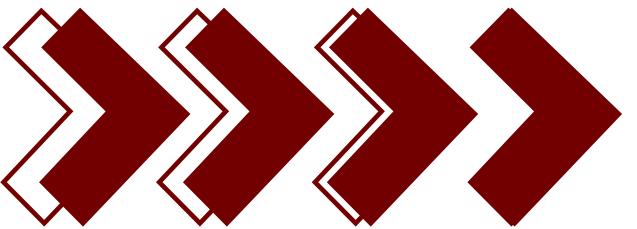
- Tantangan: Data besar & tidak berlabel
- Solusi: HDBSCAN + UMAP + SMOTE
- Hasil: Identifikasi anomali tanpa label, pseudo-label digunakan untuk pelatihan model
- Pipeline unsupervised dapat digunakan saat label tidak tersedia

Unsupervised Label Generation for Severely Imbalanced Fraud Data

- Tantangan: Label fraud sangat sedikit
- Solusi: Clustering untuk pseudo-label → dilatih dengan Random Forest & GB
- Hasil: Performa mendekati model berlabel
- Cocok untuk data fraud real-world yang sulit dilabeli

Explainable Deep Behavioral Sequence Clustering for Transaction Fraud Detection

- Fokus: Urutan perilaku transaksi
- Teknik: Bi-LSTM → GPU HDBSCAN → Pseudo-label → Model supervised
- Hasil: Deteksi fraud baru + interpretasi yang jelas
- Gabungan deep learning & clustering = sistem deteksi yang akurat dan mudah dijelaskan



Tujuan

- Memprediksi apakah suatu transaksi merupakan penipuan atau bukan
- Mengembangkan model machine learning berbasis data historis
- Mendeteksi pola transaksi mencurigakan secara otomatis

Manfaat Dari Sistem ini

- Memberikan sistem peringatan dini bagi pihak bank secara real-time
- Mengurangi jumlah transaksi fraud dan kerugian finansial
- Memberikan insight untuk peningkatan keamanan sistem bank secara berkelanjutan



Dataset Overview

Penelitian ini menggunakan dataset transaksi perbankan dari LOL Bank Pvt. Ltd.

Dataset ini mencakup data nasabah, transaksi, merchant, dan perangkat yang digunakan.

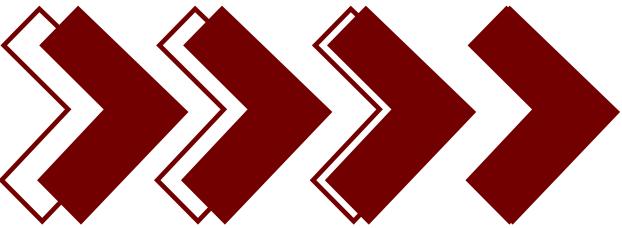


Karakteristik Dataset:

- Memiliki label asli 'Is_Fraud' yang kami gunakan untuk evaluasi model unsupervised
- Dimensi: 200.000 x 24
- Customer_ID: Identifikasi unik untuk nasabah
- Transaction_ID: Identifikasi unik untuk setiap transaksi
- Transaction_Date & Transaction_Time: Waktu dan tanggal saat transaksi terjadi
- Transaction_Amount: Jumlah uang yang terlibat dalam transaksi
- Transaction_Type: Jenis transaksi (Withdrawal, Deposit, Transfer)
- Merchant_ID & Merchant_Category: Informasi terkait merchant
- Transaction_Device & Device_Type: Perangkat yang digunakan untuk melakukan transaksi
- Transaction_Location: Lokasi geografis transaksi
- Is_Fraud: Label target (1 jika transaksi merupakan penipuan, 0 jika bukan)
- Transaction_Currency: Mata uang yang digunakan dalam transaksi

Feature Utama Pembentuk Dataset

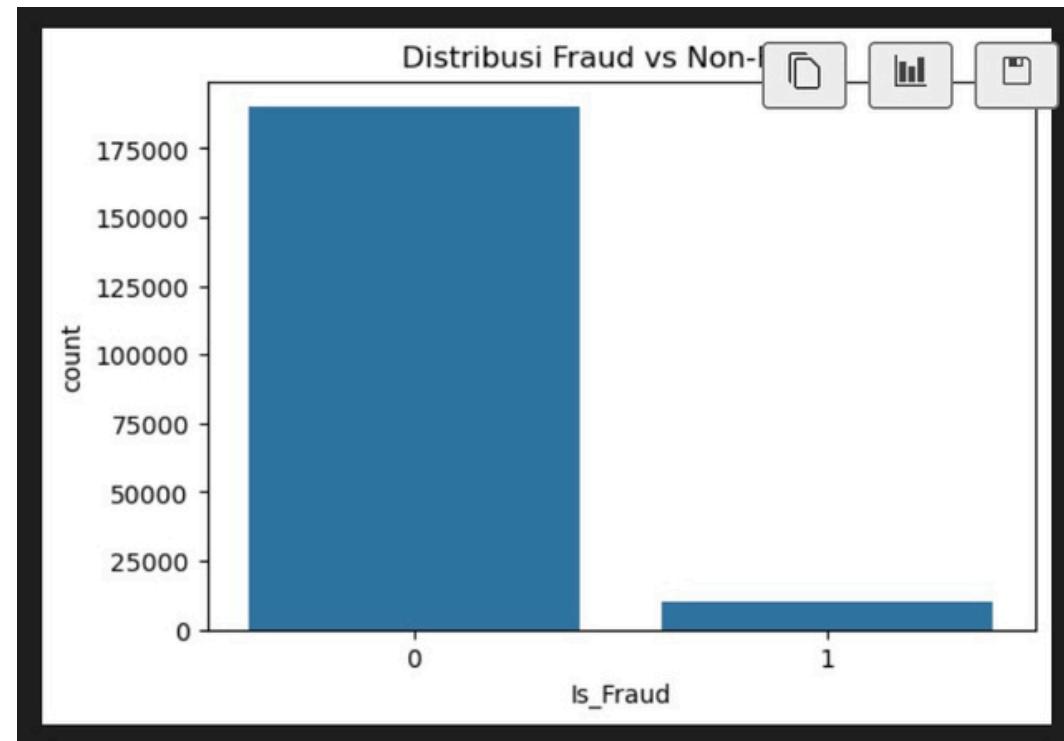
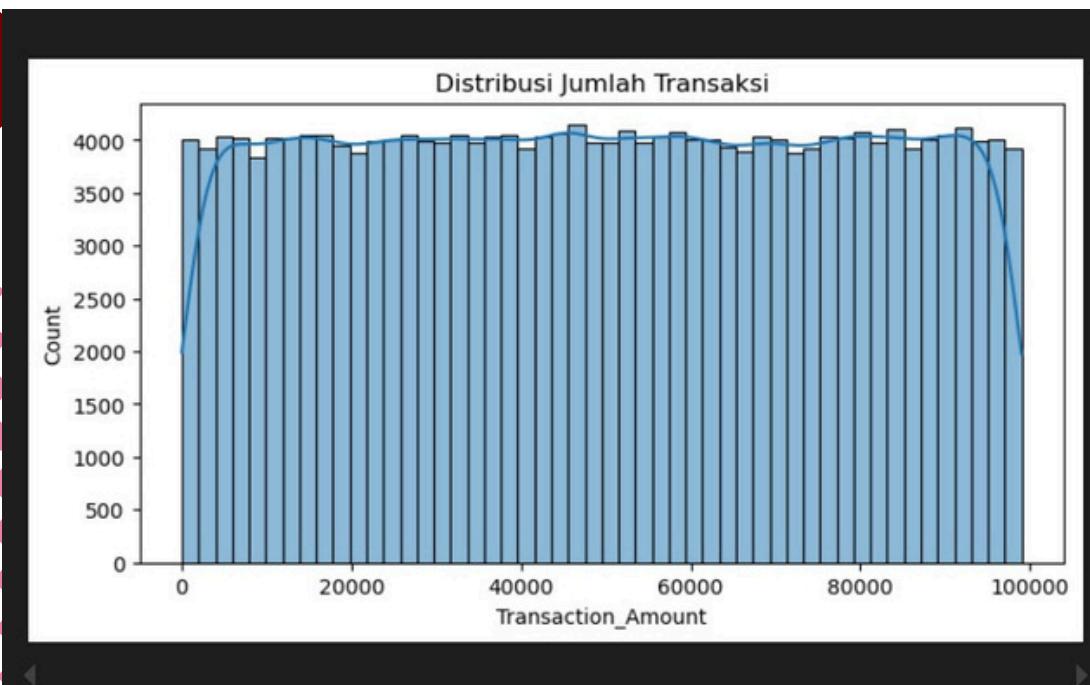
	Gender	Age	State		City	Bank_Branch	Account_Type	Transaction_Amount	Transaction_Type	Merchant_Category	Account_Balance	Transaction_Device	Device_Type	Is_Fraud
0	Male	60	Kerala	Thiruvananthapuram	Thiruvananthapuram Branch		Savings	32415.45	Transfer	Restaurant	74557.27	Voice Assistant	POS	0.0
1	Female	51	Maharashtra	Nashik	Nashik Branch		Business	43622.60	Bill Payment	Restaurant	74622.66	POS Mobile Device	Desktop	0.0
2	Male	20	Bihar	Bhagalpur	Bhagalpur Branch		Savings	63062.56	Bill Payment	Groceries	66817.99	ATM	Desktop	0.0
3	Female	57	Tamil Nadu	Chennai	Chennai Branch		Business	14000.72	Debit	Entertainment	58177.08	POS Mobile App	Mobile	0.0
4	Female	43	Punjab	Amritsar	Amritsar Branch		Savings	18335.16	Transfer	Entertainment	16108.56	Virtual Card	Mobile	0.0



EDA

Memahami Pola Transaksi dan Ketimpangan Label

- ◆ Distribusi Fraud vs Non-Fraud
 - Mayoritas transaksi adalah non-fraud (label 0)
 - Transaksi fraud (label 1) sangat sedikit, ini menunjukkan ketidakseimbangan data (imbalance class)
 - Penting untuk mempertimbangkan teknik khusus saat melatih model
- ◆ Distribusi Jumlah Transaksi
 - Jumlah transaksi tersebar cukup merata dari nominal kecil hingga besar
 - Distribusi relatif simetris, dengan sedikit penurunan di nilai ekstrem
 - Tidak ada nilai ekstrem yang sangat dominan (tidak terlalu banyak outlier)
 - Kesimpulan:
 - Model harus menangani ketidakseimbangan label dan mampu mengenali pola transaksi mencurigakan di antara data yang terlihat "normal".



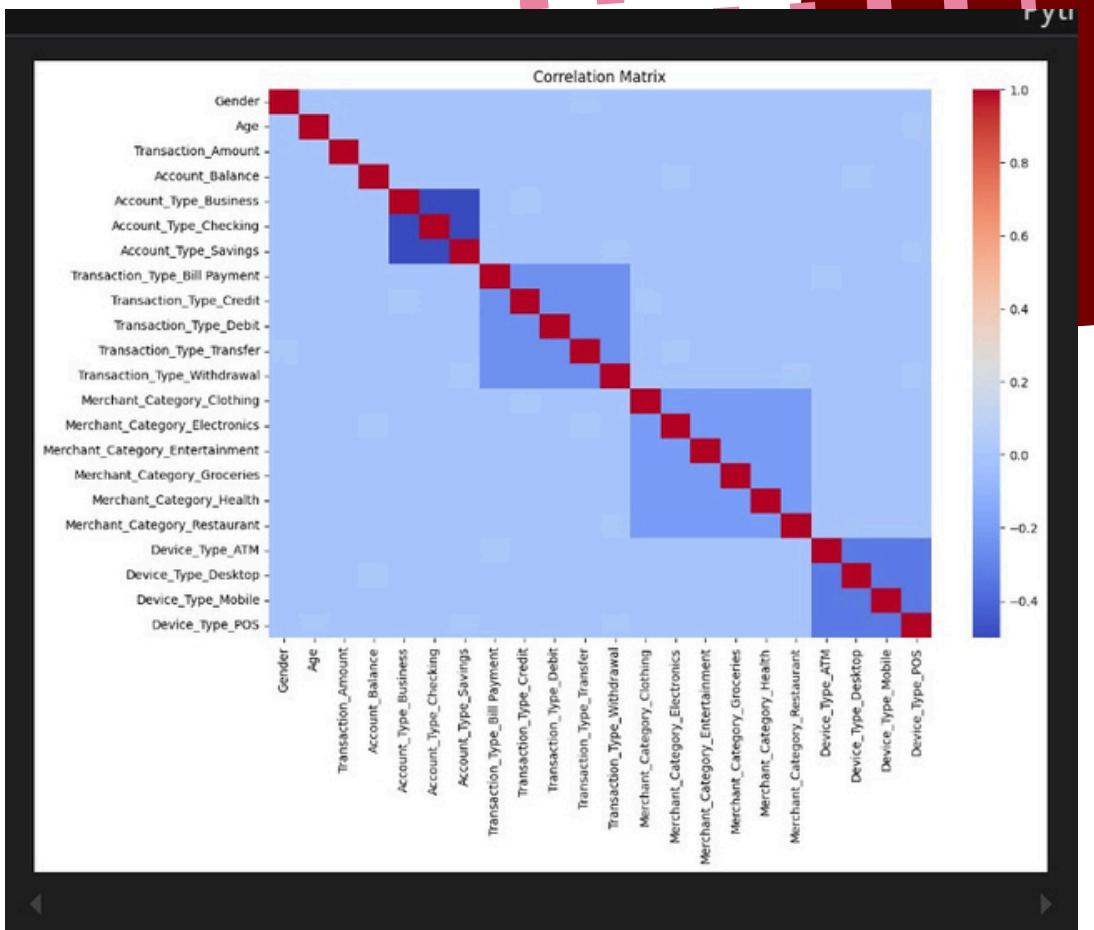
Data Preprocessing & Feature Engineering

Langkah awal

- ✓ Cek missing value → Tidak ditemukan
- 12 34 Analisis unique values → Mengidentifikasi fitur kategorikal
- 🔍 Value count → Mengecek potensi typo atau nilai serupa yang berbeda penulisan

Encoding fitur

1. Label Encoding
 - Fitur: Gender
 - Nilai: Male = 1, Female = 0
 - Alasan: Hanya 2 kategori yang saling eksklusif
2. One-Hot Encoding
 - Fitur: Account_Type, Transaction_Type, Merchant_Category, Device_Type
 - Alasan: > 2 kategori & tidak memiliki hubungan ordinal



Corr Matrix

- Tidak ada data yang multikolinearitas ekstrem
- Fitur-fitur cukup beragam dan independen
- Data layak dilanjutkan ke proses pemodelan



Feature Selection

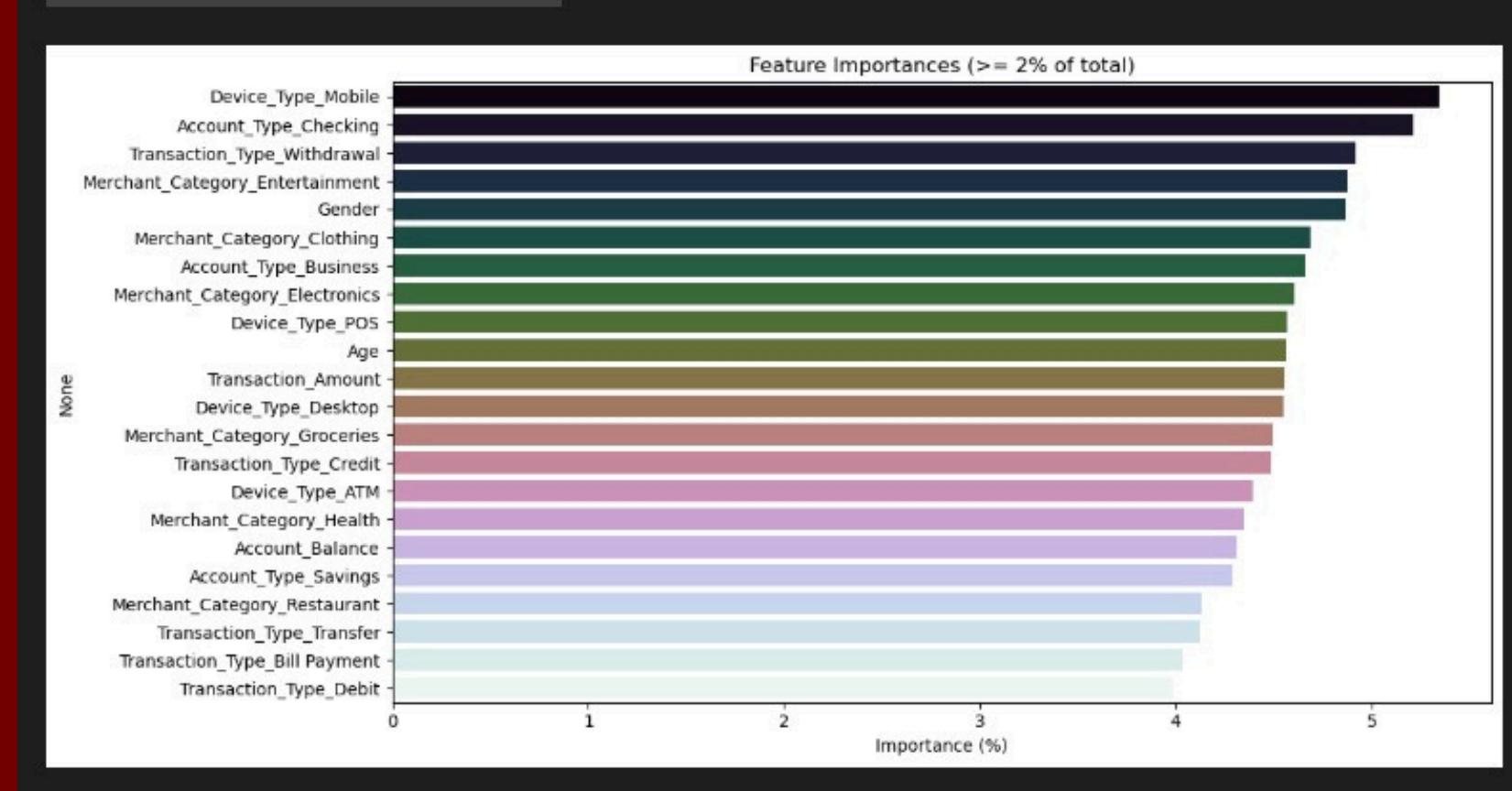
```
Fitur yang dipilih (importance >= 2%):
Device_Type_Mobile      5.34
Account_Type_Checking    5.21
Transaction_Type_Withdrawal 4.92
Merchant_Category_Entertainment 4.88
Gender                    4.87
Merchant_Category_Clothing 4.69
Account_Type_Business     4.66
Merchant_Category_Electronics 4.61
Device_Type_POS            4.57
Age                        4.56
Transaction_Amount         4.56
Device_Type/Desktop        4.55
Merchant_Category_Groceries 4.49
Transaction_Type_Credit    4.48
Device_Type_ATM             4.39
Merchant_Category_Health    4.35
Account_Balance             4.31
Account_Type_Savings         4.29
Merchant_Category_Restaurant 4.13
Transaction_Type_Transfer    4.12
Transaction_Type_Bill Payment 4.03
Transaction_Type_Debit       3.99
dtype: float32
```

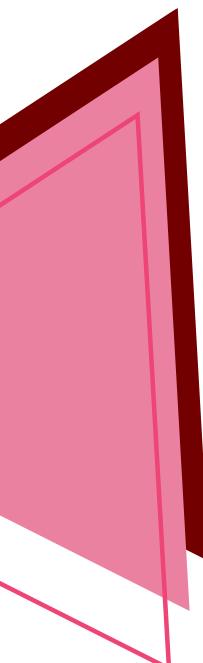
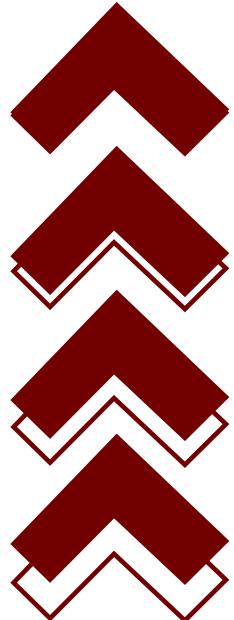
Tujuan Feature Selection

- Mengurangi noise
- Menghindari overfitting
- Meningkatkan efisiensi dan akurasi model

Metode yang Digunakan

- Menggunakan Feature Importance dari XGBoost
- Threshold kontribusi fitur $\geq 2\%$
- Fitur di bawah ambang ini dihapus dari dataset





Experiments

Model (Silhouette Scores):

KMeans: 0.069

DBSCAN: 0.26

GMM: 0.06



Model yang digunakan:

HDBSCAN: 0.34

Alasan: model yang lebih canggih daripada DBSCAN.

Masalah yang ditemukan

HDBSCAN secara otomatis membentuk banyak cluster tanpa batasan jumlah. Sedangkan kita memerlukan 2 cluster (1/0). Sebagian cluster yang dihasilkan berukuran sangat kecil, sehingga dianggap sebagai outlier atau noise.

Solusi Pertama:

Mengidentifikasi label (1/0) dengan membagi cluster kecil ke dalam kelompok besar.

Gagal:

Tidak ditemukan tuning yang cocok untuk membagi cluster

Best threshold: None
Best F1-score (fraud class): 0.0000
Final classification report:
None

Solusi Kedua:

Semi-Supervised Learning via Pseudo-Label Augmentation

Berhasil:

Ada model XGBoost Supervised learning yang dikelola untuk menjadi perbandingan dengan pseudo labeling dari unsupervised learning.

Machine Learning Project

- EVALUASI SETELAH PSEUDO LABEL ---

Optimal threshold: 0.64608365

Classification Report:

	precision	recall	f1-score	support
0	0.93	1.00	0.97	45579
1	1.00	0.93	0.96	45579
accuracy			0.96	91158
macro avg	0.97	0.96	0.96	91158
weighted avg	0.97	0.96	0.96	91158

Confusion Matrix:

```
[[45566  13]
 [ 3280 42299]]
```

ROC AUC Score: 0.9715544357878938

Recall (fraud class): 0.9280370345992672

Accuracy: 0.9638759077645407

Berdasarkan hasil evaluasi yang menunjukkan akurasi tinggi, recall yang kuat terhadap kelas fraud, serta kestabilan performa secara keseluruhan, model ini dinilai telah memiliki kualitas yang memadai untuk diintegrasikan ke dalam sistem deteksi fraud pada aplikasi perbankan digital. Dengan kemampuan mendeteksi transaksi mencurigakan secara efektif, model ini dapat berperan sebagai komponen pendukung dalam proses pemantauan real-time dan pengambilan keputusan.

Result

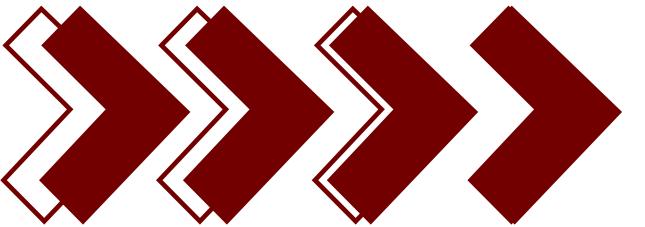
Langkah-langkah Semi-Supervised Learning via Pseudo-Label Augmentation:

1. HDBSCAN digunakan tanpa label untuk menemukan struktur dan menghasilkan pseudo-label
2. Untuk meningkatkan hasil dari pseudo-label, model supervised (XGBoost) dilatih dan dievaluasi

Kesimpulan: supervised adalah alat bantu untuk menguatkan dan memvalidasi hasil unsupervised

Notes: supervised digunakan untuk evaluasi saja dan tidak digunakan dalam eksplorasi data awal

Machine Learning Project

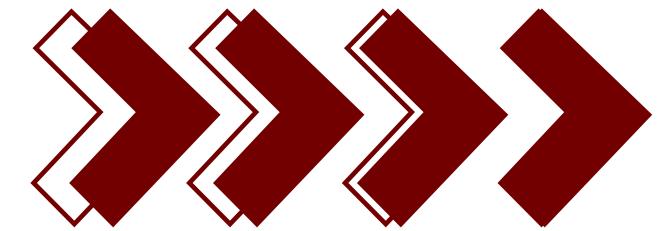


Application

Notes: Input yang diminta disesuaikan dengan fitur yang digunakan untuk menjalankan model.

The screenshot shows a user interface for a fraud detection application. At the top, there is a header with three circular icons and the text "Fraud Detection – LOL Bank". Below the header, a sub-header says "Masukkan data transaksi untuk memprediksi apakah transaksi tersebut berpotensi fraud." The main form consists of two columns of input fields. The left column includes fields for "Gender" (Male), "Age" (30), "Account Balance" (1000,00), "Account Type" (Business), "Transaction Type" (Debit), "Merchant Category" (Food), "Device Type" (Desktop), and "Transaction Amount" (85269,00). A "Prediksi" button is located below these fields. The right column includes fields for "Age" (30), "Account Balance" (1000,00), "Account Type" (Savings), "Transaction Type" (Withdrawal), "Merchant Category" (Retail), "Device Type" (Mobile), and "Transaction Amount" (100,00). Another "Prediksi" button is located below these fields. Below each set of "Prediksi" buttons are "Hasil Prediksi:" sections. The left section shows a red bar with the text "Transaksi ini terindikasi FRAUD." The right section shows a green bar with the text "Transaksi ini NORMAL."

Machine Learning Project



Thank You

Kelompok 6 Machine Learning LA08