تقرير مشروع

نظام كشف الاحتيال في المعاملات المالية

Credit Card Fraud Detection — Machine Learning Project

الملخص التنفيذي

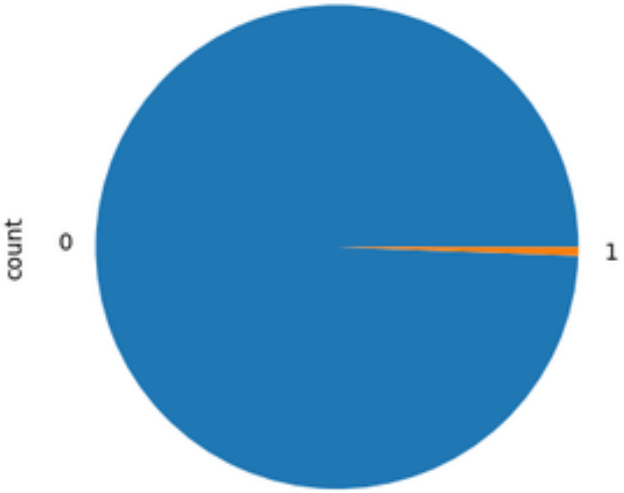
المشروع ده بيهدف لبناء نظام تعلم آلي قادر على اكتشاف المعاملات المالية الاحتيالية وسط ملايين المعاملات السليمة. تم استخدام بيانات محاكاة لمعاملات كروت ائتمان (أكتر من 1.29 مليون معاملة)، وتم بناء أكتر من 10 خصائص (Features) جديدة تعتمد على السلوك التاريخي للعميل، الموقع الجغرافي، والتوقيت، بدل الاعتماد على البيانات الخام فقط. الموديل النهائي (XGBoost) حقق دقة (Precision) 95% وقدرة اكتشاف (Recall) 80% لحالات الاحتيال الفعلية، وهي نتيجة قوية تسمح باكتشاف معظم حالات الاحتيال مع أقل قدر ممكن من إزعاج العملاء الأبرياء.

المشكلة والبيانات

الاحتيال المالي بيمثل تحدي حقيقي لأي جهة بتعالج معاملات مالية، لأن عدد حالات الاحتيال ضئيل جدًا مقارنة بحجم المعاملات الكلي، وده بيخلي اكتشافه صعب على المراجعة اليدوية أو القواعد الثابتة البسيطة.

تفاصيل البيانات

- عدد المعاملات: 1,296,675 معاملة
- عدد الأعمدة الأصلية: 22 عمود (بيانات معاملة، بيانات عميل، بيانات تاجر)
- نسبة الاحتيال: أقل من 1% من إجمالي المعاملات (عدم توازن شديد بين الفئتين)

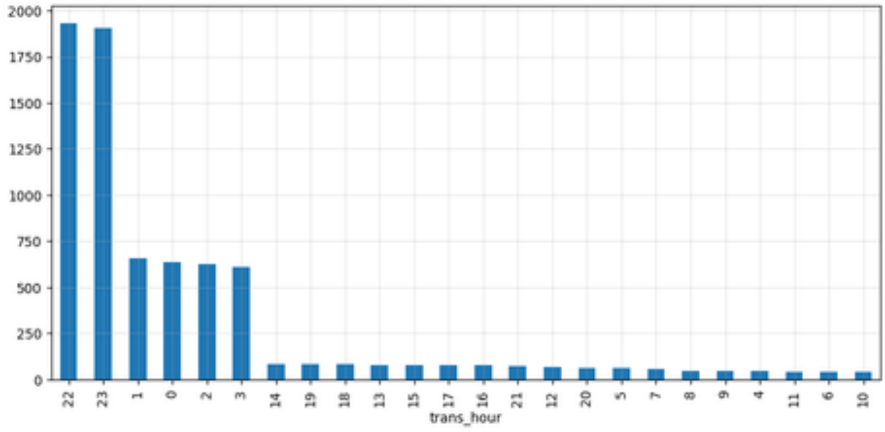


شكل *1* — توزيع المعاملات *(سليمة مقابل احتيال)*، يوضح الحجم الحقيقي لمشكلة عدم التوازن في البيانات

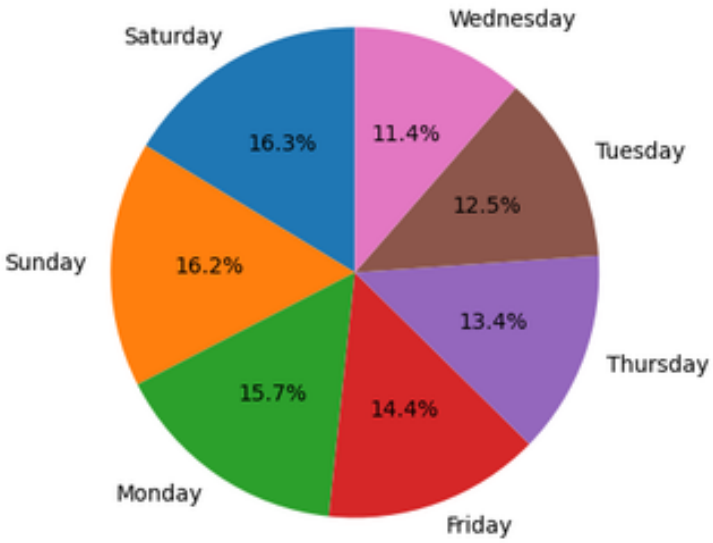
أبرز نتائج تحليل البيانات (EDA)

قبل بناء الموديل، تم تحليل البيانات لفهم متى وأين وإزاي بيحصل الاحتيال، وده ساعد في بناء خصائص (Features) مبنية على أنماط حقيقية بدل التخمين.

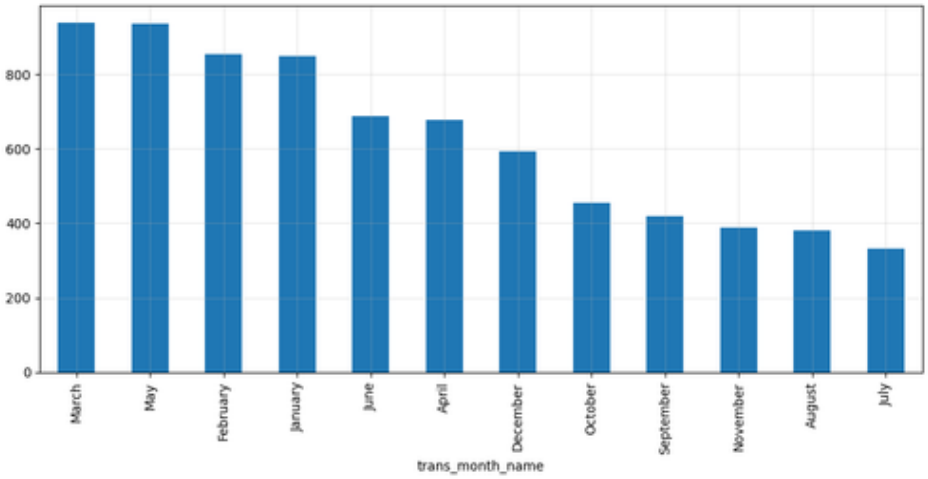
التوزيع الزمني للاحتيال



شكل *2* — عدد حالات الاحتيال حسب ساعة اليوم: يتضح تركز الاحتيال بشكل واضح في ساعات الليل المتأخر والفجر *(من 10 مساءً حتى 3 صباحًا)*

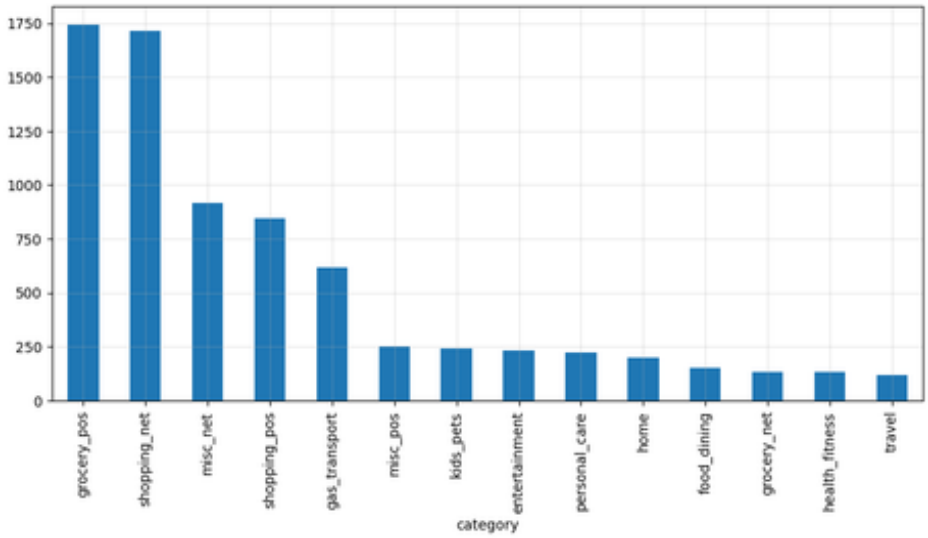


شكل *3* — عدد حالات الاحتيال حسب يوم الأسبوع: عطلة نهاية الأسبوع *(السبت والأحد)* الأعلى في عدد حالات الاحتيال

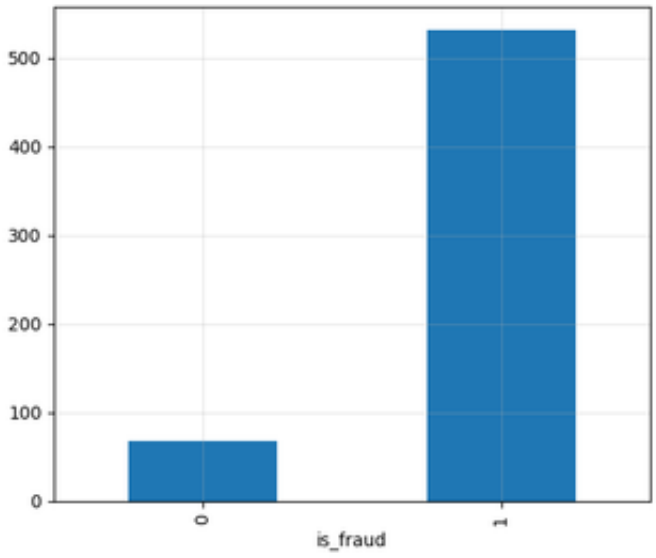


شكل *4* — عدد حالات الاحتيال حسب الشهر: شهور مارس ومايو وفبراير ويناير الأعلى، بينما شهور الصيف الأقل

فئة التاجر ومبلغ المعاملة



شكل *5* — عدد حالات الاحتيال حسب فئة التاجر: التسوق أونلاين *(shopping_net)* والبقالة *(grocery_pos)* من أعلى الفئات بالعدد المطلق لحالات الاحتيال



شكل 6 — متوسط مبلغ المعاملة: سليمة مقابل احتيال. معاملات الاحتيال متوسط مبلغها أعلى بوضوح من المعاملات السليمة

الخصائص (Features) التي تم بناؤها

بدل الاعتماد على الأعمدة الخام فقط، تم اشتقاق مجموعة من الخصائص المبنية على منطق تحليلي واضح، وكل خاصية ليها سبب واضح لاختيارها:

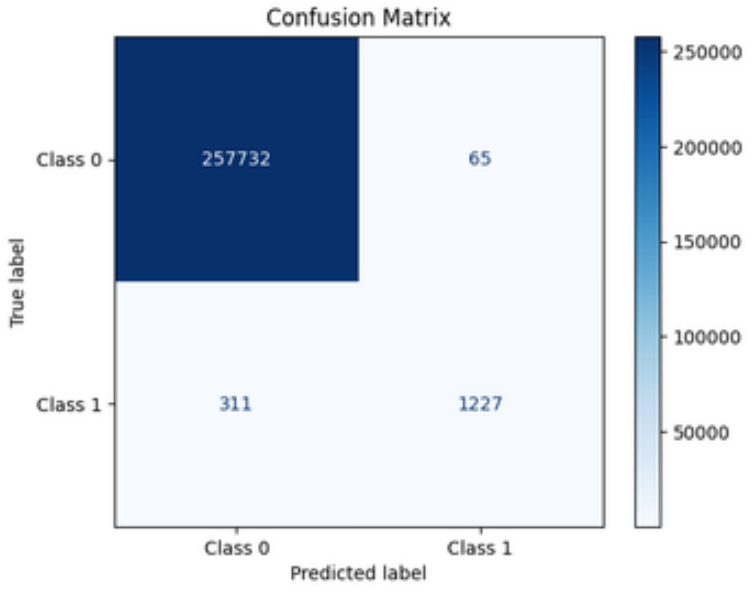
الهدف منها	المصدر	الخاصية
رصد أنماط الاحتيال المرتبطة بوقت معين من اليوم	trans_date_trans_time	trans_hour
رصد أنماط موسمية أو مرتبطة بأيام معينة	trans_date_trans_time	trans_weekday / trans_month
بعض الفئات العمرية أكثر عرضة للاحتيال	dob	customer_age
كشف المعاملات البعيدة جغرافيًا عن مكان سكن العميل	lat/long + merch_lat/merch_long	distance_customer_merchant
كشف حالات السفر المستحيل فيزيائيًا بين معاملتين متتاليتين	الموقع + الوقت	max_distance_last_txn
كشف تكرار المعاملات في وقت قصير جدًا	cc_num + الوقت	• customer_txn_count_1h
معرفة متوسط إنفاق العميل التاريخي (بدون تسريب بيانات مستقبلية)	cc_num + amt	customer_avg_amt_so_far
قياس مدى غرابة المبلغ الحالي عن سلوك العميل المعتاد	amt - customer_avg_amt_so_far	amt_deviation_from_avg

ملاحظة: تم بناء جميع الخصائص المعتمدة على تاريخ العميل بحيث تعتمد فقط على المعاملات السابقة زمنيًا لتجنب تسريب بيانات من المستقبل *(Data Leakage)*.

الموديل والنتائج

تم استخدام Logistic Regression كموديل مبدئي (Baseline)، ثم تم بناء موديل XGBoost كموديل أساسي نظرًا لقدرته العالية على التعامل مع البيانات غير المتوازنة والعلاقات المعقدة بين الخصائص.

مصفوفة الالتباس (Confusion Matrix)

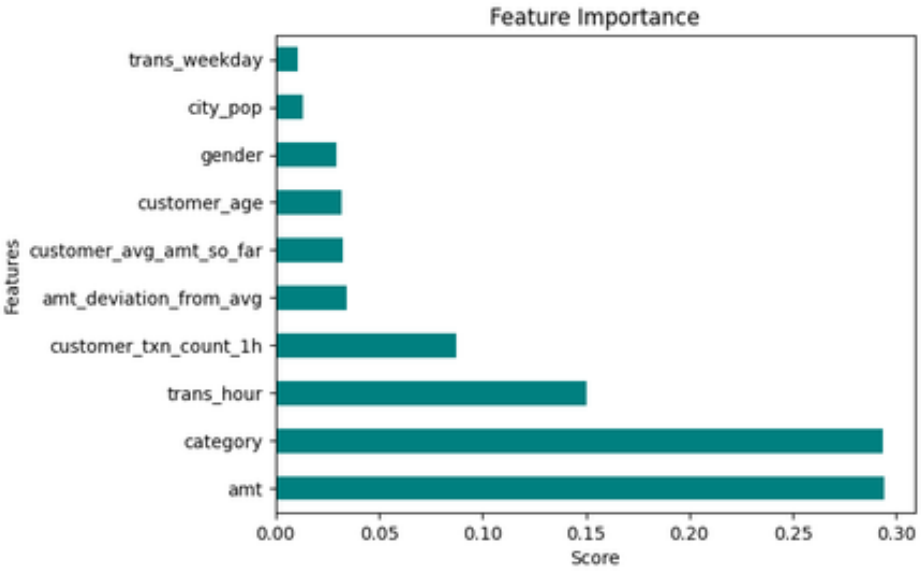


شكل *7* — من أصل *1,538* حالة احتيال حقيقية، تمكن الموديل من اكتشاف *1,227* حالة *(Recall = 80%)*، مع *65* إنذار كاذب فقط من أصل أكثر من *257* ألف معاملة سليمة

المقياس	القيمة	التفسير
Precision	0.95	95% من إنذارات الموديل كانت احتيال فعلي
Recall	0.80	الموديل اكتشف 80% من كل حالات الاحتيال الحقيقية
F1-Score	0.87	توازن جيد بين الدقة والقدرة على الاكتشاف

ملاحظة مهمة: تم تجاهل مقياس *Accuracy* عمدًا في تقييم الأداء، لأنه مضلل في المشاكل غير المتوازنة (يعطي نتيجة عالية وهمية حتى لو تجاهل الموديل الاحتيال تمامًا).

أهم العوامل المؤثرة في قرار الموديل (Feature Importance)



شكل *8* — مبلغ المعاملة *(amt)*، فئة التاجر *(category)*، وساعة المعاملة *(trans_hour)* هي أكثر *3* عوامل تأثيرًا على قرار الموديل

القرار البيزنس: التوازن بين الدقة والإزعاج

قرار حساسية الموديل (Threshold) مش قرار تقني بس، لأنه بيحدد التوازن بين نوعين من الأخطاء:

- رفع الحساسية ← اكتشاف حالات احتيال أكتر، لكن زيادة في عدد العملاء الأبرياء اللي هتتوقف معاملاتهم غلط
- خفض الحساسية ← إزعاج أقل للعملاء، لكن زيادة في حالات الاحتيال اللي هتفوت من غير اكتشاف

في الوضع الحالي، الموديل يحقق توازن جيد (65 إنذار كاذب فقط مقابل اكتشاف 80% من الاحتيال)، وهو نقطة بداية قوية يمكن تعديلها لاحقًا حسب أولوية الجهة المستخدمة (تقليل الخسائر المالية أو تقليل إزعاج العملاء).