Republic of Yemen
Ministry of Education and Scientific Research
University of Science and Technology
Deanship of Postgraduate Studies and Scientific Research

Improving Fraud Detection in Credit Cards using Ensemble Learning with a Boosting Approach and Deep Learning Models

A Thesis Submitted by

Al-Maha Hashem Ali Al-Wadie

To

The Council of Postgraduate Studies and Scientific Research, in Partial Fulfillment of the Requirements for the Master Degree in Computing

Supervisor

Prof. Dr. Abdullah Hussein Ahmed Al-Hashedi

Professor of Information Systems
University of Science & Technology

August, 2026AD **Sana'a** **Safar, 1448AH**

Republic of Yemen
Ministry of Education and Scientific Research
University of Science and Technology
Deanship of Postgraduate Studies and Scientific Research

Improving Fraud Detection in Credit Cards using Ensemble Learning with a Boosting Approach and Deep Learning Models

Abstract

Advances in technology have led to the emergence of digital payment. Since credit card transactions are the most common payment method and advanced methods have emerged for fraudsters, detecting fraudulent transactions is crucial due to the loss it causes to both cardholders and financial institutions. Existing studies suffer from limited interpretability and insufficient focus on behavioral and temporal feature engineering. This thesis aims to build models using state-of-the-art Ensemble Learning (EL) and Deep Learning (DL) algorithms for detecting credit card fraudulent transactions to decrease the losses for both cardholders and financial institutions. To achieve the objectives, the study highlights the importance of feature engineering by creating new features that include behavioral and temporal features aimed at enhancing model performance. Nine models were developed and evaluated; five of them follow a boosting approach in EL, namely Gradient Boosting Machine (GBM), Histogram-based Gradient Boosting (HGBM), Light Gradient Boosting Machine (LightGBM), eXtreme Gradient Boosting (XGBoost), and Categorical Boosting (CatBoost). The other four models follow DL, namely Artificial Neural Network (ANN), Multilayer Perceptron (MLP), Long Short-Term Memory (LSTM), and Gated Recurrent Unit (GRU). The study used European credit card transactions dataset in 2023, comprising 568,630 transactions. The models were trained on the European dataset twice, once with only parameters adjustment and once with parameters adjustment and feature engineering. In addition, understanding the features that most influence a model's decision to classify a transaction as fraudulent is crucial in the financial sector to enhance the reliability of models. Therefore, Shapley Additive Explanations (SHAP) method was applied to the EL and DL models. The results demonstrate the efficiency of both EL and DL models in detecting fraudulent transactions in credit cards. LightGBM and XGBoost models achieved the highest accuracy of 0.9998 on the original dataset. While in the dataset with new features, the HGBM, LightGBM



and XGBoost models achieved the highest accuracy of 0.9997. In DL models, the highest accuracy was 0.9995 for the MLP, LSTM, and GRU models on the dataset with new features. The proposed models achieved the highest recall, ranging between 0.9989 and 1.0000, demonstrating their ability to detect fraudulent transactions. Meanwhile, precision ranged between 0.9838 and 0.9998, indicating that the models significantly reduce false alarms. Furthermore, F1 score values ranged between 0.9918 and 0.9998, indicating that the models achieved an excellent balance between recall and precision. The result highlights the ability of LSTM and GRU models to capture the temporal and behavioral sequences of transactions, where they are primarily designed to deal with time series. The findings highlight the reliability and robustness of the proposed models and their ability to accurately and efficiently detect fraudulent transactions. Furthermore, the proposed models may support financial institutions in improving credit card fraud detection decisions.

Candidate

Al-Maha Hashem Ali Al-Wadie

Supervisor

Prof. Dr. Abdullah H. A. Al-Hashedi

Professor of Information Systems
University of Science and Technology

August, 2026AD **Sana'a** **Safar, 1448AH**

الجمهورية اليمنية
وزارة التربية والتعليم والبحث العلمي
جامعة العلوم والتكنولوجيا
عمادة الدراسات العليا والبحث العلمي

تحسين كشف الاحتيال في بطاقات الائتمان باستخدام التعلم الجماعي مع نهج التعزيز ونماذج التعلم العميق

المُلخص

لقد أدى التقدم في التكنولوجيا إلى ظهور الدفع الرقمي. وبما أن معاملات بطاقات الائتمان هي طريقة الدفع الأكثر شيوعًا وظهرت طرق متقدمة للمحتالين، فإن اكتشاف المعاملات الاحتيالية أمر بالغ الأهمية بسبب الخسارة التي تسببها لكل من حاملي البطاقات والمؤسسات المالية. تعاني الدراسات الحالية من محدودية القدرة على التفسير وعدم التركيز الكافي على هندسة الميزات السلوكية والزمنية. تهدف هذه الرسالة إلى بناء نماذج باستخدام أحدث خوارزميات التعلم الجماعي (EL) والتعلم العميق (DL) للكشف عن المعاملات الاحتيالية لبطاقات الائتمان لتقليل الخسائر لكل من حاملي البطاقات والمؤسسات المالية. ولتحقيق الأهداف، تسلط الدراسة الضوء على أهمية هندسة الميزات من خلال إنشاء ميزات جديدة تتضمن ميزات سلوكية وزمنية تهدف إلى تحسين أداء النموذج. تم تطوير وتقييم تسعة نماذج؛ خمسة منها تتبع نهج التعزيز في EL، وهي آلة تعزيز التدرج (GBM)، تعزيز التدرج القائم على الهيستوجرام (HGBM)، آلة تعزيز التدرج الخفيف (LightGBM)، تعزيز التدرج المتطرف (XGBoost) والتعزيز التصنيفي (CatBoost). وتتبع النماذج الأربعة الأخرى التعلم العميق، وهي الشبكة العصبية الاصطناعية (ANN)، الإدراك متعددة الطبقات (MLP)، الذاكرة طويلة المدى (LSTM) ووحدة التكرار الموجهة (GRU). استخدمت الدراسة مجموعة بيانات معاملات بطاقات الائتمان الأوروبية في عام 2023، والتي تضم 568,630 معاملة. تم تدريب النماذج على مجموعة البيانات الأوروبية مرتين، مرة بتعديل المعلمات فقط ومرة بتعديل المعلمات وهندسة الميزات. بالإضافة إلى ذلك، يُعد فهم الميزات التي تؤثر بشكل كبير على قرار النموذج بتصنيف المعاملة على أنها احتيالية أمر بالغ الأهمية في القطاع المالي لتعزيز موثوقية النماذج. لذلك، تم تطبيق تقنية تفسيرات شابلي المضافة (SHAP) على نماذج EL وDL. أثبتت النتائج كفاءة كل من نماذج EL وDL في الكشف عن المعاملات الاحتيالية في بطاقات الائتمان. حيث حققت نماذج LightGBM وXGBoost أعلى دقة بلغت 0.9998 على مجموعة البيانات الأصلية، بينما في مجموعة البيانات ذات الميزات الجديدة حققت نماذج HGBM، LightGBM و XGBoost أعلى دقة بلغت 0.9997. في نماذج DL، كانت أعلى دقة هي 0.9995 لنماذج MLP، LSTM وGRU في مجموعة البيانات ذات الميزات الجديدة. حققت النماذج المقترحة أعلى معدل Recall يتراوح بين 0.9989 و1.0000، مما يدل على قدرتها على اكتشاف المعاملات الاحتيالية. وفي الوقت نفسه، تراوحت قيم Precision بين 0.9838 و0.9998، مما يشير إلى أن النماذج تقلل بشكل كبير من الإنذارات الكاذبة. وعلاوة على ذلك، تراوحت قيم مقياس F1 بين 0.9918 و0.9998، مما يشير إلى أن النماذج حققت توازناً ممتازاً بين Recall و Precision.

الجمهورية اليمنية

وزارة التربية والتعليم والبحث العلمي

جامعة العلوم والتكنولوجيا

عمادة الدراسات العليا والبحث العلمي

تسلط النتيجة الضوء على قدرة نماذج LSTM وGRU على إلتقاط التسلسلات الزمنية والسلوكية للمعاملات، حيث تم تصميمها في المقام الأول للتعامل مع السلاسل الزمنية. تسلط النتائج الضوء على موثوقية ومتانة النماذج المقترحة وقدرتها على اكتشاف المعاملات الاحتيالية بدقة وكفاءة. علاوة على ذلك، قد تدعم النماذج المقترحة المؤسسات المالية في تحسين قرارات الكشف عن الاحتيال ببطاقات الائتمان.

الطالبة

المها هاشم علي الوادعي

المشرف

أ.د. عبدالله حسين أحمد الحاشدي

أستاذ نظم المعلومات

جامعة العلوم والتكنولوجيا

أغسطس، 2026م **صنعاء** **صفر، 1448هـ**

الجمهورية اليمنية
وزارة التربية والتعليم والبحث العلمي
جامعة العلوم والتكنولوجيا
عمادة الدراسات العليا والبحث العلمي

تحسين كشف الاحتيال في بطاقات الائتمان باستخدام التعلم الجماعي مع نهج التعزيز ونماذج التعلم العميق

رسالة مقدمة من الطالبة

المها هاشم علي الوادعي

إلى

مجلس الدراسات العليا والبحث العلمي، وهي جزء من متطلبات الحصول على درجة الماجستير في الحوسبة

المشرف

أ.د. عبدالله حسين أحمد الحاشدي
أستاذ نظم المعلومات
جامعة العلوم والتكنولوجيا

أغسطس، 2026م **صنعاء** **صفر، 1448هـ**