Information Technology Innovations and Applied Communication

Vol. 4, No. 2, Summer, 2026, Serial No. 10,pp.61-81

Fraud Detection and Prediction in Credit Card Transactions Using Machine Learning Algorithms

Hosna Rajaei[1], Ali Bohlooli[*2]

Associate Professor, Faculty of Computer Engineering, University of Isfahan, Isfahan, Iran.

(**Received:** 21 April 2026, **Revised:** 09 June 2026, **Accepted:** 21 June 2026, **Published:** 23 August 2026)

Abstract

With the rapid growth of online financial transactions and the increasing sophistication of fraudulent behaviors, credit card fraud detection has become a critical operational challenge for banks and financial institutions. Conventional rule-based and statistical approaches often fail to capture complex, evolving patterns and typically degrade under severe class imbalance. This study presents a comprehensive machine-learning framework for detecting and predicting fraudulent credit card transactions under imbalanced data conditions. A well-known fraud detection dataset from Kaggle was preprocessed through data cleaning, normalization, and class balancing. Four baseline algorithms—Logistic Regression, Decision Tree, Random Forest, and Support Vector Machine—were trained and evaluated using accuracy, recall, F1-score, F2-score, ROC AUC, and PR AUC. To enhance fraud detection performance, complementary techniques were incorporated, including class weighting, F2-driven decision-threshold adjustment, and hyperparameter optimization. Experimental results indicate that Random Forest provides the most reliable overall performance, particularly on recall-oriented measures that are essential for reducing false negatives in fraud detection. For practical adoption, two application programming interfaces were implemented using Flask and FastAPI, and a graphical user interface was developed with Gradio to support real-time prediction. Beyond delivering an accurate detection model, this work provides an operational framework for deploying the proposed system within the banking infrastructure of Iran, contributing to improved transaction security and reduced financial losses.

Keywords: Financial fraud detection, credit card transactions, machine learning, imbalanced data, Logistic Regression, Decision Tree, Random Forest, Support Vector Machine

[*] Corresponding Author E-mail: bohlooli@eng.ui.ac.ir

مجله علمی - «نوآوری‌های فناوری اطلاعات و ارتباطات کاربردی»
سال چهارم، شماره 2، فصل تابستان 1404؛ ص 81-61.

شناسایی و پیش‌بینی تراکنش‌های جعلی در کارت‌های اعتباری با استفاده از الگوریتم‌های یادگیری ماشین

حسنا رجائی[1]، علی بهلولی*[2]

1- کارشناسی‌ارشد، 2- دانشیار، دانشکده مهندسی کامپیوتر، دانشگاه اصفهان، اصفهان، ایران.

(دریافت: 06 خرداد 1405 بازنگری: 25 تیر 1405 پذیرش: 18 مرداد 1405 انتشار: 01 شهریور 1405)

چکیده

با گسترش روزافزون تراکنش‌های مالی برخط و افزایش پیچیدگی الگوهای تقلب در سامانه‌های پرداخت الکترونیکی، تشخیص به‌موقع و دقیق تراکنش‌های جعلی به یکی از چالش‌های اساسی بانک‌ها و مؤسسات مالی تبدیل شده است. روش‌های سنتی مبتنی بر قوانین ثابت یا تحلیل‌های آماری، به‌ویژه در مواجهه با داده‌های نامتوازن و رفتارهای پویای متقلبان، کارایی محدودی دارند. اگرچه در سال‌های اخیر از الگوریتم‌های یادگیری ماشین برای حل این مسئله استفاده شده است، بسیاری از پژوهش‌های پیشین به‌صورت هم‌زمان به چالش‌هایی نظیر عدم توازن کلاس‌ها، اهمیت خطاهای نامتقارن و انتخاب معیارهای ارزیابی متناسب با ماهیت مسئله توجه کافی نداشته‌اند .در این پژوهش، باهدف رفع این کاستی‌ها، یک چارچوب جامع برای تشخیص و پیش‌بینی تقلب در تراکنش‌های کارت اعتباری ارائه شده است. بدین منظور، مجموعه‌داده معتبر تشخیص تقلب کارت اعتباری پس از مراحل پاک‌سازی، نرمال‌سازی و متوازن‌سازی داده‌ها آماده‌سازی شد. سپس عملکرد چهار الگوریتم متداول یادگیری ماشین شامل رگرسیون لجستیک، درخت تصمیم، جنگل تصادفی و ماشین بردار پشتیبان با استفاده از معیارهایی نظیر دقت، بازخوانی، شاخص‌های F1 وF2 ، سطح زیر منحنی ROC و سطح زیر منحنی دقت - بازخوانی مورد ارزیابی قرار گرفت. همچنین، به‌منظور بهبود عملکرد مدل‌ها، از تکنیک‌های تکمیلی نظیر وزن‌دهی کلاس‌ها، تنظیم آستانه تصمیم‌گیری مبتنی بر امتیاز F2 و بهینه‌سازی ابرپارامترها استفاده شد. نتایج تجربی نشان می‌دهد که الگوریتم جنگل تصادفی، به‌ویژه در معیارهای مبتنی بر بازخوانی، عملکرد باثبات‌تری نسبت به سایر روش‌ها ارائه می‌دهد. در ادامه، جهت تسهیل به‌کارگیری عملی مدل، دو رابط برنامه‌نویسی کاربردی مبتنی بر فریم‌ورک‌های فلاسک و فستاِی‌پی‌آی و یک رابط کاربری گرافیکی با ابزار گرادیو توسعه‌یافته است .این پژوهش علاوه بر معرفی یک مدل دقیق، یک طرح عملیاتی برای استقرار سامانه در زیرساخت بانکی ایران ارائه می‌کند که می‌تواند در کاهش خسارات ناشی از تراکنش‌های جعلی و افزایش امنیت نظام پرداخت الکترونیکی مؤثر باشد.

کلیدواژه‌ها: تشخیص تقلب مالی، تراکنش‌های کارت اعتباری، یادگیری ماشین، داده‌های نامتوازن، رگرسیون لجستیک، درخت تصمیم، جنگل تصادفی، ماشین بردار پشتیبان.

* Corresponding Author E-mail: bohlooli@eng.ui.ac.ir

.

1. مقدمه

استفاده گسترده از سامانه‌های پرداخت الکترونیکی و کارت‌های اعتباری باعث شده امنیت تراکنش‌های مالی به چالشی جدی بدیل شود. خسارت‌های ناشی از تقلب، اعتماد عمومی به‌نظام بانکی را تهدید می‌کند و روش‌های سنتی دیگر پاسخگوی پیچیدگی تقلب‌های جدید نیستند.

یادگیری ماشین باقابلیت شناسایی الگوهای پنهان و غیرعادی در داده‌های تراکنش، رویکردی کارآمد برای شناسایی خودکار تقلب‌ها فراهم می‌کند. پروژه حاضر باهدف ارائه چارچوبی علمی و عملی برای کشف تقلب در کارت‌های اعتباری طراحی شده است.

هدف اصلی، توسعه مدل‌های یادگیری ماشین برای شناسایی و پیش‌بینی تراکنش‌های جعلی است. چهار الگوریتم رگرسیون لجستیک، درخت تصمیم، جنگل تصادفی و ماشین بردار پشتیبان[1] آموزش‌داده‌شده و بر اساس معیارهای علمی ارزیابی شدند. همچنین برای بهبود عملکرد، روش‌هایی مانند روش نمونه‌سازی افزایشی[2]، وزن‌دهی کلاس‌ها، تنظیم آستانه و کالیبراسیون احتمال به کار گرفته شد.

مهم‌ترین کاربرد این مدل‌ها، ارتقای امنیت سامانه‌های بانکی و کاهش خسارات مالی ناشی از تقلب است. علاوه بر بانک‌ها، شرکت‌های پرداخت الکترونیک، تجارت آنلاین و حتی صنعت بیمه می‌توانند از این سامانه‌ها بهره‌مند شوند. توسعه رابط برنامه‌نویسی کاربردی[3] و رابط کاربری گرافیکی موجب شده پروژه قابلیت استقرار عملی و استفاده توسط کاربران غیرمتخصص را هم داشته باشد.

نوآوری‌های این پژوهش شامل سه محور اصلی است :

1) طراحی و مقایسه جامع چندین الگوریتم یادگیری ماشین بر پایه معیارهای پیشرفته ارزیابی؛
2) به‌کارگیری روش‌های بهبود عملکرد مانند وزن‌دهی کلاس‌ها، نمونه‌سازی افزایشی و تنظیم آستانه مبتنی بر هزینه
3) توسعه رابط‌های نرم‌افزاری و رابط کاربری گرافیکی برای استقرار و بهره‌برداری عملی از مدل در محیط بانکی واقعی.

در ادامه، ساختار مقاله به‌صورت زیر تنظیم شده است: در بخش دوم مفاهیم پایه، مرور ادبیات و روش پیشنهادی معرفی شده‌اند. بخش سوم شامل نتایج به‌دست‌آمده، معیارهای ارزیابی و تحلیل عملکرد مدل‌ها است. در بخش چهار، نتیجه‌گیری ارائه شده و به کارهای آتی اشاره می‌شود.

[1] Support Vector Machine (SVM)
[2] Synthetic Minority Oversampling Technique (SMOTE)
[3] Application Programming Interface (API)

2-1. مفاهیم پایه

2-1-1. داده‌کاوی و یادگیری ماشین

داده‌کاوی به معنای استخراج دانش از داده‌های خام و کشف الگوهای پنهان میان حجم انبوه داده‌هاست. این دانش می‌تواند به تصمیم‌گیری هوشمندانه در کسب‌وکار و صنایع مختلف کمک کند.

یادگیری ماشین یکی از مهم‌ترین شاخه‌های داده‌کاوی است که به رایانه‌ها امکان می‌دهد با استفاده از الگوریتم‌ها و بدون برنامه‌نویسی صریح، الگوها و روابط میان داده‌ها را شناسایی کرده و پیش‌بینی‌های دقیق‌تری ارائه دهند. یادگیری ماشین به طور گسترده در مسائل تشخیص تقلب، تحلیل ریسک مالی، پیش‌بینی بازار و سایر حوزه‌های مالی استفاده می‌شود. در پروژه حاضر، یادگیری ماشین نه‌تنها برای شناسایی الگوهای غیرعادی، بلکه برای بهینه‌سازی مدل بر اساس معیارهایی مانند سطح زیر منحنی ROC [4] و سطح زیر منحنی دقت - بازخوانی[5] و تنظیم آستانه‌ها برای کاهش خطاهای پرهزینه (مانند خطای منفی کاذب[6]) به کار گرفته شده است.

2-1-2. انواع تقلب در بانکداری و تراکنش‌ها

تقلب در بانکداری معمولاً به مجموعه‌ای از رفتارهای غیرمجاز و مخرب اشاره دارد که باهدف کسب منفعت مالی و به ضرر مشتریان یا مؤسسات انجام می‌شود. انواع تقلب‌ها عبارت‌اند از:

- تقلب در تراکنش کارت اعتباری: خرید یا برداشت غیرمجاز با استفاده از اطلاعات کارت سرقت‌شده یا فیشینگ؛
- تقلب داخلی: دست‌کاری حساب‌ها توسط کارکنان؛
- تقلب در انتقال وجه و حواله: جابه‌جایی غیرقانونی وجوه؛
- کلاهبرداری اینترنتی: سوءاستفاده از درگاه‌های آنلاین، فیشینگ و... .

تشخیص به‌موقع و دقیق این تقلب‌ها به‌ویژه در حجم بالای داده‌های بانکی بسیار دشوار است و استفاده از الگوریتم‌های خودکار را ضروری می‌سازد.

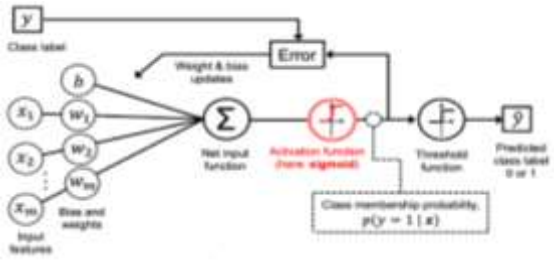
2-1-3. الگوریتم‌های یادگیری ماشین مورداستفاده

در این پژوهش چهار الگوریتم پرکاربرد پیاده‌سازی و ارزیابی شدند:

رگرسیون لجستیک[7] یکی از ساده‌ترین و پرکاربردترین الگوریتم‌های طبقه‌بندی[8] در یادگیری ماشین است که به‌ویژه

[4] Receiver Operating Characteristic – Area Under Curve (ROC AUC)
[5] Precision–Recall Area Under Curve (PR AUC)
[6] False Negative (FN)
[7] Logistic Regression
[8] Classification

برای مسائل دسته‌بندی دودویی (مانند تقلب یا عدم تقلب) مناسب است. این الگوریتم بر مبنای یک مدل خطی عمل کرده و هدف آن تخمین احتمال تعلق یک نمونه به هر یک از دو کلاس است. همان‌طور که در شکل ۱ نشان‌داده‌شده است، برخلاف رگرسیون خطی که مقدار خروجی را به طور مستقیم پیش‌بینی می‌کند، رگرسیون لجستیک با استفاده از تابع سیگموئید[1]، خروجی را به بازه‌ای بین ۰ و ۱ نگاشت می‌نماید. براین‌اساس، اگر مقدار پیش‌بینی‌شده بالاتر از یک آستانه مشخص (مانند ۰.۵) باشد، داده به‌عنوان کلاس مثبت (تقلب) و در غیر این صورت به‌عنوان کلاس منفی (غیر متقلب) طبقه‌بندی می‌شود.

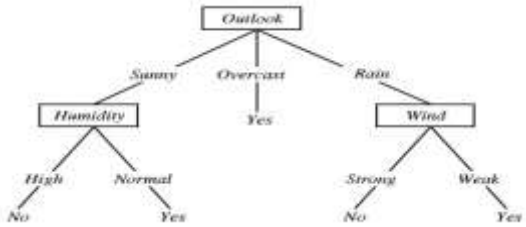


شکل (1). معماری و سازوکار رگرسیون لجستیک برای طبقه‌بندی دودویی

مزیت اصلی رگرسیون لجستیک، سادگی، سرعت اجرا و تفسیرپذیری بالای آن است. عامل‌های مدل به‌راحتی قابل‌فهم هستند و می‌توان تحلیل کرد که هر ویژگی[2] تا چه اندازه روی پیش‌بینی مدل تأثیرگذار است. بااین‌حال، رگرسیون لجستیک محدودیت‌هایی دارد؛ از جمله اینکه فرض می‌کند رابطه بین ویژگی‌ها و خروجی خطی است و نسبت به داده‌هایی که ویژگی‌های آن‌ها با هم همبستگی بالایی دارند، حساس است. به همین دلیل در مسائل پیچیده با الگوهای غیرخطی، ممکن است کارایی این مدل کاهش یابد. در این پروژه، نسخه وزن‌دهی شده بر اساس کلاس‌های[3] این مدل برای مقابله با عدم توازن داده‌ها به کار گرفته شد و عملکرد آن با نسخه پایه مقایسه گردید.

درخت تصمیم[4]: یک الگوریتم طبقه‌بندی غیرخطی است که داده‌ها را به‌صورت سلسله‌مراتبی بر اساس ویژگی‌هایشان تقسیم می‌کند. همان‌طور که در شکل 2 نمایش‌داده‌شده است، این مدل از یک ساختار گرافی شبیه درخت استفاده می‌کند که در آن هر گره[5] نمایانگر یک شرط یا پرسش درباره یک ویژگی داده، و هر شاخه[6] نمایانگر نتیجه آن شرط است. فرایند تقسیم داده‌ها تا جایی ادامه پیدا می‌کند که گره‌های[7] پایانی صرفاً شامل داده‌های متعلق به یک کلاس شوند یا شرایط توقف مدل برقرار شود.

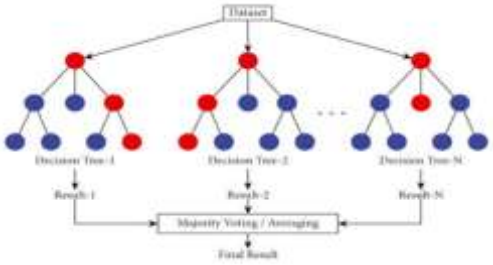
[1] Sigmoid Function
[2] Feature
[3] Class-Weighted Version
[4] Decision Tree
[5] Node
[6] Branch
[7] Leaf (Leaves)



شکل (2). ساختار درخت تصمیم و فرایند طبقه‌بندی سلسله‌مراتبی

مزیت کلیدی درخت تصمیم این است که به‌صورت شفاف و قابل‌تفسیر تصمیم‌گیری می‌کند و حتی می‌توان مسیر رسیدن به یک پیش‌بینی خاص را به‌صورت نموداری نمایش داد. درخت تصمیم قادر است با داده‌های دارای روابط پیچیده، مقادیر گمشده و حتی داده‌های ترکیبی (عددی و متنی) به‌خوبی کار کند. بااین‌حال، درخت تصمیم اگر به‌درستی تنظیم نشود (مثلاً عمیق باشد)، مستعد بیش برازش[8] است؛ یعنی مدل فقط روی داده‌های آموزش عملکرد خوبی دارد ولی روی داده‌های جدید دقت کمتری پیدا می‌کند. روش‌هایی مانند هرس‌کردن برای کاهش این مشکل به کار می‌رود. این مدل به‌عنوان یک خط پایه ساده و قابل‌تفسیر در پروژه استفاده شد و با مدل‌های پیچیده‌تر مقایسه گردید.

جنگل تصادفی[9]: جنگل تصادفی، یک روش قدرتمند و مبتنی بر یادگیری جمعی[10] است که با ترکیب چندین درخت تصمیم، عملکرد بهتری نسبت به یک درخت تصمیم منفرد ارائه می‌دهد. مطابق شکل 3، ایده اصلی جنگل تصادفی این است که به‌جای آموزش یک درخت، مجموعه‌ای از درخت‌های تصمیم را با داده‌های تصادفی و ویژگی‌های تصادفی آموزش می‌دهد و در نهایت با رأی‌گیری بین خروجی این درخت‌ها، تصمیم نهایی را اتخاذ می‌کند. این مدل استحکام بالاتری نسبت به نویز و داده‌های پرت دارد و خطر بیش برازش را به میزان زیادی کاهش می‌دهد. جنگل تصادفی به‌ویژه برای داده‌های با ابعاد زیاد و ویژگی‌های متنوع مناسب است و می‌تواند روابط غیرخطی پیچیده را نیز به‌خوبی مدل کند.

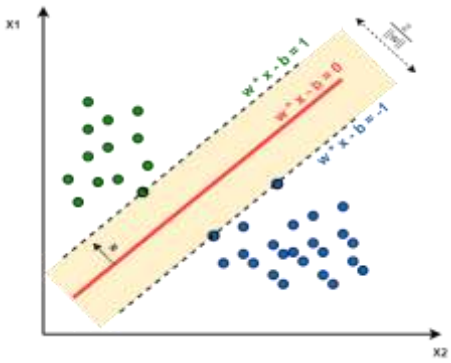


شکل (3). معماری جنگل تصادفی و فرایند یادگیری جمعی

[8] Overfitting
[9] Random Forest
[10] Ensemble Learning

یکی از مزیت‌های مهم این الگوریتم، این است که می‌تواند اهمیت نسبی هر ویژگی را به طور عددی گزارش کند و به تحلیل‌گر کمک کند تا بداند کدام عوامل بیشتر روی پیش‌بینی مدل تأثیرگذارند. درعین‌حال، جنگل تصادفی به دلیل داشتن چندین درخت، نسبت به مدل‌های ساده‌تر محاسباتی‌تر است و ممکن است زمان پیش‌بینی یا آموزش آن در داده‌های بسیار بزرگ طولانی‌تر باشد. در این پروژه علاوه بر نسخه پایه، نسخه‌های وزن‌دهی شده بر اساس کلاس‌ها[1] و نسخه آموزش با نمونه‌سازی افزایشی[2] این مدل بررسی شد و یک تیونینگ سریع ابرپارامترها با جست‌وجوی تصادفیِ فضای ابرپارامترها همراه با ارزیابی متقاطع[3] نیز برای بهبود عملکرد انجام گرفت.

ماشین بردار پشتیبان: یکی از پیشرفته‌ترین و کارآمدترین الگوریتم‌های طبقه‌بندی در یادگیری ماشین است، ساختار کلی این الگوریتم در شکل 4 نمایش‌داده‌شده است. ماشین بردار پشتیبان تلاش می‌کند یک «مرز تصمیم‌گیری[4]» به نام ابر صفحه بیابد که داده‌های دو کلاس را با بیشترین فاصله ممکن از هم جدا کند. این مرز به‌گونه‌ای تعیین می‌شود که داده‌های هر کلاس تاحدامکان در یک سمت ابر صفحه قرار بگیرند و داده‌هایی که نزدیک به مرز هستند، به‌عنوان «بردارهای پشتیبان» شناخته می‌شوند و نقش کلیدی در تعیین مرز ایفا می‌کنند.



شکل (4). نمایش بصری مرز بهینه‌سازی و بردارهای پشتیبان درSVM

یکی از مزیت‌های اساسی ماشین بردار پشتیبان این است که با استفاده از توابع کرنل[5] ، قابلیت مدل‌سازی روابط غیرخطی میان داده‌ها را نیز دارد و می‌تواند داده‌هایی که با روش‌های خطی قابل‌جداسازی نیستند را نیز به‌خوبی طبقه‌بندی کند. ماشین بردار پشتیبان نسبت به داده‌های با ابعاد زیاد مقاوم است و معمولاً در مسائل با حجم داده نه‌چندان زیاد و تعداد ویژگی‌های بالا، دقت بسیار بالایی ارائه می‌دهد. بااین‌وجود، آموزش مدل روی داده‌های بزرگ و نامتوازن (مانند بسیاری از داده‌های واقعی مالی) می‌تواند از لحاظ محاسباتی زمان‌بر و نیازمند تنظیمات دقیق (تنظیم عامل‌های کرنل، جریمه و...) باشد. انتخاب صحیح کرنل و تنظیم مناسب عامل‌ها در موفقیت این مدل بسیار مؤثر است. در این پروژه، مدل ماشین بردار پشتیبان با کرنل پایه شعاعی[6] و قابلیت محاسبه احتمال پیاده‌سازی شد و سپس با استفاده از روش مقیاس‌گذاری پلت[7] کالیبره گردید تا کیفیت پیش‌بینی‌های احتمالی بهبود یابد.

2-2. مروری بر کارهای گذشته

در این بخش مروری بر پیشینه و تاریخچه‌ی موضوع پژوهش ارائه می‌شود؛ ابتدا چشم‌اندازی کلی از نقش روش‌های یادگیری ماشین و هوش مصنوعی در تشخیص و پیشگیری تقلب ارائه شده، سپس مطالعات کلیدی به‌صورت متوالی معرفی، روش‌های به‌کاررفته، نتایج اصلی و محدودیت‌های هر پژوهش بیان می‌گردد.

شیردل و خداپرست[1] در پژوهشی با عنوان «شناسایی تقلب در پرداخت‌های الکترونیکی با استفاده از الگوریتم‌های هوش مصنوعی و یادگیری ماشین» چارچوبی مبتنی بر الگوریتم‌های یادگیری ماشین برای تشخیص تراکنش‌های مشکوک ارائه کردند. در این مطالعه، از الگوریتم جنگل تصادفی به‌عنوان مدل اصلی طبقه‌بندی استفاده شد و عملکرد آن با معیارهایی مانند دقت، مثبت کاذب و امتیاز F1ارزیابی گردید. نتایج نشان داد که مدل پیشنهادی توانسته است نرخ شناسایی تراکنش‌های متقلبانه را به طور معناداری افزایش دهد. پژوهشگران تأکید کرده‌اند که الگوریتم‌های یادگیری ماشین می‌توانند ابزاری کارآمد در کاهش تقلب مالی در سامانه‌های پرداخت الکترونیکی باشند، هرچند استفاده از داده‌های واقعی بانکی و آزمون در محیط‌های عملی برای تعمیم‌پذیری نتایج ضروری است.

محمد شریفی و همکاران [2] در مقاله‌ای با عنوان «مروری بر استفاده از یادگیری ماشین و یادگیری عمیق در شناسایی تقلب در سامانه‌های مالی» به بررسی جامع پژوهش‌های انجام‌شده در زمینه تشخیص تقلب باتکیه‌بر الگوریتم‌های یادگیری ماشین پرداختند. در این مرور، روش‌هایی چون درخت تصمیم، جنگل تصادفی، ماشین بردار پشتیبان و شبکه‌های عصبی مصنوعی به‌عنوان پرکاربردترین الگوریتم‌ها معرفی شدند. نتایج نشان می‌دهد که انتخاب داده‌های ورودی مناسب، پیش‌پردازش دقیق و گزینش صحیح معیارهای ارزیابی نقش اساسی در بهبود عملکرد مدل‌ها دارد. نویسندگان همچنین چالش‌هایی مانند عدم

[1] Class-Weighted Version
[2] SMOTE-Train
[3] RandomizedSearchCV
[4] Decision Boundary (Hyperplane)
[5] Kernel Functions
[6] Radial Basis Function (RBF) Kernel
[7] Platt Scaling

توازن داده‌ها، پیچیدگی محاسباتی مدل‌ها و نیاز به تبیین‌پذیری خروجی را از مهم‌ترین محدودیت‌های موجود دانسته و پیشنهاد کرده‌اند که استفاده از روش‌های ترکیبی و مدل‌های یادگیری عمیق قابل‌تفسیر می‌تواند کارایی سامانه‌های ضد تقلب را افزایش دهد.

تقوی منش[3] در مقاله‌ای با عنوان «تشخیص نفوذ تزریق کد در سامانه‌های پایگاه‌داده مبتنی بر استخراج ویژگی‌های مؤثر»، مدلی هوشمند برای شناسایی حملات تزریق کد در پایگاه‌داده ارائه کرده است. در این پژوهش، از الگوریتم‌های یادگیری ماشین شامل درخت تصمیم و متغیرهای وابسته برای تحلیل سه مجموعه‌داده مختلف استفاده شده و فرایند انتخاب ویژگی‌های مؤثر به‌صورت دستی و خودکار مورد ارزیابی قرار گرفته است. نتایج نشان می‌دهد که استخراج هدفمند ویژگی‌ها باتکیه‌بر دانش تخصصی و داده‌های بهینه‌شده موجب افزایش دقت مدل تا ۹۹،۵۷ درصد شده است. پژوهش حاضر نشان می‌دهد که ترکیب یادگیری ماشین با انتخاب ویژگی می‌تواند در شناسایی الگوهای نفوذ، ناهنجاری و حتی تراکنش‌های جعلی در سامانه‌های بانکی نیز به کار گرفته شود.

مهدی نورمحمدی و عدالت پناه[4] مدلی جدید مبتنی بر درخت تصمیم طبقه‌بندی و رگرسیون[1] در چارچوب نوتروسفیک بازه‌ای[2] برای تشخیص تقلب در بانکداری الکترونیک ارائه کردند و با استفاده از مجموعه‌داده‌های تراکنش‌های آنلاین (مورداستفاده در پیشینه) نشان دادند که ترکیب منطق نوتروسفیک با درخت تصمیم می‌تواند مزایای نظری قابل‌توجهی فراهم آورد؛ بااین‌وجود نویسندگان نیاز به آزمون‌های مقایسه‌ای گسترده‌تر و ارزیابی عملکرد در شرایط واقعی را مطرح کرده‌اند.

کیومرث پور قدیمی و همکاران[5] الگوی توسعه‌یافته‌ای از مدل بنیش را با تأکید بر ویژگی‌های خاص شرکت و با استفاده از شبکه عصبی، ماشین بردار پشتیبان و جنگل تصادفی پیشنهاد دادند؛ نتایج گزارش‌شده نشان‌دهنده برتری جنگل تصادفی بادقت حدود 99٪ نسبت به سایر مدل‌ها (حدود 94٪) است و اهمیت احتساب ویژگی‌های شرکت محور در بهبود پیش‌بینی تقلب در صورت‌های مالی تأکید شد.

قمری مقدم و نخعی[6] راهکاری ترکیبی برای پیش‌بینی شرکت‌های متقلب مالیاتی ارائه کردند که در آن درختِ تصمیمِ بهبودیافته (بر پایه الگوریتم شاخص آنتروپی)، به همراه شبکه بیزین و ماشینِ بردارِ پشتیبان به‌صورت وزن‌دهی شده تجمیع می‌شود؛ انتخابِ ویژگی نیز با ترکیب «مجموعه راف» و «فرایند تحلیل سلسله‌مراتبی» انجام‌گرفته تا ویژگی‌های مؤثر حفظ و سربار محاسباتی کاهش یابد. آنان با داده‌های سه‌سالهٔ ۶۰ شرکت، دقت ۸۰ درصد، سربار زمانی متناسب با حاصل‌ضرب m و n و سربار حافظه متناسب با n گزارش کردند و نشان دادند روش ترکیبی پیشنهادی نسبت به درخت تصمیم و شبکه بیزین به ترتیب حدود ۶۶.۶ و ۲۷.۸ درصد بهبود دارد؛ درعین‌حال به محدودیت اندازه داده و لزوم آزمون روش در سناریوهای واقعی‌تر اشاره شده است.

حسن ملکی کاکلر و همکاران[7] کارایی مدل‌های آماری و الگوهای یادگیری ماشین را در پیش‌بینی گزارشگری مالی متقلبانه مقایسه کردند و دریافتند که روش‌های یادگیری ماشین و به‌ویژه ترکیب الگوریتم‌ها در اغلب موارد کارایی بیشتری نسبت به مدل‌های آماری سنتی دارند؛ بهترین ترکیب‌ها دقت‌هایی بالای 91–92% نشان دادند، اگرچه نیاز به تعمیم‌پذیری نتایج و بررسی پایداری مدل‌ها در دوره‌های زمانی مختلف ذکر شده است.

حبیب اعیانی[8] مدلی ترکیبی برای کشف تقلب در داده‌های بانکی پیشنهاد داد که شامل انتخاب ویژگی و استفاده از طبقه‌بندهای یادگیری ماشینی است؛ نتایج این پژوهش نشان می‌دهد که جنگل تصادفی نسبت به سایر روش‌های مقایسه شده کارایی بالاتری دارد، اما نیاز به اعتبارسنجی در مجموعه‌داده‌های داخلی و خارجی و گزارش جزئیات پیش‌پردازش مشهود است.

مریم دهقانی و همکاران[9] الگوریتم‌های یادگیری ماشین را برای پیش‌بینی سری‌های زمانی در بازارهای مالی بررسی کردند و یافته‌هایشان نشان می‌دهد انتخاب ویژگی‌های فنی مناسب می‌تواند خطای پیش‌بینی را کاهش دهد و در ترکیب با ماشین بردار پشتیبان و شبکه‌های پرسپترون چندلایه[3] نتایج پیش‌بینی دقیق‌تری حاصل گردد؛ بااین‌حال تعمیم‌پذیری بین بازارها و ثبات عامل‌ها موضوعاتی است که نیاز به پژوهش بیشتر دارد.

امیرحسین صدیقی و همکاران[10] رویکردی مبتنی بر یادگیری عمیق برای کشف کلاهبرداری در سرویس‌های پرداخت مالی ارائه کردند و در ارزیابی خود روی مجموعه‌داده معیار، صحت 96٪ و دقت 98٪ گزارش نمودند؛ نویسندگان درعین‌حال به چالش‌های عملیاتی مانند تأخیر در پردازش بلادرنگ و هزینه‌های محاسباتی اشاره کرده و الزام به بررسی هزینه - فایده در محیط‌های عملی را یادآور شدند.

در پژوهش‌های خارج از کشور نیز رشد چشمگیری رخداده است:

چن و همکاران[11] در یک مطالعه مروری جامع با موضوع «نوآوری‌ها، چالش‌ها و کاربردهای یادگیری عمیق در کشف تقلب مالی» روندهای اصلی این حوزه را دسته‌بندی کرده‌اند. آن‌ها ضمن ارائه چارچوبی مفهومی برای به‌کارگیری یادگیری عمیق در

[1] CART — Classification and Regression Tree
[2] Interval Neutrosophic Logic
[3] Multilayer Perceptron (MLP)

سامانه‌های کشف تقلب، بر انتخاب معماری مناسب شبکه‌های عصبی، بهینه‌سازی مدل، مقابله با نامتوازنی داده‌ها، و تبیین‌پذیری تأکید می‌کنند. جمع‌بندی مقاله نشان می‌دهد روش‌های مبتنی بر شبکه‌های عصبی پیچشی، بازگشتی و گرافی در ارتقای دقت و بازخوانی مؤثرند، اما چالش‌هایی مانند هزینه محاسباتی، نیاز به داده‌های برچسب خورده و نبود استاندارد ارزیابی همچنان باقی است. نویسندگان توصیه می‌کنند در محیط‌های مالی، استفاده از امتیازهای F1 و F2، سطح زیر منحنی دقت - بازخوانی و تنظیم آستانه در اولویت ارزیابی قرار گیرد.

ژائو و همکاران[12] در مطالعه‌ای با عنوان «شبکه دروازه‌ای سلسله‌مراتبی مبتنی بر رفتار تراکنش برای تشخیص تقلب کارت اعتباری» رویکردی نوین ارائه کرده‌اند که رفتارهای تراکنش کاربران را از منظر توالی زمانی و ساختار رابطه‌ای تحلیل می‌کند. در این پژوهش، ابتدا ماژولی استخراج ویژگی طراحی شده که ویژگی‌های کلیدی از تراکنش‌های اولیه را بیرون می‌کشد و سپس ماژولی گرایش‌مند برای تحلیل همبستگی میان رفتار تاریخی و جاری کاربران تدوین شده است. شبکه سلسله‌مراتبی تعریف شده، ابتدا از سطح ویژگی‌های منفرد به سطح تعامل ویژگی‌ها می‌پردازد و سپس نمای تراکنش نهایی را برای طبقه‌بندی ایجاد می‌کند. بر پایه مجموعه‌داده‌های واقعی، این روش میانگین امتیاز اف ۱ را بین ٪۱.۴۲ تا ٪۶.۵۳ و میانگین AUCرا بین ٪۰.۶۳ تا ٪۲.۷۸ نسبت به بهترین روش‌های پیشین بهبود داده است.

احمد و همکاران[13] رویکردی برای کشف تقلب در تراکنش‌های کارت اعتباری ارائه کرده‌اند که بر پایه‌ی یک طبقه‌بند تجمیعی و نمونه‌برداری ترکیبی بنا شده است. در این پژوهش، برای رفع نامتوازنی کلاس‌ها از نمونه‌برداری افزایشی مصنوعی همراه با ویرایش نزدیک‌ترین همسایه استفاده شده تا داده‌ی آموزشی هم از نظر کمّی غنی شود و هم نمونه‌های مرزیِ ناسالم پاک‌سازی گردد. سپس چند مدل یادگیری به‌صورت همکارانه ترکیب شده‌اند تا هم‌زمان بازخوانی افزایش یابد و خطاهای نوع اول کاهش پیدا کند. نتایج گزارش‌شده نشان می‌دهد این راهبرد ترکیبی در مقایسه با روش‌های پایه، بهبود معناداری در سنجه‌هایی مانند امتیاز اف ۱ و سطح زیر منحنی دقت - بازخوانی ایجاد می‌کند؛ بااین‌حال نویسندگان بر ضرورت ارزیابی بر مجموعه‌داده‌های متنوع‌تر و بررسی هزینه‌ی محاسباتی در مقیاس عملیاتی تأکید کرده‌اند.

گوپتا و همکاران[14] در پژوهشی با عنوان «چارچوب تقویت‌شده برای تشخیص تقلب کارت اعتباری با استفاده از انتخاب ویژگی مقاوم و مدل تجمیعی پشته‌ای»، روشی چندمرحله‌ای برای بهبود عملکرد سامانه‌های کشف تقلب ارائه کردند. در این رویکرد، ابتدا با بهره‌گیری از تکنیک‌های انتخاب ویژگی مقاوم، ویژگی‌های نامرتبط و نویزی حذف می‌شوند تا داده‌ی ورودی برای مدل‌ها بهینه گردد. سپس از یک مدل تجمیعی پشته‌ای استفاده شده است که ترکیبی از چند طبقه‌بند پایه (مانند جنگل تصادفی، درخت تصمیم و رگرسیون لجستیک) را با یک فرا طبقه‌بند نهایی ادغام می‌کند. نتایج آزمایش‌ها بر مجموعه‌داده‌های واقعی نشان می‌دهد که این چارچوب نسبت به مدل‌های منفرد، بهبود قابل‌توجهی در دقت، بازخوانی و امتیاز اف ۱ به دست آورده و توانسته است نرخ مثبت‌های کاذب را کاهش دهد. بااین‌حال، نویسندگان بر نیاز به کاهش هزینه‌ی محاسباتی و آزمون در داده‌های جریانی واقعی تأکید کرده‌اند.

سورندرانادها ردی بیراپو ردی و همکاران[15] یک پلتفرم کلان‌داده برای خرده‌فروشان آنلاین معرفی کردند که با بهره‌گیری از الگوریتم‌های یادگیری ماشینی و هوش مصنوعی به تحلیل الگوها و ناهنجاری‌ها می‌پردازد تا شناسایی و کاهش ریسک کلاهبرداری در تجارت الکترونیک تسهیل شود. این پژوهش یک چارچوب فنی شامل جمع‌آوری داده‌های تراکنشی، پیش‌پردازش برای حذف نویز و مهندسی ویژگی، و سپس اعمال چندین الگوریتم طبقه‌بندی برای تشخیص ناهنجاری‌ها ارائه می‌دهد. در گزارش نتایج، نویسندگان نشان می‌دهند که تلفیق تحلیل کلان‌داده با مدل‌های یادگیری ماشینی موجب افزایش حساسیت تشخیص و کاهش نرخ مثبت کاذب در محیط‌های تجاری واقعی می‌شود؛ بااین‌حال محدودیت‌هایی مانند نیاز به زیرساخت محاسباتی مقیاس‌پذیر و وابستگی به کیفیت برچسب‌گذاری داده‌ها برای آموزش مدل‌ها موردتأکید قرار گرفته است.

اولوابوسایو آدیجات بلو و همکاران[16] در بررسی جامعی تکنیک‌های هوش مصنوعی - از جمله یادگیری ماشینی، یادگیری عمیق و پردازش زبان طبیعی - را در زمینه پیشگیری از تقلب تحلیل کردند. این مطالعه، مزایا و معایب خانواده‌های مختلف روش‌ها را بازنگری کرده و به‌ویژه پتانسیل یادگیری عمیق را در تحلیل داده‌های بدون ساختار (مانند متن و تصویر) برجسته می‌سازد. درعین‌حال چالش‌هایی از قبیل نیاز به مجموعه‌داده‌های بزرگ برچسب خورده، پیچیدگی محاسباتی و مشکل تبیین‌پذیری[1] مدل‌های عمیق مورد بحث قرار گرفته‌اند؛ پژوهش پیشنهاد می‌کند برای کاربردهای حساس به خطای مثبت کاذب، ترکیب روش‌های قابل‌تبیین با مدل‌های عمیق مورداستفاده قرار گیرد.

جورجیوس کاریزانوس و همکاران[17] چارچوبی فازی و آنی

[1] Interpretability

(آنلاین) برای تشخیص تقلب در تراکنش‌های کارت اعتباری پیشنهاد کردند که به‌منظور عملیاتی‌سازی بلادرنگ طراحی شده است. در این کار، یک مدل رگرسیون لجستیک فازی به همراه مکانیزم‌های مقابله با عدم تعادل طبقاتی و جداسازی ویژگی‌ها به کار گرفته شد؛ نتایج آزمایشی نشان می‌دهد که چارچوب پیشنهادی حتی در نمونه‌های کوچک، حساسیت و ویژگی بالاتر از 0.90 و مقدار ضریب همبستگی مَتیو[1] بیش از 0.80 را کسب می‌کند. بااین‌حال نویسندگان خود اشاره می‌کنند که بررسی عملکرد در مجموعه‌داده‌های متنوع‌تر و تحلیل هزینه - زمان[2] برای کاربرد در محیط‌های عملی موردنیاز است.

شانجیتا آکتر پروم و همکاران[18] در یک مرور سامان‌مند به بررسی مطالعات طراحی‌شده برای تشخیص فریب با استفاده از روش‌های یادگیری ماشین و یادگیری عمیق پرداختند. این مرور، تکنیک‌های مختلف (از الگوریتم‌های سنتی تا شبکه‌های عصبی عمیق)، معیارهای ارزیابی به‌کاررفته، و چالش‌های روش‌شناختی مانند کمبود داده‌های برچسب خورده و ناسازگاری معیارها را دسته‌بندی کرد. نتیجه‌گیری این مقاله تأکید بر ضرورت توسعه سامانه‌های غیر مزاحم، مقیاس‌پذیر و باقابلیت تعمیم‌پذیری بالاست و پیشنهادهایی برای جهت‌گیری تحقیقاتی آینده (مانند ترکیب چند منبع داده و ارزیابی در میدان) ارائه می‌دهد.

اسماً شریف و همکاران[19] یک معماری رمزگذار - رمزگشا[3] مبتنی بر شبکه‌های عصبی گرافی[4] برای تشخیص تقلب کارت اعتباری معرفی کردند. آن‌ها پیش‌پردازش و مهندسی ویژگی را به‌عنوان یک گام مقدماتی انجام داده، سپس از ساختار گراف برای مدل‌سازی روابط میان مشتریان، بازرگانان و تراکنش‌ها بهره بردند؛ استفاده از مبدل‌های گراف[5] و نرمال‌سازی دسته‌ای نیز به همگرایی سریع‌تر و کارایی بهتر مدل کمک کرد. نتایج تجربی بر مجموعه‌داده‌های بزرگ نشان‌دهنده بهبود دقت، یادآوری و F1 نسبت به مدل‌های پایه است؛ بااین‌وجود، حساسیت مدل به چگونگی تعریف گراف و هزینه محاسباتی ایجاد و نگهداری آن در مقیاس بزرگ از محدودیت‌های مطرح‌شده توسط پژوهشگران بود.

نصرت سامیه و همکاران[20] با بهره‌گیری از تکنیک‌های داده‌کاوی و یادگیری ماشینی به پیش‌بینی و کاهش تهدیدات سایبری پرداختند. این مطالعه نشان می‌دهد که رخدادهای سایبری نه کاملاً تصادفی‌اند و از طریق تحلیل الگوها و روندهای تاریخی می‌توان نقاط آسیب‌پذیر و الگوهای تهاجمی را شناسایی کرد. آنها مدل‌هایی پیشنهاد کردند که علاوه بر پیش‌بینی احتمال وقوع واقعه، می‌توانند اقدامات کاهش‌دهنده ریسک را اولویت‌بندی کنند؛ آن‌ها به‌ضرورت به‌روزرسانی مداوم مدل‌ها و چالش‌های ناشی از تغییر تاکتیک‌های مهاجمان اشاره کردند.

نوراحمی مولدیه و همکاران[21] چارچوبی مبتنی بر پایگاه‌داده گراف[6] برای تشخیص تقلب کارت اعتباری پیاده‌سازی کردند که قابلیت نمایش روابط پیچیده بین نهادها، تحلیل مسیرها و اعلان‌دهی[7] را فراهم می‌سازد. پژوهش نشان داد که تحلیل گراف می‌تواند الگوهای پنهان کلاهبرداری را کشف کند و به‌صورت بلادرنگ برای تیم‌های نظارتی قابل‌نمایش باشد؛ بااین‌حال مطالعات مقایسه‌ای بیشتر برای سنجش عملکرد در برابر روش‌های مبتنی بر بردار ویژگی و بررسی نیازمندی‌های زیرساختی گراف (هزینه، نگهداری، ادغام با سامانه‌های موجود) ضرورت دارد.

ژوناتان کواکو آفری و همکاران[22] عملکرد سه مدل یادگیری نظارت شده - رگرسیون لجستیک، جنگل تصادفی و درخت تصمیم - را برای شناسایی تقلب در تراکنش‌های کارت اعتباری مقایسه کردند. نتایج تجربی نشان می‌دهد جنگل تصادفی در دامنه آزمایش‌ها بیشترین دقت را نسبت به دو مدل دیگر ارائه کرده است، اما نویسندگان به بررسی معیارهای دیگر (مانند یادآوری، نرخ مثبت کاذب[8] و ضریب همبستگی مَتیو) و ارزیابی روی مجموعه‌داده‌های نامتوازن و واقعی‌تر تأکید کرده‌اند تا تعمیم‌پذیری ادعا شده اثبات شود.

تی. کارتیکیان و همکاران[23] مدلی مبتنی بر شبکه عصبی عمیق با بهینه‌سازی ازدحام رقابتی[9] برای تشخیص ناهنجاری‌های تقلب پیشنهاد دادند و استدلال کردند که ویژگی‌های تقلب بسیار پویا هستند و استفاده از یادگیری بدون نظارت برای کشف الگوهای نوظهور ضروری است. نتایج آن‌ها در چند مجموعه‌داده نشان‌دهنده دقت‌های بسیار بالا (برای نمونه تا حدود 99.77٪ در برخی مجموعه‌ها) بود؛ بااین‌حال نویسندگان هشدار دادند که احتمال بیش برازش و کاهش تعمیم‌پذیری به داده‌های جدید می‌تواند یک نقطه‌ضعف باشد و نیازمند تنظیمات منظم و ارزیابی بیرونی است.

ام. جی. مدهوریا و همکاران[24] در یک تحلیل اکتشافی تشخیص تقلب کارت اعتباری، مجموعه‌ای از تکنیک‌های یادگیری ماشین از جمله ماشین بردار پشتیبان، تقویت گرادیان[10] و جنگل تصادفی را مقایسه کردند. آن‌ها نشان دادند که بسته به معیار و تنظیمات داده، الگوریتم‌های مختلف می‌توانند برتری نشان دهند؛ برای مثال در برخی آزمایش‌ها رگرسیون لجستیک عملکرد مناسبی ارائه نمود؛ ولی در منحنی‌های یادگیری

[1] Matthews Correlation Coefficient (MCC)
[2] Latency / Computational Cost
[3] Encoder–Decoder
[4] Graph Neural Network (GNN)
[5] Graph Transformer
[6] TigerGraph
[7] Alerts
[8] False Positive Rate (FPR)
[9] Competitive Swarm Optimization
[10] Gradient Boosting

نزدیک‌ترین همسایه[1] نشان داد که قابلیت یادگیری متفاوتی دارد. مقاله بر اهمیت رسم منحنی‌های یادگیری و تحلیل برازش تأکید می‌نماید.

آشا آر. بی و همکاران[25] در مطالعه‌ای عملکرد شبکه عصبی مصنوعی[2] را در تشخیص تقلب کارت اعتباری بررسی و گزارش دادند که شبکه‌های عصبی در مقایسه با چند الگوریتم سنتی، دقت بالاتری ارائه داده‌اند؛ بااین‌وجود در گزارش نتایج هشداری درباره کمبود جزئیات در مورد قابل‌پردازش داده‌ها، روش‌های مقابله با عدم تعادل کلاس و ارزیابی آماری مطرح شده است که تکرارپذیری نتایج را تحت‌تأثیر قرار می‌دهد.

شینچون لیو[26] تحلیل تجربی تقلب در صورت‌های مالی شرکت‌های پذیرفته‌شده در بورس را بر پایه رگرسیون لجستیک و جنگل تصادفی انجام داد؛ وی نشان داد که ترکیب درخت تصمیم و جنگل تصادفی می‌تواند ابزار مؤثری برای شناسایی گزارشگری مالی متقلبانه باشد و جنگل تصادفی در این مطالعه عملکرد قابل‌قبولی ارائه کرد. بااین‌حال پژوهشگر به نیاز به داده‌های گسترده‌تر و آزمون‌های بین‌بخشی اشاره کرد تا اطمینان از قابلیت تعمیم روش حاصل شود.

خوزه دی ژسوس روشا - سالازار و همکاران[27] مدلی جامع برای شناسایی پول‌شویی و تأمین مالی تروریسم با استفاده از شبکه‌های عصبی و یک «شاخص غیرعادی» نوآورانه ارائه نمودند؛ آن‌ها با افزودن مجموعه‌ای از ویژگی‌های غیر معامله‌ای و خوشه‌بندی گروهی، توانستند نرخ مثبت کاذب را کاهش و دقت تشخیص را افزایش دهند. بااین‌حال تعمیم‌پذیری بین نهادهای مالی مختلف و الزام به سازوکارهای دقیق شناخت مشتری[3] از جمله محدودیت‌هایی است که نویسندگان به آن اشاره کردند.

امیر صالح حسین و همکاران[28] رویکردی ترکیبی ارائه دادند که از نزدیک‌ترین همسایه خشن فازی[4] و بهینه‌سازی حداقل متوالی به‌عنوان پایه‌ها استفاده کرده و خروجی را در یک‌لایه متا بر پایه رگرسیون لجستیک ادغام کردند؛ نتایج شبیه‌سازی حاکی از نرخ‌های شناسایی رقابتی (حدود 84.90٪ و 76.30%) بود، ولی پژوهش به نیاز به ارزیابی در مقیاس‌های بزرگ‌تر و مقاومت در برابر نویز و حملات داده‌ای اشاره کرد.

جیا وی لی و همکاران[29] با استفاده از مدل‌های یادگیری ماشینی بدون نظارت و پردازش زبان طبیعی، داده‌های توییتر را برای استخراج تجربیات خودگزارشی مرتبط با فساد تحلیل کردند؛ آن‌ها از مدل‌های موضوعی[5] برای استخراج مضامین مرتبط بهره بردند و نشان دادند که می‌توان مجموعه‌ای از پیام‌ها را که احتمالاً حاوی گزارش فسادند جدا کرد؛ اما محدودیت‌هایی مانند نویز ذاتی شبکه‌های اجتماعی و نیاز به اعتبارسنجی انسان‌محور برای تأیید یافته‌ها برشمرده شده است.

وایشنوی ناث دورنادولا و همکاران] 30] روش‌هایی برای تشخیص تقلب در داده‌های تراکنش جریانی ارائه کردند که شامل استخراج الگوهای رفتاری مشتریان با استفاده از پنجره کشویی[6] و خوشه‌بندی پویا[7] است؛ نتایج نشان داد رگرسیون لجستیک، درخت تصمیم و جنگل تصادفی در بسیاری از سناریوها عملکرد مناسبی دارند، اما پردازش جریانی واقعی و به‌روزرسانی زمان - واقعی مدل‌ها همچنان چالشی فنی محسوب می‌شود.

پل دی. لارسون[31] در کار نظری - تجربی خود به رابطه بین فساد، نابرابری جنسیتی و عملکرد لجستیک پرداخت و با استفاده از شاخص‌های بین‌المللی و تحلیل رگرسیونی نشان داد که متغیرهای نهادی و ساختارهای اجتماعی می‌توانند بر عملکرد لجستیک و در نتیجه محیط فساد اثر بگذارند؛ این مطالعه حوزه تحلیل فساد را از منظر نهادی و آماری تقویت می‌کند.

کورنلیه رابوزین و همکاران[32] به کاربرد متن‌کاوی و روش‌های یادگیری ماشین در پیش‌بینی شاخص‌های فساد در تدارکات عمومی پرداختند؛ آن‌ها با استخراج ویژگی‌های متنی از اسناد مناقصه و استفاده از الگوریتم‌های طبقه‌بندی متن مانند بیز ساده، رگرسیون لجستیک و ماشین بردار پشتیبان نشان دادند که می‌توان مناقصه‌های مشکوک را شناسایی کرد، هرچند کمبود برچسب‌زنی دقیق و نادر بودن نمونه‌های فاسد چالش‌های اصلی این حوزه هستند.

نتیجه‌گیری کلی از مطالعات مرور شده نشان می‌دهد که الگوریتم‌های یادگیری ماشین و یادگیری عمیق (از جمله جنگل تصادفی، شبکه‌های عصبی، شبکه عصبی گرافی و روش‌های فازی) ظرفیت بالایی در تشخیص تقلب و کشف پول‌شویی دارند؛ هر روش نقاط قوت و محدودیت‌های خاص خود را داراست (مانند توانایی یادگیری عمیق در پردازش داده‌های بدون ساختار یا توانایی چارچوب‌های فازی در مدیریت عدم تعادل) و چالش‌های مشترکی از قبیل عدم تعادل شدید کلاس‌ها، تغییرپذیری رفتاری کلاهبرداران، نیاز به داده‌های برچسب خورده و هزینه‌های محاسباتی وجود دارد. در نتیجه پژوهش‌های آینده می‌بایست بر ترکیب روش‌های نظارت شده و بدون نظارت، بهره‌گیری از ساختارهای گرافی برای مدل‌سازی روابط بین بازیگران، مکانیزم‌های کاهش عدم تعادل (نمونه‌برداری هوشمند، یادگیری هزینه‌محور) و آزمون‌پذیری در مجموعه‌داده‌های متعدد و واقعی

[1] K-Nearest Neighbors (KNN)
[2] Artificial Neural Network (ANN)
[3] Know Your Customer (KYC)
[4] Fuzzy Rough Nearest Neighbor
[5] Topic Modeling
[6] Sliding Window
[7] Dynamic Clustering

(از جمله آزمون‌های برخط) متمرکز شوند[1] -[32].

همان‌گونه کـه در مـرور مطالعـات پیشـین و جـداول 1 و 2 مشاهده می‌شود، بخش قابل‌توجهی از پژوهش‌های انجام‌شـده در حوزه تشخیص تقلب کارت اعتباری، تمرکز خود را بر بهبود دقت مـدل‌ها قـرار داده‌انـد، درحالی‌کـه بـه چالش‌هـای مهمـی نظیـر نـامتوازن بـودن شـدید داده‌هـا و پیامـدهای آن بـر شناسـایی تراکنش‌های جعلی توجه کافی نشده اسـت. در از ایـن مطالعـات، استفاده از معیارهای ارزیابی متناسب بـا ماهیـت مسـئله، بـه‌ویژه معیارهایی که حساسـیت بـه خطاهـای منفـی کـاذب را افـزایش می‌دهند، به‌صورت محدود یا غیرمنسجم گزارش شده است.

علاوه بر این، در بخشی از پژوهش‌هـا، اگرچـه الگوریتم‌هـای متنوع یادگیری ماشین مورداستفاده قـرار گرفته‌انـد، امـا تحلیـل خطـا و بررسـی عملـی پیامـدهای اشـتباهات مـدل، بـه‌ویژه در سناریوهای واقعی تشخیص تقلب، ارائه نشده اسـت. براین‌اسـاس، پژوهش حاضر با تمرکز هم‌زمان بـر تحلیـل داده‌هـای نـامتوازن، استفاده از معیارهای ارزیابی چندمعیاره متناسب با مسئله، و ارائه یک مقایسه کمی جامع میان الگوریتم‌های متداول، تلاش می‌کند شکاف موجود میان دقت عـددی مـدل‌ها و الزامـات کاربردهـای عملی تشخیص تقلب را پوشش دهد.

جدول (1). خلاصه مقاله‌های فارسی

نام نویسندگان	کاربرد تحقیق	تکنیک استفاده شده	نتیجه	نقد
شیردل و خداپرست[1]	ارائه چارچوبی برای شناسایی تقلب در پرداخت‌های الکترونیکی	الگوریتم جنگل تصادفی در چارچوب یادگیری ماشین	افزایش دقت و امتیاز F1 در تشخیص تراکنش‌های متقلبانه	نیاز به ارزیابی بر داده‌های واقعی بانکی و آزمون در محیط عملی
محمد شریفی و همکاران[2]	مرور مطالعات انجام‌شده در حوزه شناسایی تقلب مالی با یادگیری ماشین	الگوریتم‌های درخت تصمیم، جنگل تصادفی، ماشین بردار پشتیبان و شبکه عصبی مصنوعی	انتخاب داده و پیش‌پردازش دقیق موجب بهبود عملکرد مدل‌های ضد تقلب می‌شود	عدم توازن داده‌ها و پیچیدگی مدل‌ها نیاز به مدل‌های ترکیبی و قابل‌تبیین را برجسته می‌کند
تقوی منش[3]	تشخیص حملات تزریق کد در پایگاه‌داده‌ها	الگوریتم‌های یادگیری ماشین (درخت تصمیم، متغیرهای وابسته) + انتخاب ویژگی دستی و خودکار	افزایش دقت مدل تا ٪۹۹،۵۷ با استخراج ویژگی‌های مؤثر	نیاز به تعمیم نتایج در سایر حوزه‌های امنیتی مانند تراکنش‌های مالی و بررسی پایداری مدل در داده‌های حجیم
مهدی نور محمودی و همکاران[4]	ارائه یک مدل کارا و مؤثر ضمن حفظ منافع بانک‌ها	مجموعه‌داده از تراکنش‌های آنلاین در بانک‌های آفریقا	از این مدل در زمینه‌های مختلف با کاربردهای علمی در تصمیم‌گیری‌ها استفاده می‌شود	به‌سرعت و دقت در مسئله تشخیص تقلب دقت شود
کیومرث پور قدیمی و همکاران[5]	مدل‌هایی برای کشف تقلب در صورت‌های مالی	ماشین بردار و جنگل تصادفی و شبکه عصبی	جنگل تصادفی (دقت 99 درصد)	تفسیرپذیری در جنگل‌های تصادفی کم است.
قمری مقدم و همکاران[6]	پیش‌بینی شرکت‌های متقلب مالیاتی بر پایهٔ صورت‌های مالی شرکت‌ها	تجمیعِ وزنیِ درختِ تصمیمِ بهبودیافته، شبکه بیزین و ماشین بردار پشتیبان+ انتخاب ویژگی با مجموعه راف	دقت ٪۸۰؛ بهبود عملکرد نسبت به روش‌های پایه	حجم داده محدود، نیاز به ارزیابی بر مجموعه‌داده‌های بزرگ‌تر و واقعی‌تر.
حسن ملکی کاکلر و همکاران[7]	مدل‌های آماری و یادگیری برای بررسی دقت پیش‌بینی تقلب در صورت‌های مالی	درخت تصمیم‌گیری C5، مدل درخت CHAID و مدل درخت C&R. مدل‌های پروبیت و گامبیت (آماری)	دقت پیش‌بینی مدل‌های یادگیری ماشین به‌صورت معنی‌داری از مدل‌های آماری بیشتر است.	بهتر است برای دقت در پیش‌بینی فسادهای مالی، از الگوریتم‌های یادگیری ماشین استفاده کنیم.
حبیب اعیانی[8]	ارائه یک مدل کشف کلاهبرداری مالی بهینه	تکنیک‌های مدرن و جدید در شبکه عصبی	جنگل تصادفی از روش‌های دیگر بهتر عمل کرده است	تعداد متغیر برای این مدل کم است
مریم دهقانی و همکاران[9]	بررسی الگوریتم‌های هوشمند مختلف در حوزه یادگیری ماشین برای پیش‌بینی سری‌های زمانی در بازارهای مالی	به‌کارگیری الگوریتم‌های یادگیری ماشینِ مبتنی بر رگرسیون، با تأکید بر روش انتخاب ویژگی پیشرو.	کارایی الگوریتم‌های MLP و SVR نسبت به درخت تصمیم بالاتر است.	بهتر است از شبکه عصبی عمیق به دلیل پیچیدگی این روش استفاده نشود.
امیرحسین صدیقی و همکاران[10]	ارائه سیستمی هوشمند که بتواند با استفاده از ویژگی‌های مختلف یک تراکنش مالی، قانونی یا غیرقانونی بودن آن را بادقت قابل‌قبولی تشخیص دهد.	الگوریتمی مبتنی بر یادگیری عمیق	الگوریتم پیشنهادی با 96 درصد صحت، 98 درصد دقت و 94 درصد حساسیت در تشخیص کلاهبرداری کاربرد دارد.	به دلیل انبوه بودن داده‌ها، نیازمند فضای ذخیره‌سازی زیادی داریم که پرهزینه است.

جدول (2). خلاصه مقاله‌های انگلیسی

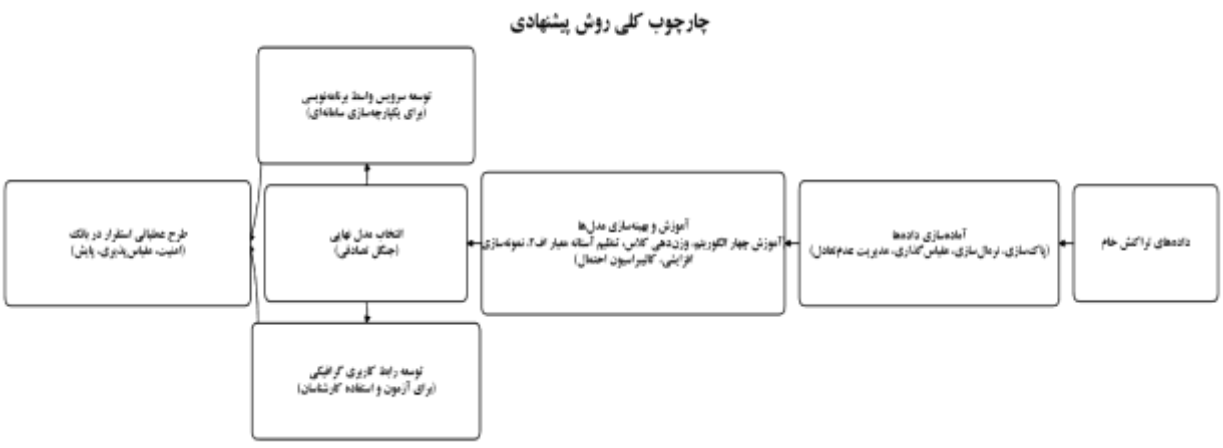
نام نویسندگان	کاربرد تحقیق	تکنیک استفاده شده	نتیجه	نقد
چن و همکاران[11]	مرور روزآمدِ یادگیری عمیق در کشف تقلب مالی و ارائه راهنمای کاربردی برای محیط‌های بانکی و پرداخت	مطالعه مروری و تحلیلی بر خانواده‌های شبکه عصبی (پیچشی، بازگشتی، گرافی) و رویکردهای ترکیبیِ مقابله با نامتوازنی و تبیین‌پذیری	تدوین چارچوب مفهومی برای انتخاب معماری و بهینه‌سازی؛ تأکید بر امتیازهای اف ۱ و اف ۲، سطح زیر منحنی دقت - بازخوانی و تنظیم آستانه؛ توصیه به استقرار مقیاس‌پذیر	محدودیت شواهد تجربی گسترده روی مجموعه‌داده‌های واقعی و اشاره به هزینه محاسباتی بالای مدل‌های یادگیری عمیق
ژائو و همکاران[12]	توسعه رویکردی سلسله‌مراتبی برای تشخیص تقلب کارت اعتباری با تحلیل رفتار تراکنش‌ها	شبکه دروازه‌ای سلسله‌مراتبی مبتنی بر رفتار تراکنش‌ها (استخراج ویژگی + تحلیل تعامل ویژگی)	بهبود امتیاز اف ۱ به طور میانگین ۱.۴۲٪-۶.۵۳٪ و بهبود AUC بین ۰.۶۳٪-۲.۷۸٪ نسبت به روش‌های پیشین	نیاز به بررسی عملکرد در مجموعه‌داده‌های متنوع، هزینه محاسباتی و پیچیدگی مدل‌بالا
احمد و همکاران[13]	کشف تقلب در تراکنش‌های کارت اعتباری با تمرکز بر نامتوازنی داده	طبقه‌بند تجمیعی + نمونه‌برداری ترکیبی (نمونه‌برداری افزایشی مصنوعی همراه با ویرایش نزدیک‌ترین همسایه)	بهبود معنادار در بازخوانی، امتیاز اف ۱ و سطح زیر منحنی دقت - بازخوانی نسبت به روش‌های پایه	نیاز به ارزیابی روی مجموعه‌داده‌های متنوع و سنجش هزینه محاسباتی و تنظیم ابرپارامترها برای محیط عملیاتی
گوپتا و همکاران[14]	ارائه چارچوب تقویت‌شده برای تشخیص تقلب کارت اعتباری	انتخاب ویژگی مقاوم + مدل تجمیعی پشته‌ای شامل چند طبقه‌بند پایه و فرا طبقه‌بند نهایی	بهبود چشمگیر در دقت، بازخوانی و امتیاز اف ۱ و کاهش مثبت‌های کاذب	نیاز به کاهش پیچیدگی محاسباتی و بررسی عملکرد در داده‌های جریانی و محیط واقعی
سورندرانادها ردی بیراپوردی و همکاران[15]	معرفی پلت فرم کلان‌داده برای خرده‌فروشان آنلاین	الگوریتم‌های یادگیری ماشین و هوش مصنوعی	روش تشخیص کلاهبرداری از یادگیری ماشین نظارت شده	انجام نشدن در محیط ORC
اولوابوسایو آدیجات بلو و همکاران[16]	بررسی تکنیک‌های مختلف هوش مصنوعی و کاربردهای آن‌ها در پیشگیری از تقلب	یادگیری ماشینی، یادگیری عمیق و پردازش زبان طبیعی	مبارزه با تقلب و ایجاد محیط دیجیتال امن	نگرانی از حریم خصوصی داده‌ها، کیفیت مجموعه‌داده‌ها و قابلیت تفسیر مدل همراه
جورجیوس کاریزانوس و همکاران[17]	توسعه یک چارچوب جدید کشف تقلب در زمان واقعی	یک مدل رگرسیون لجستیک فازی	تراکنش‌های متقلبانه بادقت بیش از 0.99	حل مشکلات غیرخطی را با رگرسیون لجستیک امکان‌پذیر نیست
شانجیتا آکتر پروم و همکاران[18]	معرفی ML و DL برای تشخیص فریب	تکنیک ML و DL و حالت چهره	دقت و پیشرفت حاصل شده در توسعه این دو مدل	توسعه مدل‌های قوی‌تر و قابل تعمیم‌پذیر
اسماً شریف و همکاران[19]	استفاده از شبکه‌های عصبی نمودار (GNN)برای تشخیص تقلب در کارت اعتباری	GNN مبتنی بر رمزگذار - رمزگشا	به‌دقت قابل‌توجه، یادآوری، امتیاز F1 و مقادیر ROC دست می‌یابد.	پیچیدگی زیاد مسئله.
نصرت سامیه و همکاران [20]	تجزیه‌وتحلیل جرایم سایبری با استفاده از داده‌کاوی و یادگیری ماشین	استفاده از شبکه‌های عصبی بازگشتی و شبکه‌های عصبی کانولوشنال	دقت بسیار بالا در تجزیه‌وتحلیل جرایم سایبری	نیاز به داده بزرگ. نیاز به محاسبات سنگین. توضیح‌پذیری محدود.
نوراحمی مولدیه و همکاران[21]	TigerGraph برای تجزیه‌وتحلیل داده‌ها	استفاده از الگوریتم Louvain	دستیابی به نرخ دقت بسیار بالای 70 درصد	هزینه‌بربودن این روش
جاناتان کواکو آفری و همکاران[22]	اجرای سه الگوریتم بر روی داده‌های بانکی در کشور غنا	رگرسیون لجستیک، جنگل تصادفی و درخت تصمیم	جنگل تصادفی بهینه‌ترین الگوریتم در تشخیص فساد در تراکنش‌های کارت اعتباری	مقایسه تعداد بیشتری از الگوریتم‌ها جهت دقت بیشتر
تی کارتیکیان و همکاران[23]	حل تقلب در بانک‌ها با تکنیک‌های یادگیری عمیق	ساخت یک مدل شبکه عصبی پیچیده عمیق	موفق در شناسایی حملات سایبری، میزان خطا حداقل است.	سوابق قبلی یا یادگیری نظارت شده (CSO) قابل‌شناسایی نیستند.
ام جی مدهوریا و همکاران[24]	بررسی چند الگوریتم برای تشخیص تقلب کارت اعتباری	پشتیبان ماشین بردار، تقویت گرادیان، جنگل تصادفی و مخلوط آنها.	الگوریتم KNN طبقه‌بندی‌کننده بهتری برای تشخیص تقلب کارت اعتباری	استفاده از سایر الگوریتم‌های یادگیری ماشین برای دقت بیشتر.

نام نویسندگان	کاربرد تحقیق	تکنیک استفاده شده	نتیجه	نقد
آشا آر بی و همکاران[25]	کشف تقلب در تراکنش‌های کارت اعتباری مبتنی بر یادگیری عمیق	ماشین بردار پشتیبان، نزدیک‌ترین همسایه و شبکه عصبی مصنوعی (ANN)	الگوریتم شبکه عصبی مصنوعی که دقتی تقریباً برابر با 100٪ می‌دهد.	نیاز به حجم زیادی از داده‌ها است که جمع‌آوری آن زمان و هزینه بالایی دارد.
شینچون لیو[26]	ارائه یک مدل یادگیری ماشین در تقلب صورت‌های مالی	درخت تصمیم و جنگل تصادفی	درخت تصمیم در تشخیص تصویر و پردازش کلمه موفق‌تر	استفاده از ماشین بردار پشتیبان جهته دقت بیشتر
خوزه دی ژسوس روشا - سالازار و همکاران[27]	ارائه مدلی جامع جهت پول‌شویی و تأمین مالی تروریسم در سامانه‌های مالی	شاخصی از ناهنجاری بر اساس واریانس متغیرها	کاهش هزینه‌ها، سرمایه انسانی و زمان تحقیق به دلیل بهبود نرخ پیش‌بینی است.	جامعه آماری پایین
امیر صالح حسین و همکاران[28]	ارائه مدل طبقه‌بندی‌شده برای تشخیص تقلب در کارت اعتباری	الگوریتم نزدیک‌ترین همسایه فازی، بهینه‌سازی حداقل متوالی و رگرسیون لجستیک	دقت این مدل در شناسایی تقلب کارت اعتباری به بیش از 80 درصد می‌رسد	استفاده از تکنیک‌های دیگر جهت توسعه مدل
جیاوی لی و همکاران[29]	شناسایی فساد در بخش‌های مختلف صنعتی	یک روش یادگیری ماشینی بدون نظارت با استفاده از پردازش زبان طبیعی	دسته‌ای از پیام‌هایی که مشکوک بود شناسایی شد.	دقت خروجی یادگیری بدون ناظر کم است.
وایشنوی ناث دورنادولا و همکاران[30]	طراحی و توسعه روش جدید کشف تقلب برای جریان داده‌های تراکنش	رگرسیون لجستیک، درخت تصمیم و جنگل تصادفی	ضریب همبستگی متیوز عامل بهتری برای مقابله با مجموعه‌داده عدم تعادل	الگوریتم جنگل تصادفی باید بهبود یابد.
پل دی. لارسون[31]	فرضیه‌های مبتنی بر نظریه در مورد تأثیر فساد و نابرابری جنسیتی بر عملکرد لجستیک	تحلیل رگرسیون	نابرابری جنسیتی برای عملکرد لجستیک مضر است.	حل مشکلات غیرخطی با رگرسیون لجستیک امکان‌پذیر نیست.
کورنلیه رابوزین و همکاران[32]	مقایسه مدل‌های پیش‌بینی با استفاده از تکنیک‌های متن‌کاوی	بیز ساده، رگرسیون لجستیک و ماشین‌های بردار پشتیبان.	در اکثر موارد الگوریتم ساده بیز نتایج بهتری نشان داد.	تحلیل متن‌هایی که دارای گویش است پیچیده می‌شود.

2-3. روش پیشنهادی

روش پیشنهادی این پـژوهش شـامل چنـد مرحلـه‌ی اصـلی است که از آماده‌سازی داده‌ها تا توسعه و استقرار سـامانه را دربـر می‌گیرد. هدف، طراحی مدلی کارآمد برای شناسایی و پیش‌بینی تراکنش‌هـای جعلـی در کارت‌هـای اعتبـاری بـا اسـتفاده از الگوریتم‌های یادگیری ماشین و تکنیک‌های بهبود عملکرد است.

شکل (5) نمای کلی از مراحل اجرای روش پیشـنهادی را نشـان می‌دهد. این مراحل به ترتیب شامل آماده‌سازی داده‌هـا، انتخـاب الگوریتم‌ها، آموزش و ارزیابی مدل‌ها، توسعه رابط‌های نرم‌افـزاری و طراحی طرح عملیاتی پیشنهادی بـرای پیاده‌سـازی در محـیط واقعی بانکی است.



شکل (5). ساختار کلی مدل پیشنهادی

2-3-1. آماده‌سازی داده‌ها

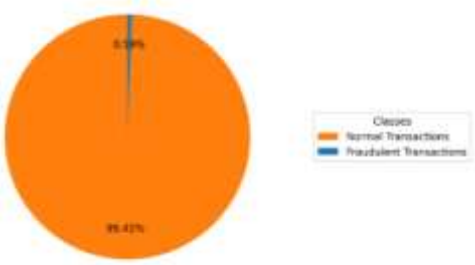
داده‌های مورداستفاده در این پژوهش از مجموعه‌داده «تشخیص تقلب در تراکنش‌های کارت اعتباری» استخراج شده است که از طریق پایگاه‌داده‌های پژوهشی کَگل در دسترس قرار دارد. این مجموعه‌داده شامل تراکنش‌های کارت اعتباری شبیه‌سازی‌شده در بازه زمانی اول ژانویه ۲۰۱۹ تا سی و یکم دسامبر ۲۰۲۰ بوده و رفتار مالی ۱۰۰۰ مشتری را در تعامل با حدود ۸۰۰ پذیرنده پوشش می‌دهد .این داده‌ها با استفاده از یک ابزار تولید داده مبتنی بر شبیه‌سازی[1] تولید شده‌اند که بر اساس پروفایل‌های رفتاری[2] مختلف (نظیر گروه‌های سنی، جنسیت، محل سکونت و الگوهای مصرف) و توزیع‌های آماری تعریف‌شده برای مبلغ و زمان تراکنش‌ها عمل می‌کند. در این فرایند، تراکنش‌ها ابتدا برای پروفایل‌های جمعیتی متفاوت به‌صورت جداگانه تولید شده و سپس با یکدیگر ادغام شده‌اند تا نمایی متنوع و واقع‌گرایانه از رفتارهای مالی کاربران ایجاد شود .اگرچه داده‌ها ماهیت شبیه‌سازی‌شده دارند، اما فرایند تولید آن‌ها مبتنی بر سناریوهای رفتاری واقعی و توزیع‌های آماری نزدیک به داده‌های بانکی حقیقی طراحی شده است و ازاین‌رو، این مجموعه‌داده به طور گسترده در پژوهش‌های مرتبط با تشخیص تقلب کارت اعتباری به‌عنوان یک معیار استاندارد مورداستفاده قرار می‌گیرد.

ویژگی‌های این مجموعه‌داده شامل اطلاعاتی نظیر مبلغ تراکنش، زمان انجام تراکنش، نوع پذیرنده، دسته‌بندی تراکنش، اطلاعات مکانی تقریبی و شاخص‌های رفتاری کارت است. برچسب هدف، هر تراکنش را به یکی از دو کلاس «عادی» یا «جعلی» تخصیص می‌دهد.

در این پژوهش، تمرکز اصلی بر بهبود کیفیت داده از طریق پاک‌سازی داده‌ها، نرمال‌سازی، مقیاس‌بندی ویژگی‌ها و مدیریت عدم توازن کلاس‌ها بوده است. همچنین از انجام مهندسی ویژگی‌های پیچیده یا تولید ویژگی‌های مصنوعی گسترده که می‌تواند منجر به بیش برازش مدل شود، اجتناب شده تا امکان ارزیابی منصفانه عملکرد الگوریتم‌های یادگیری ماشین در شرایطی نزدیک به کاربردهای عملی فراهم گرد .مطالعات اخیر نشان داده‌اند که به‌کارگیری ترکیب روش‌های خوشه‌بندی فازی و تحلیل مؤلفه‌های اصلی می‌تواند کارایی مدل‌های یادگیری ماشین را در مسائل چندهدفه به‌صورت محسوسی افزایش دهد] 33[.

2-3-2. تحلیل آماری توزیع کلاس‌ها در داده‌ها

تحلیل توزیع کلاس‌ها در داده‌های مورداستفاده نشان می‌دهد که مسئله تشخیص تقلب کارت اعتباری با عدم توازن شدید داده‌ها مواجه است. همان‌گونه که در بررسی اولیه مشخص شد، بخش عمده‌ای از تراکنش‌ها به کلاس «عادی» تعلق داشته و تنها درصد بسیار اندکی از آن‌ها به‌عنوان «جعلی» برچسب‌گذاری شده‌اند؛ موضوعی که بیانگر غلبه قابل‌توجه کلاس اکثریت در مجموعه‌داده است .توزیع عددی و درصدی نمونه‌ها در هر یک از کلاس‌ها در جدول (3) و شکل (6) ارائه شده است. این جدول به‌روشنی نشان می‌دهد که نسبت تراکنش‌های جعلی به کل داده‌ها بسیار ناچیز بوده و مسئله مورد بررسی از منظر یادگیری ماشین، در زمره مسائل دارای نامتوازنی شدید کلاس‌ها قرار می‌گیرد. چنین سطحی از عدم توازن می‌تواند منجر به گمراه‌کننده بودن معیار دقت کلی شود؛ به‌گونه‌ای که یک مدل ساده با پیش‌بینی تمامی تراکنش‌ها به‌عنوان «عادی» نیز به‌دقت بالایی دست یابد، درحالی‌که در شناسایی تراکنش‌های جعلی ناکارآمد است. ازاین‌رو، در ادامه پژوهش از معیارهایی فراتر از دقت کلی، از جمله بازخوانی، امتیازهای F1 و F2 و منحنی دقت - بازخوانی استفاده شده و همچنین روش‌هایی برای مقابله با عدم توازن کلاس‌ها در فرایند آموزش و ارزیابی مدل‌ها به کار گرفته شده است.



شکل (۶). توزیع کلاس‌های تراکنش‌های عادی و جعلی در مجموعه‌داده

جدول (3). توزیع کلاس‌ها در مجموعه‌داده

کلاس تراکنش	تعداد نمونه	درصد از کل داده
عادی	1607761	٪99.41
جعلی	9592	٪0.59
جمع کل	1616353	٪100

2-3-3. انتخاب الگوریتم‌ها

چهار الگوریتم پرکاربرد یادگیری ماشین شامل رگرسیون لجستیک، درخت تصمیم، جنگل تصادفی و ماشین بردار پشتیبان برای شناسایی تراکنش‌های جعلی به کار گرفته شدند. این الگوریتم‌ها به دلیل کارایی، سادگی نسبی و قابلیت مقایسه در مسائل طبقه‌بندی[3] انتخاب شدند.

[1] Sparkov Data Generation Tool
[2] Behavioral Profiles
[3] Classification Problems

2-3-4.آموزش و ارزیابی مدل‌ها

داده‌ها به دو بخش آموزشی و آزمایشی تقسیم شدند. مجموعه‌ی آموزشی برای آموزش مدل‌ها و مجموعه‌ی آزمایشی برای ارزیابی عملکرد آن‌ها مورداستفاده قرار گرفت. معیارهای مختلفی از جمله دقت، دقت مثبت، حساسیت، امتیاز F1 ، سطح زیر منحنیROC و سطح زیر منحنی دقت - بازخوانی برای مقایسه مدل‌ها در نظر گرفته شد. همچنین برای بهبود عملکرد، روش‌هایی مانند تنظیم آستانه با تأکید بر امتیاز F2 ، وزن‌دهی کلاس‌ها، کالیبراسیون احتمال و تنظیم ابرپارامترها به کار گرفته شد.

2-3-5.توسعه نرم‌افزاری سامانه

به‌منظور عملیاتی‌سازی مدل و فراهم‌کردن امکان استفاده از آن در محیط‌های واقعی بانکی، در این بخش مراحل توسعه نرم‌افزاری سامانه شامل طراحی رابط‌های برنامه‌نویسی کاربردی و رابط کاربری گرافیکی تشریح می‌شود. این بخش پلی میان مدل‌های یادگیری ماشین و استفاده عملی از نتایج آن‌ها در سامانه‌های بانکی ایجاد می‌کند.

2-3-5-1. طراحی رابط برنامه‌نویسی کاربردی

رابط برنامه‌نویسی کاربردی بستری برای ارائه مدل پیش‌بینی به‌عنوان یک سرویس فراهم می‌کند تا سایر سامانه‌ها بدون نیاز به اطلاع از جزئیات فنی، بتوانند از آن استفاده کنند .

در این پژوهش، دو رابط برنامه‌نویسی کاربردی با استفاده از چارچوب‌های فلاسک[1] و فست‌اِی‌پی‌آی[2] طراحی شد که امکان ارسال داده‌های تراکنش و دریافت نتیجه‌ی پیش‌بینی را در قالب ساختار جیسون[3] فراهم می‌کنند .

این رابط‌ها به‌گونه‌ای پیاده‌سازی شدند که خروجی شامل برچسب پیش‌بینی (تقلبی یا عادی) و احتمال وقوع تقلب باشد .

پیاده‌سازی این سرویس‌ها باعث شد مدل بتواند به‌سادگی در زیرساخت‌های بانکی مستقر شده و پاسخ‌گویی بلادرنگ[4] به درخواست‌های تشخیص تقلب داشته باشد.

OUTPUT:
{"prediction": 1,
"fraud_probability": 0.84{

خروجی نهایی رابط کاربری به‌صورت ساختار JSON شامل برچسب پیش‌بینی (۰ یا ۱) و احتمال وقوع تقلب (مثلاً 0.84) بازگردانده می‌شود.

[1] Flask Framework
[2] Flask Framework
[3] JavaScript Object Notation (JSON)
[4] Real-time Response

2-3-5-2. طراحی رابط کاربری گرافیکی(GUI)

به‌منظور تسهیل تعامل کاربران غیرمتخصص با سامانه، یک رابط کاربری گرافیکی[5] ساده و کاربردی با استفاده از ابزار گرادیو[6] طراحی شد.

این رابط به کاربران اجازه می‌دهد مشخصات تراکنش کارت اعتباری (مانند مبلغ، زمان، شناسه پذیرنده و...) را وارد کرده و نتیجه‌ی پیش‌بینی مدل را به‌صورت بلادرنگ مشاهده کنند .

مزیت اصلی این رابط در آن است که بدون نیاز به دانش فنی یا برنامه‌نویسی، کاربران بانکی یا تحلیل‌گران مالی می‌توانند احتمال تقلب را مشاهده کرده و تصمیم مناسب اتخاذ کنند . این بخش از سامانه باهدف ساده‌سازی تجربه کاربری[7] و افزایش کارایی در فرایند تشخیص تقلب طراحی شده است.

OUTPUT:
Fraud Probability: 0.83 | Fraud

2-3-6. طرح عملیاتی پیشنهادی

باتوجه‌به شرایط خاص زیرساخت‌های بانکی ایران، جهت عملیاتی‌سازی سامانه تشخیص تقلب مبتنی بر یادگیری ماشین، یک طرح مرحله‌بندی شده و متناسب با نیازهای فنی، امنیتی و عملیاتی بانک‌های ایرانی پیشنهاد می‌شود. این طرح چهار محور اصلی را شامل می‌شود:

1. داده‌ها و اتصال: سامانه باید قابلیت پردازش نزدیک به لحظه[8] در کلیدهای بانکی یا شرکت‌های ارائه‌دهنده خدمات پرداخت داشته باشد. داده‌های موردنیاز شامل حداقل ویژگی‌های ضروری نظیر مبلغ و زمان تراکنش، شناسه پذیرنده و پایانه، کد دسته‌بندی فروشگاه، موقعیت جغرافیایی تقریبی و شمارنده رفتار کارت است. به‌منظور رعایت حریم خصوصی، اطلاعات شناسایی فردی[9] حذف یا رمزنگاری شده و صرفاً داده‌های تجمیع‌شده نگهداری می‌شوند.

2. استقرار و پیاده‌سازی: مدل پیشنهادی باید به‌صورت یک سرویس سبک[10] در بستر بانکی مستقر شود تا امکان پاسخ‌گویی سریع فراهم گردد. برای این منظور استفاده از الگوریتم‌های جنگل تصادفی و رگرسیون لجستیک توصیه می‌شود. علاوه بر این، آستانه‌های پویا[11] متناسب با زمان روز، ریسک پذیرنده یا هزینه خطاهای نوع اول و دوم تنظیم می‌شوند. جهت بهبود حساسیت، می‌توان از روش وزن‌دهی کلاس‌ها در پردازش آنلاین و از الگوریتم نمونه‌سازی افزایشی در بازآموزی دوره‌ای بهره گرفت.

[5] Graphical User Interface (GUI)
[6] Gradio Tool
[7] User Experience (UX)
[8] Near Real-Time Processing
[9] Personally Identifiable Information (PII)
[10] Lightweight Scoring Service
[11] Dynamic Thresholding

3. امنیت و عملیات: باتوجه‌به حساسیت بالای حوزه مالی، رعایت الزامات امنیتی ضروری است. استفاده از پروتکل‌های رمزنگاری استاندارد(TLS/SSL) ، توکن‌های احراز هویت[1]، محدودیت نرخ درخواست‌ها و ثبت ایمن رخدادها برای جلوگیری از حملات و تقلب توصیه می‌شود. همچنین وجود یک زنجیره تصمیم شامل اجازه عبور، ارسال رمز یک‌بارمصرف برای تأیید اضافی یا مسدودسازی تراکنش ضروری است. علاوه بر این، پایش تغییرات رفتاری[2] در داده‌ها و مدل همراه با داشبورد مدیریتی به‌منظور نظارت بلادرنگ بر عملکرد سامانه اهمیت ویژه‌ای دارد.

4. نقشه راه: افزایش تهدیدات امنیتی در سامانه‌های اطلاعاتی، لزوم تقویت لایه‌های رمزنگاری و ارزیابی آسیب‌پذیری الگوریتم‌های رمز را بیش‌ازپیش آشکار ساخته است. تحلیل حملات مبتنی بر بدافزارهای رمزی و شبیه‌سازی آسیب‌پذیری کلیدهای رمز در الگوریتم‌های RSA نشان می‌دهد که پایش مستمر و به‌روزرسانی روش‌های حفاظتی برای کاهش خطر نفوذ ضروری است] 34] . در مرحله نخست، یک پایلوت آفلاین بر روی داده‌های تاریخی اجرا می‌شود تا کارایی مدل در شرایط واقعی اعتبارسنجی گردد. در مرحله دوم، مدل به مسیر صدور مجوز تراکنش‌ها متصل شده و باید زمان پاسخ‌گویی کمتر از ۱۵۰ میلی‌ثانیه داشته باشد. در نهایت، استقرار کامل در محیط عملیاتی با قابلیت‌هایی نظیر تحلیل شبکه کارت - پذیرنده، شفافیت تصمیم‌گیری مدل‌ها با استفاده از روش‌های توضیح‌پذیری[3]، بهینه‌سازی آستانه بر اساس هزینه و بازآموزی دوره‌ای (هفتگی یا ماهانه) انجام خواهد شد.

5. ارزش افزوده و کارکردهای آینده: این سامانه علاوه بر شناسایی تقلب می‌تواند به‌عنوان یک ماژول ریسک‌سنجی پویا برای بانک‌ها عمل کرده و با اتصال به زیرساخت‌های پرداخت کشور، نرخ خطای تراکنش‌های مشکوک را کاهش دهد. همچنین قابلیت توسعه برای بهره‌گیری از شبکه‌های عصبی گرافی[4] در آینده وجود دارد که می‌تواند دقت کشف الگوهای پیچیده تقلب را افزایش دهد.

در مجموع، روش پیشنهادی با ترکیب چند الگوریتم یادگیری ماشین و فراهم‌سازی زیرساخت‌های نرم‌افزاری برای استفاده بلادرنگ، گامی در جهت عملیاتی‌سازی تشخیص تقلب در سامانه‌های بانکی ایران فراهم می‌سازد.

[1] JSON Web Token (JWT)
[2] Drift Monitoring
[3] SHAP – SHapley Additive exPlanations
[4] Graph Neural Networks (GNNs)

ساختار مرحله‌ای این روش از داده تا پیاده‌سازی، امکان ارزیابی دقیق عملکرد مدل و تسهیل استقرار آن را در محیط‌های واقعی بانکی ایجاد می‌کند.

3. نتایج و بحث

3-1. معیارهای ارزیابی مدل‌ها

برای ارزیابی علمی مدل‌های یادگیری ماشین، به‌ویژه در مسائل طبقه‌بندی نظیر تشخیص تقلب، استفاده از معیارهای کمی ضروری است تا عملکرد مدل‌ها از جنبه‌های مختلف قابل‌مقایسه باشد. در ادامه مهم‌ترین معیارها به همراه فرمول هر یک ارائه شده است.

- دقت[5]: نسبت پیش‌بینی‌های صحیح مدل به کل نمونه‌هاست و از رابطه زیر محاسبه می‌شود:

$$Accuracy = \frac{TP + TN}{FN + FP + TN + TP} \quad (1)$$

که در آن:

- TP[6]: تعداد نمونه‌های مثبت درست پیش‌بینی‌شده؛
- TN[7]: تعداد نمونه‌های منفی درست پیش‌بینی‌شده؛
- FP[8]: تعداد نمونه‌های منفی که ندانسته مثبت پیش‌بینی شده‌اند؛
- FN[9]: تعداد نمونه‌های مثبتی که ندانسته منفی پیش‌بینی شده‌اند.

این معیار برای داده‌های متوازن مناسب است، اما در داده‌های نامتوازن (مانند تراکنش‌های بانکی) می‌تواند گمراه‌کننده باشد.

- دقت مثبت[10] : نسبت نمونه‌های مثبت درست پیش‌بینی‌شده به کل نمونه‌هایی است که مدل مثبت پیش‌بینی کرده است:

$$Precision = \frac{TP}{FP + TP} \quad (2)$$

این معیار زمانی اهمیت دارد که هزینه مثبت کاذب زیاد باشد، مثلاً هنگامی‌که تراکنش سالم ندانسته تقلب تشخیص داده شود.

- حساسیت[11] یا نرخ شناسایی مثبت‌ها: نسبت نمونه‌های مثبت واقعی است که به‌درستی شناسایی شده‌اند:

[5] Accuracy
[6] True Positives (TP)
[7] True Negatives (TN)
[8] False Positives (FP)
[9] False Negatives (FN)
[10] Precision

$$Recall = \frac{TP}{FN + TP} \quad (3)$$

در کاربردهایی مانند تشخیص تقلب، این معیار اهمیت بالایی دارد؛ زیرا ازدست‌دادن حتی یک تراکنش جعلی می‌تواند خسارت‌زا باشد.

- امتیاز F1[1]: میانگین هماهنگ دقت مثبت و حساسیت است و زمانی که داده‌ها نامتوازن باشند معیار مناسبی برای سنجش عملکرد کلی مدل محسوب می‌شود:

$$F1 = \frac{Precision \times Recall}{Precision + Recall} \times 2 \quad (4)$$

این معیار تنها زمانی بالا است که هر دو مقدار دقت مثبت و حساسیت در سطح قابل‌قبولی باشند.

- امتیاز F2[2]: مشابه F1 است؛ اما وزن بیشتری به حساسیت می‌دهد و برای حالاتی که شناسایی نمونه‌های مثبت واقعی اهمیت بالاتری دارد مناسب است:

$$F2 = \frac{(Precision \times Recall) \times (2^2 + 1)}{(Precision \times 2^2) + Recall} \quad (5)$$

در تشخیص تقلب، این معیار با تأکید بر افزایش حساسیت، در تنظیم آستانه تصمیم‌گیری برای دستیابی به بهترین تعادل میان شناسایی و خطا به کار می‌رود.

- سطح زیر منحنی ROC[3]: نمایانگر توان مدل در تفکیک کلاس‌های مثبت و منفی است. این منحنی نرخ مثبت کاذب را در برابر نرخ شناسایی مثبت‌ها نمایش می‌دهد و مساحت زیر آن، عددی بین ۰ و ۱ است که هرچه به ۱ نزدیک‌تر باشد، بیانگر عملکرد بهتر مدل است.
- منحنی دقت - بازخوانی[4] و سطح زیر منحنی دقت - بازخوانی[5]: این منحنی رابطه بین دقت مثبت و حساسیت را نشان می‌دهد و در داده‌های بسیار نامتوازن، شاخصی دقیق‌تر از سطح زیر منحنی ROC به شمار می‌آید. هرچه مساحت زیر این منحنی به ۱ نزدیک‌تر باشد، مدل در شناسایی نمونه‌های مثبت (تراکنش‌های جعلی) موفق‌تر عمل کرده است .در داده‌های بانکی، سطح زیر منحنی دقت - بازخوانی معیار مناسبی برای مقایسه مدل‌ها محسوب می‌شود.

3-2. نتایج مدل‌های پایه

چهار الگوریتم رگرسیون لجستیک، درخت تصمیم، جنگل تصادفی و ماشین بردار پشتیبان بر روی داده‌های آماده‌سازی شده پیاده‌سازی و ارزیابی شدند. نتایج نشان داد که مدل جنگل تصادفی بهترین عملکرد کلی را ارائه داد و در معیارهای بازخوانی و سطح زیر منحنی دقت - بازخوانی به طور قابل‌توجهی از سایر الگوریتم‌ها بهتر بود. در مقابل، مدل‌های رگرسیون لجستیک و ماشین بردار پشتیبان عملکرد ضعیف‌تری در شناسایی نمونه‌های تقلبی داشتند. به‌منظور تسهیل مقایسه کمی عملکرد الگوریتم‌های مورد بررسی، نتایج ارزیابی چهار الگوریتم بر اساس معیارهای مختلف در جدول (4) به‌صورت کنار هم ارائه شده است.

برتری مدل جنگل تصادفی را می‌توان به ماهیت ساختاری این الگوریتم نسبت داد. این مدل با ترکیب چندین درخت تصمیم و تجمیع نتایج آن‌ها، قادر است الگوهای پیچیده و غیرخطی موجود در داده‌های نامتوازن را بهتر شناسایی کند. همچنین، استفاده از نمونه‌برداری تصادفی در فرایند آموزش درخت‌ها موجب کاهش بیش برازش و افزایش توان تعمیم‌پذیری مدل، به‌ویژه در شناسایی تراکنش‌های جعلی که سهم اندکی از داده‌ها را تشکیل می‌دهند، شده است.

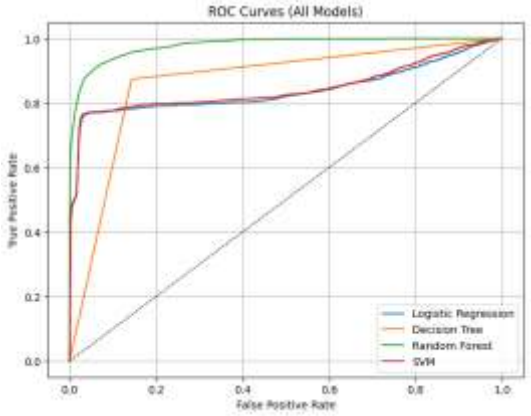
در مسئله تشخیص تقلب، خطاهای از نوع منفی کاذب (عدم شناسایی تراکنش‌های جعلی) از اهمیت ویژه‌ای برخوردارند، زیرا می‌توانند منجر به خسارات مالی مستقیم شوند. نتایج نشان می‌دهد که مدل جنگل تصادفی با دستیابی به مقادیر بالاتر بازخوانی و امتیاز F2 ، در مقایسه با سایر الگوریتم‌ها، تعداد کمتری از تراکنش‌های جعلی را به‌اشتباه به‌عنوان عادی طبقه‌بندی کرده است. این ویژگی، استفاده از این مدل را در کاربردهای عملی که حساسیت به خطاهای منفی کاذب بالا است، توجیه‌پذیرتر می‌سازد.

تحلیل نمودارهای ROC و دقت - بازخوانی ارائه‌شده در شکل‌های (7) و (8) نیز این نتایج را تأیید می‌کند. همان‌گونه که مشاهده می‌شود، منحنی مدل جنگل تصادفی در هر دو نمودار، به‌ویژه در نواحی بازخوانی بالا، عملکرد بهتری نسبت به سایر الگوریتم‌ها دارد. این موضوع نشان می‌دهد که این مدل قادر است با نرخ خطای مثبت کاذب قابل‌قبول، بخش بزرگ‌تری از تراکنش‌های جعلی را شناسایی کند؛ امری که در داده‌های نامتوازن اهمیت ویژه‌ای دارد..

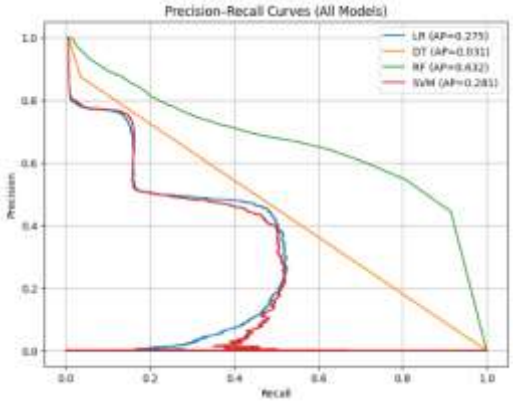
[11] Recall (Sensitivity)
[1] F1-Score
[2] F2-Score
[3] Receiver Operating Characteristic (ROC)
[4] Precision–Recall Curve
[5] Precision–Recall AUC (PR AUC)

جدول (۴). مقایسه مدل‌ها و تحلیل عملکرد

الگوریتم	Accuracy	Precision	Recall	F1-Score	F2-Score	ROC AUC	PR AUC
Logistic Regression	0.948	0.082	0.769	0.149	0.287	0.838	0.274
Decision Tree	0.856	0.035	0.873	0.067	0.151	0.865	0.031
Random Forest	0.934	0.076	0.914	0.141	0.285	0.978	0.632
SVM	0.962	0.112	0.767	0.196	0.354	0.844	0.281



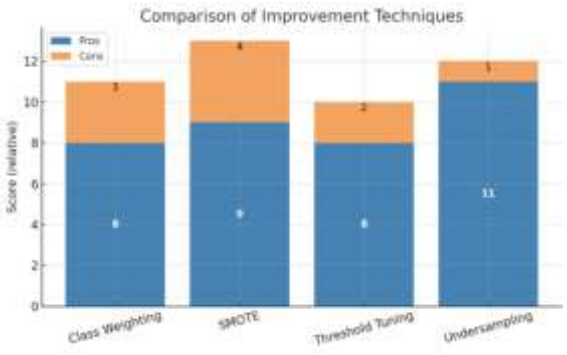
شکل (۷). مقایسه منحنی‌های ROC الگوریتم‌های مورداستفاده



شکل (۸). مقایسه منحنی‌های دقت - بازخوانی الگوریتم‌های مورداستفاده

3-3. بهبود عملکرد با تکنیک‌های تکمیلی

به‌منظور ارتقای عملکرد مدل‌ها در مواجهه با داده‌های نامتوازن، مجموعه‌ای از تکنیک‌های تکمیلی به‌صورت نظام‌مند مورداستفاده قرار گرفت. این فن‌ها شامل تنظیم آستانه تصمیم‌گیری، وزن‌دهی کلاس‌ها، نمونه‌سازی افزایشی، نمونه‌برداری کاهشی، کالیبراسیون احتمال و بهینه‌سازی ابرپارامترهای مدل‌ها بودند که هر یک باهدف بهبود شناسایی تراکنش‌های جعلی و کاهش خطاهای منفی کاذب به کار گرفته شدند.



شکل (۹). مقایسه اثر نسبی تکنیک‌های بهبود عملکرد

در این پژوهش، برای نمونه‌سازی افزایشی کلاس اقلیت از روش اسموت[1] استفاده شده است. این روش با تولید نمونه‌های مصنوعی در فضای ویژگی‌ها و بدون تکرار مستقیم داده‌های موجود، تلاش می‌کند توزیع کلاس‌ها را متعادل‌تر سازد و از بیش برازش مدل جلوگیری نماید. فرایند نمونه‌سازی افزایشی صرفاً بر روی داده‌های آموزشی اعمال شده و داده‌های آزمون بدون هیچ‌گونه تغییری نگه داشته شده‌اند تا ارزیابی عملکرد مدل‌ها به‌صورت منصفانه انجام گیرد.

بهینه‌سازی ابرپارامترهای الگوریتم‌ها با استفاده از روش جست‌وجوی شبکه‌ای[2] انجام شده است. در این فرایند، مجموعه‌ای از مقادیر محتمل برای ابرپارامترهای کلیدی هر الگوریتم تعریف گردید و بهترین ترکیب عامل‌ها بر اساس بیشینه‌سازی امتیاز F2 بر روی داده‌های اعتبارسنجی انتخاب شد. انتخاب این معیار به دلیل اهمیت بالای کاهش خطاهای منفی کاذب در مسئله تشخیص تقلب صورت‌گرفته است.

نتایج حاصل از به‌کارگیری این فن‌ها نشان می‌دهد که هر یک دارای مزایا و محدودیت‌های خاص خود هستند. روش وزن‌دهی کلاس‌ها و تنظیم آستانه تصمیم‌گیری توانستند توازن نسبی میان معیارهای دقت و بازخوانی ایجاد کنند، درحالی‌که

[1] SMOTE (Synthetic Minority Over-sampling Technique)
[2] Grid Search

روش نمونه‌سازی افزایشی با افزایش حساسیت مدل نسبت به کلاس اقلیت، در برخی موارد به کاهش دقت کلی منجر شد. در مقابل، روش نمونه‌برداری کاهشی باوجود کاهش حجم داده‌ها، در این پژوهش بهترین عملکرد را برای الگوریتم جنگل تصادفی به همراه داشت و موجب بهبود معنادار در شناسایی تراکنش‌های جعلی گردید.

براین‌اساس، در ادامه تحلیل‌ها و ارزیابی نهایی، مدل جنگل تصادفی همراه با تکنیک نمونه‌برداری کاهشی به‌عنوان رویکرد اصلی انتخاب شد. مقایسه اثر نسبی تکنیک‌های مختلف بهبود عملکرد بر اساس معیار دقت - بازخوانی در شکل (9) ارائه شده است که برتری این رویکرد را نسبت به سایر روش‌ها تأیید می‌کند.

همچنین ترکیب چند الگوریتم مکمل در قالب یادگیری گروهی (از جمله پشته‌سازی) در مطالعات اخیر توانسته است دقت و پایداری مدل‌های طبقه‌بندی را به طور معناداری بهبود دهد] 35 .

4-3. تحلیل نتایج

به‌طورکلی، ارزیابی‌ها نشان داد که استفاده از روش‌های ترکیبی بهبود عملکرد، به‌ویژه وزن‌دهی کلاس‌ها و تنظیم آستانه، در افزایش نرخ کشف تراکنش‌های جعلی بسیار مؤثر بوده است. نتایج به‌دست‌آمده با یافته‌های پژوهش‌های پیشین هم‌خوانی دارد که الگوریتم جنگل تصادفی را به‌عنوان یکی از روش‌های مؤثر در تشخیص تقلب کارت اعتباری، به‌ویژه در شرایط داده‌های نامتوازن، معرفی کرده‌اند. بااین‌حال، در این پژوهش با تمرکز هم‌زمان بر تحلیل عدم توازن داده‌ها، استفاده از معیارهای ارزیابی متناسب با حساسیت مسئله و بررسی خطاهای منفی کاذب، تفسیر جامع‌تر و کاربردی‌تری از دلایل برتری این الگوریتم ارائه شده است.

4. نتیجه‌گیری

در این پژوهش، مسئله تشخیص تقلب کارت اعتباری در شرایط داده‌های به‌شدت نامتوازن مورد بررسی قرار گرفت و عملکرد چند الگوریتم متداول یادگیری ماشین با تمرکز بر معیارهای ارزیابی متناسب با ماهیت مسئله تحلیل شد. نتایج نشان داد که انتخاب الگوریتم و معیار ارزیابی نقش تعیین‌کننده‌ای در کارایی عملی سامانه‌های تشخیص تقلب دارد و مدل جنگل تصادفی، به دلیل توانایی در یادگیری الگوهای غیرخطی و کاهش اثر عدم توازن داده‌ها، عملکرد باثبات‌تری در شناسایی تراکنش‌های جعلی نسبت به سایر مدل‌ها ارائه می‌دهد؛ به‌ویژه در معیارهایی که بر کاهش خطاهای منفی کاذب تأکید دارند.

از منظر کاربردی، یافته‌های این پژوهش نشان می‌دهد که مدل پیشنهادی می‌تواند به‌عنوان یک‌لایه پشتیبان تصمیم‌گیری در سامانه‌های بانکی مورداستفاده قرار گیرد. در چنین سناریویی، مدل می‌تواند تراکنش‌های پرریسک را در زمان نزدیک به واقعی شناسایی کرده و برای بررسی‌های تکمیلی، اعمال سیاست‌های امنیتی بیشتر یا مداخله انسانی علامت‌گذاری نماید. این رویکرد امکان بهره‌برداری از مدل را بدون جایگزینی کامل سامانه‌های موجود فراهم کرده و با الزامات عملیاتی سامانه‌های بانکی سازگار است.

بااین‌حال، پیاده‌سازی عملی سامانه پیشنهادی با محدودیت‌هایی نیز همراه است. از جمله، ملاحظات مربوط به حریم خصوصی داده‌ها ایجاب می‌کند که فرایند آموزش، نگه‌داری و به‌روزرسانی مدل در چارچوب سیاست‌های امنیتی و مقررات بانکی انجام شود. همچنین، در سناریوهای برخط، تأخیر پردازشی (latency)می‌تواند به‌عنوان یک چالش مطرح باشد و نیازمند بهینه‌سازی مدل یا استفاده از زیرساخت‌های پردازشی کارآمد است. افزون بر این، با افزایش حجم تراکنش‌ها، مسئله مقیاس‌پذیری اهمیت بیشتری می‌یابد که مستلزم به‌کارگیری معماری‌های توزیع‌شده و راهکارهای پایش و به‌روزرسانی مستمر مدل خواهد بود.

در مجموع، پژوهش حاضر گامی در جهت نزدیک‌تر کردن روش‌های یادگیری ماشین به الزامات عملی تشخیص تقلب در سامانه‌های بانکی محسوب می‌شود و می‌تواند مبنایی برای مطالعات آینده در زمینه استفاده از داده‌های واقعی، بهبود مقیاس‌پذیری و ارزیابی مدل‌ها در محیط‌های عملیاتی با محدودیت‌های زمانی و امنیتی واقعی قرار گیرد.

4-1. کارهای آتی

باوجود نتایج مطلوب به‌دست‌آمده، مسیرهای گوناگونی برای توسعه و ارتقای سامانه پیشنهادی وجود دارد. نخست، می‌توان از روش‌های پیشرفته متوازن‌سازی داده‌ها مانند تولید نمونه تطبیقی و یادگیری حساس به هزینه بهره گرفت تا عملکرد مدل در داده‌های بانکی بسیار نامتوازن بهبود یابد.

دوم، پیشنهاد می‌شود ارزیابی مدل بر داده‌های واقعی و نامتوازن انجام گیرد تا تصویر دقیق‌تری از رفتار مدل در محیط عملیاتی به دست آید.

سوم، استفاده از الگوریتم‌های ترکیبی و یادگیری جمعی (نظیر گرادیان افزایشی و پشته‌سازی مدل‌ها) می‌تواند توان تشخیص تراکنش‌های جعلی را افزایش دهد.

چهارم، توسعه ویژگی‌های زمانی، مکانی و گرافی برای شناسایی الگوهای پنهان میان مشتریان و پذیرندگان، زمینه‌ی بهبود دقت مدل را فراهم می‌سازد.

در نهایت، با به‌روزرسانی مستمر مدل در قالب چرخه یادگیری ماشینی و استقرار پروتکل‌های پایش و ارزیابی مداوم، می‌توان پایداری و سازگاری سامانه را در برابر تغییر رفتار متقلبان حفظ کرد.

5. مراجع

[1] M. R. Shirdel and F. Khodaparast, “Fraud detection in electronic payments using artificial intelligence and machine learning algorithms,” in Proc. 1st Natl. Conf. Artificial Intelligence and Emerging Research: Convergence of Humans and Intelligent Systems, Iran, 2025. [Online]. Available: https://conf.azad.ac.ir/fa/Home/Article/534c4d2a-a279-4cab-9281-0a5580f1aa3f (In Persian).

[2] M. Sharifi, M. Masoudi-Moghadam, and M. Hajiei, “A review of machine learning and deep learning methods in financial fraud detection,” in Proc. 1st Natl. Conf. Artificial Intelligence and Emerging Research: Convergence of Humans and Intelligent Systems, Iran, 2025. [Online]. Available: https://conf.azad.ac.ir/fa/Home/Article/028d765b-5bd1-4b41-97a2-43123e524624 (In Persian).

[3] S. M. Taghavimonsh, “Detecting SQL injection in database systems based on effective feature extraction,” Appl. ICT Innov. J., vol. 3, no. 3, Dec. 2024. [Online]. Available: https://journals.ihu.ac.ir/article_210085.html (In Persian).

[4] M. Nourmohammadi and S. A. Edalatpanah, “A new interval-neutrosophic decision tree model for fraud detection in electronic banking,” Ferdows Sci. Q., vol. 3, no. 9, pp. 9–37, 2023. [Online]. Available: https://www.kdip.ir/article_177245.html (In Persian).

[5] K. Poorghadimi, S. Jabbarzadeh-Kangerlouei, and J. Bahari-Sales, “Developing an enhanced Beneish model using firm-specific features with artificial neural network, support vector machine, and random forest,” J. Judgm. Decis. Mak. Account., vol. 1, no. 4, pp. 83–110, 2022. [Online]. Available: https://sanad.iau.ir/Journal/afi/Article/1088430/FullText (In Persian).

[6] A. Ghamarimoghadam and H. Nakhai, “A data-mining approach for predicting tax-fraudulent companies using optimized decision tree, support vector machine, and Bayesian network algorithms,” Appl. ICT Innov. J., vol. 2, no. 2, pp. 15–32, 2021. [Online]. Available: https://journals.ihu.ac.ir/article_208227.html (In Persian).

[7] H. Melki-Kaklar, J. Bahari-Sales, S. Jabbarzadeh-Kangerlouei, and A. Ashtab, “Effectiveness of statistical models and machine learning algorithms in predicting fraudulent financial reporting,” Financ. Econ. Q., vol. 15, no. 54, pp. 267–292, 2021. [Online]. Available: https://journals.iau.ir/article_686301.html (In Persian).

[8] H. Ayani, “Fraud detection in banking datasets,” Manag. Account. Third Millennium, vol. 2, no. 1, pp. 477–499, 2021. [Online]. Available: https://www.mhjournal.ir/fa/downloadpaper.php?pid=84&rid=10&p=A (In Persian).

[9] M. Dehghani, M. Ghasemzadeh, and H. Ansari-Samani, “Machine learning algorithms for time series in financial markets,” Soft Comput. Inf. Technol. Res. J., vol. 8, no. 3, pp. 60–67, 2019. [Online]. Available: https://jscit.nit.ac.ir/article_91216.html (In Persian).

[10] A. H. Seddighi and A. Sajdinejad, “A deep-learning-based approach for fraud detection in financial payment services,” Inf. Manag., vol. 5, no. 1, pp. 167–181, 2019. [Online]. Available: https://www.aimj.ir/article_101840.html (In Persian).

[11] Y. Chen, C. Zhao, Y. Xu, C. Nie, and Y. Zhang, “Deep learning in financial fraud detection: Innovations, challenges, and applications,” Intell. Syst. Appl., Art. no. 200451, 2025.

[12] Y. Xie, M. C. Zhou, G. Liu, L. Wei, H. Zhu, and P. De Meo, “A transactional-behavior-based hierarchical gated network for credit card fraud detection,” IEEE/CAA J. Autom. Sinica, vol. 12, no. 7, pp. 1489–1503, 2025. doi:10.1109/JAS.2025.125243.

[13] A. R. Kumar, D. Nithya, and S. M. Shamsudheen, “A credit card fraud detection approach based on ensemble machine learning classifier with hybrid data sampling,” Appl. Sci., vol. 15, no. 3, p. 1081, 2025.

Henne, H. A. Dwamena, O. O. Emmanuel, S. A. Ayeh, and J. Eshun, “A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions,” Decis. Anal. J., vol. 6, p. 100163, 2023. doi:10.1016/j.dajour.2023.100163.

[23] T. Karthikeyan, M. Govindarajan, and V. Vijayakumar, “An effective fraud detection using competitive swarm optimization based deep neural network,” Meas. Sensors, vol. 29, p. 100793, 2023. doi:10.1016/j.measen.2023.100793.

[24] M. J. Madhurya, H. L. Gururaj, B. C. Soundarya, K. P. Vidyashree, and A. B. Rajendra, “Exploratory analysis of credit card fraud detection using machine learning techniques,” Glob. Transitions Proc., vol. 3, no. 1, pp. 31–37, 2022. doi:10.1016/j.gltp.2022.04.006.

[25] A. R. B. Asha and S. K. R. Suresh Kumar, “Credit card fraud detection using artificial neural network,” Glob. Transitions Proc., vol. 2, no. 1, pp. 35–41, 2021. doi:10.1016/j.gltp.2021.01.006.

[26] X. Liu, “Empirical analysis of financial statement fraud of listed companies based on logistic regression and random forest algorithm,” J. Math., vol. 2021, pp. 1–9, 2021. doi:10.1155/2021/9241338.

[27] J.-d.-J. Rocha-Salazar, M.-J. Segovia-Vargas, and M.-d.-M. Camacho-Miñano, “Money laundering and terrorism financing detection using neural networks and an abnormality indicator,” Expert Syst. Appl., vol. 169, p. 114470, 2021. doi:10.1016/j.eswa.2020.114470.

[28] A. S. Hussein, R. S. Khairy, S. M. M. Najeeb, and H. T. S. Alrikabi, “Credit card fraud detection using fuzzy rough nearest neighbor and sequential minimal optimization with logistic regression,” Int. J. Interact. Mob. Technol. (iJIM), vol. 15, no. 5, pp. 24–42, 2021. doi:10.3991/ijim.v15i05.17173.

[29] J. Li, W.-H. Chen, Q. Xu, N. Shah, J. C. Kohler, and T. K. Mackey, “Detection of self-reported experiences with corruption on Twitter using unsupervised machine learning,” Soc. Sci. Humanit. Open, vol. 2, p. 100060, 2020. doi:10.1016/j.ssaho.2020.100060.

doi:10.3390/app15031081.

[14] R. K. Gupta, A. Hassan, S. K. Majhi, and N. Parveen, “Enhanced framework for credit card fraud detection using robust feature selection and a stacking ensemble model approach,” Results Eng., vol. 26, p. 105084, 2025. doi:10.1016/j.rineng.2025.105084.

[15] S. R. Byrapu Reddy, P. Kanagala, P. Ravichandran, R. Pulimamidi, P. V. Sivarambabu, and N. S. A. Polireddi, “Effective fraud detection in e-commerce: Leveraging machine learning and big data analytics,” Meas. Sensors, vol. 33, p. 101138, 2024. doi:10.1016/j.measen.2024.101138.

[16] O. A. Bello and K. Olufemi, “Artificial intelligence in fraud prevention: Exploring techniques, applications, challenges, and opportunities,” Comput. Sci. IT Res. J., vol. 5, no. 6, pp. 1505–1520, 2024. doi:10.51594/csitrj.v5i6.1252.

[17] G. Charizanos, H. Demirhan, and D. Içen, “An online fuzzy fraud detection framework for credit card transactions,” Expert Syst. Appl., vol. 252, p. 124127, 2024. doi:10.1016/j.eswa.2024.124127.

[18] S. A. Prome, N. A. Ragavan, M. R. Islam, D. Asirvatham, and A. J. Jegathesan, “Deception detection using machine learning (ML) and deep learning (DL) techniques: A systematic review,” Nat. Lang. Process. J., vol. 4, p. 100057, 2024. doi:10.1016/j.nlp.2024.100057.

[19] A. Cherif, H. Ammar, M. Kalkatawi, S. Alshehri, and A. Imine, “Encoder–decoder graph neural network for credit card fraud detection,” J. King Saud Univ. Comput. Inf. Sci., vol. 36, no. 1, p. 102003, 2024. doi:10.1016/j.jksuci.2024.102003.

[20] N. Samia, S. Saha, and A. Haque, “Predicting and mitigating cyber threats through data mining and machine learning,” Comput. Commun., Art. no. 107949, 2024. doi:10.1016/j.comcom.2024.107949.

[21] N. Mauliddiah and Suharjito, “Implementation graph database framework for credit card fraud detection,” Procedia Comput. Sci., vol. 227, pp. 326–335, 2023. doi:10.1016/j.procs.2023.10.531.

[22] J. K. Afriyie, K. Tawiah, W. A. Pels, S. Addai-

[30] V. N. Dornadula and S. Geetha, “Credit card fraud detection using machine learning algorithms,” Procedia Comput. Sci., vol. 165, pp. 631–641, 2020. doi:10.1016/j.procs.2020.01.057.

[31] P. Larson, “Corruption, gender inequality and logistics performance,” Int. J. Logist. Manag., ahead-of-print, 2019. doi:10.1108/IJLM-02-2019-0062.

[32] K. Rabuzin and N. Modruša, “Prediction of public procurement corruption indices using machine learning methods,” in Proc. 11th Int. Conf. Knowledge Management and Information Systems, 2019. doi:10.5220/0008353603330340.

[33] S. A. Edalatpanah and M. Nourmohammadi, “Dimensionality reduction using fuzzy clustering and principal component analysis for multi-objective learning problems,” Appl. ICT Innov. J., vol. 3, no. 2, 2023. [Online]. Available: https://ait.ihu.ac.ir/article_207100.html (In Persian).

[34] M. Shafiei and A. R. Faraji, “Simulation and vulnerability analysis of RSA cryptographic algorithms against malware-based attacks,” Appl. ICT Innov. J., vol. 3, no. 1, 2023. [Online]. Available: https://ait.ihu.ac.ir/article_206913.html (In Persian).

[35] S. M. Taghavimonsh and M. Sadeghi, “Improving classification performance using ensemble learning and stacking-based hybrid models,” Appl. ICT Innov. J., vol. 3, no. 3, 2024. [Online]. Available: https://journals.ihu.ac.ir/article_210155.html (In Persian).