

MDDI-01-2026.0105
MNR--1-CBECC4

کاربرد یادگیری ماشین و پایش هوشمند در کشف تراکنش‌های مشکوک و مبارزه با پولشویی در عصر بانکداری دیجیتال

دکتر محمدرضا کریمی

استادیار گروه مدیریت رسانه، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران

mohammadrezakarimi@iau.ac.ir

مهدی داداشی

دانشجوی دکتری گروه مدیریت فرهنگی و برنامه‌ریزی، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران

mahdidadashi1353@gmail.com

چکیده

گسترش خدمات برخط و رشد بی‌سابقهٔ حجم تراکنش‌ها، سامانه‌های سنتی قاعده‌محور مبارزه با پولشویی را که به آستانه‌های ثابت مبلغ و تعداد تکیه دارند، با دو مشکل هم‌زمان روبه‌رو کرده است: انبوهی از هشدارهای کاذب و ناتوانی در دیدن الگوهای چندلایه‌ای مانند اجاره حساب بانکی. این پژوهش کاربردی با رویکرد کمی و آزمایشی، چهار مدل نظارت‌شده (رگرسیون لجستیک، درخت تصمیم، جنگل تصادفی و گرادیان بوستینگ از خانوادهٔ XGBoost) و دو روش بدون نظارت (K-Means و جنگل انزوا) را با یک سامانهٔ قاعده‌محور مقایسه می‌کند. داده‌ها شامل حدود ۵۴۰٬۰۰۰ تراکنش شبیه‌سازی‌شدهٔ ۹۰ روزه با نرخ تراکنش مشکوک نزدیک به ۱٫۵ درصد و سه الگوی ساختارشکنی، حساب واسط (مول) و لایه‌گذاری زنجیره‌ای است. ارزیابی به‌صورت زمانی (آموزش روی روزهای آغازین، آزمون روی ۲۷ روز پایانی)، با معیارهای مناسب داده نامتوازن و در پنج تکرار مستقل انجام شد. نتایج نشان داد سامانهٔ قاعده‌محور با F1 برابر ۰٫۱۳۵ حدود ۹۲ درصد هشدارهایش را کاذب تولید می‌کند، در حالی که جنگل تصادفی و گرادیان بوستینگ به F1 نزدیک ۰٫۸۶۴ تا ۰٫۸۷۱ و PR-AUC حدود ۰٫۹۲۹ می‌رسند و تفاوت این دو مدل معنادار نیست؛ روش‌های بدون نظارت به‌تنهایی کافی نیستند. در نمونهٔ اصلی، حجم هشدارها حدود ۷۹ درصد و هشدارهای کاذب حدود ۹۷ درصد کاهش یافت. یافته‌ها از استقرار نظارت ترکیبی انسانی–الگوریتمی، تفسیرپذیری تصمیم‌ها و پایش رانش مدل حمایت می‌کند. اعداد گزارش‌شده بر پایهٔ داده شبیه‌سازی‌شده‌اند و پیش از تعمیم باید با داده واقعی بانکی راستی‌آزمایی شوند.

واژگان کلیدی: مبارزه با پولشویی، یادگیری ماشین، کشف تراکنش‌های مشکوک، بانکداری دیجیتال، پایش هوشمند

مقدمه

بانکداری دیجیتال در یک دههٔ اخیر شکل ارائهٔ خدمات مالی را عوض کرده است. اینترنت‌بانک، همراه‌بانک، درگاه‌های پرداخت و انتقال آنی وجه، سرعت و سهولت امور مالی را بالا برده‌اند و تجربه‌ای را برای مشتری ساخته‌اند که تا چند سال پیش ممکن نبود. اما همین بسترهای سریع و بی‌مرز، برای فعالیت‌های مجرمانه نیز کارآمدند. گسترش شبکه‌های پرداخت موبایلی و ابزارهای متصل، پیچیدگی بررسی جرائم مالی را بیشتر کرده و نیاز به پایش بلادرنگ را جدی‌تر ساخته است (Fan et al, 2025). پولشویی به معنای پنهان‌سازی یا تغییر چهرهٔ منشأ نامشروع درآمدهای مجرمانه و واردکردن آن‌ها به جریان قانونی اقتصاد است و آثارش بر ثبات اقتصادی، شفافیت مالی و امنیت ملی جبران‌ناپذیر توصیف شده است (تذهیبی، ۱۳۸۹).

بانک‌ها و مؤسسات مالی، شریان‌های اصلی گردش پول‌اند و ناگزیر در خط مقدم مبارزه با پولشویی قرار می‌گیرند. در چارچوب استانداردهای گروه ویژهٔ اقدام مالی (FATF)، مؤسسات مالی باید مشتری را شناسایی کنند، رفتار مالی او را در طول رابطه پایش نمایند و تراکنش مشکوک را گزارش دهند (FATF, 2012). در ایران نیز قانون مبارزه با پولشویی (مجلس شورای اسلامی، ۱۳۸۶) با اصلاحات ۱۳۹۷ و آیین‌نامهٔ اجرایی آن (هیئت وزیران، ۱۳۸۸) اشخاص مشمول را به گزارش موارد مشکوک به مرجع اطلاعات مالی مکلف کرده‌اند و ادبیات حرفه‌ای نیز بر الزام استقرار ابزارهای نظارتی دقیق و به‌روز تأکید دارد (تجلی، ۱۳۹۰). پرسش اجرایی اینجاست که این پایش، در حجم میلیونی تراکنش روزانه، با چه ابزاری انجام شود.

پاسخ سنتی، سامانه‌های قاعده‌محور بوده‌اند: مجموعه‌ای از قواعد ایستا مانند سقف مشخص انتقال وجه یا تعداد مشخص تراکنش در روز. این سامانه‌ها هم مجرم آگاه به آستانه را دور می‌زنند و هم ده‌ها هزار تراکنش مشروع تجاری را مشکوک علامت می‌زنند. یکی از نمونه‌های روشن، «اجارهٔ حساب بانکی» است؛ مجرم یا فرد متخلف با پرداخت مبلغی به صاحب حساب، از حساب او برای گردش وجوه استفاده می‌کند. بشیری و همکاران (۱۴۰۰) این پدیده را از شایع‌ترین راه‌های کتمان درآمد معرفی کرده‌اند که به فرار مالیاتی، پولشویی و جرائم دیگر پیوند خورده است و هشدار دادستان انتظامی مالیاتی دربارهٔ آن نیز در رسانه‌ها بازتاب یافته است (بهزاد، ۱۳۹۷). سامانهٔ قاعده‌محور چنین الگویی را معمولاً نمی‌بیند، چون هر تراکنش به‌تنهایی عادی است و نشانه فقط در رفتار مجموعهٔ حساب‌ها پیداست. نتیجه، صفی از هشدارهای نادرست است که بار سنگینی بر دوش واحد انطباق می‌گذارد (علوی، ۱۳۹۳). در یکی از معدود مطالعات میدانی منتشرشده، پیش از استقرار مدل کمکی، همهٔ هشدارها باید به‌صورت دستی بررسی می‌شد (Halford et al, 2025).

یادگیری ماشین به‌عنوان شاخه‌ای از هوش مصنوعی، می‌تواند از داده‌های تاریخی رفتار بیاموزد و بدون نوشتن قاعدهٔ دستی، الگوهای نامتعارف را نشان دهد. مرورها نشان می‌دهند این حوزه از تحلیل لینک و مدل‌سازی رفتار تا امتیازدهی ریسک و تشخیص ناهنجاری گسترش یافته است (Chen et al, 2018) و نمونه‌های کاربردی روی داده بانک‌های واقعی هم منتشر شده‌اند (Jullum et al, 2020). با این حال سه شکاف دیده می‌شود. نخست، داده واقعی در اختیار پژوهشگر نیست و بسیاری از مطالعات یا روی یک مجموعهٔ داده و یک الگوریتم تمرکز کرده‌اند یا ارزیابی را بدون جداسازی زمانی انجام داده‌اند. دوم، مرور انتقادی این حوزه نشان داده است که بخش بزرگی از روش‌ها تفسیرناپذیرند و داده‌های برچسب‌خورده کم و بسیار نامتوازن است (Kute et al, 2021). سوم، ادبیات

فارسی پیرامون پایش هوشمند تراکنش در بانکداری، بیشتر به الگوریتم یا به حقوق می‌پردازد و کمتر این دو را با تصمیم مدیریتی پیوند می‌دهد.

هدف این پژوهش، ارزیابی عملکرد مدل‌های مختلف یادگیری ماشین در کشف تراکنش مشکوک، با طرح ارزیابی دقیق‌تر از معمول و برگرداندن نتایج به زبان تصمیم مدیریتی است. پرسش‌های پژوهش و فرضیه‌ها از این قرارند:

پرسش ۱: مدل‌های یادگیری ماشین نظارت‌شده تا چه اندازه بر سامانهٔ قاعده‌محور برتری دارند؟ (فرضیهٔ ۱: F1 مدل‌های نظارت‌شده به‌طور معنادار از سامانهٔ قاعده‌محور بالاتر است.)

پرسش ۲: مدل‌های جمعی (جنگل تصادفی و گرادیان بوستینگ) نسبت به درخت تصمیم منفرد چه مزیتی دارند؟ (فرضیهٔ ۲: PR-AUC مدل‌های جمعی به‌طور معنادار از درخت تصمیم بالاتر است.)

پرسش ۳: آیا روش‌های بدون نظارت می‌توانند جایگزین مدل‌های نظارت‌شده شوند؟ (فرضیهٔ ۳: روش‌های بدون نظارت از نظر PR-AUC عملکرد ضعیف‌تری از مدل‌های نظارت‌شده دارند.)

پرسش ۴: نتیجهٔ این مقایسه برای بار کاری و هزینهٔ واحد انطباق بانک چه معنایی دارد؟

مبانی نظری و پیشینه پژوهش

چرخه پولشویی و چالش‌های بانکداری دیجیتال

پولشویی در ادبیات کلاسیک مالی سه مرحله دارد: جایگذاری (Placement) یعنی ورود وجوه آلوده به نظام مالی؛ لایه‌گذاری (Layering) یعنی جداکردن وجوه از منشأ مجرمانه با تراکنش‌های متعدد و پیچیده؛ و یکپارچه‌سازی (Integration) یعنی بازگشت وجوه پاک‌شده به اقتصاد رسمی. در بانکداری دیجیتال، آنی‌بودن انتقال و حذف مرز جغرافیایی، مرحلهٔ لایه‌گذاری را برای مجرم ارزان کرده است: مبلغ کلان خرد می‌شود و در چند دقیقه میان ده‌ها حساب جابه‌جا می‌گردد.

سه الگو در این پژوهش مبنای طراحی داده و تحلیل‌اند. الگوی نخست ساختارشکنی (Structuring) است؛ شکستن مبلغ به قطعه‌هایی کمی پایین‌تر از آستانهٔ گزارش‌دهی. اگر این کار با به‌کارگیری چند نفر و چند حساب انجام شود، به آن اسمرفینگ (Smurfing) می‌گویند. الگوی دوم حساب واسط یا «مول» (Money Mule) است: حسابی که وجوه چندین منبع را در زمانی کوتاه جمع می‌کند و به‌سرعت به مقصدی دیگر منتقل می‌سازد؛ اجارهٔ حساب بانکی یکی از شکل‌های رایج آن است. الگوی سوم زنجیرهٔ لایه‌گذاری است که در آن مبلغ از چند حساب پیاپی می‌گذرد و در هر مرحله اندکی کم می‌شود. برای پژوهش‌هایی که به‌دنبال ردیابی حساب‌های واسط‌اند، تحلیل شبکهٔ تراکنش‌ها ابزار مهمی شده است (Huang, 2025; Cheng et al, 2023).

از سیستم‌های قاعده‌محور تا پایش هوشمند

در سامانهٔ سنتی، اگر تراکنشی از آستانه‌ای مشخص (برای نمونه یک‌صد میلیون تومان) بگذرد، هشدار صادر می‌شود. این رویکرد دو ضعف دارد. اول، مجرم با دانستن آستانه، مبلغ را به قطعه‌های کوچک‌تر تقسیم می‌کند. دوم، بسیاری از تراکنش‌های تجاری و کاملاً مشروع بالای آستانه‌اند و به اشتباه مشکوک تلقی می‌شوند. یادگیری ماشین با تحلیل سابقهٔ رفتاری مشتری و گروه همتایان او «پروندهٔ رفتاری» پویا می‌سازد و انحراف از الگوی عادی را نشان می‌دهد؛ ایدهٔ اصلی که در ادبیات تشخیص تقلب آماری هم از دیرباز مطرح بوده است (Bolton and Hand,

(2002. فهرست روش‌های رایج شامل مدل‌های نظارت‌شده روی برچسب‌های تاریخی، روش‌های بدون نظارت برای ناهنجاری و خوشه‌بندی، و مدل‌های گرافی است (Chen et al, 2018).

در میان مدل‌های نظارت‌شده، مدل‌های درختی جمعی جایگاه ویژه‌ای در داده‌ٔ جدولی دارند. جنگل تصادفی با ترکیب تعداد زیادی درخت تصمیم، واریانس مدل را کم می‌کند (Breiman, 2001) و گرادیان بوستینگ درخت‌ها را پیاپی و برای اصلاح خطای مرحله‌ٔ قبل می‌سازد (Friedman, 2001). XGBoost پیاده‌سازی مقیاس‌پذیر و منظم‌شده‌ٔ این ایده است (Chen and Guestrin, 2016) و نسخه‌های مبتنی بر هیستوگرام مانند LightGBM آن را سریع‌تر کرده‌اند (Ke et al, 2017). در مقابل، K-Means داده را در خوشه‌هایی با میانگین مشترک بخش می‌کند (Lloyd, 1982) و جنگل انزوا (Isolation Forest) نقاط را بر اساس سهولت جداسازی از بقیه امتیاز می‌دهد (Liu et al, 2008)؛ هر دو بدون برچسب کار می‌کنند.

پیشینه تجربی

جولوم و همکاران (Jullum et al, 2020) در بزرگ‌ترین بانک نروژ مدلی نظارت‌شده برای اولویت‌بندی تراکنش‌هایی که باید دستی بررسی شوند ساختند و نشان دادند کنارگذاشتن هشدارهای بررسی‌شده اما گزارش‌نشده از داده آموزش، نتیجه را بدتر می‌کند؛ مدل آن‌ها از رویکرد جاری بانک بهتر عمل کرد. هالفورد و همکاران (Halford et al, 2025) مدل امتیازدهی را «روی» سامانه‌ٔ قاعده‌محور بانک گذاشتند: حدود ۱۹ درصد هشدارها خودکار به حالت کم‌ریسک رفتند، حدود ۱۸ درصد خودکار ارجاع شدند و زمان بررسی و ارسال گزارش حدود ۶۱ درصد کوتاه شد. رایته و همکاران (Reite et al, 2024) با طبقه‌بندی ریسک مشتری و افزودن داده حسابداری و اعتباری، هشدار کاذب را کم کردند. هاشمی و همکاران (Hashemi et al, 2023) در تشخیص تقلب روی داده بانکی، وزن‌دهی کلاس و معیارهای دقت-فراخوانی را به‌جای صحت صرف به‌کار بردند و مدل‌های گرادیان بوستینگ را برتر یافتند. شفیعی و همکاران (Shafiee et al, 2025) نیز چارچوبی مبتنی بر یادگیری ماشین و یادگیری عمیق برای تشخیص تقلب در مبارزه با پولشویی ارائه و آن را با روش‌های حسابداری سنتی و قاعده‌محور مقایسه کرده‌اند.

شاخه‌ٔ گرافی نیز رشد کرده است. چنگ و همکاران (Cheng et al, 2023) رفتار گروهی حساب‌ها را مدل کردند، ایرشاد و همکاران (Irshad et al, 2024) تحلیل شبکه و خوشه‌بندی را روی داده بانکی کشورهای در حال توسعه ترکیب کردند و لو و همکاران (Luo et al, 2024) چارچوبی نیمه‌نظارتی برای کمبود برچسب پیشنهاد دادند. دپرز و همکاران (Deprez et al, 2025) تأکید می‌کنند که مجرمان مدام روش خود را عوض می‌کنند و مدل باید بدون فراموشی دانش قبلی به‌روز شود. از طرف دیگر، کوته و همکاران (Kute et al, 2021) نشان دادند حدود نیمی از روش‌های یادگیری ماشین در این حوزه تفسیرناپذیرند و کار با داده قدیمی رایج است؛ و کارآمدبودن مدل بدون توضیح‌پذیری، در عمل برای بازرس و مقام ناظر کافی نیست. در عین حال ایلبری و همکاران (Ileberi et al, 2021) برای مقابله با نامتوازنی از SMOTE بهره بردند، اما ما و همکاران (Ma et al, 2026) نشان دادند در داده بسیار نامتوازن نمونه‌برداری مجدد همیشه مفید نیست و ارزیابی باید روی توزیع اصلی و بدون نشت داده انجام شود. پژوهش حاضر این توصیه را در طرح ارزیابی خود به کار می‌گیرد.

ابعاد مدیریتی، حقوقی و اقتصادی

پایش هوشمند فقط یک مسئلهٔ فنی نیست و بخشی از مدیریت ریسک سازمانی است. کشف‌نشدن پولشویی به جریمه‌های نظارتی سنگین، آسیب به اعتبار برند و کاهش اعتماد عمومی می‌انجامد. پژوهش‌های مربوط به فناوری اطلاعات در زنجیرهٔ تأمین نشان می‌دهد توان فناوری اطلاعات می‌تواند به مزیت رقابتی بینجامد (Hazen and Byrd, 2012)؛ منطق مشابهی برای فناوری انطباق در بانک قابل‌طرح است. افزون بر آن، حافظه و قابلیت یادگیری سازمانی، یعنی تبدیل تجربهٔ بازرسان به دانشی قابل‌استفاده، از عوامل پیشین مزیت رقابتی پایدار شمرده شده است (Camisón and Villar-López, 2011) و سرمایهٔ فکری در شرکت‌های خدماتی (از جمله بیمه) نیز به‌عنوان یکی از منابع مزیت رقابتی گزارش شده است (نجمی‌نیا و صالحی، ۱۳۹۱).

از منظر حقوقی و اقتصاد اسلامی، شفافیت معاملات و بستن راه‌های کسب درآمد نامشروع از الزامات سلامت نظام بانکی است. اجارهٔ حساب با ضمانت اجرای کیفری همراه است و به‌صورت ابزاری برای پنهان‌کردن درآمد و جرائمی مانند فرار مالیاتی و پولشویی به‌کار می‌رود (بشیری و همکاران، ۱۴۰۰). بنابراین ابزارهای هوشمند، مکمل و نه جایگزین، چارچوب حقوقی و آگاه‌سازی عمومی‌اند.

روش تحقیق

پژوهش از نظر هدف کاربردی و از نظر ماهیت، کمی و آزمایشی است و بر شبیه‌سازی داده تراکنشی تکیه دارد؛ دلیل، محرمانگی داده واقعی بانکی و محدودیت دسترسی پژوهشگر به آن است (برای مفهوم پژوهش کاربردی و طبقه‌بندی روش‌ها: حافظنیا، ۱۳۸۸). استفاده از داده مصنوعی واقع‌نما در مدل‌سازی ضدپولشویی هم در ادبیات پذیرفته شده است (Altman et al, 2023)، هرچند به معنای جایگزینی کامل داده واقعی نیست. بنابراین «جامعهٔ آماری» به معنای مرسوم وجود ندارد و آنچه در ادامه می‌آید، طرح آزمایشی روی یک جمعیت شبیه‌سازی‌شده است.

داده و شبیه‌سازی

در هر اجرا، حدود ۳۰٬۰۰۰ حساب (۱۵ درصد تجاری) و ۹۰ روز فعالیت تولید شد که به ۵۳۷٬۱۳۱ تا ۵۴۲٬۷۸۸ تراکنش (بسته به بذر تصادفی) می‌رسد. تراکنش‌های مشروع از رفتار هر حساب (نرخ فعالیت، میانگین مبلغ، ساعات کاری و مخاطبان ثابت) نمونه‌گیری شدند و برای واقع‌نمایی، بخشی از تراکنش‌های مشروع بزرگ‌تر از آستانهٔ یک‌صد میلیون تومان تعریف گردید. تراکنش‌های مشکوک از سه الگوی بخش پیشین و با ۱ تا ۳ رویداد برای هر حساب واسط ساخته شد و حدود ۳۰ درصد رویدادها عمداً «استتارشده» اند، یعنی در ساعت کاری و با مبلغ پایین رخ می‌دهند. برای دشوارکردن مسئله، حدود ۸ درصد حساب‌های تجاری «فروشگاه اینترنتی» اند که در بازه‌های کوتاه تراکنش‌های ورودی بسیار می‌گیرند و بلافاصله پرداخت می‌کنند؛ رفتاری که از نظر ظاهر شبیه حساب واسط است ولی مشروع است. جدول ۱ مشخصات اصلی را نشان می‌دهد.

جدول ۱: مشخصات داده شبیه‌سازی‌شده

مؤلفه	مقدار
تعداد حساب‌ها	۳۰٬۰۰۰ (۱۵٪ تجاری)

مؤلفه	مقدار
بازه زمانی	۹۰ روز
تعداد تراکنش در هر اجرا	۱۳۱٬۵۳۷ تا ۵۴۲٬۷۸۸
سهم تراکنش مشکوک	۱٫۴۷٪ تا ۱٫۵۶٪
الگوهای مشکوک	حساب واسط ۵۰٪؛ ساختارشکنی ۳۰٪؛ لایه‌گذاری ۲۰٪
رویدادهای استتارشده	حدود ۳۰٪ (ساعت کاری، مبلغ کم)
نمونه‌های دشوار مشروع	حساب‌های فروشگاهی پرتراکنش؛ تراکنش‌های مشروع بالای آستانه
آستانه سامانه قاعده‌محور	۱۰۰ میلیون تومان
تقسیم زمانی	آموزش: روز ۰ تا ۵۱؛ اعتبارسنجی: ۵۲ تا ۶۲؛ آزمون: ۶۳ تا ۸۹

مهندسی ویژگی‌ها

از هر تراکنش ۲۲ ویژگی ساخته شد که همگی فقط از رویدادهای پیش از آن لحظه محاسبه می‌شوند تا نشت اطلاعات آینده به مدل رخ ندهد. گروه‌های اصلی در جدول ۲ آمده‌اند. ویژگی‌های «تازگی طرف حساب» و «ورودی گیرنده» نقش یک شاخص شبکه‌ای ساده را دارند و برای شناسایی حساب‌های جمع‌کننده به‌کار می‌روند.

جدول ۲: گروه‌های ویژگی‌های ساخته‌شده

گروه	ویژگی‌ها	کاربرد
مبلغ	لگاریتم مبلغ؛ نسبت به میانگین پیشین فرستنده؛ نزدیک آستانه؛ بالای آستانه	ساختارشکنی
زمان	ساعت؛ شبانه (۲۲ تا ۶)	رفتار غیرعادی
سرعت	تعداد خروجی فرستنده و ورودی گیرنده در ۵ دقیقه، ۱ ساعت و ۲۴ ساعت؛ مجموع مبالغ ۲۴ ساعت	تجمع و پخش سریع
عبور وجه	مجموع و تعداد ورودی فرستنده در ۱ ساعت؛ نسبت ورودی به مبلغ خروجی	حساب واسط
تازگی و شبکه	طرف حساب جدید؛ تعداد جفت‌های جدید فرستنده و گیرنده در ۲۴ ساعت	اجاره حساب
زمینه	نوع حساب (تجاری/فردی)؛ کانال تراکنش	کنترل ساختار

مدل‌ها و تنظیمات

مدل‌های نظارت‌شده عبارت‌اند از رگرسیون لجستیک (مبنای خطی)، درخت تصمیم (عمق ۱۰)، جنگل تصادفی (۲۰۰ درخت) و گرادیان بوستینگ (۳۰۰ تکرار، نرخ یادگیری ۰٫۰۸). نامتوازنی کلاس‌ها با وزن‌دهی کلاس مدیریت شد و از نمونه‌برداری مجدد مانند SMOTE (Chawla et al, 2002) استفاده نشد تا توزیع واقعی داده حفظ شود. مدل‌های بدون نظارت، K-Means با ۸ خوشه (امتیاز: فاصله تا نزدیک‌ترین مرکز) و جنگل انزوا با ۲۰۰ درخت‌اند. سامانهٔ قاعده‌محور تراکنش را در چهار حالت هشدار می‌دهد: مبلغ بیش از آستانه؛ ۱۰ تراکنش خروجی

یا بیشتر در ۲۴ ساعت؛ ۱۲ ورودی یا بیشتر در ۲۴ ساعت؛ یا مبلغ ۸۵ تا ۱۰۰ درصد آستانه با دست‌کم ۲ تراکنش خروجی در ۲۴ ساعت.

نکتهٔ مهم دربارهٔ نام‌گذاری: کتابخانهٔ XGBoost در محیط اجرای پژوهش در دسترس نبود. به همین دلیل، نمایندهٔ خانوادهٔ XGBoost در اینجا گرادیان بوستینگ مبتنی بر هیستوگرام در کتابخانهٔ scikit-learn (Pedregosa et al, 2011) است که از همان خانوادهٔ درخت‌های تقویت‌شده با گرادیان بهره می‌برد. بنابراین هر نتیجه‌ای که برای «گرادیان بوستینگ» گزارش می‌شود، درباره XGBoost به‌طور مستقیم اثبات‌شده نیست و باید با آن کتابخانه نیز تکرار شود.

طرح ارزیابی

برای مشابهت با شرایط واقعی، تقسیم داده زمانی است: مدل با رویدادهای روز ۰ تا ۵۱ آموزش می‌بیند، آستانهٔ تصمیم (حداکثرکنندهٔ F1) روی روزهای ۵۲ تا ۶۲ تعیین می‌شود و ارزیابی نهایی فقط یک‌بار روی ۲۷ روز پایانی انجام می‌گیرد. کل فرایند با پنج بذر تصادفی مستقل تکرار شد. معیارها از ماتریس درهم‌ریختگی (TP، FP، FN و TN) به شرح روابط ۱ تا ۵ به دست می‌آیند. افزون بر آن، سطح زیر منحنی دقت-فراخوانی (PR-AUC) گزارش می‌شود، چون در داده نامتوازن آگاهی‌بخش‌تر از ROC است (Saito and Rehmsmeier, 2015)، و حجم هشدار به‌صورت رابطه ۶ تعریف می‌شود.

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

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

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

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

$$\text{MCC} = (TP \times TN - FP \times FN) / \sqrt{[(TP+FP)(TP+FN)(TN+FP)(TN+FN)]} \quad (5)$$

$$\text{Alert reduction} = (A_{rule} - A_{model}) / A_{rule}, \quad A = TP + FP \quad (6)$$

یافته‌ها

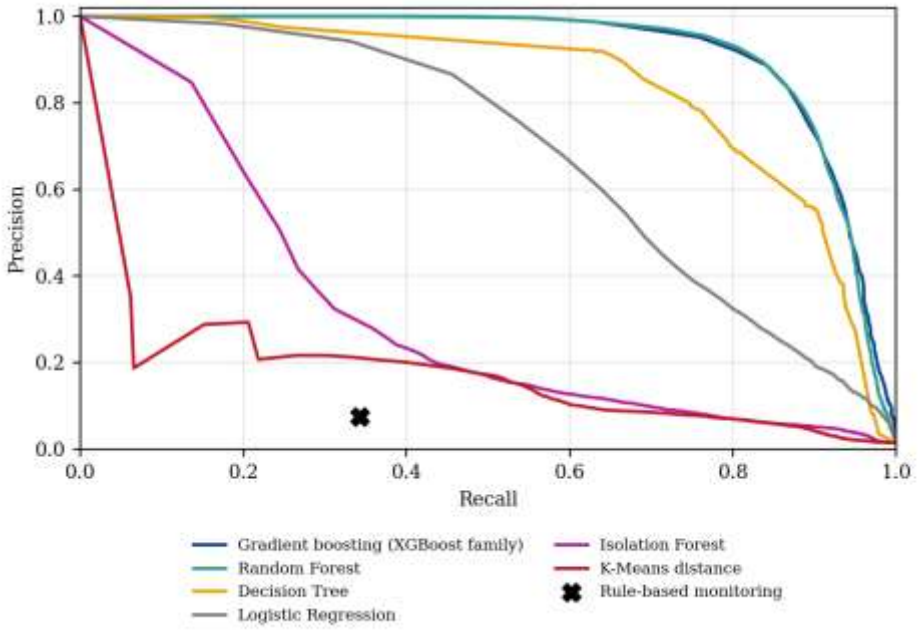
جدول ۳ نتایج اجرای اصلی را روی دادهٔ آزمون (۱۶۲٬۹۶۹ تراکنش که ۲٬۳۲۵ مورد آن مشکوک است) نشان می‌دهد. نخستین نکته، بی‌اعتباری صحت کلی (Accuracy) است: سامانه قاعده‌محور با صحت ۹۳٫۰ درصد کارنامهٔ قابل‌قبولی دارد، در حالی که تنها ۷٫۵ درصد هشدارهایش درست است و از هر ۱۰۰ مورد مشکوک فقط حدود ۳۴ مورد را می‌بیند. این پدیده نتیجهٔ نامتوازنی کلاس‌هاست و به همین دلیل معیار اصلی مقایسه، F1 و PR-AUC قرار گرفت.

جدول ۳: عملکرد مدل‌ها روی دادهٔ آزمون (اجرای اصلی)

مدل	صحت کلی	Precision	Recall	F1	PR-AUC	MCC
سامانه قاعده‌محور	۰٫۹۳۰	۰٫۰۷۵	۰٫۳۴۲	۰٫۱۲۳	—	۰٫۱۳۵
رگرسیون لجستیک	۰٫۹۹۱	۰٫۷۵۳	۰٫۵۴۱	۰٫۶۳۰	۰٫۶۸۶	۰٫۶۳۴
درخت تصمیم	۰٫۹۹۴	۰٫۷۸۱	۰٫۷۶۲	۰٫۷۷۱	۰٫۸۱۶	۰٫۷۶۸
جنگل تصادفی	۰٫۹۹۶	۰٫۸۹۱	۰٫۸۴۱	۰٫۸۶۵	۰٫۹۱۹	۰٫۸۶۴

مدل	صحت کلی	Precision	Recall	F1	PR-AUC	MCC
گرادیان بوستینگ	۰٫۹۹۶	۰٫۸۸۶	۰٫۸۴۲	۰٫۸۶۳	۰٫۹۲۱	۰٫۸۶۲
K-Means (بدون نظارت)	۰٫۹۶۹	۰٫۲۰۱	۰٫۳۹۵	۰٫۲۶۶	۰٫۱۶۵	۰٫۲۶۷
جنگل انزوا (بدون نظارت)	۰٫۹۸۵	۰٫۴۸۳	۰٫۲۴۹	۰٫۳۲۹	۰٫۳۱۸	۰٫۳۴۱

شکل ۱ منحنی دقت-فراخوانی همه مدل‌ها و نقطهٔ عملکرد سامانه قاعده‌محور را نشان می‌دهد. منحنی دو مدل جمعی تقریباً روی هم افتاده و بالاتر از درخت تصمیم و رگرسیون لجستیک قرار دارد؛ هر دو روش بدون نظارت پایین‌ترند و نقطهٔ سامانهٔ قاعده‌محور با Precision کمتر از ۰٫۱ در بخش پایین نمودار قرار دارد.



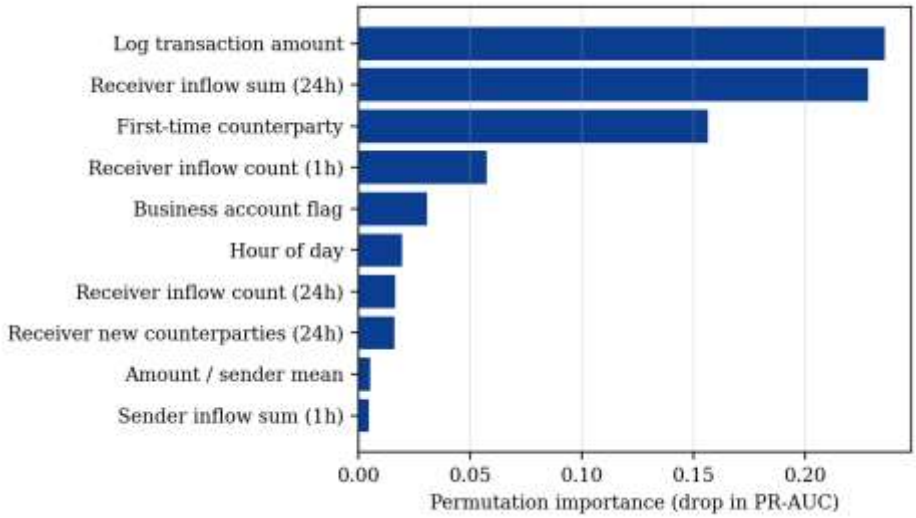
شکل ۱: منحنی دقت-فراخوانی مدل‌ها روی دادهٔ آزمون (اجرای اصلی؛ ▫ سامانه قاعده‌محور)

برای اینکه نتیجه به یک بذر خاص وابسته نباشد، کل فرایند پنج بار تکرار شد. جدول ۴ میانگین و انحراف معیار را نشان می‌دهد. ترتیب کلی گروه‌ها در همهٔ تکرارها یکسان بود (مدل‌های جمعی، سپس درخت تصمیم، رگرسیون لجستیک، روش‌های بدون نظارت و در پایان سامانهٔ قاعده‌محور). در مقایسهٔ زوجی (آزمون t وابسته با ۴ درجهٔ آزادی)، F1 گرادیان بوستینگ به‌طور میانگین ۰٫۷۲۹ واحد از سامانه قاعده‌محور بیشتر بود ($p < ۰٫۰۰۱$) و جنگل تصادفی نیز مشابه آن؛ بنابراین فرضیهٔ ۱ تأیید شد. PR-AUC هر دو مدل جمعی حدود ۰٫۰۹۶ واحد از درخت تصمیم بالاتر بود ($p < ۰٫۰۰۱$) و فرضیهٔ ۲ تأیید شد. فرضیهٔ ۳ نیز تأیید شد: میانگین PR-AUC روش‌های بدون نظارت (۰٫۱۹۰ و ۰٫۳۶۷) بسیار پایین‌تر از مدل‌های نظارت‌شده بود. اما نکتهٔ مهم این است که میان جنگل تصادفی و گرادیان بوستینگ تفاوت معناداری دیده نشد (PR-AUC: $p = ۰٫۷۸$؛ F1: $p = ۰٫۲۲$)؛ پس برتری قطعی یکی بر دیگری از این داده نتیجه نمی‌شود.

جدول ۴: میانگین ± انحراف معیار معیارها در پنج اجرای مستقل

مدل	Precision	Recall	F1	PR-AUC
سامانه قاعده‌محور	۰٫۰۸۳ ± ۰٫۰۰۸	۰٫۳۵۴ ± ۰٫۰۲۹	۰٫۱۳۵ ± ۰٫۰۱۲	—
رگرسیون لجستیک	۰٫۷۶۶ ± ۰٫۰۴۸	۰٫۶۰۲ ± ۰٫۰۳۷	۰٫۶۷۳ ± ۰٫۰۲۸	۰٫۷۲۸ ± ۰٫۰۳۱
درخت تصمیم	۰٫۸۰۴ ± ۰٫۰۶۴	۰٫۷۸۸ ± ۰٫۰۴۶	۰٫۷۹۴ ± ۰٫۰۲۰	۰٫۸۳۳ ± ۰٫۰۱۸
جنگل تصادفی	۰٫۸۹۹ ± ۰٫۰۳۴	۰٫۸۴۷ ± ۰٫۰۲۹	۰٫۸۷۱ ± ۰٫۰۰۸	۰٫۹۲۸ ± ۰٫۰۰۶
گرادیان بوستینگ	۰٫۹۱۰ ± ۰٫۰۳۶	۰٫۸۲۵ ± ۰٫۰۴۷	۰٫۸۶۴ ± ۰٫۰۱۵	۰٫۹۲۹ ± ۰٫۰۰۶
K-Means	۰٫۲۵۸ ± ۰٫۰۶۹	۰٫۴۰۳ ± ۰٫۰۹۵	۰٫۳۰۳ ± ۰٫۰۳۰	۰٫۱۹۰ ± ۰٫۰۲۱
جنگل انزوا	۰٫۴۳۶ ± ۰٫۰۷۶	۰٫۳۴۱ ± ۰٫۰۶۵	۰٫۳۷۷ ± ۰٫۰۵۲	۰٫۳۶۷ ± ۰٫۰۵۱

شکل ۲ اهمیت جایگشتی ویژگی‌ها را برای گرادیان بوستینگ نشان می‌دهد؛ یعنی هر ویژگی را در دادهٔ آزمون درهم می‌ریزیم و افت PR-AUC را اندازه می‌گیریم. لگاریتم مبلغ، مجموع ورودی گیرنده در ۲۴ ساعت و تازگی طرف حساب در صدر قرار دارند. دو نتیجه از اینجا برمی‌آید: ویژگی‌های «شبکه‌ای» ساده (ورودی گیرنده، طرف حساب جدید) بیش از ویژگی‌های زمانی در کشف الگوی حساب واسط سهم دارند و تنها نگاه به هر تراکنش به‌صورت جداگانه، بدون تاریخچهٔ حساب، کافی نیست. این یافته با ایده‌ای که پژوهش‌های گرافی برای حساب‌های واسط دنبال می‌کنند، هم‌خوان است (Huang, 2025).



شکل ۲: ده ویژگی با بیشترین اهمیت جایگشتی در مدل گرادیان بوستینگ

از نظر مدیریتی، جدول ۵ بار کاری را مقایسه می‌کند. سامانهٔ قاعده‌محور در پنجرهٔ آزمون ۱۰٬۶۶۲ هشدار صادر کرده که فقط ۷۹۶ مورد آن درست است؛ یعنی برای هر مورد مشکوک واقعی، به‌طور میانگین ۱۳٫۴ هشدار باید بررسی شود. در مدل گرادیان بوستینگ همین نسبت ۱٫۱۳ است. حجم هشدار حدود ۷۹ درصد (رابطه ۶) و تعداد هشدار کاذب حدود ۹۷ درصد کم شده، در حالی که تعداد موارد مشکوک کشف‌شده بیش از دو برابر است. اگر برای

بررسی هر هشدار ۲۰ دقیقه کار کارشناس در نظر بگیریم (فرضی و صرفاً برای نمایش مقیاس، نه اندازه‌گیری‌شده)، این تفاوت در پنجرهٔ ۲۷ روزهٔ آزمون حدود ۲٬۸۱۷ ساعت کار کارشناسی را آزاد می‌کند. در سنجش بهره‌وری، این همان دو بُعد کارایی (مصرف کمتر منابع) و اثربخشی (کشف بیشتر موارد واقعی) است که با هم بهبود یافته‌اند (فقیهی و موسوی‌کاشی، ۱۳۸۹).

جدول ۵: بار کاری و نتایج هشدار در دادهٔ آزمون (اجرای اصلی)

مدل	تعداد هشدار	هشدار درست (TP)	هشدار کاذب (FP)	مورد از دست‌رفته (FN)	هشدار به‌ازای هر مورد واقعی
سامانه قاعده‌محور	۱۰٬۶۶۲	۷۹۶	۹٬۸۶۶	۱٬۵۲۹	۱۳٫۴
جنگل تصادفی	۲٬۱۹۵	۱٬۹۵۵	۲۴۰	۳۷۰	۱٫۱۲
گرادیان بوستینگ	۲٬۲۱۱	۱٬۹۵۸	۲۵۳	۳۶۷	۱٫۱۳

بحث و نتیجه‌گیری

یافته‌ها در امتداد پژوهش‌های میدانی و بین‌المللی است. برتری مدل‌های نظارت‌شده بر نظام قاعده‌محور با گزارش جولوم و همکاران در بانکی بزرگ (Jullum et al, 2020) و بهبود هشدار کاذب در مطالعهٔ رایته و همکاران (Reite et al, 2024) هم‌جهت است و کاهش حجم هشدار در این پژوهش با نتیجهٔ هالفورد و همکاران همسو است (Halford et al, 2025)، اگرچه اندازهٔ آن در این‌جا بزرگ‌تر است؛ دلیل روشن آن، تمیزبودن ساختار داده شبیه‌سازی‌شده نسبت به محیط واقعی است، پس این عدد را باید حد بالای ممکن دانست نه پیش‌بینی عملیاتی. برابری عملی جنگل تصادفی و گرادیان بوستینگ با گزارش هاشمی و همکاران دربارهٔ رقابت نزدیک مدل‌های درختی جمعی هم‌خوان است (Hashemi et al, 2023) و نشان می‌دهد انتخاب بین این دو بیشتر به هزینهٔ اجرا و نگهداری وابسته است تا به دقت. ضعف روش‌های بدون نظارت، اگر به‌عنوان ابزار مستقل به کار روند، قابل‌پیش‌بینی بود؛ اما این نتیجه با نقش مکمل آن‌ها برای کشف الگوهای ناشناخته و بدون برچسب ناسازگار نیست (Chen et al, 2018; Sizan, 2025). یافتهٔ این پژوهش دربارهٔ اهمیت ویژگی‌های شبکه‌ای، مسیر استفاده از مدل‌های گرافی را برجسته می‌کند (Cheng et al, 2023; Luo et al, 2024). تفاوت اصلی کار حاضر با پژوهش‌هایی که بر دقت الگوریتم متمرکزند (Shafiee et al, 2025)، ترجمهٔ نتیجه به بار کاری و تصمیم مدیریتی است.

بر پایهٔ یافته‌ها، پیشنهادهای کاربردی زیر برای مدیران ارشد شبکهٔ بانکی و سیاست‌گذاران مالی ارائه می‌شود:

۱. استقرار پایش هوشمند به‌صورت «لایهٔ امتیازدهی» روی سامانهٔ قاعده‌محور موجود: به‌جای حذف قواعد فعلی، مدل امتیاز ریسک هشدارها را محاسبه کند و هشدارهای کم‌ریسک با نظارت نمونه‌ای بسته شوند؛ این مسیر با تجربهٔ عملیاتی گزارش‌شده سازگار است (Halford et al, 2025).

۲. نظارت ترکیبی (Human-in-the-loop): مدل لایهٔ اول غربالگری باشد و تصمیم نهایی، به‌ویژه برای مسدودسازی حساب مشتری و ارسال گزارش، با کارشناس باشد. بازخورد کارشناسان باید به‌صورت منظم به

آموزش مدل برگردد؛ این همان حافظه و یادگیری سازمانی است که به‌عنوان زمینهٔ مزیت رقابتی پایدار مطرح شده است (Camisón and Villar-López, 2011).

۳. تفسیرپذیری: برای هر هشدار «بسته» شواهد» (مهم‌ترین ویژگی‌های اثرگذار) در اختیار بازرس قرار گیرد؛ روش‌های توضیح‌پذیری مانند SHAP برای مدل‌های درختی مناسب‌اند (Lundberg and Lee, 2017) و کمبود این بخش در ادبیات، از ایرادهای اصلی گزارش‌شده است (Kute et al, 2021).

۴. پایش رانش مدل: چون مجرمان رفتار خود را تغییر می‌دهند، عملکرد مدل باید به‌صورت ماهانه روی داده جدید سنجیده و در صورت افت، بازآموزی یا یادگیری مداوم اجرا شود (Deprez et al, 2025).

۵. تبادل داده بین‌بانکی با رعایت حریم خصوصی: به‌جای پایگاه‌داده متمرکز، می‌توان از ساختارهای حافظ حریم خصوصی استفاده کرد؛ مدل‌های AML با داده محدود و محدودیت‌های مقرراتی روبه‌رو هستند (Fan et al, 2025).

۶. آموزش و آگاه‌سازی عمومی دربارهٔ پیامدهای حقوقی اجارهٔ حساب و کارت بانکی، با همکاری واحدهای حقوقی، فناوری اطلاعات و روابط عمومی بانک‌ها (بشیری و همکاران، ۱۴۰۰).

مهم‌ترین محدودیت این پژوهش، شبیه‌سازی‌بودن داده است. مدل‌ها بر الگوهایی آموزش دیدند که خود طراحی کرده‌ایم و بنابراین توان واقعی آن‌ها در برابر الگوهای ناشناخته ناپیدا است؛ برچسب‌گذاری واقعی بانکی نیز معمولاً ناقص و با تأخیر است. محدودیت دوم، استفاده از گرادیان بوستینگ هیستوگرامی به‌جای کتابخانه XGBoost است. محدودیت سوم، تعداد پایین تکرارها (پنج اجرا) است که تنها برای نتایج با اختلاف بزرگ اطمینان کافی می‌دهد. پژوهش‌های آینده می‌توانند با داده بانکی واقعی یا مجموعه‌های معیار مانند Elliptic (Weber et al, 2019)، مدل‌های گرافی، یادگیری مداوم و سنجش مستقیم هزینه و زمان بررسی هشدار، نتایج را تکمیل کنند.

منابع

منابع فارسی

بشیری، عارف؛ رضایی‌راد، عبدالحسین و دهکلانی، محمدمحسن (۱۴۰۰). شیوه‌های مقابله با اجاره حساب‌های بانکی از منظر حقوق و اقتصاد اسلامی. مطالعات اقتصاد اسلامی.

بهزاد، عباس (۱۳۹۷، ۲۵ بهمن). هشدار دادستان انتظامی مالیاتی درباره اجاره حساب‌های بانکی [مصاحبه]. خبرگزاری اطلاعات.

تجلی، سید آیت‌الله (۱۳۹۰). مبارزه با پولشویی و تأمین مالی تروریسم در بانک‌ها. تهران: آراد کتاب.

تذهیبی، فریده (۱۳۸۹). پولشویی و روش‌های مبارزه با آن. تهران: کمیته ایرانی اتاق بازرگانی بین‌المللی.

حافظ‌نیا، محمدرضا (۱۳۸۸). مقدمه‌ای بر روش تحقیق در علوم انسانی (چاپ شانزدهم). تهران: انتشارات سمت.

علوی، سیدمحمد (۱۳۹۳). مدیریت ریسک و فناوری‌های نوین در بانکداری. تهران: انتشارات سمت.

فقیهی، ابوالحسن و موسوی‌کاشی، زهره (۱۳۸۹). مدل سنجش بهره‌وری (اثربخشی و کارایی) در بخش خدمات دولتی ایران. مجله مدیریت دولتی، ۲(۴)، ۱۰۷–۱۲۶.

مجلس شورای اسلامی (۱۳۸۶، ۲ بهمن). قانون مبارزه با پولشویی (با اصلاحات ۳/۷/۱۳۹۷ و تأیید مجمع تشخیص مصلحت نظام در ۱۵/۱۰/۱۳۹۷).



نجمی‌نیا، رضا و صالحی، محمدرضا (۱۳۹۱، مهر). بررسی تأثیر سرمایه فکری در ایجاد مزیت رقابتی شرکت‌های بیمه استان اصفهان. چهارمین کنفرانس بین‌المللی بازاریابی خدمات بانکی، تهران: مرکز همایش‌های بین‌المللی صدا و سیما.

هیئت وزیران (۱۳۸۸، ۱۴ آذر). آیین‌نامه اجرایی قانون مبارزه با پولشویی (اصلاحی ۱۳۹۵).

English References

Altman, E., Blanuša, J., von Niederhäusern, L., Egressy, B., Anghel, A., & Atasu, K. (2023). Realistic synthetic financial transactions for anti-money laundering models. Advances in Neural Information Processing Systems (NeurIPS), Datasets and Benchmarks Track, 36.

Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. Statistical Science, 17(3), 235–255.

Breiman, L. (2001). Random forests. Machine Learning, 45(1), 5–32.

Camisón, C., & Villar-López, A. (2011). Non-technical innovation: Organizational memory and learning capabilities as antecedent factors with effects on sustained competitive advantage. Industrial Marketing Management, 40(8), 1294–1304.

Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic minority over-sampling technique. Journal of Artificial Intelligence Research, 16, 321–357.

Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 785–794.

Chen, Z., Van Khoa, L. D., Teoh, E. N., Nazir, A., Karuppiah, E. K., & Lam, K. S. (2018). Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: A review. Knowledge and Information Systems, 57(2), 245–285. https://doi.org/10.1007/s10115-017-1144-z

Cheng, D., et al. (2023). Anti-money laundering by group-aware deep graph learning. IEEE Transactions on Knowledge and Data Engineering.

Deprez, B., Wei, W., & Verbeke, W. (2025). Advances in continual graph learning for anti-money laundering systems: A comprehensive review. Wiley Interdisciplinary Reviews: Computational Statistics.

Fan, J., Shar, L. K., Zhang, R., Liu, Z., Yang, W., Niyato, D., Mao, B., & Lam, K.-Y. (2025). Deep learning approaches for anti-money laundering on mobile transactions: Review, framework, and directions. IEEE Internet of Things Journal.

Financial Action Task Force [FATF]. (2012, updated). International standards on combating money laundering and the financing of terrorism & proliferation: The FATF Recommendations. Paris: FATF/OECD.

Friedman, J. H. (2001). Greedy function approximation: A gradient boosting machine. The Annals of Statistics, 29(5), 1189–1232.

Halford, E., et al. (2025). Developing a scoring model for managing money laundering transactions using machine learning. Journal of Money Laundering Control.

Hashemi, S. K., et al. (2023). Fraud detection in banking data by machine learning techniques. IEEE Access.

Hazen, B. T., & Byrd, T. A. (2012). Toward creating competitive advantage with logistics information technology. International Journal of Physical Distribution & Logistics Management, 42(1), 8–35.

Huang, Z.-F. (2025). Enhancing anti-money laundering by money mules detection on transaction graphs. Proceedings of the 2025 International Conference on Generative Artificial Intelligence for Business.

Ileberi, E., Sun, Y., & Wang, Z. (2021). Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost. IEEE Access, 9.

Irshad, F., et al. (2024). GCF-MLD: Integrated approach for money laundering detection using machine learning and graph network analysis. IEEE Access.

Jullum, M., Løland, A., Huseby, R. B., Ånonsen, G., & Lorentzen, J. (2020). Detecting money laundering transactions with machine learning. Journal of Money Laundering Control, 23(1), 173–186.

Ke, G., Meng, Q., Finley, T., Wang, T., Chen, W., Ma, W., Ye, Q., & Liu, T.-Y. (2017). LightGBM: A highly efficient gradient boosting decision tree. Advances in Neural Information Processing Systems, 30, 3146–3154.

Kute, D. V., Pradhan, B., Shukla, N., & Alamri, A. (2021). Deep learning and explainable artificial intelligence techniques applied for detecting money laundering: A critical review. IEEE Access, 9, 82300–82317.

Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2008). Isolation forest. Proceedings of the 2008 Eighth IEEE International Conference on Data Mining, 413–422.

Lloyd, S. P. (1982). Least squares quantization in PCM. IEEE Transactions on Information Theory, 28(2), 129–137.

Lundberg, S. M., & Lee, S.-I. (2017). A unified approach to interpreting model predictions. Advances in Neural Information Processing Systems, 30, 4765–4774.

Luo, X., et al. (2024). MLaD²: A semi-supervised money laundering detection framework based on decoupling training. IEEE Transactions on Information Forensics and Security.

Ma, C., et al. (2026). Credit card fraud detection under extreme class imbalance using leakage-safe feature selection and GA-based hyperparameter optimization. Applied Sciences.

Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., et al. (2011). Scikit-learn: Machine learning in Python. Journal of Machine Learning Research, 12, 2825–2830.

Reite, E. J., et al. (2024). Improving client risk classification with machine learning to increase anti-money laundering detection efficiency. Journal of Money Laundering Control.

Saito, T., & Rehmsmeier, M. (2015). The precision-recall plot is more informative than the ROC plot when evaluating binary classifiers on imbalanced datasets. PLoS ONE, 10(3), e0118432.

Shafiee, S., Estilaiee, M., & Dastyar, S. A. R. (2025). Applying a learning and an artificial intelligence-based framework for fraud detection in anti-money laundering. IEEE. https://doi.org/10.1109/CFIS68949.2025.11652311

Sizan, M. M. H. (2025). Machine learning-based unsupervised ensemble approach for detecting new money laundering typologies in transaction graphs. International Journal of Applied Mathematics.

Weber, M., Domeniconi, G., Chen, J., Weidele, D. K. I., Bellei, C., Robinson, T., & Leiserson, C. E. (2019). Anti-money laundering in Bitcoin: Experimenting with graph convolutional networks for financial forensics. arXiv:1908.02591.



Machine Learning and Intelligent Monitoring for Detecting Suspicious Transactions and Combating Money Laundering in the Era of Digital Banking

Abstract

Rule-based anti-money laundering (AML) systems, which rely on fixed amount and frequency thresholds, struggle with the volume and complexity of digital banking transactions: they generate large numbers of false alerts and miss multi-layer schemes such as rented bank accounts. This applied, quantitative-experimental study compares four supervised models (logistic regression, decision tree, random forest and gradient boosting from the XGBoost family) and two unsupervised methods (K-Means and isolation forest) with a rule-based system on simulated transaction data (about 540,000 transactions over 90 days, roughly 1.5% suspicious; structuring, money-mule pass-through and layering chains). Evaluation is chronological (training on early days, testing on the final 27 days), uses imbalance-aware metrics and is repeated over five independent runs. The rule-based system reached a mean F1 of about 0.135, with more than 91% of its alerts being false. Random forest and gradient boosting reached F1 of about 0.86-0.87 and PR-AUC of about 0.93, with no significant difference between them, whereas unsupervised methods were clearly weaker as stand-alone tools. In the main run, alert volume fell by about 79% and false alerts by about 97%. The findings support a human-in-the-loop scoring layer, explainability and model-drift monitoring. All figures come from simulated data and must be validated on real bank data before generalisation.

Keywords: Anti-money laundering, Machine learning, Suspicious transaction detection, Digital banking, Intelligent monitoring