Journal of
Intelligent Financial
Management Perspectives

Design of a Real-Time Financial Fraud Detection System Based on Transformer Architecture in Banking Transactions

Ali Akbari Ghaleh [1]*, Mehdi Ahmadinia [2]

[1] *Ph.D. in Financial Management, University of Shiraz, Shiraz, Iran(Coresponding autour), Email: aliakbarighale@gmail.com*
[2] *M.A. in Financial Management, University of Shiraz, Shiraz, Iran*

ARTICLE INFO

Article history:
Received:09/04/2025
Received in revised form:30/04/2025
Accepted:11/05/2025
Available online:15/06/2025

Keywords:

Financial Fraud Detection
Transformer Architecture
Deep Learning
Banking Transactions
Digital Banking

ABSTRACT

The rapid expansion of digital banking, online payment systems, and electronic financial services has significantly increased the complexity and diversity of financial fraud patterns within banking networks. Traditional fraud detection methods are primarily rule-based and rely on classical statistical techniques, which often fail to identify sophisticated and dynamic fraudulent behaviors. This study aims to design a real-time financial fraud detection system based on Transformer architecture for banking transactions. By leveraging the multi-head attention mechanism and the capability of capturing long-term temporal dependencies, the proposed model is able to identify suspicious transactions with high accuracy and efficiency. The dataset consists of simulated banking transactions generated according to realistic patterns observed in the Iranian banking system during the period 2021–2025. After data preprocessing, feature extraction, and normalization, the Transformer model was trained and evaluated against benchmark machine learning models including Random Forest, Recurrent Neural Networks, and XGBoost. The empirical findings indicate that the proposed Transformer-based framework outperforms comparative models in terms of accuracy, fraud detection rate, F1-score, and reduction of Type II errors. Moreover, the model demonstrates a strong capability in detecting complex sequential fraud behaviors and abnormal transaction patterns in real-time environments. The results suggest that Transformer architecture can serve as an intelligent, scalable, and efficient solution for financial supervision, banking risk management, and anti-fraud systems.

Article Type: Research Paper

Journal of Intelligent Financial Management, 2025, Vol. 1, No.1, pp. 1- 16

Publish by:
Tolou-e Binish-e Ayandeh Scientific Institute

https://doi.org/ 10.25843/JIFM.2025.8563.21584

Cite: Akbari Ghaleh,A. and Ahmadinia,M. (2025). Design of a Real-Time Financial Fraud Detection System Based on Transformer Architecture in Banking Transactions. *Journal of Intelligent Financial Management*, *1*(1), 1-16.

نگرش های
مدیریت مالی هوشمند
Journal of Intelligent Financial Management Perspectives

طراحی سیستم کشف تقلب مالی بلادرنگ مبتنی بر معماری ترنسفورمر در تراکنش‌های بانکی

علی اکبری قلعه [1 و *]، مهدی احمدی‌نیا [2]

۱ و *-دکتری مدیریت مالی، دانشگاه شیراز، شیراز، ایران(نویسنده مسئول)، ایمیل نویسنده مسئول:*Aliakbarighale@gmail.com*

۲-کارشناسی ارشد مدیریت مالی، دانشگاه شیراز، شیراز، ایران

اطلاعات مقاله

تاریخچه مقاله:

تاریخ دریافت:۱۴۰۴/۰۱/۲۰

تاریخ بازنگری:۱۴۰۴/۰۲/۱۰

تاریخ پذیرش:۱۴۰۴/۰۲/۲۱

تاریخ انتشار:۱۴۰۴/۰۳/۲۵

کلیدواژه‌ها:

کشف تقلب مالی

معماری ترنسفورمر

یادگیری عمیق

تراکنش بانکی

بانکداری دیجیتال

چکیده

افزایش شتابان بانکداری دیجیتال، توسعه پرداخت‌های الکترونیکی و رشد خدمات مالی برخط، موجب افزایش پیچیدگی و تنوع الگوهای تقلب مالی در شبکه بانکی شده است. روش‌های سنتی کشف تقلب عمدتاً مبتنی بر قواعد ایستا و مدل‌های آماری کلاسیک هستند که در مواجهه با رفتارهای پیچیده و پویای متقلبانه کارایی محدودی دارند. پژوهش حاضر با هدف طراحی یک سیستم کشف تقلب مالی بلادرنگ مبتنی بر معماری ترنسفورمر در تراکنش‌های بانکی انجام شده است. در این پژوهش، با بهره‌گیری از سازوکار توجه چندسری و قابلیت استخراج وابستگی‌های زمانی بلندمدت، مدلی هوشمند جهت شناسایی تراکنش‌های مشکوک طراحی شد. داده‌های پژوهش شامل مجموعه‌ای از تراکنش‌های بانکی شبیه‌سازی‌شده مبتنی بر الگوهای واقعی شبکه بانکی ایران طی دوره ۱۴۰۰ تا ۱۴۰۴ است. پس از مرحله پاک‌سازی، استخراج ویژگی و نرمال‌سازی داده‌ها، مدل ترنسفورمر آموزش داده شد و عملکرد آن با مدل‌های جنگل تصادفی، شبکه عصبی بازگشتی و XGBoost مقایسه گردید. یافته‌های پژوهش نشان می‌دهد مدل پیشنهادی در معیارهای دقت، نرخ کشف تقلب، امتیاز F1 و کاهش خطای نوع دوم عملکرد بهتری نسبت به مدل‌های مقایسه‌ای دارد. همچنین مدل ترنسفورمر توانسته است الگوهای پیچیده تقلب زنجیره‌ای و رفتارهای غیرعادی را در محیط بلادرنگ با سرعت و دقت بالا شناسایی کند. نتایج پژوهش بیانگر آن است که استفاده از معماری ترنسفورمر می‌تواند به ارتقای سامانه‌های مدیریت ریسک و نظارت مالی در صنعت بانکداری کشور کمک کند.

نشریه مدیریت مالی هوشمند، ۱۴۰۴، دوره ۱، شماره ۱، صفحه ۱-۱۶.

ناشر: موسسه علمی طلوع بینش آینده

https://doi.org/ 10.25843/JIFM.2025.8563.21584

نوع مقاله: پژوهشی

استناد: اکبری قلعه، علی و احمدی نیا مهدی.(۱۴۰۴). طراحی سیستم کشف تقلب مالی بلادرنگ مبتنی بر معماری ترنسفورمر در تراکنش‌های بانکی .*مدیریت مالی هوشمند*، (۱)۱، ۱-۱۶.

۱-مقدمه

گسترش روزافزون فناوری‌های مالی و تحول دیجیتال در صنعت بانکداری طی دهه اخیر، ساختار سنتی ارائه خدمات مالی را به‌صورت بنیادین دگرگون کرده است. توسعه بانکداری الکترونیکی، افزایش استفاده از سامانه‌های پرداخت برخط، گسترش کیف‌پول‌های دیجیتال و رشد زیرساخت‌های پرداخت هوشمند، موجب افزایش چشمگیر حجم تراکنش‌های مالی در سطح جهانی شده است. این تحولات اگرچه موجب افزایش سرعت، سهولت و کارایی خدمات مالی شده‌اند، اما هم‌زمان بستر مناسبی را برای شکل‌گیری الگوهای پیچیده‌تر تقلب مالی فراهم ساخته‌اند. در بسیاری از کشورها، تقلب مالی به یکی از مهم‌ترین چالش‌های نظام بانکی تبدیل شده و خسارات گسترده‌ای را به مؤسسات مالی، بانک‌ها و مشتریان تحمیل کرده است. بر اساس گزارش انجمن بررسی‌کنندگان تقلب رسمی، سازمان‌های مالی سالانه بخش قابل‌توجهی از درآمد خود را به دلیل فعالیت‌های متقلبانه از دست می‌دهند که این مسئله اهمیت توسعه سامانه‌های هوشمند کشف تقلب را دوچندان کرده است (Association of Certified Fraud Examiners, 2022). در ایران نیز هم‌زمان با رشد بانکداری دیجیتال و توسعه زیرساخت‌های شاپرک، تعداد تراکنش‌های بانکی و پرداخت‌های الکترونیکی با رشد قابل‌توجهی همراه بوده است. افزایش تعداد کاربران خدمات بانکی آنلاین، توسعه اپلیکیشن‌های پرداخت و افزایش استفاده از خدمات غیرحضوری، موجب شده است که شبکه بانکی کشور در معرض تهدیدات پیچیده‌تری قرار گیرد. مجرمان مالی با استفاده از فناوری‌های نوین، ضعف‌های موجود در سامانه‌های نظارتی سنتی را هدف قرار داده و از خلأهای امنیتی برای انجام تراکنش‌های غیرمجاز، جعل هویت، پول‌شویی و سوءاستفاده مالی استفاده می‌کنند. در چنین شرایطی، استفاده از روش‌های سنتی مبتنی بر قواعد ایستا و نظارت انسانی، دیگر پاسخگوی پیچیدگی الگوهای نوین تقلب نیست و نظام بانکی نیازمند بهره‌گیری از فناوری‌های پیشرفته تحلیل داده و هوش مصنوعی است (Ngai et al., 2011).

سامانه‌های سنتی کشف تقلب عمدتاً مبتنی بر قواعد از پیش تعریف‌شده و الگوهای رفتاری ثابت هستند. این سامانه‌ها معمولاً با استفاده از آستانه‌های مشخص، رفتارهای مشکوک را شناسایی می‌کنند. اگرچه این روش‌ها در شناسایی برخی الگوهای ساده تقلب عملکرد مناسبی دارند، اما در مواجهه با رفتارهای پویا و پیچیده، دچار ضعف می‌شوند. مهم‌ترین محدودیت این سامانه‌ها، وابستگی شدید آن‌ها به دانش قبلی و عدم توانایی در شناسایی الگوهای ناشناخته است. علاوه بر این، توسعه مداوم تکنیک‌های تقلب باعث می‌شود قواعد ثابت به‌سرعت کارایی خود را از دست بدهند و نرخ خطای سیستم افزایش یابد. از سوی دیگر، افزایش حجم تراکنش‌های بانکی باعث شده است که تحلیل دستی یا نیمه‌خودکار داده‌ها عملاً غیرممکن شود(Bolton & Hand, 2002) . در سال‌های اخیر، پیشرفت‌های قابل‌توجه در حوزه یادگیری ماشین و یادگیری عمیق، افق‌های جدیدی را برای تحلیل داده‌های مالی و کشف تقلب ایجاد کرده است. الگوریتم‌های یادگیری ماشین قادرند با تحلیل حجم عظیمی از داده‌ها، الگوهای پنهان و رفتارهای غیرعادی را شناسایی کنند. استفاده از مدل‌هایی نظیر درخت تصمیم، جنگل تصادفی، ماشین بردار پشتیبان و شبکه‌های عصبی موجب افزایش دقت سیستم‌های کشف تقلب شده است. این مدل‌ها برخلاف روش‌های سنتی، توانایی یادگیری الگوهای پیچیده را از داده‌ها دارند و می‌توانند با تغییر رفتار متقلبان سازگار شوند. با این حال، بسیاری از مدل‌های یادگیری ماشین کلاسیک در تحلیل روابط زمانی و وابستگی‌های بلندمدت میان تراکنش‌ها محدودیت دارند و در مواجهه با داده‌های ترتیبی پیچیده، عملکرد مطلوبی ارائه نمی‌کنند (Bhattacharyya et al., 2011). اما توسعه یادگیری عمیق و شبکه‌های عصبی پیشرفته، زمینه استفاده از مدل‌های پیچیده‌تر در تحلیل داده‌های مالی را فراهم کرده است. شبکه‌های عصبی بازگشتی و مدل‌های حافظه بلندمدت[1] از جمله روش‌هایی هستند که برای تحلیل داده‌های ترتیبی مورد استفاده قرار گرفته‌اند. این مدل‌ها توانایی مناسبی در استخراج الگوهای زمانی دارند، اما به دلیل ساختار بازگشتی، معمولاً با مشکلاتی نظیر کاهش گرادیان، زمان پردازش بالا و محدودیت در پردازش موازی مواجه‌اند. علاوه بر این، در حجم بالای داده‌های بانکی و محیط‌های بلادرنگ، سرعت پردازش و مقیاس‌پذیری این مدل‌ها به یکی از چالش‌های اصلی تبدیل می‌شود(Hochreiter & Schmidhuber, 1997).

در این میان، معماری ترنسفورمر به‌عنوان یکی از مهم‌ترین نوآوری‌های حوزه یادگیری عمیق، توجه گسترده پژوهشگران را به خود جلب کرده است. معماری ترنسفورمر نخستین‌بار توسط Vaswani و همکاران معرفی شد و بر پایه سازوکار توجه یا Attention Mechanism طراحی گردید. برخلاف مدل‌های بازگشتی، ترنسفورمر قادر است وابستگی‌های کوتاه‌مدت و بلندمدت را به‌صورت هم‌زمان تحلیل کند و تمامی داده‌های

[1] LSTM

ورودی را به‌طور موازی پردازش نماید. این ویژگی موجب افزایش چشمگیر سرعت پردازش، بهبود مقیاس‌پذیری و ارتقای دقت مدل در تحلیل داده‌های پیچیده می‌شود (Vaswani et al., 2017).

سازوکار توجه در معماری ترنسفورمر این امکان را فراهم می‌کند که مدل بتواند مهم‌ترین بخش‌های داده را شناسایی کرده و بر روابط معنادار میان تراکنش‌ها تمرکز کند. در حوزه مالی، بسیاری از رفتارهای متقلبانه به‌صورت زنجیره‌ای و وابسته به زمان رخ می‌دهند و شناسایی آن‌ها نیازمند تحلیل دقیق روابط میان تراکنش‌ها است. معماری ترنسفورمر به دلیل توانایی در مدل‌سازی این وابستگی‌ها، ظرفیت بالایی برای کاربرد در سامانه‌های کشف تقلب مالی دارد. پژوهش‌های اخیر نشان داده‌اند که مدل‌های مبتنی بر Transformer در تحلیل رفتار مشتریان، پیش‌بینی ریسک اعتباری و شناسایی تراکنش‌های مشکوک عملکرد بسیار مطلوبی دارند (Khan et al., 2021) .یکی از مهم‌ترین ویژگی‌های سامانه‌های نوین کشف تقلب، قابلیت پردازش بلادرنگ داده‌ها است. در محیط‌های مالی، زمان واکنش سیستم اهمیت بسیار بالایی دارد، زیرا تأخیر در شناسایی تراکنش‌های متقلبانه می‌تواند خسارات جبران‌ناپذیری ایجاد کند. سامانه‌های بلادرنگ باید بتوانند میلیون‌ها تراکنش را در کسری از ثانیه تحلیل کرده و رفتارهای مشکوک را شناسایی کنند. این مسئله نیازمند مدل‌هایی است که علاوه بر دقت بالا، از سرعت پردازش و مقیاس‌پذیری مناسبی نیز برخوردار باشند. معماری ترنسفورمر به دلیل قابلیت پردازش موازی و تحلیل هم‌زمان داده‌ها، گزینه‌ای مناسب برای طراحی سامانه‌های کشف تقلب بلادرنگ محسوب می‌شود(Zhang et al., 2022) . با وجود رشد سریع مطالعات بین‌المللی در حوزه کاربرد هوش مصنوعی در کشف تقلب مالی، در ادبیات پژوهشی ایران همچنان خلأ محسوسی در زمینه استفاده از معماری‌های پیشرفته یادگیری عمیق، به‌ویژه ترنسفورمر، مشاهده می‌شود. بخش عمده مطالعات داخلی بر روش‌های سنتی یا مدل‌های کلاسیک یادگیری ماشین متمرکز بوده و کمتر به توسعه سامانه‌های بلادرنگ مبتنی بر تحلیل عمیق داده‌های تراکنشی پرداخته شده است. از سوی دیگر، ویژگی‌های خاص شبکه بانکی ایران، از جمله حجم بالای تراکنش‌های خرد، تنوع ابزارهای پرداخت و پیچیدگی الگوهای رفتاری مشتریان، ضرورت طراحی مدل‌های بومی و هوشمند را افزایش داده است. پژوهش حاضر با هدف طراحی سیستم کشف تقلب مالی بلادرنگ مبتنی بر معماری ترنسفورمر در تراکنش‌های بانکی انجام شده است. این پژوهش تلاش می‌کند با بهره‌گیری از قابلیت‌های یادگیری عمیق و سازوکار توجه، مدلی کارآمد برای شناسایی رفتارهای غیرعادی و تراکنش‌های متقلبانه ارائه دهد. نوآوری اصلی پژوهش در استفاده از معماری ترنسفورمر برای تحلیل ترتیبی تراکنش‌های بانکی و ترکیب آن با ساختار پردازش بلادرنگ است. انتظار می‌رود نتایج این پژوهش بتواند علاوه بر ارتقای دانش نظری در حوزه مدیریت مالی و فناوری مالی، کاربردهای عملی مهمی برای بانک‌ها، مؤسسات مالی و نهادهای نظارتی کشور فراهم سازد. همچنین یافته‌های این پژوهش می‌تواند زمینه توسعه سامانه‌های هوشمند ضدتقلب و ارتقای امنیت مالی در شبکه بانکی ایران را فراهم کند.

۲- مبانی نظری و پیشینه پژوهش

۲ تقلب مالی در نظام بانکی به مجموعه‌ای از رفتارها و اقدامات عمدی اطلاق می‌شود که با هدف کسب منفعت غیرقانونی از طریق فریب، دستکاری اطلاعات، سوءاستفاده از زیرساخت‌های مالی و نقض مقررات بانکی انجام می‌گیرد.(Delamaire, Abdou, & Pointon, 2009) . این پدیده یکی از مهم‌ترین تهدیدهای پیش‌روی نظام‌های مالی و اقتصادی جهان به شمار می‌رود؛ زیرا علاوه بر تحمیل خسارت‌های مالی مستقیم به بانک‌ها و مشتریان، موجب تضعیف اعتماد عمومی به نظام بانکی، کاهش امنیت اقتصادی و اختلال در جریان سالم مبادلات مالی می‌شود Ngai) (et al., 2011. تقلب مالی می‌تواند در اشکال متنوعی نظیر تراکنش‌های غیرمجاز، جعل اسناد و هویت، سوءاستفاده از کارت‌های بانکی، کلاهبرداری اینترنتی، پول‌شویی، اختلاس، دستکاری حساب‌ها، حملات سایبری مالی و سوءاستفاده از سامانه‌های پرداخت الکترونیکی ظاهر شود (Bolton & Hand, 2002).

در ادبیات مالی و اقتصادی، تقلب رفتاری تصادفی یا ناشی از خطای انسانی تلقی نمی‌شود، بلکه کنشی آگاهانه، هدفمند و مبتنی بر برنامه‌ریزی است که معمولاً در پاسخ به فرصت‌های ناشی از ضعف نظارت، ناکارآمدی کنترل‌های داخلی و خلأهای قانونی شکل می‌گیرد(Albrecht, Albrecht, & Albrecht, 2008). بر اساس نظریه «مثلث تقلب»، وقوع تقلب معمولاً حاصل ترکیب سه عامل اصلی یعنی فشار یا انگیزه مالی، وجود فرصت مناسب و توجیه‌پذیری رفتار متقلبانه است. (Cressey, 1953) هرچه ساختارهای نظارتی و کنترلی ضعیف‌تر باشند، فرصت برای ارتکاب تقلب افزایش می‌یابد و احتمال بروز رفتارهای فرصت‌طلبانه بیشتر می‌شود(Singleton & Singleton, 2010) . از منظر نظریه اقتصاد اطلاعات، تقلب مالی نتیجه مستقیم عدم تقارن اطلاعاتی میان بازیگران اقتصادی است. در چنین شرایطی، برخی افراد یا گروه‌ها به اطلاعات،

ابزارها یا دسترسی‌هایی دست می‌یابند که سایر بازیگران بازار یا نهادهای نظارتی از آن محروم‌اند. این عدم توازن اطلاعاتی، زمینه را برای سوءاستفاده و رفتارهای متقلبانه فراهم می‌کند. (Akerlof, 1970) برای مثال، مجرمان مالی ممکن است با بهره‌گیری از دانش فنی، ضعف سامانه‌های امنیتی یا دسترسی به اطلاعات محرمانه مشتریان، تراکنش‌هایی را انجام دهند که در ظاهر قانونی و عادی به نظر برسند، اما در واقع با هدف انتقال غیرقانونی منابع مالی طراحی شده‌اند(Levi & Burrows, 2008) .

با گسترش بانکداری الکترونیک و توسعه فناوری‌های مالی، ماهیت تقلب نیز پیچیده‌تر و چندلایه‌تر شده است .در نظام بانکی سنتی، بسیاری از تقلب‌ها محدود به جعل اسناد یا سوءاستفاده فیزیکی از حساب‌ها بود؛ اما در بانکداری مدرن، بخش عمده‌ای از تقلب‌ها در بستر دیجیتال و از طریق سامانه‌های برخط رخ می‌دهد. (Phua et al., 2010) ظهور خدماتی مانند بانکداری اینترنتی، پرداخت موبایلی، کیف پول‌های دیجیتال و تراکنش‌های برخط، اگرچه سرعت و سهولت خدمات مالی را افزایش داده‌اند، اما هم‌زمان سطح آسیب‌پذیری بانک‌ها را نیز گسترش داده‌اند (Kou et al., 2021). مجرمان سایبری امروزه با استفاده از روش‌هایی نظیر فیشینگ، بدافزارهای بانکی، حملات مهندسی اجتماعی و نفوذ به پایگاه‌های داده، قادرند اطلاعات حساس مشتریان را سرقت کرده و از آن‌ها برای انجام تراکنش‌های جعلی استفاده کنند (Button & Cross, 2017).

افزون بر این، پیچیدگی ابزارهای مالی و افزایش حجم و سرعت گردش اطلاعات موجب شده است که شناسایی رفتارهای متقلبانه دشوارتر از گذشته باشد(Bhattacharyya et al., 2011) . در بسیاری از موارد، تقلب‌ها به‌صورت زنجیره‌ای و در قالب شبکه‌ای از تراکنش‌های مرتبط انجام می‌شوند؛ به‌گونه‌ای که یک عملیات متقلبانه ممکن است شامل ده‌ها حساب، چندین مؤسسه مالی و تعداد زیادی تراکنش خرد باشد که در ظاهر مستقل‌اند، اما در واقع بخشی از یک الگوی سازمان‌یافته محسوب می‌شوند. (Kirkos, Spathis, & Manolopoulos, 2007) این ویژگی شبکه‌ای باعث می‌شود که روش‌های سنتی نظارت و تحلیل ایستا، توانایی کافی برای کشف الگوهای پنهان و روابط پیچیده میان تراکنش‌ها را نداشته باشند(Ngai et al., 2011) . در چنین شرایطی، استفاده از رویکردهای داده‌محور و هوشمند به ضرورتی اجتناب‌ناپذیر تبدیل شده است. بانک‌ها و مؤسسات مالی در سال‌های اخیر به‌طور گسترده از فناوری‌هایی مانند داده‌کاوی، یادگیری ماشین، هوش مصنوعی و تحلیل شبکه‌های پیچیده برای شناسایی رفتارهای مشکوک استفاده می‌کنند (Bahnsen et al., 2016) این فناوری‌ها قادرند با تحلیل حجم عظیمی از داده‌های تراکنشی، الگوهای غیرعادی و رفتارهای انحرافی را شناسایی کرده و پیش از وقوع خسارت گسترده، هشدارهای لازم را ارائه دهند.,Chen et al) (2018. برای مثال، الگوریتم‌های یادگیری ماشین می‌توانند با بررسی الگوهای رفتاری مشتریان، تراکنش‌هایی را که با رفتار معمول کاربر همخوانی ندارند شناسایی کرده و به‌عنوان تراکنش مشکوک علامت‌گذاری کنند(Pozzolo et al., 2015) . از سوی دیگر، مبارزه با تقلب مالی تنها به توسعه ابزارهای فناورانه محدود نمی‌شود، بلکه نیازمند ایجاد چارچوب‌های حقوقی، نظارتی و مدیریتی کارآمد نیز هست. (Reurink, 2018) تدوین مقررات ضدپول‌شویی، تقویت نظام احراز هویت دیجیتال، آموزش کاربران، افزایش شفافیت اطلاعات مالی و همکاری بین‌المللی میان بانک‌ها و نهادهای نظارتی از جمله اقداماتی است که می‌تواند نقش مؤثری در کاهش جرایم مالی ایفا کند. (FATF, 2020) همچنین، ارتقای فرهنگ امنیت سایبری در میان کاربران و کارکنان بانک‌ها می‌تواند احتمال موفقیت بسیاری از حملات مبتنی بر فریب انسانی را کاهش دهد(Wall, 2007) . در مجموع، تقلب مالی در نظام بانکی پدیده‌ای پویا، پیچیده و چندبعدی است که هم‌زمان ابعاد اقتصادی، فناورانه، حقوقی و رفتاری را در بر می‌گیرد (Dorminey et al., 2012) رشد سریع فناوری‌های مالی و دیجیتالی‌شدن خدمات بانکی، اگرچه فرصت‌های گسترده‌ای برای توسعه اقتصادی ایجاد کرده است، اما در مقابل، زمینه ظهور الگوهای نوین تقلب را نیز فراهم ساخته است. (Kou et al., 2021) ازاین‌رو، مقابله مؤثر با این پدیده مستلزم بهره‌گیری از فناوری‌های هوشمند، تقویت زیرساخت‌های نظارتی و توسعه سیاست‌های پیشگیرانه‌ای است که بتوانند همگام با تحول مداوم روش‌های تقلب، امنیت و سلامت نظام بانکی را تضمین کنند (West & Bhattacharya, 2016).

۲-۲ روش‌های سنتی کشف تقلب

روش‌های سنتی کشف تقلب در نظام بانکی عمدتاً بر پایه قواعد از پیش تعریف‌شده، مدل‌های آماری کلاسیک و سیستم‌های خبره طراحی شده‌اند. این روش‌ها نخستین نسل سامانه‌های تشخیص تقلب را تشکیل می‌دهند و برای سال‌ها به‌عنوان ابزار اصلی شناسایی فعالیت‌های مالی مشکوک در بانک‌ها و مؤسسات مالی مورد استفاده قرار گرفته‌اند. (Bolton & Hand, 2002) در این رویکردها، کارشناسان حوزه مالی و امنیت بانکی مجموعه‌ای از قوانین و شاخص‌ها را تعریف می‌کنند که بر اساس آن‌ها رفتارهای غیرعادی یا مشکوک شناسایی می‌شود. برای مثال، اگر مبلغ یک تراکنش از حد مشخصی بیشتر باشد، تعداد تراکنش‌های انجام‌شده در بازه زمانی کوتاه به‌طور غیرمعمول افزایش یابد، یا محل جغرافیایی

تراکنش با الگوی معمول مشتری سازگار نباشد، سامانه هشدار صادر کرده و تراکنش به‌عنوان مورد مشکوک علامت‌گذاری می‌شود (Phua et al., 2010). سیستم‌های مبتنی بر قواعد از رایج‌ترین روش‌های سنتی کشف تقلب محسوب می‌شوند. در این سیستم‌ها، قوانین به‌صورت «اگر–آنگاه» تعریف می‌شوند و هر تراکنش بر اساس این قوانین ارزیابی می‌گردد. برای نمونه، قانونی ممکن است تعیین کند که اگر برداشت وجه در مدت کوتاهی از چند موقعیت جغرافیایی مختلف انجام شود، احتمال سوءاستفاده از کارت بانکی وجود دارد. مزیت اصلی این روش‌ها سادگی، شفافیت و قابلیت تفسیر بالای آن‌هاست؛ به‌گونه‌ای که تحلیلگران بانکی می‌توانند به‌راحتی منطق تصمیم‌گیری سیستم را درک و بررسی کنند (Ngai et al., 2011). علاوه بر این، پیاده‌سازی این روش‌ها نسبتاً کم‌هزینه بوده و در محیط‌هایی که حجم داده محدود است عملکرد قابل قبولی دارند. در کنار سیستم‌های مبتنی بر قواعد، روش‌های آماری نیز نقش مهمی در کشف تقلب ایفا کرده‌اند. این روش‌ها معمولاً بر تحلیل الگوهای رفتاری مشتریان و شناسایی انحراف از رفتار عادی تمرکز دارند. تکنیک‌هایی مانند تحلیل رگرسیون، مدل‌های احتمالاتی، آزمون‌های ناهنجاری و تحلیل خوشه‌بندی از جمله ابزارهای آماری مورد استفاده در این حوزه هستند. (Bhattacharyya et al., 2011) در این رویکرد، رفتار معمول هر مشتری یا گروهی از مشتریان مدل‌سازی می‌شود و هرگونه انحراف معنادار از الگوی عادی به‌عنوان رفتار مشکوک در نظر گرفته می‌شود. به‌عنوان مثال، اگر مشتری‌ای که معمولاً تراکنش‌های کوچک و محلی انجام می‌دهد ناگهان اقدام به انتقال مبلغی کلان به حسابی خارجی کند، سامانه آماری آن را به‌عنوان یک ناهنجاری شناسایی می‌کند. سیستم‌های خبره نیز از دیگر رویکردهای سنتی کشف تقلب به شمار می‌روند. این سیستم‌ها بر پایه دانش و تجربه کارشناسان انسانی طراحی می‌شوند و تلاش می‌کنند فرآیند تصمیم‌گیری متخصصان را شبیه‌سازی کنند .در این سامانه‌ها، پایگاه دانش شامل مجموعه‌ای از قوانین، تجربیات و سناریوهای تقلب است که به موتور استنتاج اجازه می‌دهد وضعیت تراکنش‌ها را ارزیابی کند. اگرچه سیستم‌های خبره در دوره‌ای تحول بزرگی در نظارت مالی ایجاد کردند، اما محدودیت آن‌ها در یادگیری خودکار و وابستگی شدید به دانش انسانی، موجب کاهش کارایی آن‌ها در محیط‌های پیچیده و متغیر شده است(West & Bhattacharya, 2016) . با وجود کاربرد گسترده این روش‌ها در مراحل اولیه توسعه نظام‌های بانکی، افزایش پیچیدگی رفتارهای مالی و ظهور تقلب‌های هوشمند باعث شده است که کارایی آن‌ها به‌تدریج کاهش یابد. یکی از مهم‌ترین محدودیت‌های روش‌های سنتی، وابستگی شدید آن‌ها به دانش قبلی و قواعد ثابت است. (Bolton & Hand, 2002) از آنجا که مجرمان مالی به‌طور مداوم روش‌های خود را تغییر می‌دهند و از فناوری‌های نوین برای پنهان‌سازی فعالیت‌های خود استفاده می‌کنند، قوانین از پیش تعریف‌شده به‌سرعت منسوخ می‌شوند و نیازمند بازنگری و به‌روزرسانی مداوم هستند. این فرآیند نه‌تنها زمان‌بر است، بلکه هزینه‌های عملیاتی بالایی نیز به بانک‌ها تحمیل می‌کند. یکی دیگر از چالش‌های مهم روش‌های سنتی، نرخ بالای هشدارهای اشتباه یا «مثبت کاذب» است. در بسیاری از موارد، سامانه‌های مبتنی بر قواعد تراکنش‌های سالم را نیز به‌عنوان مشکوک شناسایی می‌کنند که این مسئله موجب افزایش بار کاری تحلیلگران انسانی و کاهش رضایت مشتریان می‌شود. (Bahnsen et al., 2016) برای مثال، ممکن است یک مشتری در سفر خارجی اقدام به خریدی غیرمعمول کند و سیستم به اشتباه کارت او را مسدود نماید. افزایش مثبت‌های کاذب علاوه بر هزینه‌های مالی، می‌تواند اعتماد مشتریان به خدمات بانکی را نیز کاهش دهد. علاوه بر این، روش‌های سنتی معمولاً توانایی تحلیل روابط پیچیده و وابستگی‌های چندلایه میان تراکنش‌ها را ندارند و اغلب هر تراکنش را به‌صورت مستقل بررسی می‌کنند. (Kirkos, Spathis, & Manolopoulos, 2007) در حالی که در واقعیت، بسیاری از تقلب‌های مالی در قالب زنجیره‌ای از تراکنش‌های مرتبط و وابسته به زمان رخ می‌دهند. برای نمونه، عملیات پول‌شویی معمولاً شامل مجموعه‌ای از تراکنش‌های کوچک و پراکنده است که به‌تنهایی طبیعی به نظر می‌رسند، اما در کنار یکدیگر الگویی سازمان‌یافته را تشکیل می‌دهند. روش‌های سنتی به دلیل ناتوانی در تحلیل ساختارهای شبکه‌ای و توالی زمانی داده‌ها، قادر به شناسایی چنین الگوهای پیچیده‌ای نیستند(Chen et al., 2018) . از سوی دیگر، رشد سریع حجم داده‌های مالی و توسعه بانکداری دیجیتال محدودیت‌های روش‌های سنتی را آشکارتر کرده است. امروزه بانک‌ها روزانه میلیون‌ها تراکنش را پردازش می‌کنند و تحلیل دستی یا مبتنی بر قواعد ثابت برای چنین حجم عظیمی از داده‌ها عملاً امکان‌پذیر نیست .(Ngai et al., 2011) روش‌های آماری کلاسیک نیز در مواجهه با داده‌های بزرگ، غیرخطی و با ابعاد بالا عملکرد محدودی دارند؛ زیرا این مدل‌ها معمولاً مبتنی بر فرضیات ساده‌ای درباره توزیع داده‌ها هستند که در محیط‌های واقعی مالی همواره برقرار.

۲-۳ یادگیری ماشین و کشف تقلب

یادگیری ماشین به‌عنوان یکی از مهم‌ترین شاخه‌های هوش مصنوعی، رویکردی داده‌محور برای حل مسائل طبقه‌بندی، پیش‌بینی و تصمیم‌گیری ارائه می‌دهد که در آن سیستم‌ها بدون نیاز به برنامه‌نویسی صریح، از داده‌ها الگوها و روابط پنهان را یاد می‌گیرند. (Mitchell, 1997) برخلاف روش‌های سنتی که مبتنی بر قواعد از پیش تعریف‌شده هستند، الگوریتم‌های یادگیری ماشین قادرند با تحلیل حجم عظیمی از داده‌ها، رفتارهای پیچیده و غیرخطی را شناسایی کرده و بر اساس تجربه حاصل از داده‌های گذشته، عملکرد خود را بهبود دهند .این ویژگی باعث شده است که یادگیری ماشین به یکی از مؤثرترین ابزارها در حوزه کشف تقلب مالی و امنیت بانکی تبدیل شود. در حوزه کشف تقلب مالی، هدف اصلی الگوریتم‌های یادگیری ماشین، یادگیری تابع یا مدلی است که بتواند تراکنش‌های سالم را از تراکنش‌های مشکوک تفکیک کند. (Ngai et al., 2011)این مدل‌ها معمولاً با استفاده از داده‌های تاریخی شامل تراکنش‌های عادی و متقلبانه آموزش می‌بینند و سپس قادر خواهند بود الگوهای رفتاری مرتبط با تقلب را در داده‌های جدید شناسایی کنند. مزیت اصلی این رویکرد، توانایی مدل در کشف روابط پیچیده و پنهانی است که توسط روش‌های سنتی یا تحلیل انسانی قابل شناسایی نیستند.

الگوریتم‌های مختلفی در یادگیری ماشین برای کشف تقلب مورد استفاده قرار می‌گیرند که هرکدام ویژگی‌ها و مزایای خاص خود را دارند. یکی از پرکاربردترین این الگوریتم‌ها، درخت تصمیم است. درخت تصمیم با تقسیم داده‌ها بر اساس ویژگی‌های مختلف، ساختاری سلسله‌مراتبی ایجاد می‌کند که در آن هر گره نمایانگر یک شرط تصمیم‌گیری است (Quinlan, 1986) .این مدل‌ها به دلیل سادگی و قابلیت تفسیر بالا، در سیستم‌های بانکی بسیار مورد توجه قرار گرفته‌اند؛ زیرا تحلیلگران می‌توانند فرآیند تصمیم‌گیری مدل را به‌صورت شفاف مشاهده و بررسی کنند. جنگل تصادفی نسخه پیشرفته‌تری از درخت تصمیم محسوب می‌شود که از ترکیب مجموعه‌ای از درخت‌های تصمیم برای بهبود دقت و کاهش خطا استفاده می‌کند. (Breiman, 2001) در این روش، هر درخت بر روی بخشی تصادفی از داده‌ها آموزش می‌بینند و نتیجه نهایی از طریق تجمیع خروجی تمام درخت‌ها تعیین می‌شود. این ساختار باعث کاهش واریانس مدل و افزایش پایداری پیش‌بینی می‌شود. جنگل تصادفی به دلیل مقاومت در برابر نویز داده‌ها و توانایی بالا در تحلیل روابط غیرخطی، یکی از موفق‌ترین روش‌ها در شناسایی تقلب مالی به شمار می‌رود. ماشین بردار پشتیبان نیز از دیگر الگوریتم‌های مهم در حوزه کشف تقلب است. این الگوریتم تلاش می‌کند مرزی بهینه میان داده‌های سالم و متقلب ایجاد کند، به‌گونه‌ای که فاصله میان دو کلاس بیشینه شود(Cortes & Vapnik, 1995) . مزیت اصلی این روش، عملکرد مناسب آن در داده‌های پیچیده و با ابعاد بالا است. با این حال، هزینه محاسباتی زیاد و دشواری تنظیم پارامترها، استفاده از آن را در داده‌های بسیار بزرگ محدود می‌کند.

روش‌های مبتنی بر گرادیان بوستینگ مانند XGBoost و LightGBM نیز در سال‌های اخیر کاربرد گسترده‌ای در کشف تقلب پیدا کرده‌اند. این مدل‌ها با ترکیب مجموعه‌ای از مدل‌های ضعیف و بهینه‌سازی تدریجی خطاها، عملکرد بسیار دقیقی در طبقه‌بندی داده‌ها ارائه می‌دهند (Chen & Guestrin, 2016). یکی از دلایل محبوبیت این الگوریتم‌ها در صنعت مالی، توانایی آن‌ها در مدیریت داده‌های حجیم، ویژگی‌های پیچیده و داده‌های نامتوازن است؛ زیرا در مسائل کشف تقلب معمولاً تعداد تراکنش‌های متقلبانه نسبت به تراکنش‌های سالم بسیار کمتر است. اگرچه الگوریتم‌های کلاسیک یادگیری ماشین نسبت به روش‌های سنتی دقت بسیار بالاتری دارند، اما همچنان با چالش‌های مهمی روبه‌رو هستند. یکی از اساسی‌ترین این چالش‌ها، ناتوانی بسیاری از این مدل‌ها در تحلیل وابستگی‌های زمانی و ترتیبی داده‌ها است. (Bhattacharyya et al., 2011)داده‌های تراکنشی ذاتاً ماهیتی زمانی دارند و رفتار مشتریان در طول زمان تغییر می‌کند. برای مثال، توالی تراکنش‌ها، زمان انجام پرداخت‌ها، فاصله میان تراکنش‌ها و تغییرات تدریجی رفتار مشتری می‌توانند اطلاعات ارزشمندی درباره احتمال وقوع تقلب ارائه دهند. با این حال، بسیاری از الگوریتم‌های کلاسیک مانند درخت تصمیم یا ماشین بردار پشتیبان فرض می‌کنند که داده‌ها مستقل از یکدیگر هستند و ترتیب زمانی آن‌ها اهمیتی ندارد. این فرض در عمل موجب از دست رفتن بخش مهمی از اطلاعات رفتاری می‌شود.علاوه بر وابستگی زمانی، رفتارهای متقلبانه معمولاً پویا و تطبیق‌پذیر هستند. مجرمان مالی به‌طور مداوم روش‌های خود را تغییر می‌دهند تا از شناسایی توسط سامانه‌های امنیتی جلوگیری کنند. در نتیجه، مدل‌هایی که تنها بر الگوهای گذشته تکیه دارند ممکن است در برابر تقلب‌های جدید عملکرد ضعیفی داشته باشند (Phua et al., 2010). این مسئله که با عنوان تغییر مفهوم شناخته می‌شود، یکی از چالش‌های مهم در طراحی سامانه‌های کشف تقلب است.

در سال‌های اخیر، توسعه یادگیری عمیق تلاش کرده است بخشی از این محدودیت‌ها را برطرف کند. مدل‌های یادگیری عمیق مانند شبکه‌های عصبی بازگشتی، حافظه بلندمدت کوتاه‌مدت و شبکه‌های مبتنی بر توجه قادرند وابستگی‌های زمانی و ترتیبی داده‌ها را تحلیل کنند و الگوهای

رفتاری پیچیده را با دقت بیشتری بیاموزند (Goodfellow et al., 2016) .این مدل‌ها می‌توانند توالی تراکنش‌های مشتری را به‌عنوان یک دنباله زمانی تحلیل کرده و تغییرات غیرعادی در رفتار مالی را شناسایی کنند. برای مثال، اگر مشتری‌ای که معمولاً تراکنش‌های روزانه کوچک انجام می‌دهد ناگهان در بازه زمانی کوتاه چندین انتقال مالی بزرگ و غیرمعمول داشته باشد، مدل‌های مبتنی بر LSTM قادرند این تغییر رفتاری را تشخیص دهند. علاوه بر این، ترکیب یادگیری ماشین با فناوری‌های کلان‌داده و پردازش بلادرنگ، امکان تحلیل میلیون‌ها تراکنش را در زمان واقعی فراهم کرده است .(Kou et al., 2021) این قابلیت برای بانک‌ها و مؤسسات مالی اهمیت حیاتی دارد؛ زیرا تأخیر در شناسایی تقلب می‌تواند خسارت‌های مالی سنگینی ایجاد کند. سامانه‌های مدرن کشف تقلب امروزه از مدل‌های یادگیری ماشین برای تحلیل لحظه‌ای داده‌ها، رتبه‌بندی میزان ریسک تراکنش‌ها و صدور هشدارهای خودکار استفاده می‌کنند.

۲-٤ معماری ترنسفورمر

معماری ترنسفورمر یکی از مهم‌ترین نوآوری‌های یادگیری عمیق در سال‌های اخیر است که بر پایه مکانیزم توجه طراحی شده و نخستین بار توسط واسوانی و همکاران معرفی شد. (Vaswani et al., 2017) این معماری در ابتدا برای مسائل پردازش زبان طبیعی توسعه یافت، اما به‌دلیل قدرت بالای آن در مدل‌سازی وابستگی‌های پیچیده، به‌سرعت در حوزه‌های مختلف از جمله بینایی ماشین، تحلیل سری‌های زمانی و کشف تقلب مالی نیز مورد استفاده قرار گرفت(Goodfellow et al., 2016) . برخلاف شبکه‌های عصبی بازگشتی و مدل‌های مبتنی بر حافظه کوتاه‌مدت و بلندمدت، ترنسفورمرها از ساختارهای ترتیبی و وابستگی‌های گام‌به‌گام صرف‌نظر کرده و امکان پردازش موازی داده‌ها را فراهم می‌کنند . (Vaswani et al., 2017)این ویژگی موجب افزایش چشمگیر سرعت آموزش و کاهش محدودیت‌های محاسباتی در مقایسه با مدل‌های ترتیبی سنتی می‌شود. در نتیجه، ترنسفورمرها به‌ویژه در مواجهه با داده‌های حجیم و پیچیده، عملکرد بسیار کارآمدی از خود نشان می‌دهند (Khan et al., 2021). هسته اصلی این معماری، مکانیزم Self-Attention است که به مدل اجازه می‌دهد میزان اهمیت هر بخش از ورودی را نسبت به سایر بخش‌ها به‌صورت پویا تعیین کند. در این فرآیند، هر ورودی به سه بردار کلیدی یعنیQuery ، Keyو Value تبدیل می‌شود. سپس شباهت میان Query و Key محاسبه شده و بر اساس آن وزن‌های توجه تعیین می‌گردد. در نهایت، خروجی مدل به‌صورت ترکیبی وزن‌دار از Value ها تولید می‌شود که شامل اطلاعات معنایی و ساختاری غنی از داده است (Vaswani et al., 2017) .این مکانیزم باعث می‌شود مدل بتواند روابط پیچیده و غیرمستقیم میان عناصر مختلف داده را شناسایی کند، حتی اگر این عناصر در فاصله‌های زمانی یا ساختاری دور از یکدیگر قرار داشته باشند.یکی از مهم‌ترین مزایای ترنسفورمرها، توانایی آن‌ها در مدل‌سازی وابستگی‌های بلندمدت است. در بسیاری از مسائل دنباله‌ای، از جمله تحلیل تراکنش‌های مالی، رفتار کاربران در طول زمان شکل می‌گیرد و ممکن است نشانه‌های تقلب در فاصله‌های زمانی طولانی و به‌صورت پراکنده ظاهر شوند (West & Bhattacharya, 2016) مدل‌های سنتی مانند RNN در مواجهه با این نوع وابستگی‌های بلندمدت دچار مشکل «فراموشی گرادیان» می‌شوند، اما ترنسفورمرها با استفاده از مکانیزم توجه این محدودیت را برطرف می‌کنند و امکان تحلیل هم‌زمان تمامی عناصر دنباله را فراهم می‌سازند (Khan et al., 2021). در حوزه کشف تقلب مالی، این ویژگی اهمیت ویژه‌ای دارد؛ زیرا رفتارهای متقلبانه معمولاً در قالب الگوهای پراکنده، غیرخطی و وابسته به زمان ظاهر می‌شوند. برای مثال، ممکن است یک تراکنش کوچک در ابتدای زنجیره به‌تنهایی طبیعی به نظر برسد، اما در ترکیب با چند تراکنش دیگر در بازه‌های زمانی مختلف، نشانه‌ای از یک الگوی پول‌شویی یا سوءاستفاده مالی باشد.

۲-۵ پیشینه پژوهش

کشف تقلب مالی یکی از مهم‌ترین مسائل در حوزه بانکداری الکترونیک، تجارت الکترونیک و سامانه‌های پرداخت دیجیتال محسوب می‌شود. با گسترش خدمات بانکی آنلاین، افزایش حجم تراکنش‌های مالی و توسعه پرداخت‌های لحظه‌ای، روش‌های سنتی کنترل و نظارت مالی دیگر پاسخگوی پیچیدگی الگوهای تقلب نیستند. به همین دلیل، طی سال‌های اخیر پژوهشگران تلاش گسترده‌ای برای توسعه سیستم‌های هوشمند کشف تقلب مبتنی بر داده‌کاوی، یادگیری ماشین و یادگیری عمیق انجام داده‌اند(Bolton & Hand, 2002) .در مراحل اولیه، بیشتر تحقیقات بر روش‌های آماری کلاسیک مانند رگرسیون لجستیک، تحلیل خوشه‌بندی، مدل‌های مبتنی بر قوانین و تحلیل ناهنجاری متمرکز بودند. این روش‌ها در تشخیص الگوهای ساده و ایستا عملکرد مناسبی داشتند، اما در برابر حجم عظیم داده‌های تراکنشی و تغییر مداوم رفتار متقلبان کارایی

محدودی نشان می‌دادند (Phua et al., 2010) .بولتون و هاند (۲۰۰۲) در یکی از جامع‌ترین مطالعات مروری حوزه کشف تقلب بیان کردند که سیستم‌های سنتی قادر به شناسایی الگوهای پیچیده و پویا نیستند و برای مقابله با رفتارهای متغیر متقلبانه، استفاده از روش‌های هوشمند ضروری است.با پیشرفت روش‌های داده‌کاوی، استفاده از الگوریتم‌های یادگیری ماشین مانند درخت تصمیم، جنگل تصادفی، ماشین بردار پشتیبان، شبکه‌های بیزین و KNN در تشخیص تقلب گسترش یافت. بهاتاچاریا و همکاران (۲۰۱۱) نشان دادند که الگوریتم‌های داده‌کاوی می‌توانند دقت مناسبی در شناسایی تقلب کارت اعتباری ایجاد کنند، اما مشکل اصلی این روش‌ها، عدم توازن شدید داده‌ها و نرخ بالای خطای مثبت کاذب بود. دل پوئتا و همکاران (۲۰۱۵) نیز بیان کردند که الگوریتم‌های سنتی در مواجهه با داده‌های حجیم و بلادرنگ با کاهش سرعت و افت دقت مواجه می‌شوند.

در ادامه، پژوهشگران به سمت استفاده از روش‌های یادگیری عمیق حرکت کردند. شبکه‌های عصبی مصنوعی چندلایه توانستند الگوهای پیچیده‌تری را نسبت به روش‌های کلاسیک استخراج کنند (West & Bhattacharya, 2016) .بااین‌حال، مهم‌ترین تحول در این حوزه، استفاده از شبکه‌های عصبی بازگشتی و مدل‌های حافظه بلندمدت کوتاه‌مدت بود. مدل LSTM که توسط Hochreiter و Schmidhuber (1997) معرفی شد، به دلیل توانایی در تحلیل داده‌های ترتیبی و وابستگی زمانی تراکنش‌ها، به‌طور گسترده در سیستم‌های کشف تقلب مالی مورد استفاده قرار گرفت. جی و همکاران (۲۰۱۹) نشان دادند که مدل‌های مبتنی بر LSTM نسبت به الگوریتم‌های سنتی دقت بیشتری در تحلیل رفتار کاربران و تشخیص تراکنش‌های مشکوک دارند.

با وجود مزایایLSTM ، این مدل‌ها دارای محدودیت‌هایی نظیر هزینه محاسباتی بالا، دشواری پردازش موازی و کاهش کارایی در توالی‌های طولانی هستند (Bengio et al., 1994) این محدودیت‌ها باعث شد پژوهشگران به دنبال معماری‌های پیشرفته‌تر برای تحلیل داده‌های ترتیبی باشند. در این راستا، معماری ترنسفورمر که توسط Vaswani و همکاران (۲۰۱۷) معرفی شد، تحول چشمگیری در حوزه یادگیری عمیق ایجاد کرد. این معماری با استفاده از مکانیزم توجه قادر است وابستگی‌های بلندمدت میان داده‌ها را بدون نیاز به ساختار بازگشتی تحلیل کند. همچنین قابلیت پردازش موازی در ترنسفورمر موجب افزایش سرعت آموزش و کارایی آن در داده‌های حجیم شده است.پس از موفقیت ترنسفورمرها در حوزه پردازش زبان طبیعی، پژوهشگران کاربرد این معماری را در تحلیل داده‌های مالی و کشف تقلب بررسی کردند. فیورینی و همکاران (۲۰۲۱) نشان دادند که مدل‌های مبتنی بر Self-Attention توانایی بالایی در شناسایی الگوهای پنهان در تراکنش‌های مالی دارند. همچنین زانک و همکاران (۲۰۲۲) در مطالعه‌ای درباره کشف تقلب بلادرنگ بیان کردند که مدل‌های ترنسفورمر نسبت به شبکه‌های بازگشتی، دقت بالاتر و نرخ هشدار کاذب پایین‌تری ارائه می‌دهند. نتایج پژوهش آن‌ها نشان داد که معماری ترنسفورمر می‌تواند روابط پیچیده میان تراکنش‌ها و رفتار کاربران را بهتر از مدل‌های سنتی شناسایی کند.

علاوه بر این، برخی مطالعات جدید از ترکیب ترنسفورمر با روش‌های تشخیص ناهنجاری، یادگیری گراف و یادگیری تقویتی استفاده کرده‌اند. دو و لیو (۲۰۲۳) نشان دادند که ترکیب Graph Neural Network و Transformer موجب افزایش دقت کشف تقلب در شبکه‌های بانکی می‌شود. همچنین چن و همکاران (۲۰۲۳) بیان کردند که استفاده از مدل‌های هیبریدی مبتنی بر ترنسفورمر در محیط‌های بلادرنگ، توانایی تشخیص حملات پیچیده و چندمرحله‌ای را بهبود می‌بخشد.در حوزه سامانه‌های بلادرنگ، سرعت پردازش و زمان پاسخ از عوامل بسیار مهم محسوب می‌شوند. پژوهش‌های اخیر نشان داده‌اند که استفاده از چارچوب‌های پردازش جریانی مانند Apache Kafka و Apache Flink در کنار مدل‌های یادگیری عمیق می‌تواند امکان تحلیل تراکنش‌ها در زمان واقعی را فراهم کند .(Kreps et al., 2011) همچنین برخی پژوهش‌ها بر استفاده از معماری‌های ابری و توزیع‌شده برای افزایش مقیاس‌پذیری سیستم‌های کشف تقلب تمرکز داشته‌اند(Carcillo et al., 2021) .در ادبیات پژوهشی ایران نیز مطالعات متعددی در زمینه کشف تقلب بانکی انجام شده است، اما اغلب این پژوهش‌ها بر روش‌های کلاسیک یادگیری ماشین یا شبکه‌های عصبی ساده تمرکز داشته‌اند. برای مثال، احمدی و همکاران (۱۳۹۸) از الگوریتم درخت تصمیم برای شناسایی تراکنش‌های مشکوک استفاده کردند و رضایی و همکاران (۱۴۰۰) عملکرد شبکه عصبی مصنوعی را در کشف تقلب کارت بانکی بررسی نمودند. بااین‌حال، استفاده از معماری ترنسفورمر در تحلیل تراکنش‌های بانکی کشور هنوز بسیار محدود است و پژوهش جامعی درباره کشف تقلب مالی بلادرنگ مبتنی بر ترنسفورمر در بستر بانکداری ایران مشاهده نمی‌شود.بررسی مطالعات پیشین نشان می‌دهد که اگرچه روش‌های یادگیری عمیق پیشرفت قابل‌توجهی در کشف تقلب ایجاد کرده‌اند، اما همچنان چالش‌هایی مانند عدم توازن داده‌ها، نیاز به پردازش بلادرنگ، پیچیدگی الگوهای متقلبانه

و مقیاس‌پذیری سیستم‌ها وجود دارد. ازاین‌رو، طراحی یک سیستم کشف تقلب مالی بلادرنگ مبتنی بر معماری ترنسفورمر می‌تواند با بهره‌گیری از قابلیت تحلیل توالی‌ها، پردازش موازی و یادگیری وابستگی‌های پیچیده، راهکاری مؤثر برای ارتقای امنیت سامانه‌های بانکی و کاهش خسارات ناشی از تقلب مالی ارائه دهد.

۳- روش‌شناسی پژوهش

پژوهش حاضر از نظر هدف در زمره پژوهش‌های کاربردی قرار می‌گیرد، زیرا به دنبال ارائه یک راهکار عملی برای حل مسئله واقعی در نظام بانکی یعنی کشف تقلب مالی است. از نظر ماهیت و روش، این پژوهش دارای رویکرد کمی بوده و مبتنی بر تحلیل داده‌های عددی و الگوریتم‌های یادگیری ماشین و یادگیری عمیق است. در این چارچوب، تلاش شده است تا با استفاده از داده‌های تراکنشی بانکی و بهره‌گیری از معماری ترنسفورمر، یک مدل هوشمند برای شناسایی تراکنش‌های مشکوک طراحی و ارزیابی شود. منطق حاکم بر پژوهش بر پایه یادگیری از داده‌های گذشته و تعمیم الگوهای رفتاری به آینده است، به‌گونه‌ای که مدل بتواند روابط پیچیده میان ویژگی‌های تراکنش‌ها را استخراج کرده و رفتارهای غیرعادی را شناسایی کند. این پژوهش از منظر روش اجرا، در چارچوب مدل‌سازی داده‌محور و شبیه‌سازی رفتاری قرار می‌گیرد و به‌دلیل ماهیت داده‌ها، از تکنیک‌های پیش‌پردازش، نرمال‌سازی و طبقه‌بندی استفاده شده است. همچنین برای ارزیابی عملکرد مدل، از معیارهای استاندارد ارزیابی در مسائل طبقه‌بندی نامتوازن استفاده شده است تا دقت، حساسیت و کارایی مدل به‌صورت جامع بررسی شود.

۳-۱ داده‌های پژوهش

داده‌های مورد استفاده در این پژوهش شامل مجموعه‌ای از تراکنش‌های بانکی شبیه‌سازی‌شده هستند که بر اساس الگوهای رفتاری واقعی در شبکه بانکی ایران طراحی شده‌اند. هدف از استفاده از داده‌های شبیه‌سازی‌شده، حفظ محرمانگی اطلاعات بانکی و در عین حال نزدیک‌سازی ساختار داده‌ها به واقعیت عملیاتی نظام بانکی بوده است. این داده‌ها شامل ویژگی‌های متنوعی از تراکنش‌ها هستند که هر یک نقش مهمی در تحلیل رفتار مالی کاربران دارند. از جمله این ویژگی‌ها می‌توان به مبلغ تراکنش اشاره کرد که نشان‌دهنده شدت و ارزش مالی فعالیت است. زمان تراکنش نیز به‌عنوان یک متغیر کلیدی در تحلیل الگوهای زمانی و شناسایی رفتارهای غیرعادی مورد استفاده قرار می‌گیرد. موقعیت جغرافیایی تراکنش‌ها امکان تحلیل رفتار مکانی مشتریان را فراهم می‌کند و در شناسایی جابه‌جایی‌های غیرمنطقی یا مشکوک نقش مهمی دارد. نوع پذیرنده نیز نشان‌دهنده ماهیت کسب‌وکار یا مقصد تراکنش است که می‌تواند در تشخیص الگوهای غیرعادی مؤثر باشد. علاوه بر این، فاصله زمانی میان تراکنش‌ها و تعداد تراکنش‌های انجام‌شده توسط هر مشتری در یک بازه زمانی مشخص، اطلاعات مهمی درباره رفتارهای تکرارشونده یا غیرطبیعی ارائه می‌دهد. در نهایت، ویژگی‌های رفتاری مشتریان که از ترکیب متغیرهای مختلف استخراج شده‌اند، نقش کلیدی در مدل‌سازی الگوهای پیچیده ایفا می‌کنند. در مجموع، این پایگاه داده شامل پنج میلیون رکورد تراکنش است که حدود ۳.۲ درصد آن‌ها به‌عنوان تراکنش‌های متقلبانه برچسب‌گذاری شده‌اند. این عدم توازن کلاس‌ها چالش مهمی در فرآیند مدل‌سازی ایجاد می‌کند و نیازمند استفاده از روش‌های پیشرفته یادگیری ماشین است.

۳-۲ پیش‌پردازش داده‌ها

پیش‌پردازش داده‌ها یکی از مراحل اساسی در فرآیند تحلیل داده‌های مالی محسوب می‌شود، زیرا کیفیت داده‌ها تأثیر مستقیمی بر عملکرد مدل‌های یادگیری ماشین دارد. در این پژوهش، ابتدا داده‌های ناقص و رکوردهایی که دارای مقادیر گمشده بودند شناسایی و حذف شدند تا از ایجاد نویز در فرآیند یادگیری جلوگیری شود. سپس داده‌های پرت که می‌توانستند موجب انحراف در یادگیری مدل شوند، با استفاده از روش‌های آماری اصلاح یا تعدیل شدند. در ادامه، برای جلوگیری از تأثیر مقیاس‌های متفاوت ویژگی‌ها بر عملکرد مدل، فرآیند نرمال‌سازی داده‌ها انجام شد تا تمامی متغیرها در یک بازه عددی یکسان قرار گیرند و امکان همگرایی بهتر مدل فراهم شود. علاوه بر این، ویژگی‌های رفتاری از داده‌های خام استخراج شدند که شامل شاخص‌هایی مانند میانگین مبلغ تراکنش، انحراف معیار تراکنش‌ها، الگوی زمانی تراکنش‌ها و رفتار تکرارشونده کاربران است. این ویژگی‌ها نقش مهمی در افزایش قدرت تفکیک مدل میان تراکنش‌های سالم و مشکوک دارند. در نهایت، داده‌ها به دو مجموعه آموزش و آزمون تقسیم شدند تا امکان ارزیابی دقیق عملکرد مدل فراهم شود. این مرحله از اهمیت بالایی برخوردار است، زیرا هرگونه ضعف در پیش‌پردازش می‌تواند منجر به کاهش دقت مدل و افزایش خطای طبقه‌بندی شود.

۳-۳ طراحی مدل

مدل پیشنهادی در این پژوهش بر پایه معماری ترنسفورمر طراحی شده است که یکی از پیشرفته‌ترین ساختارهای یادگیری عمیق برای تحلیل داده‌های ترتیبی محسوب می‌شود. این مدل شامل چندین بخش کلیدی است که هر یک نقش مشخصی در فرآیند یادگیری دارند. در ابتدا، داده‌های ورودی وارد لایه Embedding می‌شوند تا ویژگی‌های خام به بردارهای عددی قابل فهم برای شبکه عصبی تبدیل شوند. سپس لایه Positional Encodingبه مدل اضافه می‌شود تا اطلاعات مربوط به ترتیب زمانی تراکنش‌ها حفظ گردد، زیرا در معماری ترنسفورمر به‌صورت ذاتی ترتیب داده‌ها در نظر گرفته نمی‌شود. پس از آن، داده‌ها واردEncoder های ترنسفورمر می‌شوند که وظیفه اصلی استخراج روابط پیچیده میان تراکنش‌ها را بر عهده دارند. در این بخش، مکانیزم Attention به مدل اجازه می‌دهد تا اهمیت نسبی هر تراکنش را نسبت به سایر تراکنش‌ها تعیین کند و وابستگی‌های بلندمدت را شناسایی نماید. در ادامه، خروجیEncoder ها به لایه Attention نهایی منتقل می‌شود تا تمرکز مدل بر مهم‌ترین ویژگی‌های رفتاری افزایش یابد. در نهایت، لایه طبقه‌بند نهایی وظیفه دارد بر اساس نمایش‌های یادگرفته‌شده، تراکنش‌ها را به دو دسته سالم و مشکوک طبقه‌بندی کند. تابع زیان مدل نیز بر اساس معیار آنتروپی متقاطع تعریف شده است که در مسائل طبقه‌بندی دودویی به‌طور گسترده مورد استفاده قرار می‌گیرد و هدف آن کمینه‌سازی اختلاف میان برچسب‌های واقعی و پیش‌بینی‌شده مدل است. این تابع به‌صورت زیر تعریف می‌شود:

$$\text{Loss} = -\sum(y_i \log(\hat{y}_i))$$

این ساختار باعث می‌شود مدل بتواند به‌صورت تدریجی خطای خود را کاهش داده و به الگوهای پیچیده موجود در داده‌ها نزدیک‌تر شود.

٤-یافته‌ها و نتایج پژوهش

یافته‌های این پژوهش حاصل اجرای مدل پیشنهادی مبتنی بر معماری ترنسفورمر بر روی مجموعه داده تراکنش‌های بانکی شبیه‌سازی‌شده است. هدف اصلی در این بخش، ارزیابی عملکرد مدل در شناسایی تراکنش‌های متقلبانه و مقایسه آن با مدل‌های رایج یادگیری ماشین و یادگیری عمیق است. برای این منظور، داده‌ها به دو بخش آموزش (۷۰ درصد) و آزمون (۳۰ درصد) تقسیم شدند و مدل‌ها بر اساس داده‌های آزمون مورد ارزیابی قرار گرفتند. از آنجا که مسئله کشف تقلب یک مسئله به‌شدت نامتوازن است، معیارهای ارزیابی صرفاً به دقت (Accuracy) محدود نشده و شاخص‌هایی مانند دقت مثبت(Precision) ، یادآوری(Recall) ، معیار F1 و سطح زیر منحنی ROC-AUC نیز مورد استفاده قرار گرفته‌اند تا عملکرد مدل‌ها به‌صورت جامع بررسی شود. در ابتدا، عملکرد مدل ترنسفورمر با سه مدل پایه شامل جنگل تصادفی (Random Forest)، XGBoostو شبکه عصبی بازگشتی مقایسه شد. نتایج نشان داد که مدل پیشنهادی در تمامی معیارهای ارزیابی عملکرد بهتری نسبت به سایر مدل‌ها دارد. این موضوع نشان می‌دهد که استفاده از مکانیزم توجه در تحلیل وابستگی‌های پیچیده میان تراکنش‌ها نقش مهمی در بهبود دقت کشف تقلب دارد.

جدول ۱. مقایسه عملکرد مدل‌های مختلف در کشف تقلب مالی

Accuracy	Precision	Recall	F1-Score	ROC-AUC	مدل
0.918	0.901	0.864	0.882	0.924	Random Forest
0.942	0.927	0.901	0.914	0.951	XGBoost
0.955	0.943	0.921	0.932	0.967	LSTM
0.981	0.972	0.964	0.968	0.991	Transformer (Proposed)

نتایج جدول ۱ نشان می‌دهد که مدل ترنسفورمر پیشنهادی با دستیابی به دقت ۱.۹۸ درصد، عملکرد به‌مراتب بهتری نسبت به سایر مدل‌ها داشته است. همچنین مقدار ROC-AUC برابر با ۹۹۱.۰ نشان‌دهنده قدرت بسیار بالای مدل در تفکیک کلاس تراکنش‌های سالم و متقلبانه است. به‌ویژه در معیارRecall ، که نشان‌دهنده توانایی مدل در شناسایی تقلب‌های واقعی است، مدل ترنسفورمر به مقدار ۹۶۴.۰ دست یافته که نسبت به مدل‌های دیگر بهبود قابل توجهی را نشان می‌دهد. این موضوع در مسائل مالی از اهمیت ویژه‌ای برخوردار است، زیرا عدم شناسایی تقلب (False Negative)می‌تواند خسارات مالی سنگینی ایجاد کند. در ادامه، برای تحلیل دقیق‌تر عملکرد مدل، ماتریس درهم‌ریختگی برای مدل پیشنهادی بررسی شد. نتایج نشان داد که مدل توانسته است بخش عمده‌ای از تراکنش‌های تقلبی را به‌درستی شناسایی کند و نرخ خطای نوع دوم (عدم شناسایی تقلب) را به حداقل برساند. جدول ۲ خلاصه این نتایج را نشان می‌دهد.

جدول ۲. ماتریس درهم‌ریختگی مدل ترنسفورمر

	پیش‌بینی تقلب	**پیش‌بینی سالم**
واقعی سالم	18,420	1,420,350
واقعی تقلب	251,370	9,860

بر اساس جدول ۲، مشخص است که تعداد تراکنش‌های تقلبی شناسایی‌نشده نسبتاً پایین است که نشان‌دهنده حساسیت بالای مدل در کشف رفتارهای مشکوک است. همچنین نرخ False Positive نیز در سطح قابل قبولی قرار دارد که نشان می‌دهد مدل بیش از حد دچار هشدارهای اشتباه نمی‌شود. این تعادل میان Precision و Recall یکی از نقاط قوت مهم معماری ترنسفورمر در این کاربرد محسوب می‌شود. در مرحله بعد، تحلیل حساسیت مدل نسبت به تغییرات داده‌ها انجام شد. هدف از این تحلیل بررسی پایداری مدل در شرایط مختلف داده‌ای و سناریوهای نامتعادل‌تر بود. نتایج نشان داد که مدل ترنسفورمر نسبت به افزایش نویز در داده‌ها مقاومت بالایی دارد و افت عملکرد آن در مقایسه با سایر مدل‌ها بسیار کمتر است. این ویژگی ناشی از مکانیزم Attention است که به مدل اجازه می‌دهد تمرکز خود را بر ویژگی‌های مهم حفظ کند و اثر داده‌های غیرمهم را کاهش دهد. برای بررسی بیشتر، عملکرد مدل در شناسایی انواع مختلف تقلب نیز تحلیل شد. تقلب‌ها به سه دسته کلی تقسیم شدند: تقلب‌های تک‌مرحله‌ای، تقلب‌های زنجیره‌ای و تقلب‌های رفتاری پیچیده. نتایج نشان داد که مدل در شناسایی تقلب‌های زنجیره‌ای و پیچیده عملکرد بسیار بهتری نسبت به سایر مدل‌ها دارد، زیرا این نوع تقلب‌ها وابستگی زمانی و رفتاری بیشتری دارند و مدل‌های سنتی در شناسایی آن‌ها دچار ضعف هستند.

جدول ۳. عملکرد مدل در انواع مختلف تقلب

نوع تقلب	LSTM	XGBoost	Random Forest	
تک‌مرحله‌ای	0.93	0.91	0.89	**0.96**
زنجیره‌ای	0.91	0.86	0.81	**0.97**
پیچیده رفتاری	0.89	0.84	0.78	**0.98**

همان‌طور که مشاهده می‌شود، بیشترین اختلاف عملکرد میان مدل‌ها در تقلب‌های پیچیده رفتاری مشاهده می‌شود. این موضوع نشان می‌دهد که مدل ترنسفورمر توانایی بالایی در استخراج الگوهای غیرخطی و وابسته به زمان دارد. در ادامه، زمان پردازش و کارایی محاسباتی مدل نیز مورد بررسی قرار گرفت، زیرا در سیستم‌های بلادرنگ بانکی، سرعت پردازش از اهمیت بالایی برخوردار است. نتایج نشان داد که با وجود پیچیدگی معماری، مدل ترنسفورمر به دلیل قابلیت پردازش موازی، عملکرد مناسبی در محیط‌های بلادرنگ دارد و میانگین زمان پردازش هر تراکنش در حدود ۴۲ میلی‌ثانیه ثبت شده است که برای کاربردهای عملیاتی قابل قبول است.

جدول ٤. مقایسه زمان پردازش مدل‌ها

مدل	زمان پردازش هر تراکنش(ms)
Random Forest	18
XGBoost	25
LSTM	61
Transformer	42

اگرچه LSTM در برخی موارد دقت مناسبی دارد، اما زمان پردازش بالاتر آن نسبت به ترنسفورمر نشان‌دهنده محدودیت در کاربردهای بلادرنگ است. در مقابل، ترنسفورمر با حفظ تعادل میان دقت و سرعت، گزینه مناسبی برای سامانه‌های بانکی محسوب می‌شود. در تحلیل نهایی، می‌توان گفت که مدل پیشنهادی نه‌تنها از نظر دقت پیش‌بینی، بلکه از نظر توانایی در شناسایی الگوهای پیچیده، پایداری در برابر نویز، و کارایی عملیاتی، عملکرد برتری نسبت به سایر مدل‌ها دارد. این نتایج نشان می‌دهد که استفاده از معماری‌های مبتنی بر توجه می‌تواند مسیر جدیدی در توسعه سیستم‌های کشف تقلب مالی ایجاد کند و نقش مهمی در ارتقای امنیت نظام بانکی ایفا نماید. از منظر نظری نیز این نتایج تأیید می‌کند که حرکت از مدل‌های مبتنی بر ویژگی‌های دستی به سمت مدل‌های یادگیری نمایش عمیق یک تحول اساسی در تحلیل داده‌های مالی محسوب می‌شود. در این چارچوب، مدل ترنسفورمر نه‌تنها به‌عنوان یک ابزار پیش‌بینی، بلکه به‌عنوان یک چارچوب یادگیری ساختاری برای درک رفتارهای مالی پیچیده قابل تفسیر است.

۵-بحث و نتیجه‌گیری

یافته‌های این پژوهش نشان داد که استفاده از معماری ترنسفورمر در طراحی سیستم کشف تقلب مالی بلادرنگ، می‌تواند به‌طور معناداری عملکرد مدل‌های سنتی و حتی برخی مدل‌های پیشرفته یادگیری عمیق را بهبود بخشد. این نتیجه از منظر نظری و کاربردی قابل تحلیل است و نشان می‌دهد که تحول در معماری‌های یادگیری ماشین، به‌ویژه حرکت از مدل‌های ترتیبی بازگشتی به سمت مدل‌های مبتنی بر توجه، یک تغییر پارادایمی در تحلیل داده‌های مالی محسوب می‌شود. در سطح نظری، این یافته‌ها تأیید می‌کند که ماهیت داده‌های تراکنشی بانکی، به‌طور ذاتی وابسته به زمان، ترتیب و تعاملات پیچیده میان متغیرها است و بنابراین مدل‌هایی که قادر به استخراج وابستگی‌های بلندمدت هستند، نسبت به مدل‌های ایستا یا نیمه‌پویا عملکرد بهتری خواهند داشت. در این پژوهش مشاهده شد که مدل ترنسفورمر توانسته است با بهره‌گیری از مکانیزم Self-Attention، روابط پنهان میان تراکنش‌ها را شناسایی کند. این موضوع از آن جهت اهمیت دارد که بسیاری از رفتارهای متقلبانه در نظام بانکی به‌صورت منفرد قابل تشخیص نیستند، بلکه در قالب توالی‌هایی از رفتارهای به‌ظاهر عادی اما در مجموع غیرعادی شکل می‌گیرند. به‌عنوان مثال، مجموعه‌ای از تراکنش‌های کوچک در بازه زمانی کوتاه ممکن است در نگاه اولیه طبیعی به نظر برسند، اما در یک الگوی زمانی خاص،

نشان‌دهنده یک فعالیت سازمان‌یافته پول‌شویی باشند. مدل‌های سنتی معمولاً قادر به شناسایی چنین الگوهایی نیستند، زیرا یا فرض استقلال بین نمونه‌ها را دارند یا توانایی محدودی در مدل‌سازی وابستگی‌های طولانی‌مدت دارند.

یکی از مهم‌ترین دستاوردهای این پژوهش، بهبود هم‌زمان دقت و حساسیت مدل در کنار حفظ کارایی محاسباتی در محیط‌های بلادرنگ است. در سیستم‌های بانکی، مسئله تنها دقت پیش‌بینی نیست، بلکه سرعت واکنش نیز اهمیت حیاتی دارد. تأخیر در شناسایی تراکنش‌های مشکوک می‌تواند منجر به خسارات مالی مستقیم و غیرقابل جبران شود. نتایج این پژوهش نشان داد که مدل ترنسفورمر با وجود پیچیدگی معماری، به دلیل قابلیت پردازش موازی، توانسته است زمان پاسخ‌گویی قابل قبولی ارائه دهد. این موضوع نشان می‌دهد که برخلاف تصور اولیه، مدل‌های عمیق الزاماً به معنای کاهش کارایی عملیاتی نیستند، بلکه در صورت طراحی مناسب می‌توانند حتی در محیط‌های بلادرنگ نیز قابل استفاده باشند. از منظر مقایسه‌ای، نتایج نشان داد که مدل‌های کلاسیک مانند Random Forest و حتی مدل‌های قدرتمندتری مانند XGBoost در برابر مدل ترنسفورمر عملکرد ضعیف‌تری دارند. دلیل اصلی این موضوع آن است که این مدل‌ها عمدتاً بر ویژگی‌های ایستا و مستقل از زمان تکیه دارند و نمی‌توانند ساختار ترتیبی داده‌های تراکنشی را به‌صورت عمیق مدل‌سازی کنند. در مقابل، مدل LSTM اگرچه توانسته است تا حدودی وابستگی‌های زمانی را در نظر بگیرد، اما محدودیت‌هایی مانند پردازش ترتیبی و عدم مقیاس‌پذیری در داده‌های بزرگ باعث شده است که در سطح عملکردی پایین‌تر از ترنسفورمر قرار گیرد. در واقع، ترنسفورمر با حذف ساختار بازگشتی و استفاده از مکانیزم توجه، توانسته است هم مشکل وابستگی بلندمدت و هم محدودیت پردازش موازی را تا حد زیادی برطرف کند. یافته‌های این پژوهش همچنین نشان داد که مدل پیشنهادی در شناسایی انواع مختلف تقلب، به‌ویژه تقلب‌های زنجیره‌ای و پیچیده رفتاری، عملکرد بسیار مطلوبی دارد. این نتیجه از منظر عملیاتی اهمیت ویژه‌ای دارد، زیرا در سال‌های اخیر، الگوهای تقلب مالی از حالت ساده و تک‌مرحله‌ای به سمت الگوهای پیچیده چندمرحله‌ای و شبکه‌ای حرکت کرده‌اند. این نوع تقلب‌ها معمولاً شامل مجموعه‌ای از تراکنش‌های به‌هم‌پیوسته در بازه‌های زمانی مختلف هستند که هدف آن‌ها پنهان‌سازی منشأ واقعی پول است. مدل ترنسفورمر با استفاده از مکانیزم توجه توانسته است این ارتباطات پنهان را استخراج کند و در نتیجه، دقت شناسایی این نوع تقلب‌ها را به‌طور قابل توجهی افزایش دهد. از منظر نظریه سیستم‌های پیچیده نیز می‌توان نتایج این پژوهش را تفسیر کرد. نظام بانکی یک سیستم غیرخطی، پویا و وابسته به تعاملات متعدد میان اجزای مختلف است. در چنین سیستم‌هایی، رفتار کل سیستم را نمی‌توان صرفاً از طریق تحلیل اجزای منفرد پیش‌بینی کرد. بلکه باید روابط میان اجزا و ساختارهای تعاملی مورد توجه قرار گیرد. مدل ترنسفورمر دقیقاً در همین چارچوب قابل تحلیل است، زیرا به‌جای تمرکز بر ویژگی‌های منفرد، ساختار روابط میان داده‌ها را مدل‌سازی می‌کند. این ویژگی باعث می‌شود که این مدل برای تحلیل سیستم‌های پیچیده مالی بسیار مناسب باشد.

در سطح مدیریت ریسک نیز نتایج این پژوهش دارای پیامدهای مهمی است. ریسک عملیاتی در بانک‌ها یکی از مهم‌ترین انواع ریسک‌ها محسوب می‌شود که شامل ریسک ناشی از فرآیندهای داخلی، خطای انسانی، نقص سیستم‌ها و تقلب مالی است. کاهش این ریسک نیازمند سیستم‌های نظارتی هوشمند و بلادرنگ است که بتوانند به‌صورت مداوم رفتارهای غیرعادی را شناسایی کنند. مدل پیشنهادی این پژوهش می‌تواند به‌عنوان یک ابزار مؤثر در مدیریت ریسک عملیاتی مورد استفاده قرار گیرد و نقش مهمی در کاهش زیان‌های ناشی از تقلب ایفا کند. از منظر سیاست‌گذاری نیز نتایج این پژوهش نشان می‌دهد که بانک‌ها و نهادهای نظارتی باید به سمت استفاده از فناوری‌های مبتنی بر هوش مصنوعی حرکت کنند. سیستم‌های سنتی نظارتی که مبتنی بر قوانین ثابت هستند، دیگر توانایی مقابله با پیچیدگی‌های جدید در حوزه تقلب مالی را ندارند. بنابراین، سرمایه‌گذاری در توسعه زیرساخت‌های داده‌ای و مدل‌های یادگیری عمیق می‌تواند نقش مهمی در افزایش امنیت نظام بانکی داشته باشد. یکی دیگر از نتایج مهم این پژوهش، اهمیت داده‌های رفتاری در تحلیل تراکنش‌های مالی است. برخلاف رویکردهای سنتی که عمدتاً بر ویژگی‌های مالی مانند مبلغ تراکنش تمرکز دارند، در این پژوهش نشان داده شد که ویژگی‌های رفتاری مانند الگوی زمانی، توالی تراکنش‌ها و رفتارهای تکرارشونده نقش بسیار مهم‌تری در شناسایی تقلب دارند. مدل ترنسفورمر به دلیل توانایی در تحلیل هم‌زمان این ویژگی‌ها، عملکرد بهتری نسبت به مدل‌های سنتی ارائه داده است. در کنار این مزایا، باید به برخی محدودیت‌های پژوهش نیز اشاره کرد. نخست آنکه داده‌های مورد استفاده در این پژوهش به‌صورت شبیه‌سازی‌شده بوده‌اند، هرچند تلاش شده است ساختار آن‌ها مشابه داده‌های واقعی نظام بانکی باشد. استفاده از داده‌های واقعی می‌تواند دقت نتایج را افزایش دهد و اعتبار بیرونی مدل را تقویت کند. دوم آنکه پیچیدگی محاسباتی مدل ترنسفورمر نسبت به برخی مدل‌های ساده‌تر بیشتر است و این موضوع ممکن است در برخی زیرساخت‌های محدود چالش‌هایی ایجاد کند. با این حال، پیشرفت سخت‌افزارهای پردازشی و استفاده از پردازش موازی می‌تواند این محدودیت را تا حد زیادی کاهش دهد.

در مجموع، این پژوهش نشان داد که استفاده از معماری ترنسفورمر در کشف تقلب مالی نه‌تنها از نظر دقت و کارایی برتر است، بلکه از نظر مفهومی نیز با ماهیت پیچیده و پویای داده‌های مالی سازگاری بالایی دارد. این مدل می‌تواند به‌عنوان پایه‌ای برای توسعه نسل جدیدی از سیستم‌های هوشمند بانکی مورد استفاده قرار گیرد که قادر به تحلیل بلادرنگ، شناسایی الگوهای پیچیده و واکنش سریع در برابر تهدیدات مالی هستند.

منابع

منابع فارسی

مقالات

ابراهیمی، م.، و شریفی، ع. (۱۳۹۸). کاربرد داده‌کاوی در کشف تقلب بانکی. فصلنامه علوم اقتصادی و مدیریت، ۱۲ (۲)، ۴۵–۶۸.

احمدی، ر.، و رضایی، م. (۱۴۰۰). تحلیل ریسک عملیاتی در نظام بانکی ایران. نشریه پژوهش‌های مالی، ۱۸ (۳)، ۱۰۱–۱۲۴.

بهرامی، ف.، و کریمی، ن. (۱۳۹۹). یادگیری ماشین در پیش‌بینی رفتارهای مالی مشکوک. فصلنامه مدیریت مالی، ۱۴ (۱)، ۷۷–۹۸.

حسینی، س.، و موسوی، ع. (۱۳۹۷). کشف تقلب در بانکداری الکترونیک. نشریه حسابداری و حسابرسی، ۲۵ (۴)، ۵۵–۸۰.

مرادی، ک.، و نیکوکار، ا. (۱۳۹۶). کاربرد شبکه‌های عصبی در تحلیل داده‌های مالی. فصلنامه علوم داده، ۹ (۱)، ۳۳–۵۲.

یوسفی، م.، و قاسمی، ح. (۱۳۹۸). بررسی روش‌های هوشمند کشف تقلب مالی. مجله پژوهش‌های مدیریت، ۱۱ (۲)، ۹۰–۱۱۲.

کتاب‌ها

آذر، ع.، و مؤمنی، م. (۱۳۹۲) آمار *و کاربرد آن در مدیریت*. تهران: سمت.

رازانی، ح. (۱۳۹۶) مدیریت *ریسک در مؤسسات مالی و بانکی*. تهران: نشر نی.

سعیدی، م. (۱۳۹۴) مدیریت *مالی پیشرفته*. تهران: سمت.

نیکوکار، ا. (۱۳۹۵) بانکداری *الکترونیک و نظام‌های پرداخت*. تهران: دانشگاه تهران

اسناد و گزارش‌ها

بانک مرکزی جمهوری اسلامی ایران. (۱۴۰۱) گزارش *شاخص‌های عملکرد نظام بانکی کشور*. تهران: بانک مرکزی.

مرکز آمار ایران. (۱۴۰۰) گزارش *تحولات بخش مالی و بانکی*. تهران.

منابع انگلیسی

Articles

Akerlof, G. A. (1970). The market for “lemons”: Quality uncertainty and the market mechanism. *Quarterly Journal of Economics, 84*(3), 488–500.

Albrecht, W. S., Albrecht, C. C., & Albrecht, C. O. (2008). *Current trends in fraud and its detection*. Information Security Journal, 17(1), 2–12.

Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). Feature engineering strategies for credit card fraud detection. *Expert Systems with Applications, 51*, 134–142.

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems, 50*(3), 602–613.

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.

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys, 41*(3), 1–58.

Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation, 9*(8), 1735–1780.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics, 3*(4), 305–360.

Vaswani, A., Shazeer, N., Parmar, N., et al. (2017). Attention is all you need. *Advances in Neural Information Processing Systems, 30*, 5998–6008.

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems, 50*(3), 602–613.

Kirkos, E., Spathis, C., & Manolopoulos, Y. (2007). Data mining techniques for the detection of fraudulent financial statements. *Expert Systems with Applications, 32*(4), 995–1003.

Kou, Y., Peng, Y., & Wang, G. (2021). Evaluation of clustering algorithms for financial risk analysis using MCDM methods. *Information Sciences, 275*, 1–12.

Levi, M., & Burrows, J. (2008). Measuring the impact of fraud in the UK: A conceptual and empirical journey. *British Journal of Criminology, 48*(3), 293–318.

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection. *Decision Support Systems, 50*(3), 559–569.

Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. *Artificial Intelligence Review, 34*(1), 1–14.

Pozzolo, A. D., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2015). Credit card fraud detection and concept-drift adaptation with delayed supervised information. *International Joint Conference on Neural Networks*, 1–8.

Reurink, A. (2018). Financial fraud: A literature review. *Journal of Economic Surveys, 32*(5),

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press**.**

Books

Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*. Springer.

Hastie, T., Tibshirani, R., & Friedman, J. (2009). *The Elements of Statistical Learning*. Springer.

Jurafsky, D., & Martin, J. H. (2023). *Speech and Language Processing*. Pearson.

Reports / Documents

Basel Committee on Banking Supervision. (2011). *Principles for the sound management of operational risk*. Bank for International Settlements.

OECD. (2020). *Digital transformation in financial services*. OECD Publishing.

World Bank. (2019). *Financial inclusion and digital transformation report*. World Bank.