# کاربرد پیشرفته یادگیری ماشین در شناسایی وپیشگیری از تقلب‌های مالی

نویسنده * **پوهنمل محمدالله شیرپور**
نشانی برقی تکنالوژی معلوماتی، پوهنحی کمپیوترساینس، پوهنتون بدخشان
نشانی ارکاید m.shirpoor@badakhshan.edu.af
https://orcid.org/0009-0001-2115-1217

نویسنده **پوهنمل عصمت الله ناشر**
نشانی برقی تکنالوژی معلوماتی، پوهنحی کمپیوترساینس، پوهنتون بدخشان
نشانی ارکاید nashirasmatullah@gmail.com
https://orcid.org/0009-0004-9976-4461

## چکیده

رابطه‌ی هایدروجنی از جمله روابط ضعیف در بین مالیکول‌ها است که بعد از روابط کوولانسی مورد توجه کیمیادآن‌ها می‌باشد. زمانی‌که یک اتوم‌هایدروجن به یک اتوم الکترونگاتیف قوی مانند فلورین، اکسیجن و نایتروجن متصل می‌گردد، به سمت اتوم الکترونگاتیف کشیده می‌شود، این پروسه به‌نام رابطه‌ی هایدروجنی شناخته می‌شود. رابطه‌یی هایدروجنی برای ساختار و عمل‌کرد سیستم‌های بیولوژیکی ( دی ان ای، پروتین و ...) و اکثر پروسه‌های کیمیاوی نیاز است. این تحقیق به شناخت دقیق از رابطه‌ی هایدروجنی در بین مالیکول‌های آب، امونیا و هایدروجن فلوراید می‌پردازد و هدف آن بررسی قدرت رابطه‌ی هایدروجنی در بین مالیکول‌های مذکور است. این تحقیق از نوع محاسباتی بوده و برای محاسبه تمام اطلاعات از نرم افزار کوانتومی اورکا استفاده شده است. نتایج تحقیق نشان می‌دهد که انرژی رابطه‌ی هایدروجنی در مالیکول هایدروجن فلوراید برابر۳۸/۱۱ کیلوژول بر مول بوده و نسبت به انرژی رابطه‌ی هایدروجنی در بین مالیکول‌های آب و امونیا بیش‌تر است و این به سبب اتوم الکترونیگاتیف قوی در مالیکول هایدروجن فلوراید است که رابطه‌ی هایدروجنی قوی نسبت به مالیکول آب و امونیا تشکیل می‌دهد.

**کلید واژه‌ها:** الکترونیگاتیف، رابطه‌ی هایدروجنی، محاسبات کوانتومی و مودل الکتروستاتیکی انرژی.

* نویسنده مسئول: پوهنمل محمدالله شیرپور

# Advanced use of Machines in Detecting and Preventing Financial Fraud

Author * **Mohammadullah Shirpoor**
Information Technology Computer Science Faculty، Badakhshan University
Email m.shirpoor@badakhshan.edu.af
Orcid https://orcid.org/0009-0001-2115-1217

Author **Asmatullah Nashir**
Information Technology Computer Science Faculty، Badakhshan University
Email nashirasmatullah@gmail.com
Orcid https://orcid.org/0009-0004-9976-4461

## Abstract
In recent years، the rapid expansion of digital technologies and the fundamental transformation of financial activities have led to a significant increase in online financial transactions. While these advancements have provided advantages such as speed and convenience، they have also created opportunities for more sophisticated forms of financial fraud.Financial fraud، manifested in forms such as credit card fraud، account manipulation، and the misuse of sensitive user data، has become a serious threat to public trust and the stability of financial institutions.Traditional methods for detecting such fraudulent activities، which are primarily based on rule-based systems and manual analysis، are no longer sufficient to address the increasing complexity of fraud patterns. Therefore، this study aims to investigate the application of advanced machine learning techniques in the detection and prevention of financial fraud.This research adopts a descriptive–analytical approach and draws upon credible academic sources to evaluate algorithms such as decision trees، artificial neural networks، and clustering models.The findings indicate that machine learning algorithms not only demonstrate a strong capability in identifying hidden patterns but also outperform traditional methods in reducing false positives، improving detection speed، and adapting to evolving conditions. Furthermore، the study examines the fundamental concepts of financial fraud.

**Keywords:** Information Security، Financial Fraud، Machine Learning، Algorithmic Analysis، Artificial Intelligence.

Corresponding Author: m.shirpoor@badakhshan.edu.af *

مجله‌ی علمی-تحقیقی پامیر / - دپامیر علمی څېړنیزه مجله - Pamir Academic & Research Journal

## مقدمه

در سال‌های اخیر، سرعت گسترش تکنالوژی‌های دیجیتال زندگی ما را به‌گونه‌ای دگرگون کرده که حتی امور مالی نیز دیگر به شکل قدیمی گذشته انجام نمی‌شوند. امروزه، معاملات بانکی و مالی با حجمی بالا ودر کسری از ثانیه انجام می‌گیرند؛ تحولی که از یک‌سو فرصت‌هایی چشم گیر برای افزایش بهره‌وری وتسهیل خدمات مالی به‌وجود آورده و ازسوی دیگر، زمینه‌ای مناسب برای سوءاستفاده‌های پیچیده وپنهان فراهم کرده است تقلب‌های مالی که‌درقالب‌هایی مانند کلاهبرداری باکارت‌های اعتباری، پول‌شویی،دستکاری درحساب‌ها وحتی بهره‌برداری از اطلاعات شخصی مشتریان ظاهر می‌شوند، یکی ازجدی‌ترین چالش‌های امنیتی برای مؤسسات مالی به‌شمار می‌آیند.روش‌هایی که در گذشته برای شناسایی تقلب به کار می‌رفتند، بیشتر مبتنی بر قوانین ثابت، بررسی دستی و تحلیل‌های سنتی بودند. با وجودی که این شیوه‌ها در گذشته کاربرد داشتند، اما در دنیای امروز که داده‌ها با حجم بالا و درساختارهایی پیچیده تولید می‌شوند، دیگر پاسخ‌گوی نیازها نیستند. پیچیده‌تر شدن روش‌های تقلب و سرعت بالای انتقال دیتاها، باعث شده تشخیص درست وبه‌موقع این رفتارهای غیرعادی بسیار دشوار شود. درچنین شرایطی، تکنالوژی‌های نوین و هوشمند وارد میدان شده‌اند. یکی از مؤثرترین این ابزارها، یادگیری ماشین است؛ شاخه‌ای از هوش مصنوعی که با استفاده از الگوریتم‌های پیشرفته، می‌تواند دیتاها را به‌صورت خودکار و دقیق پردازش کرده و الگوهای پنهان و ناهنجار را شناسایی کند. از جمله الگوریتم‌هایی که در این زمینه کاربرد زیادی دارند می‌توان به درخت تصمیم، شبکه‌های عصبی مصنوعی، ماشین بردار پشتیبان و روش‌های خوشه‌بندی اشاره کرد. این الگوریتم‌ها با تحلیل دقیق رفتار مشتریان و مبادله های مالی، می‌توانند در زمان واقعی، هشدارهای لازم را برای شناسایی فعالیت‌های مشکوک صادر کنند. مزیت بزرگ استفاده از یادگیری ماشین در این است که نه تنها باعث افزایش دقت و سرعت در تشخیص تقلب می‌شود، بلکه از بروز زیان‌های مالی و تهدیدهای امنیتی نیز جلوگیری می‌کند.این سیستم‌ها، برخلاف روش‌های قدیمی، دارای قابلیت یادگیری مستمر هستند و می‌توانند خود را با تغییر رفتار متقلبان تطبیق دهند و در برابر حملات جدید، مقاوم باقی بمانند.

## تبیین مسأله

در دنیای امروز یکی از جدی‌ترین تهدیدهایی که پیش‌روی نهادهای مالی قرار دارد، پدیده‌ی تقلب مالی است. این پدیده،که می‌تواند دراشکال گوناگونی نظیر جعل هویت، سوءاستفاده از کارت‌های اعتباری، پول‌شویی، دستکاری عمدی در مبادله ها و ارائه‌ی گزارش‌های مالی نادرست ظاهر شود، نه‌تنها موجب خسارات سنگین اقتصادی برای سازمان‌ها می‌گردد.سیستم‌هایی که در گذشته برای شناسایی تقلب استفاده می‌شدند، اغلب بر پایه‌ی قوانین از پیش تعریف‌شده و

بررسی‌های دستی طراحی شده بودند. اما امروز در برابر پیچیدگی و پویایی الگوهای تقلبی جدید، دچار ضعف جدی هستند. هشدارهای نادرست و بیش‌ازحد، ناتوانی در تشخیص تقلب‌های نوظهور و عدم قابلیت تطبیق با حجم بالای دیتاها، تنها بخشی از محدودیت‌های این رویکردهای قدیمی است.در مقابل این چالش‌ها، پیشرفت در حوزه‌ی هوش مصنوعی و به‌ویژه یادگیری ماشین، راه‌های تازه‌ای برای مقابله با این تهدیدها گشوده است. الگوریتم‌های هوشمند اکنون این توانایی را دارند که با تحلیل خودکار میلیون‌ها دیتای مالی، الگوهای مشکوک را از دل دیتاهای به‌ظاهر عادی بیرون کشیده و در لحظه هشدارهایی دقیق صادر کنند.

## اهمیت تحقیق

در دنیای امروز که همه چیز به سرعت در حال دیجیتالی شدن است، روش‌های نوین مالی مثل پرداخت‌های الکترونیکی و بانکداری آنلاین فرصت‌های زیادی برای رشد اقتصادی و سهولت در کارهای مالی ایجاد کرده‌اند. اما در کنار این مزایا، مشکلاتی هم به وجود آمده که مهم‌ترین آن‌ها تقلب‌های مالی است. این تقلب‌ها معمولاً پنهان و پیچیده‌اند و علاوه بر ضررهای مالی، باعث کاهش اعتماد مردم به سیستم‌های مالی می‌شوند.با توجه به پیچیدگی‌های روزافزون و حجم زیاد دیتاها، روش‌های قدیمی کشف تقلب دیگر جوابگو نیستند. به همین دلیل، یادگیری ماشین که بخشی از هوش مصنوعی است، وارد شده و امکان تحلیل هوشمند و سریع دیتاها را فراهم کرده است.توسعه دانش علمی در زمینه یادگیری ماشین و کاربردهای آن در تقلب مالی و امنیت کمک می‌کند؛ با بررسی الگوریتم‌های مختلف، زمینه برای پژوهش‌های بعدی آماده می‌شود به صورت کاربردی به مسئله تشخیص تقلب پرداخته است، که با رشد مبادله های دیجیتال در بانک‌ها و بازارهای مالی، بسیار ضروری است؛ نتایج آن می‌تواند به بهبود سیستم‌های امنیتی، اهمیت اجتماعی و اقتصادی دارد. و در نهایت، از منظر تکنالوژی آینده‌نگر، یادگیری ماشین با قابلیت یادگیری خودکار و انطباق با دیتاهای جدید، ابزار قدرتمندی برای مقابله با تقلب‌های پیچیده است و این تحقیق گامی به سوی بانکداری هوشمند و امنیت مالی خودکار محسوب می‌شود.

## پرسش‌های تحقیق

پرسش اصلی: چگونه می توان به کار گیری تکنیک های یادگیری ماشین در شناسایی وپیشگیری از تقلب‌های مالی جلوگیری کرد؟

پرسش‌های فرعی

۱.کدام الگوریتم‌ها در تشخیص تقلب موثرترند ؟

۲.کدام تکنیک های یادگیری ماشین در شناسای در تقلب‌های مالی موثر است؟

## اهداف تحقیق

مجله‌ی علمی-تحقیقی پامیر / - دپامیر علمی څېړنیزه مجله - Pamir Academic & Research Journal

هدف اصلی این تحقیق مطالعه وشناسایی تکنیک های یادگیری ماشین در شناسایی وپیشگیری از تقلب‌های مالی استِ

اهداف فرعی:

۱.کشف تقلب‌ها و تحلیل روش‌های مقابله.

۲.شناسایی فرصت‌ها و روندهای آینده در کاربرد یادگیری ماشین برای مقابله با تقلب‌های مالی.

۳.به‌کارگیری یادگیری ماشین برای تشخیص تقلب مالی

## پیشینه‌ی تحقیق

تقلب مالی به اقداماتی عمدی برای فریب دیگران از طریق ارائه اطلاعات نادرست مالی گفته می‌شودکه شامل اختلاس، فساد و تغیر صورت‌های مالی است. این اقدامات معمولاً ناشی از عواملی مانند طمع، فشار مالی و ضعف در کنترل‌های داخلی هستند و می‌توانند خسارات مالی و کاهش اعتماد ذینفعان را در پی داشته باشند. حساب رسان نقش کلیدی در شناسایی و پیشگیری از تقلب دارند و با بررسی دقیق معلومات و تقویت کنترل‌های داخلی، ازوقوع تخلفات جلوگیری می کنند. (کامرانی، عابدینی، ۱۴۰۱). فساد مالی شامل استفاده نادرست از نفوذ برای منافع شخصی مانند رشوه و زورگیری اقتصادی است.سوءاستفاده از دارایی‌ها به اختلاس و تصاحب غیرقانونی دارایی‌های سازمان توسط کارکنان اشاره دارد.تقلب مالی شامل تحریف عمدی اطلاعات مالی برای ارائه تصویری نادرست از وضعیت شرکت است، که با سندسازی، تغییر مدارک و حذف عمدی اطلاعات مهم صورت می گیرد (کامرانی، عابدینی، ۱۴۰۱). عدم آگاهی کارکنان از اصول حسابداری، حقوقی و رویه‌های گزارش‌دهی، احتمال بروز رفتارهای مشکوک را افزایش می‌دهد. آموزش‌های مالی، آشنایی با نشانه‌های تقلب، و توانمندسازی پرسنل برای شناسایی ریسک‌ها، بخش مهمی از استراتژی‌های پیشگیرانه محسوب می‌شوند. در غیاب چنین آموزش‌هایی، افراد ناآگاهانه یا ندانسته ممکن است در مسیر فساد مالی قرار بگیرند (رسولی و فرهمند، ۱۴۰۲) نبود آموزش کافی درباره قوانین مالی و حقوقی ممکن است موجب بروز تقلب‌های ناخواسته شود. برخی مدیران به‌طور ناآگاهانه هزینه‌های شخصی را به حساب شرکت ثبت می کنند. در مقابل، برخی شرکت‌ها عمداً صورت‌های مالی را برای اهداف چون دریافت افزایش ارزش سهام دستکاری می کنند. که به بازار و توسعه پایدار آسیب می‌زند. حسابرسان در شناسایی این تقلب‌ها نقش دارند، اما به دلیل امکان خطا، استفاده از مدل‌های آماری و یادگیری ماشین اهمیت زیادی دارد. مطالعه‌ای روی ۶۱۱ شرکت برسی نشان داد که مدل‌های یادگیری ماشین مانند درخت تصمیم گیری در پیش‌بینی تقلب عمل کرد دقیق‌تری نسبت به مدل‌های آماری دارند (کاکلر، ثالث، کنگرلویی، و آشتاب،۱۴۰۰). نبود آموزش‌های کافی درباره شیوه‌های شناسایی و گزارش‌دهی تقلب، یک عامل کلیدی در وقوع

آن است. اگر کارکنان ندانند چگونه تقلب را تشخیص ومعلومات را گزارش دهند.آموزش‌های دوره‌ای در زمینه شفافیت مالی، قوانین ضدتقلب و آشنایی با شاخص‌های هشداردهنده می‌تواند این ریسک را کاهش دهد.(Alkalbani et al. ، .(2016

## شبکه‌های عصبی مصنوعی(ANN)

یک شبکه عصبی مصنوعی [۱]( ANN) ساختاری شبیه به نورون در مغز انسان است. این یک سیستم پردازش اطلاعات است که اعصاب بیولوژیکی را تقلید کرده و می‌تواند برای انجام پیشبینی هم چندین ورودی دریافت و ترکیب کند. شبکه عصبی مصنوعی نوعی از دستگاه هوش مصنوعی اسمت که در آن روش ریاضی برای ایجاد توانایی در کمپیوتر برای نتیجه‌گیری از طریق توانایی محاسبه سریع کمپیوتر استفاده می‌شود. این عمل باید از طریق یک فرآیند یادگیری یعنی یادگیری ماشین به طوری که بتواند توانایی استنتاج را داشته باشد یعنی کسی به آن می‌گوید که چه نوع شرایطی به چه نتیجه ای خواهد رسید. اگر نمونه‌های درست را به آن بگوئید، به درستی به شما پاسخ می‌دهد. این حتی می‌تواند نتیجه ممکن را برای نمونه‌هایی که قبلا آموخته نشده بیان سازد (کامرانی،عابدینی، ۱۴۰۱).

## ماشین بردار پشتیبانی[۲](SVM)

ماشین بردار پشتیبان(SVM) توسعه‌یافته توسط وپنیک، یک روش یادگیری هوش مصنوعی است. این تکنیک یادگیری ماشین بر اساس نظریه یادگیری آماری و به حداقل رساندن خطر ساختاری است. هدف این است که صفحه جدایش بهینه برای تقسیم دو یا چند کلاس دیتا با مکانیسم یادگیری با آموزش دیتا های ورودی را شناسایی کند. این یک نوع یادگیری نظارت شده برای پیشبینی و طبقه بندی این‌ها در زمینه استخراج دیتا است (کامرانی،عابدینی،بهار ۱۴۰۱).

## درخت تصمیم‌گیری

درخت‌های تصمیم گیری یکی از ساده تمرین روش‌های یادگیری القایی است. آن‌ها می‌توانند متغیرهای مداوم و گسسته را پردازش کنند. ساختار درختی شناخته شده به منظور تعمیم قواعد مرتبط قضیه به وجود می‌آید. درخت های تصمیم گیری در این مقاله CART[3] ، CHAID[4]، ۵/۰ Cو QUEST[5] هستند. (کامرانی،عابدینی،بهار ۱۴۰۱).

---

[۱] Artificial neural network

[۲] Support vector machine

[3] Classification and regression trees

[4] Quick unbiased efficient statistical tree

[5] Chi square automatic interaction detection

## نقش دیتای بزرگ در تشخیص تقلب مالی

با پیشرفت تکنالوژی اطلاعات و رشد نمایی دیتاهای تولیدشده در حوزه مالی، کلان‌دیتاها به یک منبع حیاتی برای کشف الگوهای پنهان و غیرمعمول تبدیل شده‌اند. حجم، تنوع و سرعت دیتاهای مالی از مرزهای سیستم‌های سنتی تحلیل دیتا فراتر رفته و ضرورت بهره‌گیری از تکنالوژی‌های جدید مانند یادگیری ماشین را دوچندان کرده است. مطالعات متعدد نشان می‌دهند که کلان‌داده‌ها نه‌تنها تشخیص تقلب را سریع‌تر و دقیق‌تر می‌سازند، بل‌که امکان پیش‌بینی رفتارهای متقلبانه را نیز فراهم می‌کنند.(Baah et al., 2024)

در سال‌های اخیر، استفاده از الگوریتم‌های یادگیری ماشین در بستر دیتای بزرگ توانسته است نرخ کشف تقلب را به‌شکل چشمگیری افزایش دهد. الگوریتم‌هایی مانندRandom Forest ، SVMو Neural Networks با پردازش میلیون‌ها مبادله مالی در زمان واقعی، ناهنجاری‌ها و الگوهای غیرعادی را شناسایی می‌کنند. این روش‌ها با ترکیب دیتاهای مبادله ای، رفتاری و زمانی، مدل‌هایی دقیق برای شناسایی تقلب می‌سازند.(Ngai et al., 2011) یکی دیگر ازدستاوردهای دیتای بزرگ درحوزه‌ی کشف تقلب، امکان استفاده از دیتاهای غیراستاندارد مانند اطلاعات شبکه‌های اجتماعی، موقعیت مکانی و دیتاهای حسگرها است. این دیتاها که پیشتر درسیستم‌های قدیمی لحاظ نمی‌شدند، اکنون به‌واسطه‌ی پلتفرم‌های تحلیل بیگ دیتا، به ابزارهای مهمی در کشف تقلب تبدیل شده‌اند. پژوهش‌ها نشان می‌دهند که تلفیق دیتاهای ساخت‌یافته و بدون ساختار در یادگیری ماشین عمل کرد سیستم‌های تشخیص تقلب راتا ٪۳۰ بهبود می‌بخشد.(Chen et al., 2012) هم‌چنین، زیرساخت‌های مبتنی بر Hadoop و Spark امکان ذخیره‌سازی و پردازش موازی حجم انبوهی از دیتاها را فراهم کرده‌اند. این تکنالوژی‌ها ابزارهای تحلیلی لازم را در اختیار محققان و بانک‌ها قرار می‌دهند تا دیتاهای تاریخی و جاری را به‌صورت هم‌زمان تحلیل کرده و الگوهای پنهان در رفتار متقلبانه را شناسایی کنند. در نتیجه، فرآیند کشف تقلب نه‌تنها سریع‌تر، بل‌که بسیار دقیق‌تر از قبل انجام می‌شود(Ghosh & Reilly, 1994) . در مجموع، دیتای بزرگ بستری قدرتمند برای تقویت عمل کرد سیستم‌های یادگیری ماشین در تشخیص تقلب مالی فراهم کرده است. این ترکیب فناورانه، چشم‌انداز نوینی را برای مقابله با فساد وسوءاستفاده‌های مالی دراختیار سازمان‌ها قرار دیتا ومطالعات آینده‌نگرانه نیز براهمیت سرمایه‌گذاری در تحلیل کلان‌داده برای امنیت مالی تأکید دارند.(Yin et al., 2019)

## دسته‌بندی انواع دیتاها و ویژگی‌های مؤثر در یادگیری ماشین

درفرآیند تشخیص تقلب با استفاده از یادگیری ماشین، دیتاها معمولاً به دو دسته‌ی ساخت‌یافته (structured)و بدون ساختار (unstructured) تقسیم می‌شوند. دیتاهای ساخت‌یافته مانند سوابق

تراکنش‌ها، اطلاعات حساب‌ها وتاریخچه پرداخت،پایه‌اصلی الگوریتم‌های نظارتی مانند Random Forestو Logistic Regression را تشکیل می‌دهند. از سوی دیگر، دیتاهای بدون ساختار مانند ایمیل‌ها یا لاگ‌های سیستم می‌توانند مکملی برای تشخیص رفتار مشکوک باشند (Ahmed et al. ،2016). ویژگی‌هایی چون زمان مبادله، مکان، مبلغ و تاریخچه رفتاری کاربران در بهبود دقت مدل‌ها نقش کلیدی دارند(Ngai et al. ،2011). پیشرفت در حوزه یادگیری عمیق (Deep Learning)و تحلیل دیتای بزرگ (Big Data Analytics) امکانات جدیدی برای مقابله با تقلب‌های پیچیده فراهم کرده است. تحقیقات اخیر نشان می‌دهند که ترکیب یادگیری تقویتی (Reinforcement Learning)با شبکه‌های عصبی عمیق، می‌تواند در آینده نقش بزرگی در تشخیص سریع‌تر تقلب‌های نوظهور ایفا کند. هم چنین استفاده از الگوریتم‌های خودنظارتی-(Self supervised) و بدون نظارت (Unsupervised) درپردازش دیتاهای ناشناخته و حجیم، فرصت‌های جدیدی را برای بهبود تشخیص فراهم کرده‌اند(Zhang ،2020; Yao et al. ،2021). یادگیری ماشین به‌دلیل توانایی‌اش در تحلیل حجم بالای دیتاهای مالی در زمان واقعی، ابزاری مؤثر برای تشخیص تقلب محسوب می‌شود. الگوریتم‌هایی مانندGradient Boosting ، SVM و Neural Networks می‌توانند الگوهای رفتاری مشکوک را از الگوهای عادی تشخیص دهند و با هشداردهی سریع، از ضررهای مالی جلوگیری کنند. هم‌چنین توانایی این الگوریتم‌ها در یادگیری از دیتاهای گذشته، موجب بهبود مستمر دقت تشخیص می‌شود(West & Bhattacharya ، 2016).کیفیت دیتا شامل دقت، کامل‌بودن و به‌روز بودن دیتاهای مالی است که نقش بسزایی در عمل‌کرد الگوریتم‌های یادگیری ماشین دارد. دیتاهای ناقص، ناهنجار یا مغشوش می‌توانند موجب خطا در پیش‌بینی و طبقه‌بندی شوند. به همین دلیل، پیش‌پردازش دیتاها، پاک‌سازی و انتخاب ویژگی‌های بهینه، جزء مراحل حیاتی در پیاده‌سازی مدل‌های تشخیص تقلب است. از طرف دیگر، حجم دیتا نیز اهمیت دارد، چرا که الگوریتم‌ها برای یادگیری مؤثر نیاز به دیتاهای متنوع و بزرگ دارند(Bahnsen et al. ،2016). یکی از چالش‌های مهم در کاربرد یادگیری ماشین در حوزه مالی، حفظ حریم خصوصی کاربران و امنیت اطلاعات مالی است. تکنیک‌هایی مانند رمزنگاری هم‌ریخت(Homomorphic Encryption) ، یادگیری فدرال(Federated Learning) ، و ناشناس‌سازی دیتاها، به‌عنوان ابزارهای مؤثر در محافظت از اطلاعات حساس معرفی شده‌اند. این روش‌ها ضمن حفظ دقت مدل، امکان اجرای تحلیل‌های یادگیری ماشین را بدون افشای اطلاعات خام فراهم می‌کنند(Shokri & Shmatikov ،2015).

## روش تحقیق

تحقیق حاضر با هدف بررسی و تحلیل نقش روش‌های یادگیری ماشین در شناسایی تقلب‌های مالی انجام شده است. برای رسیدن به این هدف، از روش‌شناسی توصیفی-تحلیلی استفاده شده که در علوم کامپیوتر و حوزه‌های مالی-اقتصادی، یکی از متداول‌ترین و معتبرترین روش‌ها محسوب می‌شود. این روش به ما اجازه می‌دهد که هم به تشریح مفاهیم اساسی و نظری بپردازیم و هم یافته‌های علمی و تجربی موجود را به‌دقت بررسی و تحلیل کنیم. در بخش اول تحقیق، تمرکز بر روی توضیح و تبیین مفاهیم کلیدی مانند تقلب مالی، انواع تقلب در سیستم‌های بانکی و اقتصادی و هم‌چنین مبانی یادگیری ماشین و الگوریتم‌های رایج در این حوزه، از جمله درخت تصمیم، جنگل تصادفی، شبکه‌های عصبی، الگوریتم K نزدیک‌ترین همسایه، ماشین بردار پشتیبان و یادگیری عمیق بوده است. هدف این بخش، فراهم آوردن چارچوبی مفهومی و درکی روشن از موضوع تحقیق است. سپس در مرحله تحلیلی، با استناد به منابع علمی معتبر و بررسی نمونه‌های واقعی از پژوهش‌های بین‌المللی، اثربخشی الگوریتم‌های یادگیری ماشین در تشخیص تقلب مالی مورد ارزیابی قرار گرفته است. این بررسی‌ها مبتنی بر شواهد مستند و دیتاهای تجربی از پروژه‌ها و مدل‌های عملی بوده است.اطلاعات مورد استفاده در این مطالعه عمدتاً به صورت کتاب‌خانه‌ی جمع‌آوری شده و از منابع ثانویه مانند کتاب‌های تخصصی، مقالات پژوهشی، پایان‌نامه‌ها و پایگاه‌های معتبر علمی مثل Google Scholar ، IEEE Xplore، Springer، ScienceDirect و ACM Digital Library بهره برده شده است. هم‌چنین، تنها منابعی که فرآیند داوری علمی (peer-reviewed)را گذرانده‌اند برای اطمینان از صحت و اعتبار دیتاها انتخاب شده‌اند. از نظر هدف، این تحقیق در دسته مطالعات کاربردی قرار می‌گیرد و ماهیت آن توصیفی-تحلیلی است. دیتاهای آن بر اساس آزمایش میدانی یا مدل‌سازی عملی جمع‌آوری نشده‌اند، از طریق تحلیل و بررسی نظری دیتاهای موجود و تجربیات پیشین به دست آمده‌اند.برای تحلیل و ارزیابی نتایج، از روش تحلیل مقایسه‌ای استفاده شده این تحقیق با بهره‌گیری از رویکردی علمی و منظم، تلاش کرده بستری مناسب برای درک بهتر کاربرد تکنالوژی‌های نوین هوش مصنوعی در حوزه‌های مالی و بانکی فراهم کند و به عنوان پایه‌ای محکم برای تحقیقات آینده در این حوزه حیاتی مطرح شود.

## نتایج ویافته‌ها

با توجه به اهداف و پرسش‌های تحقیق که یادگیری ماشین نقش بسیار مهم درگسترشی بهبود فرایند شناسایی تقلب‌های مالی دارد. هدف اصلی این پژوهش، بررسی انواع مختلف تقلب‌های مالی و پیامدهای آن‌ها بوده تا بستری مناسب برای استفاده از تکنالوژی‌های نوینی مانند یادگیری ماشین

فراهم شود. در این مسیر، دسته‌بندی دقیق دیتاها و استخراج ویژگی‌های کلیدی از دیتاهای مالی اهمیت زیادی دارد؛ چرا که کیفیت دیتاها و انتخاب صحیح ویژگی‌ها، پایه و اساس موفقیت مدل‌های یادگیری ماشین در تشخیص الگوهای تقلب است. پاسخ به پرسش اصلی تحقیق نشان داد که یادگیری ماشین با قابلیت تحلیل حجم بالایی از دیتاهای پیچیده و کشف روابط غیرخطی و الگوهای نهفته در آن ها، به عنوان ابزاری قدرتمند، توانسته است دقت و سرعت تشخیص تقلب‌های مالی را به طور قابل توجهی تشخیص دهد. این تکنالوژی می‌تواند جایگزین روش‌های قدیمی‌شود که معمولاً ناکارآمد، پرهزینه و زمان‌بر هستند. علاوه بر این، مدل‌های یادگیری ماشین با قابلیت یادگیری مداوم خود، توان تطبیق با تغییرات مکرر در شیوه‌های تقلب را دارند، که این ویژگی در فضای پرتحول مالی امروزی بسیار حیاتی است. با این حال، چالش‌های متعددی در مسیر استفاده مؤثر از یادگیری ماشین وجود دارد. یکی از مهم‌ترین آن ها کیفیت و کمیت دیتاهای آموزشی است؛ به ویژه در زمینه تشخیص تقلب که نمونه‌های تقلب نسبت به نمونه‌های عادی بسیار کمتر و نادرتر هستند، و این عدم توازن می‌تواند عمل کرد مدل را کاهش دهد. هم‌چنین، محافظت از امنیت و حریم خصوصی دیتاهای مالی به دلیل حساسیت بالای آن‌ها از نکات ضروری است که هر سیستم مبتنی بر یادگیری ماشین باید رعایت کند. این موضوع نه تنها جنبه فنی بل‌که بعد اخلاقی مهمی دارد و باید با دقت و بر اساس قوانین مربوطه پیگیری شود. هم‌چنین، شناسایی روندها و فرصت‌های پیش رو در حوزه یادگیری ماشین و کشف تقلب‌های مالی، از اهداف فرعی این تحقیق بود تا پژوهش گران و توسعه‌دهندگان تکنالوژی همواره بتوانند از جدیدترین و موثرترین روش‌ها بهره‌مند شوند. توسعه الگوریتم‌های پیشرفته‌تر، بهینه‌سازی مدل‌ها، بهره‌گیری از یادگیری عمیق و روش‌های ترکیبی، و هم‌چنین استفاده از دیتاهای بزرگ (Big Data) از مهم‌ترین مسیرهای آینده این حوزه به شمار می‌روند. در نهایت، این پژوهش نشان داد که به کارگیری هوشمندانه و علمی یادگیری ماشین می‌تواند به طور چشمگیری خسارات مالی ناشی از تقلب را کاهش دهد، امنیت سیستم‌های مالی را ارتقا بخشد و اعتماد عمومی نسبت به خدمات مالی دیجیتال را افزایش دهد. دستیابی به این اهداف نیازمند همکاری نزدیک میان پژوهش‌گران، متخصصان تکنالوژی اطلاعات، نهادهای مالی و قانون‌گذاران است تا چارچوب‌های فنی، قانونی و اخلاقی لازم برای توسعه پایدار و امن این تکنالوژی‌ها فراهم گردد.

## نتیجه‌گیری

این تحقیق به بررسی روش‌های یادگیری ماشین در تشخیص تقلب‌های مالی در حوزه‌هایی مانند بانکداری، مبادله های کارت اعتباری، بیمه و پرداخت‌های الکترونیکی پرداخته است. نتایج حاصل از تحلیل منابع علمی، مطالعه نمونه‌های واقعی و گزارش‌های تجربی به شرح زیر است: اول این‌که،

مجله‌ی علمی-تحقیقی پامیر / - دپامیر علمی څېړنیزه مجله - Pamir Academic & Research Journal

الگوریتم‌های یادگیری ماشین نسبت به روش‌های قدیمی که بر قواعد ثابت و بررسی‌های دستی مبتنی‌اند، عمل کرد به مراتب بهتری در تشخیص تقلب نشان داد الگوریتم‌هایی مثل درخت تصمیم، جنگل تصادفی، ماشین بردار پشتیبان (SVM) و شبکه‌های عصبی مصنوعی توانسته‌اند الگوهای پنهان تقلب را با دقت و حساسیت بالاتری شناسایی کنند. هم‌چنین، کیفیت دیتاها و نحوه انتخاب ویژگی‌ها نقش بسیار مهمی در موفقیت مدل‌ها داشته است. یکی از چالش‌های مهم، نامتعادل بودن دیتاها است؛ به این معنا که تعداد نمونه‌های تقلب بسیار کمتر از دیتاهای سالم است و این موضوع باعث کاهش کارایی مدل می‌شود. برای رفع این مشکل، روش‌هایی مانند (نمونه‌سازی مصنوعی دیتاهای اقلیت) و انتخاب هوشمندانه ویژگی‌ها به کار گرفته شده‌اند که باعث افزایش دقت و قابلیت تعمیم مدل‌ها شده است. عواملی مثل زمان و مکان مبادله ها، تعداد دفعات انجام تراکنش و رفتار مشتریان از مهم‌ترین ویژگی‌هایی بوده‌اند که در تشخیص تقلب موثر بوده‌اند.

## منابع

توفیقی، س.، و غلامی، ک .(۱۳۹۸). تحلیل فرهنگ سازمانی و تأثیر آن بر تقلب در مؤسسات مالی .مدیریت و توسعه منابع انسانی: ۴،۴، ۳۵-۵۰.

رسولی، ن و فرهمند، ف.(۱۴۰۲). تأثیر آموزش مالی در کاهش ریسک تقلب در شرکت های خدماتی .تحقیقات مالی و اقتصادی: ۲،۱۷، ۶۷-۸۲.

صالحی، م، و صادقی، ر .(۱۳۹۹). تاثیر ضعف کنترل داخلی بر فرصت‌های بروز تقلب .مطالعات حسابداری و ممیزی: ۲، ۷، ۴۵-۶۰.

کاکلر، ح، ثالث، ج، کنگرلویی، آشتاب.(۱۴۰۰). کارایی مدل های آماری والگوهای یادگیری ماشین در پیش بینی گزارشگری مالی متقلبانه .فصلنام-ه اقتصاد مالی

کامرانی، ح و عابدینی، ب.(۱۴۰۱).تدوین مدل کشف تقلب صورتهای مالی با استفاده از روش های شبکه عصبی مصنوعی و ماشین بردار پشتیبانی در شرکت های پذیرفته شده در بورس اوراق بهادر تهران .انجمن حسابداری مدیریت ایران

Abdullahi، R.، & Mansor، N. (2015). *Fraud triangle theory and fraud diamond theory: Understanding the convergent and divergent for future research*. International Journal of Academic Research in Accounting، Finance and Management Sciences، 5(4)، 38–45. https://doi.org/10.6007/IJARAFMS/v5-i4/1823Baah، S. S.، Adu-Twum، H. T.، Adjei، S. O.، Ampadu، G.، Martins، A. O.، & Fonkem، B. (2024).

Ahmed، M.، Mahmood، A. N.، & Hu، J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*، 60، 19–31.

Albrecht، W. S.، Albrecht، C. C.، Albrecht، C. O.، & Zimbelman، M. F. (2020). *Fraud Examination*. Cengage Learning.

Alkalbani، A.، Deng، H.، & Kam، B. (2016). Investigating the role of socio-organizational factors in information security compliance. *Information & Computer Security*، 24(2)، 148–165. DOI: 10.1108/ICS-05-2015-0025

Chen، H.، Chiang، R. H. L.، & Storey، V. C. (2012). *Business Intelligence and Analytics: From Big Data to Big Impact*. MIS Quarterly، 36(4)، 1165–1188.

Ghosh، S.، & Reilly، D. L. (1994). *Credit Card Fraud Detection with a Neural-Network*. Proceedings of the Twenty-Seventh Hawaii International Conference on System Sciences، 621–630.

Ngai، E. W. T.، Hu، Y.، Wong، Y. H.، Chen، Y.، & Sun، X. (2011). *The application of data mining techniques in financial fraud detection: A classification framework and an academic*

*review of literature*. Decision Support Systems، 50(3)، 559–569.

Stealth Advisors. (2020). *The fraud triangle، fraud risks and anti-fraud measures during COVID-19*. Retrieved from https://stealth.co.ke/article/10/the-fraud-triangle-fraud-risks-and-anti-fraud-measures-during-covid-19

Wolfe، D. T.، & Hermanson، D. R. (2004). *The fraud diamond: Considering the four elements of fraud*. The CPA Journal، 74(12)، 38–42. Retrieved from https://www.cpajournal.com/

Yin، Z.، Kaynak، H.، & Yang، H. (2019). *The role of big data analytics capabilities in developing market agility and performance: Evidence from China*. International Journal of Production Economics، 211، 123–135.

Zhang، Y. (2020). *Big Data Analytics for Financial Fraud Detection: A Survey*. Journal of Financial Crime، 27(2)، 437–455. DOI: 10.1108/JFC-06-2019-0074.