Journal of
Empirical Research In Accounting

Alzahra University, Faculty of Social Sciences and Economics
Empirical Research in Accounting, Fall 2025, V. 15, No. 57, pp.1-34

From Traditional Methods to Machine Learning: The Evolution of Fraud Detection in Auditing with New Technologies[1]

Zahra Taheri[2], Saeideh Nazari[3], Milad Samavat[4]

Received: 2025/02/02
Accepted: 2025/08/05

Research Paper

Abstract

Fraudulent financial reporting is a global issue with significant negative consequences for all stakeholders. However, detecting fraud remains challenging due to its subjective nature. This research aims to explore the opportunities, challenges, and criticisms related to the use of statistical methods and machine learning techniques for fraud detection.

This study reviews the existing literature on accounting and auditing fraud detection using machine learning and discusses the associated challenges and criticisms.

The literature review reveals that logistic regression models have traditionally been employed in fraud detection studies. However, recent advances in artificial intelligence and machine learning have introduced new opportunities for identifying financial fraud. Despite these potential benefits, the application of machine learning methods in fraud detection faces significant challenges and criticisms.

This article enhances understanding of the opportunities, challenges, and criticisms surrounding the use of emerging methods, such as machine learning, for fraud detection.

Keyword: Fraud, Financial Statement Fraud, Fraud Detection, Machine Learning, Artificial Intelligence.

JEL Classification: M42, C55.

---

1. doi: 10.22051/jera.2025.49905.3399
2. Assistant Professor, Faculty of Tourism, College of Management, Tehran University, Tehran, Iran. (Corresponding Author).(zahrataheri@ut.ac.ir).
3. Ph.D. Student, Department of Accounting, Faculty of Accounting and Financial Sciences, College of Management, University of Tehran, Tehran, Iran. (nazari.saeideh@ut.ac.ir).
4. Ph.D. Student, Department of Accounting, Faculty of Accounting and Financial Sciences, College of Management, University of Tehran, Tehran, Iran. (samavatmilad@ut.ac.ir).

فصلنامه پژوهش‌های تجربی حسابداری «نشریه علمی»

دانشگاه الزهرا (س)، دانشکده علوم اجتماعی و اقتصادی

پژوهش‌های تجربی حسابداری، سال پانزدهم، شماره ۵۷، پاییز ۱۴۰۴، صص ۳۴-۱

از روش‌های سنتی تا یادگیری ماشین: تحول کشف تقلب در حسابرسی با فناوری‌های نوین[۱]

زهرا طاهری[۲]، سعیده نظری[۳]، میلاد سماوات[۴]

مقاله پژوهشی

تاریخ دریافت: ۱۴۰۳/۱۱/۱۴
تاریخ پذیرش: ۱۴۰۴/۰۵/۱۴

چکیده

تقلب در صورت‌های مالی پدیده‌ای جهانی است که پیامدهای منفی قابل‌توجهی برای کلیه ذینفعان دارد با این حال تشخیص تقلب به‌دلیل ماهیت ذهنی آن، امری دشوار است. هدف این پژوهش بررسی فرصت‌ها و چالش‌ها و انتقادات مرتبط با روش‌های آماری و تکنیک‌های یادگیری ماشین برای کشف تقلب است. در این پژوهش ضمن مرور ادبیات در مورد کشف تقلب حسابداری و حسابرسی با استفاده از یادگیری ماشین به بحث در مورد چالش ها و انتقادات مطرح شده در این خصوص پرداخته شده است. مرور ادبیات نشان می‌دهد که مدل‌های رگرسیون لجستیک به‌طور سنتی در مطالعات کشف تقلب استفاده شده‌اند اما پیشرفت‌های اخیر در هوش مصنوعی و یادگیری ماشین، فرصت‌های جدیدی برای شناسایی تقلب مالی فراهم کرده است. علی‌رغم مزایای بالقوه، استفاده از روش‌های یادگیری ماشین در کشف تقلب با چالش‌ها و انتقادات جدی روبرو است. این پژوهش در درک بهتر فرصت‌ها و چالش‌ها و انتقادات مرتبط با کاربرد روش‌های نوینی همچون یادگیری ماشین برای کشف تقلب، یاری می‌رساند.

واژه‌های کلیدی: تقلب، تقلب در صورت‌های مالی، کشف تقلب، یادگیری ماشین، هوش مصنوعی.

طبقه‌بندی موضوعی: C55،M42

---

۱. doi: 10.22051/jera.2025.49905.3399

۲. استادیار، گروه گردشگری، دانشکده مدیریت، دانشگاه تهران، تهران، ایران. (نویسنده مسئول). (zahrataheri@ut.ac.ir).

۳. دانشجوی دکتری، گروه حسابداری، دانشکده حسابداری و علوم مالی، دانشکدگان مدیریت، دانشگاه تهران، تهران، ایران. (nazari.saeideh@ut.ac.ir).

۴. دانشجوی دکتری، گروه حسابداری، دانشکده حسابداری و علوم مالی، دانشکدگان مدیریت، دانشگاه تهران، تهران، ایران. (samavatmilad@ut.ac.ir).

مقدمه[۱]

تقلب در همه جنبه های زندگی وجود دارد و تأثیر چشمگیری بر اقتصاد، قانون و حتی ارزشهای اخلاقی انسانی دارد(الکسوپولوس و همکاران[۲]،۲۰۰۷). ادبیات حسابداری و حسابرسی هیچ توافق و اجماع نظری در خصوص تعریف تقلب در صورت‌های مالی ارائه نداده است(احمدی و همکاران،۱۴۰۳) از این رو تعاریف زیادی از تقلب و فعالیت های متقلبانه وجود دارد. انجمن بازرسان خبره تقلب[۳] در سال ۲۰۰۲ تقلب را به صورت «استفاده از شغل خود برای منتفع سازی شخصی از طریق سوء استفاده عمدی یا استفاده نادرست از منابع یا دارایی های سازمان استخدام کننده» تعریف می‌کند. و به ضرورت استفاده حسابرسان از تکنیک ها و روش‌های حرفه ای برای کشف تقلب در سطح صورت‌های مالی تأکید داشته است(عباس تفرشی و سلیمانی امیری، ۱۴۰۳). باید گفت تقلب در صورت‌های مالی نیز اثرات نامطلوب قابل‌توجهی بر اعتماد سرمایه‌گذاران و نظم بازار دارد و اعتماد به افشاهای شرکت ها را کاهش و عدم اطمینان در مورد صورت‌های مالی و هزینه سرمایه را افزایش می‌دهد(گراهام و همکاران[۴]،۲۰۰۸). افزایش در تعداد تقلب‌ها، تحریف‌ها برای شرکت‌ها و جامعه هزینه‌بر است(فتاحی نافچی و همکاران، ۱۴۰۳). باید اشاره کرد کشف تقلب در واقع دومین لایه حفاظتی در برابر تقلب بعد از پیشگیری است(عبدالله و همکارا ن[۵]، ۲۰۱۶). از آنجا که لایه پیشگیری همیشه کارآمد و قوی نیست(لوپس و همکاران[۶]،۲۰۱۱) موضوع کشف تقلب بااهمیت تر می‌شود. این امر برای حسابرسان نیز دارای اهمیت است چرا که یکی از معیارهای حسابرسی باکیفیت از منظر استفاده‌کنندگان عاری بودن صورت‌های مالی از تقلب و اشتباه است(رضایی و همکاران،۱۴۰۳). وقوع این تقلب‌ها ابهاماتی را در مورد کفایت و اثربخشی کنترل های داخلی نیز مطرح می‌کند(مشایخی و همکاران،۱۴۰۲).

پژوهش های قبلی در مورد کشف تقلب شرکتی عمدتاً بر استفاده از رگرسیون لجستیک متمرکز بود که در این خصوص می‌توان مدل‌های M-Score و F-Score که توسط بنیش[۷]

---

۱. مقاله منتخب بیست و دومین همایش ملی حسابداری ایران: اسفند ۱۴۰۳

2 . Alexopoulos et al
3 . Association of Certified Fraud Examiners
4 . Graham et al
5 . Abdallah et al
6 . Lopes et al
7 . Beneish

(۱۹۹۹) و دیچاو و همکاران[1](۲۰۱۱) انجام شده اند، را نام برد. با پیشرفت در الگوریتم‌های یادگیری ماشین و در دسترس بودن قدرت محاسباتی بالا در سال‌های اخیر، مطالعات بیشتری در مورد استقرار مدل‌های یادگیری ماشین ظاهر شده‌اند. مطالعاتی که بائو و همکاران[2](۲۰۲۰)، برتومئو و همکاران[3](۲۰۲۱) و بانسال و همکاران[4](۲۰۲۵) و همکاران انجام دادند نشان داد که الگوریتم‌های یادگیری ماشین می‌توانند به طور موثر برای شناسایی تقلب مالی و عملکرد بهتر از مدل‌های تشخیص تقلب به‌طور سنتی استفاده شوند. البته این روش‌ها نیز با نقد هایی مواجه اند که برتری آنها را بر روش‌های آماری با تردید روبه رو کرده است. علی رغم برتری که برخی پژوهش گران برای روش‌های یادگیری ماشین در حوزه کشف تقلب قائل هستند، با این حال تحقیقات اخیر صورت پذیرفته توسط انجمن بازرسان خبره تقلب نشان می‌دهد که تنها ۱۳ درصد از سازمان‌ها در سراسر صنایع از این فناوری‌ها برای شناسایی و جلوگیری از تقلب استفاده می¬کنند، که این مسأله دلایل آشکار و پنهان زیادی دارد که باعث بروز چالش های زیادی در بکارگیری این روش‌های نو شده است.

صرف‌نظر از دستورالعمل‌های تعیین‌شده در حوزه تقلب، ممکن است تشخیص تقلب امری دشوار باشد(کراجا و همکاران[5]، ۲۰۲۰). وظیفه یافتن ناهنجاری‌ها در صورت‌های مالی بر عهده حسابرسان است. با این وجود، آنطور که انجمن بازرسان رسمی تقلب در سال ۲۰۲۰ گزارش می‌دهند حسابرسان داخلی و خارجی در تشخیص تقلب، به ترتیب تنها با نرخ های پانزده و چهار درصد موفق عمل کرده اند. با وجود این خلاء، در نتیجه طبیعی است که سیستم‌های خودکار توجه بیشتری را برای شناسایی صورت‌های مالی متقلبانه را به خود جلب کنند. به طور خاص، این ابزارها برای سهامداران در قضاوت آگاهانه، برای واحدهای حسابداری و حسابرسی در تکمیل سریع و دقیق حسابرسی یاری رسان است(آگراوال و کوپر[6]، ۲۰۱۵). در این پژوهش تلاش شده است تا مروری اجمالی بر روند تکاملی روش‌های کشف تقلب، از روش‌های سنتی گرفته تا روش‌های یادگیری ماشین پرداخته شود. در جدول شماره ۱ به اختصار به مواردی که در مقاله در خصوص روش‌های سنتی و نوین به آن پرداخته خواهد شد اشاره شده است.

1 . Dechow et al
2 . Bao et al
3 . Bertomeu et al
4 . Bansal et al
5 . Craja et al
6 . Agrawal and Cooper

جدول ۱. مقایسه روش‌های سنتی و نوین در کشف تقلب، چالش ها و ملاحضات

روش کشف تقلب	سنتی	مدل بنیش و همکاران(۱۹۹۹)، مدل دیچاو و همکاران(۲۰۱۱)، قانون بنفورد[1](۱۹۳۸)	معایب	کشف تقلب در زمان غیر واقعی، مستعد خطای انسانی، نیازمند تیم های تخصصی ماهر و هزینه بر، دقت پایین، دشوار بودن، کارایی پایین، تمرکز بر داده های گسسته، شناسایی صرفاً حملات شناخته شده و مرسوم
	نوین	روش‌های یادگیری ماشین روش تشخیص ناهنجاری: (تحت نظارت، نظارت نشده، نیمه نظارتی)	معایب	تفسیر پذیری کم، نشت داده، حساسیت زیاد به داده ورودی، نیازمند داده زیاد برای فرآیند آموزش، هزینه محاسباتی زیاد
			مزایا	دقت، کارایی، قابلیت بالا، توان ارزیابی بالاتر
			هشدار	تراکنش های غیرعادی لزوماً تراکنش ناسالم نیستند تراکنش های عادی لزوماً تراکنش سالم نیستند. توضیح پذیری مدل ها
چالش های کشف تقلب	موارد نادر تقلب کشف شده		راه حل	کاهش عدم تعادل با تطبیق
	خصمانه بودن تقلب		راه حل	ندارد
	کشف نشدن تقلب		راه حل	استفاده توأم از داده های حسابداری و داده های همگن
	تقلب سریالی		راه حل	استفاده از مدل LSTM
	تغییر حالت تقلب		راه حل	استفاده از چارچوب فرایادگیری
ملاحضات عملی در مدلسازی	داده ها: کمیت، یکپارچگی، مازاد داده، سوگیری داده ها			
	روش‌ها: رگرسیون لجستیک، یادگیری ماشین			
	معیار ارزیابی برای مدل ها: دقت، دقت متعادل(BAC)، AUC			

منبع: نویسندگان

مرور ادبیات

کشف تقلب سعی می‌کند فعالیت های متقلبانه را هنگام ورود به سیستم‌ها کشف و شناسایی کند و آنها را به مدیر سیستم گزارش دهد(بهداد و و همکاران[2]، ۲۰۱۲). ادبیات موجود در حوزه

1 . Benford

2 . Behdad et al

کشف تقلب را می‌توان به دو نوع روش‌های آماری(سنتی) و روش‌های مبتنی بر یادگیری ماشین تقسیم کرد، که در قسمت های آتی سعی شده است به مرور اجمالی آن ها پرداخته شود.

۱. روش‌های آماری(سنتی) کشف تقلب

یکی از رویکرد های آماری(سنتی) موجود در خصوص کشف تقلب رویکرد مورد استفاده در مدل بنیش(۱۹۹۷ و ۱۹۹۹) است که یک مدل ریاضی است که از هشت نسبت مالی برای شناسایی اینکه آیا یک شرکت سود خود را دستکاری کرده است یا خیر استفاده می‌کند. در این روش یک امتیاز برای توصیف درجه ایجاد می‌شود(عمر و همکاران[1]، ۲۰۱۴). در ادامه بنیش و نیکولز[2] (۲۰۰۹) اقدام به اصلاح این مدل کردند به نحوی که متغیرهای مربوط به احتمال و انگیزه‌های تقلب را در نظر می‌گیرد و به کاربر این امکان را می‌دهد تا به جای بررسی مجزا، جنبه‌های مختلف عملکرد شرکت را به طور همزمان ارزیابی کند. لازم به ذکر است که این یک مدل احتمالی است، بنابراین دستکاری‌ها را با دقت صد در صد تشخیص نمی‌دهد(آگاگاله و همکاران[3]،۲۰۱۶). کردستانی و تاتلی(۱۳۹۵) نیز بیان می¬کنند که به کارگیری مدل بنیش برای پیش بینی دستکاری سود در ایران به علت آنکه ضرایب مدل اولیه در محیطی اقتصادی متفاوت نسبت به محیط ایران، تعیین شده است ممکن است با خطای زیادی همراه باشد.

یکی دیگر از رویکرد های آماری(سنتی) در ادبیات مدل دیچاو و همکاران(۲۰۱۱) است که به آن مدلF- score نیز گفته می‌شود. این مدل یک ابزار عمومی جهت ارزیابی ریسک تقلب است در این مدل از روشی مشابه با بنیش(۱۹۹۷، ۱۹۹۹) در ایجاد امتیازی برای پیش‌بینی اینکه کدام شرکت‌ها دارای تحریفات حسابداری با اهمیت هستند، پیروی کردند. اما به شکلی جامع‌تر، چرا که در آن تمامی اطلاعاتی که توسط فرآیند حسابداری و حسابرسی به صورت اجباری منتشر می‌شود را مدنظر قرار می‌دهد. در مجموع ۲۸ متغیر خوشه‌بندی شده حول ۵ نوع اطلاعات شامل کیفیت اقلام تعهدی، عملکرد، اقدامات غیرمالی، فعالیت‌های خارج از ترازنامه و معیارهای مبتنی بر بازار بررسی می‌شود. در نتیجه سه مدل رگرسیون لجستیک برآورد می‌شود که به ترتیب ۷، ۹ و ۱۱ متغیر را لحاظ کرده است. مدل اول شامل متغیرهایی از صورت‌های مالی اولیه است، مدل دوم دارایی های خارج از ترازنامه و اقدامات غیرمالی را اضافه می‌کند و مدل

1 . Omar et al
2 . Beneish and Nichols
3 . Aghghaleh et al

سوم متغیرهای مرتبط با بازار را اضافه می کند. البته دیچاو و همکاران(۲۰۱۱) دریافتند که اولین مدل آنها "بخش عمده ای از قدرت" را در پیش بینی تحریفات حسابداری با اهمیت ارائه می‌دهد. معزی و همکاران(۱۴۰۳) نیز دریافتند شاخص دیچاو در تشخیص احتمال دستکاری در صورتهای مالی شرکتهای پذیرفته شده در بازار بورس اوراق بهادار تهران بهتر از شاخص بنیش عمل کرده است.

یکی دیگر از تکنیک های کشف تقلب استفاده از قانون بنفورد(۱۹۳۸) در این زمینه است. تجزیه و تحلیل قانون بنفورد(۱۹۳۸) یک تکنیک ریاضی برای شناسایی الگوهای نامنظم در داده ها است. طبق این قانون بنفورد(۱۹۳۸) وقوع موقعیتی یک رقم خاص در یک فایل تصادفی بزرگ از اعداد با فراوانی قابل پیش بینی رخ می‌دهد. در این مدل با مقایسه نرخ وقوع واقعی ارقام با مقادیر مورد انتظار آنها بر اساس قانون بنفورد(۱۹۳۸)، یک مبنای ریاضی برای بررسی خطر تحریف با اهمیت و شناسایی فعالیت‌های بالقوه متقلبانه به وجود می‌آید(استامباغ و همکاران[1]، ۲۰۱۲). اگرچه این قانون در ابتدا صرفاً یک کنجکاوی ریاضی تلقی می‌شد، اما نیگرینی و میترمایر[2](۱۹۹۷) و نیگرینی[3](۱۹۹۹) کاربرد آن را در کشف تقلب حسابداری نشان دادند. اساس این روش بر این منطق استوار است که ساختن داده‌های مصنوعی که از قانون بنفورد(۱۹۳۸) پیروی کنند، دشوار است. هاشمی و حریری(۱۳۹۶) نیز دریافتند که توزیع ارقام صورت‌های مالی از قانون بنفورد(۱۹۳۸) تبعیت کرده و می‌توان برای بررسی تقلب در صورت‌های مالی از این قانون استفاده کرد.

۲. حرکت به سمت روش‌های جدید تر در کشف تقلب

تکنیک‌های مرسوم در کشف تقلب مانند تأیید و بازرسی دستی، غیردقیق، پرهزینه و زمان‌بر بودند. با ظهور هوش مصنوعی، سیستم‌های خودکار کشف تقلب توسعه یافتند، اما نسل اول این سیستم‌ها محدود به قوانین از پیش تعریف شده بودند که توسط متخصصان بیان می‌شد(لی و همکاران[4]، ۲۰۰۸). در این راستا سیستم‌های کشف تقلب های پیچیده تری که طیف وسیعی از روش‌های داده کاوی را با هم ادغام می کنند برای شناسایی موثر تقلب مورد نیاز هستند، که این

1 . Stambaugh et al
2 . Nigrini and Mittermaier
3 . Nigrini
4 . Li et al

قبیل سیستم‌ها در حال توسعه هستند(سراوانان و همکاران[1]، ۲۰۱۴). داده کاوی شامل تکنیک‌های آماری، ریاضی، هوش مصنوعی و یادگیری ماشینی برای استخراج و شناسایی اطلاعات مفید و دانش بعدی از پایگاه های داده بزرگ(سیستم‌های پشتیبانی تصمیم و سیستم‌های هوشمند) است. این سیستم‌ها دارای چندین مزیت اصلی شامل ، استخراج خودکار الگوی تقلب از داده ها، امکان اولویت بندی موارد مشکوک بر اساس احتمال تقلب و توانایی افشای انواع جدید تقلب شود که قبلاً تعریف نشده بودند(لی و همکاران، ۲۰۰۸). روش‌های داده کاوی شامل شش دسته اصلی می‌باشد که عبارتند از: طبقه بندی، خوشه بندی، رگرسیون، تشخیص داده‌های پرت، تجسم و پیش بینی(نور و همکاران[2]، ۲۰۱۵). البته هر یک از این روش‌ها توسط تکنیک های خاصی پشتیبانی می‌شود(هان و همکاران[3]، ۲۰۱۲).

در مورد تشخیص تقلب شرکت ها، ادبیات در درجه اول به نسبت مالی به عنوان متغیرهای مستقل متکی است. با این وجود، در سالهای اخیر تعداد متغیرهای مستقل افزایش یافته است تا عملکرد این مدل ها را افزایش دهد. بائو و همکاران(۲۰۲۰) و وی و همکاران[4](۲۰۱۷) از متغیرهای مالی خام استخراج شده از صورت‌های مالی شرکت برای ساخت مدل خود استفاده کرد و عملکرد آنها را با مدل هایی که از نسبت های مالی استفاده می‌کردند مقایسه کرد. یافته‌های آنها نشان می‌دهد که متغیرهای مالی خام می‌توانند منجر به بهبود مدل تشخیص تقلب در مقایسه با نسبت های مالی شوند. مطالعه انجام شده توسط برتومئو و همکاران(۲۰۲۱)، که برای کشف تحریف ها استفاده شد، نشان داد که وقتی متغیرهای مالی و غیر مالی برای ساخت مدل ترکیب شدند، اهمیت متغیرهای غیر مالی بیشتر از اهمیت متغیر مالی است.

کشف تقلب مبتنی بر ناهنجاری: سیستم‌های کشف تقلب رویکرد تشخیص ناهنجاری را مورد استفاده قرار می‌دهند و بر روش‌های پروفایل رفتاری تکیه می‌کنند، که در آن الگوی رفتاری هر فرد مدل شده و برای هرگونه انحراف از هنجار تحت نظارت قرار می‌گیرد(جیوثسنا و و رامافراساد[5]،۲۰۱۱) این رویکرد پتانسیل تشخیص تقلب جدید را دارد. به همین دلیل است که بیشتر توسط ادبیات سیستم‌های کشف تقلب مورد استفاده قرار می‌گیرد (سان و همکاران[6]،

1 . Saravanan et al
2 . Noor et al
3 . Han et al
4 . Wei et al
5 . Jyothsna and Rama Prasad
6 . Sun et al

۲۰۰۶). این روش را می توان به سه نوع طبقه بندی کرد که شامل تشخیص ناهنجاری بدون نظارت، نیمه نظارت شده و تحت نظارت است(آخیلومن[1]، ۲۰۱۳). که در ادامه به طور خلاصه به شرح آنها پرداخته خواهد شد.

رویکرد تحت نظارت: تکنیک‌های یادگیری تحت نظارت به مجموعه داده‌ای نیاز دارند که با عنوان «تقلب» و «غیر تقلب» برچسب‌گذاری شده است و شامل آموزش یک طبقه‌بندی کننده است، این رایج ترین رویکرد یادگیری است. مزیت اصلی یادگیری نظارت شده این است که تمام خروجی های کلاس ها که توسط الگوریتم این رویکرد دستکاری می‌شوند برای انسان معنادار هستند و به راحتی می¬توان از آن برای طبقه بندی الگوهای متمایز و رگرسیون داده ها استفاده کرد. به عبارت ساده تر در این حالت تابعی وجود دارد که متغیر های مستقل(متغیر های تأثیر گذار بر تقلب) و متغیر وابسته(تقلب) هر دو معلوم هستند که پژوهشگر به دنبال طبقه بندی کردن آنها(با اعمال یادگیری و آزمون) است. با این حال، این رویکرد دارای چندین محدودیت است، اولین محدودیت به دلیل دشواری جمع آوری برچسب ها ایجاد می‌شود. دومین محدودیت این است که، گاهی اوقات یافتن برچسب متمایز بسیار دشوار است، به عبارتی عدم قطعیت ها و ابهاماتی در نظارت یا برچسب ها وجود دارد. این محدودیت‌ها ممکن است در برخی موارد مانع اجرای رویکردهای یادگیری تحت نظارت شود. برای غلبه بر این معایب، یادگیری بدون نظارت و یادگیری نیمه نظارتی مورد استفاده قرار می گیرند(لیو و وو[2]، ۲۰۱۲). این رویکرد الگوریتم های زیادی را در بر می گیرد که برخی از آنها عبارتند از: ۱) الگوریتم‌های طبقه بندی(برای مثال؛ شبکه عصبی مصنوعی ، نزدیک ترین همسایه k ام، درختان، رگرسیون لجستیک ، تکنیک های بیز ساده و دستگاه بردار)، ۲) الگوریتم های رگرسیون(برای مثال رگرسیون خطی، رگرسیون ساده و رگرسیون لجستیک).

رویکرد نظارت نشده: تکنیک‌های یادگیری بدون نظارت، تقلب را در مجموعه داده‌های آزمایشی بدون برچسب، با این فرض که اکثر نمونه‌های مجموعه داده غیر تقلبی هستند، شناسایی می کنند. برخلاف تکنیک نظارت شده، بدون نظارت به این معنی است که هیچ برچسب کلاسی برای ساخت مدل وجود ندارد. مزیت اصلی استفاده از رویکرد بدون نظارت این است که به

1 . Akhilomen
2 . Liu and Wu

شناسایی دقیق داده‌های برچسب که اغلب کمبود دارند یا وجود ندارند، متکی نیست(بولتون و هند[1]،۲۰۰۱). دو الگوریتم کلاسیک ساده مورد استفاده در یادگیری بدون نظارت عبارتند از: ۱) الگوریتم های خوشه بندی(مانند تکنیک های کا مینز)، ۲) الگوریتم های کاهش ابعاد (مانند تجزیه و تحلیل اجزای اصلی).

رویکرد نیمه نظارتی: یادگیری نیمه نظارتی بین یادگیری نظارت شده و بدون نظارت قرار دارد زیرا شامل تعداد کمی از نمونه های برچسب دار و تعداد زیادی نمونه بدون برچسب است. هدف اصلی رویکرد نیمه نظارت شده آموزش یک طبقه‌بندی کننده از داده‌های برچسب‌دار و بدون برچسب است(ژو و همکاران[2]،۲۰۱۱؛ آخیلومن،۲۰۱۳). یادگیری نیمه نظارت شده در مقایسه با یادگیری نظارت شده مزیت بیشتری دارد زیرا با استفاده از داده های برچسب دار و بدون برچسب، اما با نمونه های برچسب گذاری شده کمتر، عملکرد بهتری را به دست می‌آورد. علاوه بر این، یادگیری نیمه نظارت شده یک مدل محاسباتی برای درک یادگیری دسته‌بندی انسانی نیز ارائه می‌کند، که در آن بیشتر ورودی‌ها به وضوح بدون برچسب هستند(ژو و گولدبرگ[3]، ۲۰۰۹).

افراد متقلب با اقدامات جدید پیشگیری و تشخیص سازگار هستند، بنابراین تشخیص تقلب باید با گذشت زمان روند تطبیقی داشته و تکامل یابد. با این حال ، کاربران مشروع نیز ممکن است به تدریج رفتار خود را در مدت زمان طولانی تر تغییر دهند و بنابراین جلوگیری از هشدارهای فریبنده مهم است(بولتون و هند، ۲۰۰۲).

توسعه اخیر در هوش مصنوعی به طور کلی و یادگیری ماشینی به طور خاص، فضاهای بالقوه جدیدی را برای مقابله با تقلب باز کرده است(حافظ و همکاران[4]، ۲۰۲۵). با این حال، تحقیقات اخیر توسط شرکت نرم‌افزاری سس و انجمن بازرسان خبره تقلب نشان می‌دهد که تنها ۱۳ درصد از سازمان‌ها در سراسر صنایع از این فناوری‌ها برای شناسایی و جلوگیری از تقلب استفاده می‌کنند. دلایل مختلفی برای این عدم اجرای نسبی وجود دارد. در واقع، استفاده از تکنیک هوش مصنوعی برای همه انواع فعالیت های متقلبانه به یک اندازه مناسب نیستند.

1 . Bolton and Hand
2 . Zhu et al
3 . Zhu and Goldberg
4 . Hafez et al

بائو و همکاران(۲۰۲۰) اشاره کردند که یادگیری ماشین هنوز با مشکلات پیچیده تری دست و پنجه نرم می کند درست است که این فناوری اخیراً در زمینه تشخیص چهره، صدا و متن پیشرفت خوبی داشته است به این علت که در این موارد، داده های فراوانی موجود است. در مقابل، یادگیری ماشینی ممکن است در موقعیت‌های اجتماعی پیچیده‌تر، به‌خوبی کار نکند، به‌ویژه اگر در دوره‌های طولانی اتفاق افتاده باشد. در این مورد، قوانین ساده یا قضاوت انسانی ممکن است مؤثرتر باشد. در قسمت بعدی این پژوهش به چند مورد از چالش های یادگیری ماشین در خصوص کشف تقلب پرداخته خواهد شد.

۳. چالش های کشف تقلب

مشکلات در مورد تقلب و یادگیری ماشین به طور کلی: مشکل اول این است که موارد تقلب کشف شده نادر هستند، یادگیری زمانی که نمونه ها نامتعادل هستند، برای الگوریتم‌ها دشوار است زیرا اغلب با موارد تقلب مواجه نمی‌شوند. مشکل دوم اینکه، تقلب حالتی خصمانه دارد، تکنیک‌های یادگیری ماشین زمانی بهترین کار را انجام می‌دهند که الگوها پایدار باشند و داده‌های مهم به طور سیستماتیک حذف نشوند یا بدتر از آن مورد دستکاری قرار نگرفته باشند. در بسیاری از کاربردهای یادگیری ماشینی، طرفین با سیستم همکاری می کنند تا یادگیری آن را تسهیل کنند یا در بدترین حالت، نسبت به آن بی طرف هستند. در مورد تقلب، مرتکبین سعی می¬کنند از یادگیری جلوگیری کنند. علاوه بر این، افرادی که درگیر تقلب کردن هستند دائماً در حال تصور طرح های جدید هستند. بنابراین، ممکن است سابقه ای برای الگوریتم ها برای شناسایی نوع جدیدی از تقلب وجود نداشته باشد.

مشکلات تقلب حسابداری و یادگیری ماشین: جدای از این نگرانی های کلی، انواع خاصی از کلاهبرداری می‌تواند مسائل خاصی داشته باشد. با تمرکز بر تقلب حسابداری باید گفت اولاً، بسیاری از موارد تقلب حسابداری کشف نشده باقی می‌مانند یا حداقل زمان زیادی طول می¬کشد تا شناسایی شوند. در مقابل، تعیین وجود یک تقلب حسابداری در بسیاری از موارد به منابع تحقیقاتی قابل توجهی نیاز دارد و تشخیص تمایز بین شیوه‌های خلاقانه اما مشروع و تقلب ممکن است دشوار باشد. علاوه بر این، موارد تقلب حسابداری اغلب توسط نظارت‌کنندگان شناسایی می‌شود. در مقابل، سایر انواع تقلب ها ممکن است توسط قربانی شناسایی شود. هر قدر که نظارت کنندگان ناکارآمد باشند و یا مغرضانه عمل کنند، مدل‌های

کشف تقلب نیز ناکارآمد و مغرضانه خواهند بود. به عنوان مثال، دایک و همکاران[1](۲۰۲۰) تخمین می زند که تنها حدود نیمی از موارد نقض شدید گزارشگری مالی توسط کمیسیون بورس و اوراق بهادار شناسایی می شود. البته این موضوع احتمالاً در کشورهای کمتر توسعه‌یافته با محیط‌های نهادی ضعیف‌تر، جدی‌تر خواهد بود.

ثانیاً، اگر شرکتی مرتکب تقلب حسابداری شود، این تمایل در آن وجود دارد که تا چندین سال قبل از برملا شدن موضوع تقلب، گزارش های حسابداری را اشتباه بیان کند، اما اکثر مطالعات پیش‌بینی تقلب موجود در ادبیات، این ویژگی تقلب سریالی را در ساخت مدل در نظر نمی¬گیرند. در عوض، آنها تمایل دارند هر سال شرکت را به عنوان یک مشاهده مستقل در نظر بگیرند، و وابستگی سری زمانی موارد تقلب سریالی را نادیده بگیرند. مطالعاتی که موضوع تقلب سریالی را در نظر می گیرند، تنها با استفاده از سال تقلب اولیه(آمیرام و همکاران[2]، ۲۰۱۵) یا همانند براون و همکاران[3](۲۰۲۰) با حذف مشاهدات تقلب زنجیره‌ای در سال آموزشی یا سال آزمون از این مشکل عبور کرده اند.

ثالثاً، به دلیل تنوع زمانی در انگیزه های مدیریتی و شدت نظارت، رفتار تقلب حسابداری هم در طول زمان و هم به صورت مقطعی تغییر حالت را نشان می‌دهد(بیزلی و همکاران[4]، ۱۹۹۹؛ بیزلی و همکاران، ۲۰۱۰). تحقیقات پیشین همچون دیچاو و همکاران(۲۰۱۱) نشان می‌دهد که فراوانی تقلب حسابداری به طور قابل توجهی در صنایع مختلف متفاوت است. عباسی و همکاران[5](۲۰۱۲) احتمالاً تنها پژوهشی از بین مدل‌های پیش‌بینی تقلب حسابداری موجود است که چنین تغییرات حالتی را در ساخت مدل گنجانده است.

٤. ملاحظات عملی در مدل سازی

همانطور که عباسی و همکاران(۲۰۱۲) در پژوهش خود اشاره کرده اند، لازمه‌ی ساخت هر مدل پیش‌بینی تقلب، آن است که محقق تصمیمات مهمی را در مورد سه جزء حیاتی به شرح زیر اتخاذ کند:(الف) چه ورودی‌های داده (پیش‌بینی کننده‌ها) و خروجی‌های داده(برچسب‌های تقلب) باید برای مدل مورد استفاده قرار گیرد؟(ب) چه روش‌های یادگیری ماشین خاصی باید

1 . Dyck et al
2 . Amiram et al
3 . Brown et al
4 . Beasley et al
5 . Abbasi et al

برای کار پیش‌بینی استفاده شود؟(ج) چه معیارهای ارزیابی باید برای قضاوت در مورد عملکرد یک مدل پیش‌بینی تقلب مورد استفاده قرار گیرد؟ در ادامه، هر یک از سه مولفه فوق توضیح داده می‌شود.

الف. داده ها

در حرکت سیستم‌ها از قوانین به مدل های ساختاری ساده، از مدل های ساختاری به یادگیری ماشین و از یادگیری ماشین به یادگیری عمیق، مقدار و کیفیت داده هایی که مدل ها به آن نیاز دارند افزایش می یابد. این مسأله چند چالش ایجاد می کند.

اولین چالش کمیت داده است. این مسئله به تدریج حل می‌شود زیرا هزینه به دست آوردن و ذخیره سازی داده های ساخت یافته در انبارهای داده و داده های بدون ساختار در دریاچه های داده[1] کاهش می یابد. با این حال، برای سازمان‌های کوچک‌تر، موقعیت‌های نادر یا برآوردهای بسیار پیچیده، این موضوع می‌تواند همچنان به عنوان یک مشکل حل نشده باقی بماند.

چالش دوم یکپارچگی و جامعیت داده ها است. یک جریان سیل آسا از داده‌هایی که از منابع ناهمگن پدید می‌آیند، اگر به درستی ساختار نیافته باشند، هیچ فایده‌ای ندارند. نگهداری داده‌ها به تنهایی یک چالش است. سیستم‌های قدیمی معمولاً زمانی که نیاز به تعامل با پلتفرم‌های یادگیری ماشین دارند، از مشکلات یکپارچه‌سازی رنج می‌برند. گردش کار، مدیریت داده، و کنترل‌های تغییر آن‌ها اغلب با نیازهای یک سیستم یادگیری ماشین مدرن هماهنگ نیست. این مشکل زمانی کاهش می‌یابد که سیستم یادگیری ماشین به طور موازی به کار گرفته شود(به عنوان مثال، تجزیه و تحلیل پس از تراکنش ها برای برآورده کردن الزامات مبارزه با پولشویی) اما زمانی که مستقیماً در جریان کار ادغام شود(مثلاً در فرآیند پرداخت) تشدید می شود. می‌توان کیفیت کلان داده ها را در چهار بعد ارزیابی کرد: حجم، سرعت، تنوع و صحت. متأسفانه، سه بعد اول می‌تواند مانع بعد چهارم(صحت) شود. همانطور که اشاره شد یکی از چالش های ما در خصوص طراحی مدل های کشف تقلب نیاز به وجود داده های با کیفیت است و باید اشاره کرد با وجود اینکه اکثر سیستم‌های برنامه‌ریزی منابع سازمانی[2] دارای قابلیت‌های شناسایی و پیشگیری از تقلب هستند، اما متأسفانه سیستم‌ها اغلب این قبیل کنترل‌ها را خاموش می‌کنند با این توجیه که به این ترتیب سیستم کارآمدتر عمل خواهد کرد.

1 . Data lakes
2 . Enterprise resource planning (ERP)

چالش سوم که تا حدودی با موارد قبلی متناقض است، مازاد داده است. با گذشت زمان، ساختار قانونی برای تنظیم جمع آوری و ذخیره اطلاعات ایجاد شده است. به عنوان مثال، در ایالات متحده مجموعه ای از مقررات ایالتی نیز به تدریج الزامات افشا را افزایش داده است گذشته از حفاظت از داده ها پس از جمع آوری آنها، سازمان باید ابتدا به قانونی بودن جمع‌آوری داده ها توجه کند.

چالش چهارم تعصب است، در واقع سوگیری‌ها نیز می‌توانند یک موضوع مهم باشند. داده‌های آموزشی برچسب‌گذاری‌شده می‌توانند دارای سوگیری باشند، زیرا افراد با سوگیری‌های ضمنی یا صریح با آنها رفتار کرده‌اند.

تقلب داده‌ها و صورت‌های مالی: اکثر مطالعات پیش‌بینی تقلب صورت‌های مالی، یادگیری نظارت شده را به کار می‌گیرند که به داده‌هایی در مورد برچسب‌های تقلب(متغیر وابسته) و پیش‌بینی‌کننده‌های تقلب(متغیرهای مستقل) نیاز دارد. اولین تصمیم مهمی که باید در ساخت یک مدل پیش‌بینی تقلب اتخاذ کرد، انتخاب یک پایگاه داده تقلب حسابداری مناسب است. داده های ورودی مختلفی وجود دارد که می¬توان از آنها برای ساخت مدل های پیش بینی تقلب استفاده کرد. بسیاری از مطالعات تنها از یک منبع داده استفاده می‌کنند. به عنوان مثال، دیچاو و همکاران(۲۰۱۱) بر روی داده های حسابداری در دسترس تمرکز دارد، سچینی و همکاران[1](۲۰۱۰) و پوردا و اسکیلی کورن[2](۲۰۱۵) فقط از داده های متنی استفاده می‌کنند، در حالی که دونگ و همکاران[3](۲۰۱۸) داده های متنی و شبکه را با هم ترکیب می‌کند. با این حال، مطالعات کمی تلاش کرده اند تا همه داده های ورودی موجود از انواع مختلف را در ساخت یک مدل پیش بینی تقلب متحد ترکیب کنند.

می‌توان ادعا کرد در این زمینه پژوهش‌های پیشین تا حدی وجود ابهام در مورد تقلب را نشان می‌دهد چرا که از اصطلاحات مختلفی برای توصیف تقلب یا تقلب ادعایی استفاده کرده است، واژه هایی مانند تقلب، رفتار نادرست، بی نظمی، گزارش نادرست و ارائه نادرست. بر این اساس، ادبیات تقلب حسابداری موجود از پایگاه‌های اطلاعاتی مختلفی برای اندازه‌گیری تقلب استفاده کرده است. در این راستا کارپوف و همکاران[4](۲۰۱۷) مقایسه دقیقی از مزایا و معایب استفاده

1 . Cecchini et al
2 . Purda and Skillicorn
3 . Dong et al
4 . Karpoff et al

از چهار پایگاه داده مختلف برای تحقیقات سوء رفتار مالی ارائه می دهند و دریافتند که نتایج آزمایش‌های تجربی می‌تواند به این بستگی داشته باشد که به کدام پایگاه داده دسترسی داشته باشد.

دومین تصمیم مهمی که باید در ساخت مدل‌های پیش‌بینی تقلب اتخاذ کرد، انتخاب فهرستی از پیش‌بینی‌کننده‌های تقلب است. با انفجار داده های بزرگ در دهه گذشته، انواع مختلفی از عوامل پیش بینی کننده وجود دارد که می‌توان از آنها برای ساخت مدل های پیش بینی تقلب حسابداری استفاده کرد. ممکن است فرد وسوسه شود تا حد امکان پیش‌بینی‌کننده‌ها را برای آموزش و پیش‌بینی وارد مدل یادگیری ماشین کند، اما بائو و همکاران(۲۰۲۰) اینطور ابراز می‌کنند که پیش بینی کننده‌های بیشتر لزوماً عملکرد پیش بینی را بهبود نمی‌بخشد و استفاده از داده های بیشتر، باعث تحمیل هزینه های بیشتری نیز می‌شود و به این ترتیب مدل پیش بینی کمتر، قابل تعمیم به کشورها و صنایع مختلف خواهد بود. از این رو، یک چارچوب هزینه-منفعت نیز در انتخاب پیش‌بینی‌کننده‌های تقلب ضروری است. با پیروی از چارچوب هزینه-منفعت، می‌توانیم پیش‌بینی‌کننده‌های تقلب را بر اساس ماهیت داده‌های ورودی طبقه‌بندی کنیم که شامل داده‌های ساختاریافته(به عنوان مثال، اعداد حسابداری) در مقابل داده‌های بدون ساختار(مانند متن، ویدیو و صدا) است. پردازش داده‌های بدون ساختار مانند متن یا ویدئو بسیار سخت‌تر از داده‌های ساختاریافته است و از این رو پرهزینه‌تر نیز می‌باشد. علاوه بر این، اطلاعات مفیدی که در داده‌های بدون ساختار تعبیه شده‌اند، می‌توانند از قبل در داده‌های ساخت‌یافته موجود باشند. با توجه به در دسترس بودن روزافزون بسیاری از منابع داده ساختاریافته، منطقی است که ابتدا تا آنجایی که ممکن است قبل از اینکه برای پیش‌بینی تقلب به منابع داده‌ای بدون ساختار مراجعه کنیم اطلاعات مفیدی را از منابع داده ساختاریافته استخراج کنیم. همچنین می‌توان پیش‌بینی‌کننده‌های تقلب را بر اساس چارچوب های مختلفی که در ادبیات حوزه تقلب وجود دارد(از قبیل مثلث تقلب و...) ساخت، کما اینکه برخی از محققان این حوزه پژوهش خود را به این نحو انجام داده اند.

ب. روش‌ها

از آنجایی که تحلیلگران و پژوهشگران این حوزه معمولاً تقلب را با یک متغیر دودویی تعریف می‌کنند، رگرسیون‌های لجستیک محبوب‌ترین روش یادگیری در ادبیات تجاری قبل از

ظهور حوزه یادگیری ماشینی بوده است که پژوهشگران به نام این حوزه مثل دیچاو و همکاران(۲۰۱۱) نیز همین روش را در مدل خود انتخاب کرده بودند. با افزایش در دسترس بودن بسیاری از پایگاه های داده بدون ساختار و ظهور پیشرفت های روش شناختی، محققان و تحلیلگران شروع به استفاده از روش‌های یادگیری پیچیده تر برای آموزش و پیش بینی تقلب حسابداری می‌کنند. به عنوان مثال، سچینی و همکاران(۲۰۱۰) و پرولز و همکاران[1](۲۰۱۷) از ماشین‌های بردار پشتیبانی[2] برای آموزش یک مدل پیش‌بینی تقلب استفاده کردند. آمیرام و همکاران(۲۰۱۵) اما قانون بنفورد(۱۹۳۸) را برای پیش‌بینی تقلب مورد استفاده قرار دادند.

ج. معیارهای ارزیابی

معیارهای ارزیابی به طور کلی : یک مسئله در مورد الگوریتم ها این است که چه چیزی را باید به حداکثر برسانند. اغلب، هدف به حداکثر رساندن دقت با این فرض است که الگوریتم‌های کارآمد می‌توانند هم مثبت کاذب و هم منفی کاذب را به حداقل برسانند. توابع زیان پیچیده‌تر را می‌توان طراحی کرد و در الگوریتم ها گنجاند. این مبادلات مختلف باید قبل از تعریف الگوریتم ها تحلیل شوند. با این حال، تعریف تابع زیان بیش از یک تعریف فنی است. به عنوان مثال، سازمان ها باید بین تشخیص و تجربه مشتری تعادل برقرار کنند. الگوریتمی که طبقه‌بندی‌های بهتری ارائه می‌کند اما به درخواست‌های داده‌های محرمانه نیاز دارد، ممکن است کمتر از حد مطلوب باشد. این نگرانی بیشتر تعیین‌کننده می شود زیرا مقررات محدودیت های بیشتری را در مورد نوع داده‌هایی که سازمان ها می‌توانند جمع آوری کنند تحمیل می‌کند و مقررات آینده نیز ممکن است محدودیت هایی را بر روی تابع زیان الگوریتم اعمال کند. این قطع ارتباط بالقوه بین طراحی الگوریتم و محدودیت‌های استفاده ممکن است توضیح دهد که چرا برخی از آمارها نشان می‌دهند که تنها ۵۰ درصد از همه مدل‌های توسعه‌یافته تا کنون به مرحله استفاده رسیده‌اند.

معیارهای ارزیابی برای مدل های پیش بینی تقلب حسابداری: روش‌های مختلفی برای ارزیابی عملکرد مدل های پیش بینی وجود دارد. اولین معیار عملکرد طبقه‌بندی در نظر گرفته شده در ادبیات معیار "دقت" است که در سنجش آن تعداد سال-شرکت متقلبانه که به درستی

1 . Perols et al

2 . Support vector machine (SVM)

به عنوان تقلب طبقه‌بندی شده‌اند، تعداد سال-شرکت متقلبانه که به اشتباه به عنوان غیر تقلبی طبقه بندی شده اند، تعداد سال-شرکت غیر متقلبانه که به درستی به عنوان غیر تقلبی طبقه‌بندی شده اند و تعداد سال-شرکت غیر متقلبانه که به اشتباه به عنوان تقلب طبقه بندی شده اند در نظر گرفته می‌شود. البته بائو و همکاران(۲۰۲۰) دقت را به دلیل ماهیت نامتعادل تقلب‌ها در مقابل داده های غیر تقلبی رد کرد. برای مثال طی دوره ۱۹۷۹-۲۰۱۴، فراوانی تقلب کشف شده توسط نظارت کنندگان ایالات متحده(مثلاً SEC) بسیار کم بود(معمولا کمتر از ۱٪ از همه شرکت‌ها در سال) از این رو، یک استراتژی ساده‌انگارانه طبقه‌بندی تمام سال-شرکت به‌عنوان غیر متقلبانه است.

در این خصوص برای سنجش صحیح عملکرد یک مدل پیش‌بینی تقلب، بائو و همکاران(۲۰۲۰)، دقت متعادل[1] را به عنوان یک معیار ارزیابی عملکرد جایگزین در نظر گرفتند که البته این معیار هم با انتقادات فروانی رو به رو است. لارکر و زاکولیوکینا[2](۲۰۱۲) به دو محدودیت مهم این معیار اشاره می‌کنند. اول اینکه این معیار بر اساس یک آستانه احتمال تقلب پیش‌بینی‌شده خاص یک طبقه‌بندی‌کننده مشخص ساخته می‌شود، و این آستانه معمولاً به‌طور خودکار توسط طبقه‌بندی‌کننده تعیین می‌شود تا این معیار را به حداکثر برساند. در غیاب هیچ گونه دانشی از هزینه های طبقه بندی اشتباهات مثبت کاذب در مقابل هزینه های طبقه‌بندی اشتباه منفی های کاذب، نمی توان آستانه احتمال تقلب پیش بینی شده بهینه را برای اهداف طبقه بندی و ایجاد تمایز بین تقلب و غیر تقلب تعیین کرد. دوم اینکه، این معیار به فراوانی نسبی موارد مثبت و منفی در نمونه(به عنوان مثال، عدم تعادل داده ها) بسیار حساس است. برای اجتناب از این محدودیت‌ها، بائو و همکاران(۲۰۲۰) به پیروی از لارکر و زاکولیوکینا(۲۰۱۲) معیار ناحیه زیر منحنی[3]را به عنوان یکی از معیارهای ارزیابی عملکرد اتخاذ کردند. ناحیه زیر منحنی ویژگی‌های عملیاتی گیرنده[4] است. فاوست[5] (۲۰۰۶) توضیح می‌دهد که منحنی ویژگی عملیاتی گیرنده یک تصویر دو بعدی از عملکرد طبقه‌بندی‌کننده است که نرخ مثبت واقعی و نرخ مثبت کاذب را در یک نمودار ترکیب می‌کند. معیار ناحیه زیر منحنی تنها یک نقطه در منحنی ویژگی‌های

1 . Balanced Accuracy Curve (BAC)
2 . Larcker and Zakolyukina
3 . Area Under the Curve (AUC)
4 . Receiver operating characteristic (ROC)
5 . Fawcett

عملیاتی گیرنده را نشان می‌دهد. بسیاری از مدل‌های پیش‌بینی تقلب از ناحیه زیر منحنی به عنوان معیار ارزیابی عملکرد اولیه استفاده می‌کنند.

۵. هشدارهایی در مورد مدل های یادگیری ماشین

یادگیری ماشین می¬تواند در زمینه مبارزه با تقلب از سه طریق شناسایی و ممنوعیت، دعوی قضایی و پیشگیری مفید باشد. نمونه ای از شناسایی و ممنوعیت زمانی است که یک موسسه مالی در صورت فعالیت مشکوک، تراکنش های کارت اعتباری را در زمان واقعی مسدود می‌کند. دادخواهی وضعیتی است که در آن از تجزیه و تحلیل یادگیری ماشین برای ایجاد یک پرونده حقوقی استفاده می¬شود. پیشگیری رویکردی است که در آن یک سازمان از بینش های یادگیری ماشین برای انجام تجزیه و تحلیل علت اصلی، سازماندهی مجدد عملیات خود و به حداقل رساندن خطر تقلب در وهله اول استفاده می‌کند. هر رویکردی مجموعه ای از مسائل خاص خود را دارد.

در مورد تشخیص و ممنوعیت، خروجی بسیاری از الگوریتم‌ها یک امتیاز است که سطح ریسک مرتبط با یک موقعیت را پیش‌بینی می کند. با این حال، کاربران باید در مورد آنچه که پیش بینی می شود هشیار باشند. چراکه در بسیاری از موارد، الگوریتم تراکنش‌های غیرعادی را شناسایی می‌کند(یعنی آنهایی که با معیار مورد انتظار تفاوت دارند)، اما یک تراکنش غیرعادی لزوماً یک تراکنش مشکل‌ساز نیست. بنابراین باید گفت اگر تجزیه و تحلیل به درستی شرطی نشده باشد، عدم وجود ناهنجاری ظاهری می تواند مشکل ساز باشد. به عنوان مثال، پارمالات(بزرگترین مورد تقلب در حسابداری اروپا تا به امروز) قبل از افشای تقلب، نسبت های حسابداری بسیار پایداری داشت. علاوه بر این، آنچه طبیعی است می‌تواند ناپایدار باشد. به عنوان مثال، تغییرات در محیط نظارتی یا محیط اجتماعی-اقتصادی(به عنوان مثال، کووید۱۹) می‌تواند رفتار افراد را تغییر دهد و بنابراین به یک معیار جدید نیاز دارد. به طور طبیعی، الگوریتم‌ها می‌توانند یاد بگیرند، اما بعید است که تنظیم فوری انجام شود. همچنین، بسیاری از الگوریتم‌ها بر اساس آمار غیرخطی هستند که مدل‌های ناپایدار را به دست می‌دهند.

یکی دیگر از مسائل مربوط به امتیاز پیش بینی تقلب، توضیح پذیری است. الگوریتم‌های یادگیری ماشین کنونی در برخورد با این موضوع بسیار بد هستند. اهمیت این ضعف با هدف کشف تقلب

متفاوت است. اگر هدف پیشگیری از طریق ممنوعیت باشد(مثلاً کارت اعتباری)، نیاز به توضیح می‌تواند کمتر باشد. با این حال حتی در این شرایط نیز نمی‌توان موضوع را نادیده گرفت.

اگر هدف جلوگیری از تقلب از طریق دعوی قضایی باشد، همانند پژوهش سیترون[1](۲۰۰۸) انگیزه طبقه بندی مرکزی می‌شود و نیاز به روند قانونی در زمینه الکترونیکی وجود دارد. همچنین در این موارد، تمایز بین موقعیت‌های تهاجمی(اما قانونی) و متقلبانه(و موارد غیرقانونی) مهم است. در حالی که در برخی موارد می توان تفاوت را به وضوح مشخص کرد(به عنوان مثال، مالک کارت اجازه پرداخت را داده است یا خیر)، توضیح تفاوت بین این دو در موارد پیچیده(مثلاً تقلب حسابداری) می تواند دشوار باشد. اگرچه یادگیری ماشین نیز می تواند به حل این سوال کمک کند، این تحلیل لایه دیگری از پیچیدگی را در طبقه بندی به وجود می‌آورد.

اگر هدف جلوگیری از تقلب از طریق پیش‌بینی باشد(مثلاً مهندسی مجدد فرآیند)، انگیزه طبقه‌بندی باید به خوبی درک شود تا بتوان تحلیل علت اصلی را انجام داد و اقدامات اصلاحی را اجرا کرد. این فرآیند ممکن است شامل تجزیه و تحلیل داده‌های عملیاتی باشد که معمولاً در بسیاری از الگوریتم‌های تشخیص تقلب فعلی گنجانده نشده‌اند. علاوه بر این، رفتن از مجموعه‌ای از موارد مشکوک ایجاد شده از طریق یادگیری ماشینی به تغییر در فرآیندها و سازمان ها ممکن است دشوار باشد. به عنوان مثال، به خوبی مشخص شده است که انسان ها به طور کلی، و حسابرسان به طور خاص، توانایی محدودی برای پردازش مقادیر زیادی از اطلاعات مورد نیاز برای تصمیم گیری های پیچیده دارند(ایزلین[2]، ۱۹۸۸). آشتون[3](۱۹۷۴) نشان داده است که حجم زیادی از اطلاعات حسابداری می‌تواند منجر به قضاوت های مالی و حسابرسی نامناسب شود. در این زمینه، الگوریتم های یادگیری ماشینی می‌توانند به عنوان ابزار کاهش داده برای صرفه جویی در منابع ذهنی عمل کنند. با این حال، توانایی افراد برای ترکیب نشانه ها از منابع متعدد نیز محدود است(بنباسات و تیلور[4]، ۱۹۸۲).

1 . Citron
2 . Iselin
3 . Ashton
4 . Benbasat and Taylor

٦. تمایز بین پیش بینی و استنتاج علّی

استنتاج علّی و پیش‌بینی اساساً مسائل متفاوتی هستند. هدف استنتاج علّی استفاده از ابزارهای آماری برای آزمایش روابط علّی است. در مقابل، هدف پیش‌بینی اعمال یک مدل آماری یا الگوریتم داده‌کاوی برای داده‌ها به منظور پیش‌بینی مشاهدات جدید است (کلینبرگ و همکاران[1]، ۲۰۱۵). تمایز بین پیش‌بینی و استنتاج علّی بسیار با اهمیت است، چرا که اکثر تحقیقات آکادمیک حسابداری و مالی موجود بر استنتاج علّی تمرکز دارند، در حالی که شاغلان حرفه ممکن است علاقه بیشتری به پیش‌بینی داشته باشند. مطالعات استنتاج علّی برای تصمیم‌گیرندگانی که مایل به طراحی راهکارهای سیاست مؤثر برای جلوگیری و کاهش تقلب حسابداری هستند، مرتبط است. با این حال، بسیاری از تصمیمات مهم(به عنوان مثال، سرمایه‌گذاری یا عدم سرمایه‌گذاری در سهام با رشد بالا) وجود دارد که نیاز به پیش بینی دقیق و به موقع دارد که آیا یک شرکت درگیر تقلب است یا خیر. علاوه بر این، استنتاج علّی و پیش‌بینی دو امر متقابل تلقی نمی‌شوند. برای مثال، واریان[2](۲۰۱۴) استدلال می‌کند که مدل‌سازی پیش‌بینی‌کننده می‌تواند به تحقیقات استنتاج علّی نیز کمک کند.

۷. برتری تکنیک های یادگیری ماشین در کشف و پیش بینی تقلب

دانشمندان داده اغلب از مدل های آماری پیچیده برای شناسایی تقلب ها استفاده می‌کنند. با این حال، این روش معایب زیادی دارد. کشف تقلب در زمان واقعی نیست و بنابراین، در بسیاری از موارد، فعالیت های متقلبانه تنها پس از وقوع تقلب واقعی شناسایی می‌شوند. این روش‌ها مستعد خطاهای انسانی هستند. علاوه بر این، به تیم های متخصص در آن حوزه و دانشمندان داده گران قیمت و بسیار ماهر نیاز دارد. با این وجود، دقت روش‌های تشخیص تقلب دستی پایین است و به همین دلیل، پردازش حجم زیادی از داده‌ها بسیار دشوار است. بیشتر اوقات، برای شناسایی الگوهای فعالیت متقلبانه، به بررسی های زمان بر در مورد سایر معاملات مرتبط با فعالیت متقلبانه نیاز دارد. علیرغم منابع و پولی که برای این روش‌های سنتی خرج می‌شوند، بازده کافی ایجاد نمی‌کنند. بیشتر روش‌های سنتی کشف تقلب بر روی نقاط داده‌ای گسسته متمرکز بودند. باید توجه داشت این روش‌ها دیگر برای نیازهای امروزی کافی نیستند. از آنجایی که کلاهبرداران و هکرها از تکنیک‌های پیشرفته‌تری برای پنهان کردن فعالیت‌های تقلبی خود حتی

1 . Kleinberg
2 . Varian

از تیزبین‌ترین چشم‌ها استفاده می‌کنند. این روش‌شناسی‌ها فقط می‌توانند انواع شناخته شده حملات را شناسایی کنند، بنابراین یک رویکرد تحلیلی برای رفع این اشکالات روش‌های سنتی مورد نیاز است(آماراسینگه[1]، ۲۰۱۸).

علی‌رغم وجود اختلاف نظر بین پژوهشگران حوزه تقلب، در مورد برتری روش‌های یادگیری ماشین در پیش بینی و کشف تقلب نسبت به سایر روش‌ها اما برخی پژوهش ها بصورت قوی مدعی برتری این تکنیک ها هستند. به طور مثال پژوهش بائو و همکاران(۲۰۱۹) دفاع تمام قدی از این تکنیک ها به عمل آورده است. ملکی کاکلر و همکاران(۱۴۰۰) نیز مدعی هستند مدل‌های یادگیری ماشین در پیش بینی گزارشگری مالی متقلبانه، دقت و کارایی بیشتری نسبت به مدل‌های آماری دارد. رضایی و همکاران(۱۳۹۹) نیز با بکارگیری پنج تکنیک شامل شبکه های بیزین، درخت تصمیم، شبکه های عصبی، ماشین بردار پشتیبان و روش ترکیبی(که از جمله برترین تکنیک های یادگیری ماشین محسوب میشوند) در کشف تقلب صورت‌های مالی دریافتند که تمامی آنها از قابلیت بالایی در کشف تقلب برخوردارند و از سایر روش‌ها دقیق تر بودند و توان ارزیابی بالاتری نیز دارند.

۸. مروری کوتاه بر پژوهش های موجود در مورد کشف تقلب

ادبیات موجود در مورد پیش‌بینی تقلب، یک ادبیات بین‌رشته‌ای است واگر لازم باشد تقسیم‌بندی در این خصوص ارائه شود می‌توان به دو جریان پژوهش های موجود در رشته حسابداری و پژوهش های موجود در سایر رشته ها(مانند علوم کامپیوتر) تقسیم کرد.

الف. پیش‌بینی تقلب با یادگیری ماشینی در زمینه‌های دانشگاهی غیرحسابداری

ادبیات یادگیری ماشین در زمینه‌های غیرحسابداری راه‌حل‌های مختلفی را برای برخی از چالش‌های روش یادگیری ماشین پیشنهاد کرده است. این مدل‌ها تلاش می‌کنند تا انواع مختلفی از تقلب مانند تقلب بیمه‌ای و تقلب در تجارت الکترونیک را پیش‌بینی کنند.

اول، همانطور که ذکر شد تقلب شناسایی شده معمولاً یک رویداد نادر است. یکی از روش‌های رایج برای مقابله با نادر بودن، کاهش عدم تعادل مشاهدات تقلبی و غیر تقلبی با تطبیق است (هامفریس و همکاران[2]، ۲۰۱۱؛ سیچینی و همکاران، ۲۰۱۰). در حالی که استفاده از نمونه

1 . Amarasinghe
2 . Humpherys et al

مشابه تقلب و غیرتقلب برای آموزش مدل مناسب است، استفاده از سال-شرکت‌های تقلبی و غیرمتقلب منطبق در نمونه آزمون نگهداری شده برای ارزیابی عملکرد خارج از نمونه مشکل ساز است. انجام این کار باعث سویه آینده نگری می¬شود.

دوم، کشف تقلب دشوار است زیرا بسیاری از موارد تقلب پنهان می‌ماند. در حالی که موضوع تقلب نادر را می توان به خوبی با ترکیب یادگیری عدم تعادل و یادگیری گروهی به خوبی حل کرد، مسئله تقلب پنهان به ندرت مورد توجه قرار می‌گیرد. برای رسیدگی به این دو موضوع، محققان شناسایی نظرات جعلی را با استفاده از یادگیری بدون برچسب مثبت پیشنهاد می‌کند(بکر و دیویس[1]، ۲۰۲۰). یادگیری بدون برچسب مثبت یک روش طبیعی برای پرداختن به این دو موضوع به طور همزمان است.

سوم، تقلب سریالی، که در آن یک متقلب قبل از دستگیر شدن در چندین دوره متوالی مرتکب تقلب می‌شود. این چالش به دلیل تاخیر در شناسایی، بسیار رایج است. تقریباً تمام مدل‌های موجود، هر دوره تقلب را به عنوان یک وقوع تقلب مستقل در نظر می‌گیرند و وابستگی سری زمانی موارد کلاهبرداری سریالی را نادیده می‌گیرند. برای پرداختن به این موضوع، گائو و همکاران[2](۲۰۱۸) مدل رایج شبکه عصبی مکرر حافظه کوتاه م مدت[3]را برای استخراج ویژگی‌های مفید از رفتارهای متقلبانه سریالی تطبیق می‌دهد. اونتاریو و همکاران[4](۲۰۱۴) نیزدریافتند که ویژگی‌های سری زمانی استخراج‌شده می‌تواند عملکرد تشخیص تقلب را بهبود بخشد.

چهارم، تقلب در طول زمان تکامل می‌یابد و متقلبان بسیار سازگار هستند زیرا از موارد تقلب کشف‌شده درس می‌گیرند. برای ساخت مدل‌های تشخیص تقلب تطبیقی، عباسی و همکاران(۲۰۱۲) یک چارچوب فرا یادگیری را پیشنهاد می‌کند که می‌تواند به شیوه ای خودسازگارانه برای بهبود دقت پیش بینی آموخته شود. شو و همکاران[5](۲۰۱۷) یک الگوریتم یادگیری آنلاین برای تشخیص کمپین تقلب در شهرت پیشنهاد می‌کند که می تواند به طور موثر بر اساس موارد تقلب جدید برای تطبیق پذیری تغییر جهت حالت به روز شود.

---

1 . Bekker and Davis
2 . Guo et al
3 . Long short-term memory (LSTM)
4 . Oentaryo et al
5 . Xu et al

آخرین(اما نه کم‌اهمیت) چالش، تحقیقات رو به رشدی در مورد استفاده از یادگیری ماشین چندوجهی (بالتراسیتیس و همکاران ، ۲۰۱۸) برای بهبود تشخیص تقلب وجود دارد. علاوه بر داده‌های حسابداری، انواع مختلف داده‌های ناهمگن(مانند متن، تصویر، صدا، ویدئو و شبکه) وجود دارد که می‌تواند حاوی اطلاعات مفیدی برای کشف تقلب باشد. نمونه‌هایی از پژوهش‌های انجام شده از این دست شامل سچینی و همکاران (۲۰۱۰)، بیوتل و همکاران[1] (۲۰۱۵) و ژونگ و همکاران[2](۲۰۲۰) است.

ب. پیش بینی تقلب در ادبیات حسابداری

ادبیات طولانی در حسابداری در مورد پیش بینی تقلب وجود دارد. با این حال، بیشتر مطالعات پیش‌بینی تقلب حسابداری به جای پیش‌بینی تقلب با استنتاج علّی (یعنی اینکه چه عواملی بر وقوع تقلب حسابداری تأثیر می‌گذارند) سر و کار دارند. حتی اگر برخی از مطالعات از اصطلاح «پیش‌بینی تقلب» استفاده کنند، اغلب به معنای پیش‌بینی تقلب درون نمونه‌ای است تا برون نمونه‌ای(برازل و همکاران[3]، ۲۰۰۹؛ هابسون و همکاران[4]، ۲۰۱۲).

از آنجا که بسیاری از مطالعات پیش‌بینی تقلب در زمینه حسابداری با استنتاج علی سروکار دارند، بعضاً چارچوب شناخته شده مانند مثلث تقلب را از جرم‌شناسی برای سازماندهی بررسی خود اتخاذ کرده اند. همچنین بسیاری از تحقیقات حسابداری موجود از جمله دیچاو و همکاران(۲۰۱۱) از داده‌های صورت‌های مالی استفاده می‌کنند. در سال‌های اخیر نیز شاهد استفاده روزافزون محققان حسابداری از داده‌های متنی(مانند پژوهش های انجام شده توسط سچینی و همکاران، ۲۰۱۵ و براون و همکاران، ۲۰۲۰) و منابع آنلاین(پیش‌بینی تقلب) بوده‌ایم که از جمله این پژوهش‌ها می‌توان به پژوهش انجام شده توسط دونگ و همکاران(۲۰۱۸) اشاره کرد.

از آنجایی که تقلب های حسابداری در اکثر پژوهش های پیشین رشته حسابداری به عنوان یک متغیر دودویی تلقی شده است و بیشتر مطالعات در این زمینه بر استنتاج علی تمرکز دارند، رگرسیون های لجستیک رایج ترین روش آماری در توضیح عوامل تعیین کننده تقلب حسابداری است. مطالعات پیش‌بینی خارج از نمونه واقعی هنوز در ادبیات حسابداری نسبتاً کم

1 . Beutel et al
2 . Zhong et al
3 . Brazel et al
4 . Hobson et al

انجام شده است. با این حال، علاقه فزاینده ای در میان محققان حسابداری به استفاده از روش‌های بین‌رشته‌ای برای پیش بینی تقلب حسابداری خارج از نمونه وجود دارد. از جمله این پژوهش ها می‌توان به پژوهش هایی همچون سچینی و همکاران(۲۰۱۰)، عباسی و همکاران(۲۰۱۲)، پوردا و اسکیلی کورن(۲۰۱۵)، پرولز و همکاران(۲۰۱۷)، دونگ و همکاران(۲۰۱۸)، براون و همکاران(۲۰۲۰) و بائو و همکاران(۲۰۲۰) اشاره کرد.

۹. نتیجه‌گیری در مورد یادگیری ماشین

به نظر می‌رسد استقرار یادگیری ماشینی برای تشخیص ناهنجاری ها، خطاها و تقلب یک حوزه رو به رشد در پژوهش‌های این حوزه است. این قبیل بحث ها باید مورد توجه پژوهشگران و تصمیم گیرندگان در بسیاری از سازمان ها باشد چرا که پلتفرم‌های یادگیری ماشینی ممکن است برای سازمان‌ها این فرصت را فراهم آورد تا تراکنش‌ها را تقریباً در زمان واقعی تحت نظارت قرار دهند. این پلتفرم ها ممکن است امکان تجزیه و تحلیل جامع(به جای نمونه برداری) و اصلاح سریعتر را فراهم کنند. تجزیه و تحلیل متنی را می‌توان تا حد زیادی به کار برد، برای مثال، پلتفرم‌های یادگیری ماشین می‌توانند قراردادهای اجاره پیچیده را بخوانند و تجزیه و تحلیل کنند تا طبقه‌بندی حسابداری مناسب خود را تعیین کنند. به نوبه خود، می‌تواند فرآیند حسابداری و حسابرسی را بهبود ببخشد به نحوی که مسیر حسابرسی بهتری برای تشخیص ناهنجاری‌های داخلی فراهم کند. تجزیه و تحلیل متنی می‌تواند اسناد مربوطه را از طریق تقسیم بندی موضوع و تجزیه و تحلیل کلمات کلیدی شناسایی کند. به عنوان مثال، اداره تقلب سنگین بریتانیا[1] با همین ابزار رشوه و فساد در مقیاس بزرگ در رولز رویس را افشا کرد. آنها از یادگیری ماشین برای بررسی ۳۰ میلیون سند استفاده کردند و روزانه ۶۰۰ هزار سند را پردازش کردند. در مقابل، مدیر ارشد فناوری این سازمان اشاره کرد که میانگین نرخ پردازش انجام شده توسط وکلا ۳۰۰ سند در روز است که به نسبت روش یادگیری ماشین با دقت کمتری انجام می‌شود. این اسناد همچنین می توانند به طور خودکار ترجمه و خلاصه شوند. به عنوان مثال، تجزیه و تحلیل احساسات می‌تواند امکان تشخیص استرس پیش بینی کننده تقلب را فراهم کند. شبکه‌های داخلی ارتباطی را می توان به راحتی ترسیم کرد. با ظهور منابع داده جدید(به عنوان مثال، اینترنت اشیا (التاوی[2] ، ۲۰۲۵) و...)، کنترل های داخلی جدیدی را می‌توان طراحی کرد. برای مثال،

1. Serious Fraud Office (SFO)
2 . Alatawi

می‌توان تصور کرد که پردازش خودکار ویدیوها می‌تواند امکان نظارت فیزیکی مداوم بر موجودی و تطبیق آن‌ها با سوابق حسابداری را فراهم کند. از همین مسیر منابع خارجی داده نیز می¬توانند یکپارچه شوند. برای مثال، تجزیه و تحلیل شبکه های اجتماعی می‌تواند امکان پیش‌بینی مشکلات محصول را فراهم کند.

با این حال، استقرار این ابزارها در سازمان ها همچنان چالش برانگیز است. جدای از مسائل فنی که پیشتر به طور مختصر به آن اشاره شد، این ابزارها شیوه های موجود را به چالش می کشند و به مهارت های مدیریت تغییر نیاز دارند. از آنجایی که تشخیص تقلب از رویکرد مبتنی بر تجربه به رویکرد مبتنی بر داده می‌رود، دانش تخصصی با یادگیری ماشینی نیاز به اصلاح دارد. برای توضیح بیشتر باید گفت الگوریتم‌ها اغلب بر سه نوع ناهنجاری برای تشخیص تقلب متکی هستند که شامل موارد زیر است؛ ۱) الگوریتم‌هایی که بر اساس نقاط دورافتاده در توزیع(مثلاً تراکنش‌های بالاتر از یک آستانه معین) کار می کنند، ۲) الگوریتم‌هایی که به داده هایی که به دلیل شرایط غیرعادی هستند(مانند برداشت زیاد در دوره‌ای کم) سر و کار دارند و ۳) الگوریتم‌هایی که وقتی مشاهدات متعدد به طور مشترک تحلیل می‌شوند، داده هایی را غیرعادی تلقی می کند(مانند تراکنش‌های ATM از دو قاره در یک دوره زمانی کوتاه). در این خصوص باید گفت ناهنجاری‌های نوع اول احتمالاً با حداقل دانش تخصصی قابل شناسایی هستند. با این حال، نوع دوم و سوم اغلب برای موثر بودن نیاز به دانش تخصصی دارند. علیرغم همه چالش‌ها، به نظر می‌رسد استفاده از یادگیری ماشین برای مبارزه با تقلب، هم برای پژوهشگران و هم برای دست اندرکاران صنعت، یک مسیر امیدوارکننده است.

۱۰. انتقادات پیرامون روش‌های آماری و تکنیک های یادگیری ماشین

همانطور که پیش از این شرح داده شد ادبیات در حوزه کشف تقلب مسیری رو به پیشرفت طی کرده است و از استفاده از مدل های سنتی به استفاده از روش‌های جدیدتری همچون یادگیری ماشین گرایش پیدا کرده است علی رغم قدرت و دقتی که از روش‌های یادگیری ماشین در ذهن متبلور می‌شود، تحقیقات انجام شده در این حوزه نیز مورد نقد قرار گرفته و این تفکر را القا می کند که شاید نباید با این سرعت آنها را پذیرفته و به خصوص در موضوع حساسی همچون کشف تقلب تمام قد به آن اعتماد کنیم. به عنوان مثال والکر[1] (۲۰۲۱) در پژوهش خود

1 . Walker

نتایج پژوهش بائو و همکاران(۲۰۲۰) را که سعی داشت روش یادگیری ماشین را روشی برتر و دقیق تر از روش‌های سنتی معرفی کند، به نقد می¬کشد و بیان می کند که با اینکه نتایج پژوهش بائو و همکاران(۲۰۲۰) حاکی از آن است که یادگیری ماشینی تشخیص تقلب را ۷۰ درصد بالاتر از رگرسیون لجستیک(روش‌های سنتی) بهبود می‌بخشد اما با تکرار پژوهش آنها با استفاده از فایل های مورد استفاده در تحلیل آن پژوهش مشخص شد که در این پژوهش برخی از شرکت‌های متقلب هم در نمونه‌های آموزش و هم در نمونه‌های تست موجود بودند و اصطلاحاً نشت داده در این پژوهش رخ داده است، که نتایج مدل آنها را بهبود می‌بخشد، اما با آنچه در آن پژوهش توضیح داده شد، تناقض دارد و این امر اعتبار نتایج آنها را زیر سوال می‌برد. این نقد والکر(۲۰۲۱) به نظر حائز توجه است چرا که با وجود اینکه بائو و همکاران(۲۰۲۲) در پژوهش خود سعی کرده اند پاسخ نقد وارد شده والکر(۲۰۲۱) را بدهند با این وجود باز هم والکر(۲۰۲۲) در پژوهشی پاسخ بائو را به نقد کشیده و در نهایت چون پاسخ بائو به نقد های مطرح شده توسط والکر نامربوط به نظر رسیده است والکر از مجله تحقیقات حسابداری که اقدام به چاپ این مقالات بائو کرده اند درخواست کرده است اقدامات و تحقیقاتی در خصوص تخلفات پژوهش های آکادمیک به عمل آورند.

در ادامه والکر(۲۰۲۱) در پژوهش دیگری اشاره می کند که با وجود نقد نشت داده در پژوهش بائو و همکاران(۲۰۲۰)، پژوهش آن‌ها هیچ بهبودی را در ادبیات این حوزه ایجاد نکرده است، اما بنظر می‌رسد والکر یک مسأله را خواسته یا ناخواسته نادیده گرفته است. حتی اگر ما نقد نشت داده را در کار بائو بپذیریم(که البته نقد صحیحی نیز می‌باشد) اما با این حال پژوهش بائو(۲۰۲۰) با انتخاب روش یادگیری ماشین این برتری را نسبت به کار پژوهشگرانی همچون دیچاو و همکاران(۲۰۱۱) دارد که پژوهشی که دیچاو و همکاران(۲۰۱۱) انجام دادند پیش‌بینی به صورت درون نمونه ای انجام شده است در حالی که پژوهش بائو و همکاران(۲۰۲۰) پیش‌بینی به صورت برون نمونه ای است و این برتری بزرگی محسوب می‌شود.

والکر(۲۰۲۲) در ادامه شروع به نقد پژوهش امیرام و همکاران(۲۰۱۷) می کند که در آن بر اساس قانون بنفورد(۱۹۳۸) ادعا شده که مدل ارائه شده آنها می‌تواند هم تحریف‌های بااهمیت که توسط انتشارات اجرایی حسابداری و حسابرسی SEC شناسایی شده‌اند را پیش بینی کند، و هم به عنوان یک شاخص اصلی برای این تحریف‌ها عمل کند. از آنجایی که این پژوهش مورد اقبال زیادی واقع شده است والکر(۲۰۲۲) به استفاده کنندگان از این مدل هشدار می‌دهد و

اینگونه ابراز می‌کند که قانون بنفورد(۱۹۳۸) برای پیش بینی تحریف‌های بااهمیت مناسب نیست. در نهایت اینگونه ابراز می‌کند که قانون بنفورد(۱۹۳۸) دارای خواص شگفت انگیز و اسرارآمیزی است که تصورات عموم را به خود جلب کرده است، اما این قانون جادویی نیست و کاربردهای آن محدود است.

بحث و نتیجه گیری

پدیده تقلب در صورت‌های مالی به‌عنوان یک مشکل جهانی که تأثیرات منفی قابل‌توجهی بر کلیه ذینفعان دارد، مورد توجه بسیاری از پژوهشگران و متخصصان قرار گرفته است. کشف تقلب به دلیل ماهیت پیچیده و ذهنی آن، چالشی بزرگ محسوب می‌شود و روش‌های مختلفی برای شناسایی و پیشگیری از آن به کار گرفته شده است. در این پژوهش، به بررسی فرصت‌ها، چالش‌ها و انتقادات مرتبط با روش‌های آماری سنتی و تکنیک‌های نوین یادگیری ماشین برای کشف تقلب پرداخته شد.

روش‌های آماری سنتی، از جمله مدل‌های رگرسیون لجستیک مانند مدل بنیش(۱۹۹۷،۱۹۹۹) و مدل F-score دیچاو و همکاران(۲۰۱۱)، به‌طور گسترده‌ای در مطالعات کشف تقلب مورد استفاده قرار گرفته‌اند. این مدل‌ها با تحلیل نسبت‌های مالی و سایر شاخص‌ها، تلاش می‌کنند تا تقلب در صورت‌های مالی را شناسایی کنند. با این حال، این روش‌ها با محدودیت‌هایی مواجه هستند. از جمله این محدودیت‌ها می‌توان به عدم توانایی در شناسایی تمامی موارد تقلب، زمان‌بر بودن و وابستگی به دقت داده‌های ورودی اشاره کرد.

در سال‌های اخیر، با پیشرفت‌های قابل‌توجه در حوزه هوش مصنوعی و یادگیری ماشین، فرصت‌های جدیدی برای شناسایی تقلب مالی فراهم شده است(سلیمانی امیری و محمدی سه دران، ۱۴۰۳). الگوریتم‌های یادگیری ماشین، به‌ویژه تکنیک‌هایی مانند شبکه‌های عصبی، ماشین‌های بردار پشتیبان و خوشه‌بندی K-means، می‌توانند الگوهای پیچیده‌تری از داده‌ها را تحلیل کرده و تقلب را با دقت بیشتری شناسایی کنند. این تکنیک‌ها به‌طور خودکار از داده‌ها یاد می‌گیرند و الگوهای متقلبانه را شناسایی می‌کنند. با این حال، این روش‌ها نیز با چالش‌ها و انتقادات خاص خود روبه‌رو هستند.

یکی از چالش‌های اصلی در استفاده از تکنیک‌های یادگیری ماشین برای کشف تقلب، عدم توازن داده‌هاست. به این معنا که موارد تقلب نسبت به موارد غیرتقلبی بسیار کم هستند، که این

موضوع می‌تواند عملکرد الگوریتم‌ها را تحت تأثیر قرار دهد. علاوه بر این، تقلب به‌طور مداوم در حال تکامل است و افراد متقلب سعی می‌کنند الگوریتم‌ها را دور بزنند، بنابراین مدل‌ها باید به‌طور مداوم به‌روزرسانی شوند. چالش دیگر مربوط به پیچیدگی و توضیح‌پذیری مدل‌های یادگیری ماشین است. بسیاری از الگوریتم‌های یادگیری ماشین به‌صورت جعبه‌سیاه عمل می‌کنند و فهم اینکه چرا یک تصمیم خاص اتخاذ شده است، دشوار است. این مسئله در مواردی که نیاز به توضیح دقیق و قانونی برای تصمیمات اتخاذ شده وجود دارد، می‌تواند مشکل‌ساز باشد. انتقادات وارد شده به تکنیک‌های یادگیری ماشین نیز نشان‌دهنده برخی از محدودیت‌های این روش‌هاست. به عنوان مثال، نتایج پژوهش‌های انجام شده در این حوزه، گاهی به دلیل نشت داده‌ها یا سایر مسائل تکنیکی، ممکن است دقت مورد انتظار را نداشته باشند. علاوه بر این، برخی از روش‌های آماری سنتی مانند قانون بنفورد(۱۹۳۸)، به‌رغم داشتن خواص ریاضی شگفت‌انگیز، در کاربردهای عملی ممکن است نتایج مطلوبی ارائه ندهند.

با این وجود، با توجه به مزایای بالقوه‌ای که تکنیک‌های یادگیری ماشین برای کشف تقلب فراهم می‌کنند، استفاده از این روش‌ها همچنان مورد توجه قرار دارد. یادگیری ماشین می‌تواند به‌طور موثری در تشخیص ناهنجاری‌ها و الگوهای متقلبانه کمک کند و با ترکیب با روش‌های سنتی، مدل‌های پیش‌بینی قدرتمندتری را ارائه دهد. این پژوهش نشان می‌دهد که علی‌رغم وجود چالش‌ها و انتقادات، یادگیری ماشین و هوش مصنوعی فرصت‌های مناسبی را برای بهبود فرآیند کشف تقلب فراهم می‌کنند. پژوهش‌های آینده می‌توانند با تمرکز بر حل مسائل مربوط به توضیح‌پذیری، بهبود دقت مدل‌ها و به‌روزرسانی مداوم الگوریتم‌ها، به ارتقای بیشتر این حوزه کمک کنند. در نهایت، ترکیب روش‌های سنتی و نوین و استفاده هوشمندانه از داده‌ها می‌تواند به ایجاد سیستم‌های کشف تقلب موثرتر و کارآمدتر منجر شود.

ملاحظات اخلاقی

حامی‌مالی: مقاله حامی مالی ندارد.

مشارکت نویسندگان: تمام نویسندگان در آماده‌سازی مقاله مشارکت داشته‌اند.

تعارض‌منافع: بنا بر اظهار نویسندگان در این مقاله هیچ‌گونه تعارض منافع وجود ندارد.

منابع

احمدی، فغانی ماکرانی و فاضلی. (۱۴۰۳). تکنیک‌های داده کاوی و پیش بینی تقلب صورت‌های مالی. دانش حسابداری و حسابرسی مدیریت، ۱۳(۵۲)، ۱۵-۲۸.

رضائی، حمیدرضا؛ مرادی، مهدی؛ باقرپور ولاشانی، محمد علی و جباری نوقابی، مهدی . (۱۴۰۳). معیارهای سنجش کیفیت حسابرسی از دیدگاه استفاده‌کنندگان. پژوهش های تجربی حسابداری ۱۴(۴)، ۱-۳۰.

رضائی، ناظمی اردکانی، و ناصر صدرآبادی. (۱۳۹۹). کشف تقلب صورت‌های مالی با توجه به گزارش حسابرسی صورت‌های مالی. حسابداری مدیریت، ۱۳(۴۵)، ۱۴۱-۱۵۳.

سلیمانی امیری، غلامرضا و محمدی سه دران، سارا . (۱۴۰۳). حسابرسی در عصر هوش مصنوعی. حسابداری و منافع اجتماعی ۱۴(۳)، ۱-۳۶.

عباس تفرشی، زهره و سلیمانی امیری، غلامرضا . (۱۴۰۳). مدل بلوغ حسابداری دادگاهی در ایران. پژوهش های تجربی حسابداری، ۱۴(۳)، ۱۴۳-۱۶۸.

فتاحی نافچی، حسن؛ جودکی، محمد و قنبری، سارا . (۱۴۰۳). رابطه تقلب در گزارشگری مالی شرکت‌های همتای فعال در یک منطقه جغرافیایی همسان با تقلب در گزارشگری مالی شرکت؛ نقش تعدیلی رقابت صنعت. حسابداری و منافع اجتماعی۱۴(۲)، ۱۰۳-۱۲۴.

کردستانی و تاتلی (۱۳۹۵). پیش بینی دستکاری سود: توسعهٔ یک مدل. بررسی های حسابداری و حسابرسی، ۲۳(۱)، ۷۳-۹۶.

مشایخی، بیتا؛ سماوات، میلاد و جهانگرد، امین . (۱۴۰۲). ترسیم نقشه علمی پژوهش‌های کیفیت‌حسابرسی‌داخلی. مطالعات تجربی حسابداری مالی ۲۰(۷۸)، ۳۵-۷۵.

معزی، پورآقاجان و جعفری. (۱۴۰۳). کشف تقلب صورتهای مالی: قیاس توانایی مدل های مبتنی بر متغیرهای حسابداری. دانش حسابداری و حسابرسی مدیریت, ۱۳(۵۲)، ۱۷۳-۱۸۸.

ملکی کاکلر، ح؛ بحری ثالث، ج؛ جبارزاده کنگرلویی و آشتاب. (۱۴۰۰). کارایی مدل‌های آماری والگوهای یادگیری ماشین در پیش بینی گزارشگری مالی متقلبانه. اقتصاد مالی, ۱۵(۵۴)، ۲۹۲-۲۶۷.

هاشمی، ع و حریری، ا. (۱۳۹۶). ارزیابی توانایی قانون بنفورد در شناسایی و پیش بینی کشف تقلب مالی. بررسی های حسابداری و حسابرسی، ۲۴(۲)، ۲۸۳-۳۰۲.

References

Abbas Tafreshi, Z. & Soleimany Amiri, G. (2024). Forensic Accounting Maturity Model in Iran. Empirical Research in Accounting, 14(3), 143-168. [In Persian]

Abbasi, A; Albrecht, C; Vance, A; & Hansen, J. (2012). Metafraud: A meta-learning framework for detecting financial fraud. MIS Quarterly, 1293–1327.

Abdallah, A; Maarof, M. A; & Zainal, A. (2016). Fraud detection system: A survey. Journal of Network and Computer Applications, 68, 90-113.

Aghghaleh, S. F; Mohamed, Z. M; & Rahmat, M. M. (2016). Detecting Financial Statement Frauds in Malaysia: Comparing the Abilities of Beneish and Dechow Models. Asian Journal of Accounting & Governance, 7.

Agrawal, A; & Cooper, T; (2015). Insider trading before accounting scandals. J. Corp. Finan. 34, 169–190.

Ahmadi, M; Faghani Makrani, K; & Fazeli, A. (2024). Data mining techniques and prediction of financial statement fraud. Journal of Management Accounting and Auditing Knowledge, 13(52), 15-28. [In Persian]

Akhilomen, John, (2013). Data mining application for cyber credit-card fraud detection system. In Lecture Notes in Engineering and Computer Science. 1537– 1542.

Alatawi, M. N. (2025). Detection of fraud in IoT based credit card collected dataset using machine learning. Machine Learning with Applications, 19, 100603.

Alexopoulos, P; Kafentzis, K; Benetou, X; Tagaris, T; & Georgolios,. (2007, July). Towards a generic fraud ontology in e-government. In International Conference on E-business .2. 269-276. SCITEPRESS.

Amarasinghe, T; Aponso, A; & Krishnarajah, N. (2018, May). Critical analysis of machine learning based approaches for fraud detection in financial transactions. In Proceedings of the 2018 International Conference on Machine Learning Technologies. 12-17.

Amiram, D; Bozanic, Z; & Rouen, E. (2015). Financial statement errors: Evidence from the distributional properties of financial statement numbers. Review of Accounting Studies, 20, 1540–1593.

Ashton, R. H. (1974). Behavioral implications of information overload in managerial accounting reports. Cost and Management, 48(4), 37–40.

Baltrušaitis, T; Ahuja, C; & Morency, L. P. (2018). Multimodal machine learning: A survey and taxonomy. IEEE Transactions on Pattern Analysis and Machine Intelligence, 41(2), 423–443.

Bansal, K; Paliwal, A. C; & Singh, A. K. (2025). Analysis of the benefits of artificial intelligence and human personality study on online fraud detection. International Journal of Law and Management, 67(2), 191-209.

Bao, Y; Ke, B; Li, B; Yu, Y. J; & Zhang, J. (2020). Detecting accounting fraud in publicly traded US firms using a machine learning approach. Journal of Accounting Research, 58(1), 199–235.

Beasley, M. S; Carcello, J. V; & Hermanson, D. R. (1999). Fraudulent financial reporting: 1987– 1997: An Analysis of U.S. Public Companies. Sponsored by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Beasley, M. S; Carcello, J. V; Hermanson, D. R; & Neal, T. L. (2010). Fraudulent financial reporting: 1998–2007: An Analysis of U.S. Public Companies." Sponsored by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Behdad, Mohammad, Barone, Luigi, Bennamoun, Mohammed, & French, Tim, (2012). Nature-inspired techniques in the context of fraud detection. IEEE Trans. Syst. Man Cybern. Part C .42 (6), 1273–1290.

Bekker, J; & Davis, J. (2020). Learning from positive and unlabeled data: A survey. Machine Learning, 109(4), 719–760.

Benbasat, I; & Taylor, R. N. (1982). Behavioral aspects of information processing for the design of management information systems. IEEE Transactions on Systems, Man, and Cybernetics, 12(4), 439–450.

Beneish, M. D. (1997). Detecting GAAP violation: Implications for assessing earnings management among firms with extreme financial performance. Journal of Accounting and Public Policy, 16, 271–309.

Beneish, M. D. (1999). The detection of earnings manipulation. Financial Analysts Journal, 55, 24–36.

Beneish, M.D. & Nichols, D.C. 2009. Identifying overvalued equity. Johnson School Research Paper Series(09-09).

Benford, F. (1938). The law of anomalous numbers. Proceedings of the American philosophical society, 551-572.

Bertomeu, J; Cheynel, E; Floyd, E; & Pan, W. (2021). Using machine learning to detect misstatements. Review of Accounting Studies, 26(2), 468–519.

Beutel, A; Akoglu, L; & Faloutsos, C. (2015). Graph-based user behavior modeling: from prediction to fraud detection. Proceedings of the 21th ACM SIGKDD international conference on knowledge discovery and data mining. 2309–2310.

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

Brazel, J. F; Jones, K. L; & Zimbelman, M. F. (2009). Using nonfinancial measures to assess fraud risk. Journal of Accounting Research, 47(5), 1135–1166.

Brown, N. C; Crowley, R. M; & Elliott, W. B. (2020). What are you saying? Using topic to detect financial misreporting. Journal of Accounting Research, 58, 237–291.

Cecchini, M; Aytug, H; Koehler, G. J; & Pathak, P. (2010). Making words work: Using financial text as a predictor of financial events. Decision Support Systems, 50(1), 164–175.

Citron, D. K. (2008). Technological due process. Wash UL Rev, 85, 1249.

Craja, P; Kim, A; & Lessmann, S; (2020). Deep learning for detecting financial statement fraud. Decis. Support. Syst. 139, 113421.

Dechow, P. M; Ge, W; Larson, C. R; & Sloan, R. G. (2011). Predicting material accounting misstatements. Contemporary Accounting Research, 28(1), 17–82.

Dong, W; Liao, S; & Zhang, Z. (2018). Leveraging financial social media data for corporate fraud detection. Journal of Management Information Systems, 35(2), 461–487.

Dyck, A; Morse, A; & Zingales, L. (2020). How pervasive is corporate fraud. University of Toronto. working paper.

Fattahi Nafchi, H. , joodaki, M. & Ghanbari, S. (2024). The Relationship between Fraud in Financial the Relationship between Fraud in Financial Reporting of Peer Firms in the Same Geographical Region and Fraud in Company Financial Reporting: The Moderating Role of Industry Competition. Journal of Accounting and Social Interests, 14(2), 103-124. [In Persian]

Fawcett, T. (2006). An introduction to roc analysis. Pattern Recognition Letters, 27, 861–874.

Graham, J. R; Li, S; & Qiu, J. (2008). Corporate misreporting and bank loan contracting. Journal of Financial Economics, 89(1), 44–61.

Guo, J; Liu, G; Zuo, Y; & Wu, J. (2018). Learning sequential behavior representations for fraud detection. 2018 IEEE international conference on data mining (ICDM). IEEE. 127–136.

Hafez, I. Y; Hafez, A. Y; Saleh, A; Abd El-Mageed, A. A; & Abohany, A. A. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. Journal of Big Data, 12(1), 6.

Han, Jiawei, Kamber, Micheline, & Pei, Jian, (2012). Data mining concepts and techniques. In: Kamber, Jiawei Han Micheline, Pei, Jian (Eds.), Data Mining (The Morgan Kaufmann Series in Data Management Systems), Third ed. Morgan Kaufmann, Boston.

Hashemi, A; & Hariri, A. (2017). Evaluating the ability of Benford's law in identifying and predicting financial fraud detection. Accounting and Auditing Review, 24(2), 283-302. [In Persian]

Hobson, J. L; Mayew, W. J; & Venkatachalam, M. (2012). Analyzing speech to detect financial misreporting. Journal of Accounting Research, 50(2), 349–392.

Humpherys, S. L; Moffitt, K. C; Burns, M. B; Burgoon, J. K; & Felix, W. F. (2011). Identification of fraudulent financial statements using linguistic credibility analysis. Decision Support Systems, 50(3), 585–594.

Iselin, E. R. (1988). The effects of information load and information diversity on decision quality in a structured decision task. Accounting, Organizations and Society, 13(2), 147–164.

Jyothsna, V; & Rama Prasad, V.V; (2011). A review of anomaly based intrusion detection systems. Int. J. Comput. Appl. 28 (7), 26–35.

Karpoff, J. M; Koester, A; Lee, D. S; & Martin, G. S. (2017). Proxies and databases in financial misconduct research. The Accounting Review, 92(6), 129–163.

Kleinberg, J; Ludwig, J; Mullainathan, S; & Obermeyer, Z. (2015). Prediction policy problems. American Economic Review: Papers & Proceedings, 105(5), 491–495.

Kordestani, G; & Tatli, R. (2016). Earnings manipulation prediction: Development of a model. Accounting and Auditing Review, 23(1), 73-96. [In Persian]

Larcker, D; & Zakolyukina, A. A. (2012). Detecting deceptive discussion in conference calls. Journal of Accounting Research, 50, 495–540.

Li, Jing, Huang, Kuei-Ying, Jin, Jionghua, & Shi, Jianjun, (2008). A survey on statistical methods for health care fraud detection. Health Care Manag. 11 (3), 275–287.

Liu, Q; & Wu, Y; (2012). Supervised learning. Encycl. Sci. Learn.

Lopes, J; Belo, O; & Vieira, C. (2011). Applying user signatures on fraud detection in telecommunications networks. In Advances in Data Mining. Applications and Theoretical Aspects: 11th Industrial Conference, ICDM 2011, New York, NY, USA, August 30–September 3, 2011. Proceedings 11 (286-299). Springer Berlin Heidelberg.

Maleki Kaklar, H; Bahri Sales, J; Jabbarzadeh Kangarluei, S; & Ashtab, A. (2021). Efficiency of statistical models and machine learning patterns in predicting fraudulent financial reporting. Financial Economics, 15(54), 267-292. [In Persian]

Mashayekhi, B; Samavat, M; & Jahangard, A. (2023). Scientific Mapping of the Literature on Internal Audit Quality. Empirical Studies in Financial Accounting, 20(78), 35-75. [In Persian]

Moezzi, F; Pouraghajan, A; & Jafari, M. (2024). Financial statement fraud detection: Comparing the capability of accounting variable-based models. Journal of Management Accounting and Auditing Knowledge, 13(52), 173-188. [In Persian]

Nigrini, M. J. (1999). I've got your number. Journal of Accountancy May 79–83.

Nigrini, M. J. & Mittermaier, L. J. (1997). The use of Benford's law as an aid in analytical procedures. Auditing: A Journal of Practice and Theory 16 52–67.

Noor, N.M.M; Hamid, S.Ha, Mohemad, R; Jalil, & Ma, Hitam, M.S; (2015). A review on a classification framework for supporting decision making in crime prevention.

Oentaryo, R; Lim, E.-P; Finegold, M; Lo, D; Zhu, F; & Phua, C. (2014). Detecting click fraud in online advertising: A data mining approach. The Journal of Machine Learning research, 15(1), 99–140.

Omar, N; Koya, R. K; Sanusi, Z. M; & Shafie, N. A. (2014). Financial statement fraud: A case examination using Beneish Model and ratio analysis. International Journal of Trade, Economics and Finance, 5(2), 184.

Perols, J. L; Bowen, R. M; Zimmermann, C; & Samba, B. (2017). Finding needles in a haystack: Using data analytics to improve fraud prediction. The Accounting Review, 92, 221–245.

Purda, L; & Skillicorn, D. (2015). Accounting variables, deception, and a bag of words: Assessing the tools of fraud detection. Contemporary Accounting Research, 32(3), 1193–1223.

Rezaei, H; Moradi, M; Bagherpour Velashani, M. A. & Jabbari noghabi, M. (2024). Audit Quality Measurement Criteria. Empirical Research in Accounting, 14(4), 1-30. [In Persian]

Rezaei, M; Nazemi Ardakani, M; & Naser Sadrabadi, M. (2020). Financial statement fraud detection considering the audit report of financial statements. Management Accounting, 13(45), 141-153. [In Persian]

Saravanan, P; Subramaniyaswamy, V; Sivaramakrishnan, N; Arun Prakash, M; & Arunkumar, T; (2014). Data Mining Approach For Subscription-Fraud Detection in Telecommunication Sector. 7, 11. 515–522.

Soleimani Amiri, G. & mohammadi sedaran, S. (2024). Auditing in the Age of Artificial Intelligence. Journal of Accounting and Social Interests, 14(3), 1-36. [In Persian]

Stambaugh, C; Tipgos, M. A; Carpenter, F; & Smith, M. (2012). Using Benford analysis to detect fraud. Internal auditing, 27(3), 24-29.

Sun, Bo, Yu, Fei, Wu, Kui, Xiao, Yang, Senior Member, Leung, & Victor C.M; (2006). Enhancing security using mobility-based anomaly detection in cellular mobile networks. IEEE Trans. Veh. Technol. 55 (4), 1385–1396.

Varian, H. R. (2014). Big data: New tricks for econometrics. Journal of Economic Perspectives, 28, 3–28.

Walker, S. (2021). Critique of an article on machine learning in the detection of accounting fraud. Econ Journal Watch, 18(2), 61.

Walker, S. (2021). Rejoinder to the Critique of an Article on Machine Learning in the Detection of Accounting Fraud. Econ Journal Watch, 18(2), 230.

Walker, S. (2022). Compared to What? Does Benford's Law Really Detect Corporate Fraud? Econ Journal Watch, 19 (1).

Walker, S. (2022). Erroneous erratum to accounting fraud article. Econ Journal Watch, 19(2), 190.

Wei, Y; Chen, J; & Wirth, C. (2017). Detecting fraud in Chinese listed company balance sheets. Pacific Accounting Review, 29(3), 356–379.

Xu, C; Zhang, J; & Sun, Z. (2017). Online reputation fraud campaign detection in user ratings. IJCAI, 3873–3879.

Zhong, Q; Liu, Y; Ao, X; Hu, B; Feng, J; & Tang, J; (2020). Financial defaulter detection on online credit payment via multi-view attributed heterogeneous information network. Proceedings of the Web Conference 2020. 785–795.

Zhu, Shunzhi, Wang, Yan, Wu, & Yun, (2011). Health care fraud detection using nonnegative matrix factorization. In: Proceedings of the 2011 6th International Conference on Computer Science & Education, ICCSE. IEEE. 499–503.

Zhu, Xiaojin, & Goldberg, Andrew B; (2009). Introduction to Semi-Supervised Learning. Zliobaite, Indre, 2010. Learning under Concept Drift: an Overview. CoRR abs/1010.4.