سامانه‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)

Winter 2024, 5 (4), 47-58
DOI: 10.71856/impcs.2024.903603

Received: 7 Nov 2024
Accepted: 16 Dec 2024

مقاله پژوهشی

A Survey of Intelligent Data Mining Methods to Combat Money Laundering and Establish Data Governance in the Banking Network

Hedayat Alimoradi dokoohi [1], Erfaneh Noroozi[2*]

1.Department of Computer Engineering, Qeshm branch, Islamic Azad university, Qeshm, Iran.
Hedayat.Alimoradi@gmail.com
2. Department of Computer Engineering, Qeshm branch, Islamic Azad university, Qeshm, Iran.
**Corresponding Author*, NorooziErfaneh@gmail.com

Abstract

Introduction: Money laundering refers to the process of concealing the illicit origins of dirty money and presenting it as legitimate funds. Dirty money signifies sums obtained from criminal or illegal activities such as drug trafficking, human trafficking, bribery, and tax evasion. Money laundering can be defined as the process of cleansing dirty money. Detecting financial crimes has become a crucial priority for governments, and with the advancement of modern technologies and global communications, fraudulent methods are also significantly growing and evolving, leading to substantial damages to legitimate businesses. With the growth of electronic services in the financial sector and the increasing prevalence of non-face-to-face payment gateways worldwide, methods to combat money laundering have also experienced significant advancement. To the extent that nowadays, through intelligent software, tracking cryptocurrency transactions has become feasible.

Method: This study is a literature review that focuses on keywords such as Anti-Money Laundering, Money Laundering, suspicious transaction, machine learning, and Data Mining. The research involves searching for relevant articles related to these keywords, and suitable articles will be selected for further analysis.

Results: This study will present a classification based on approaches to combat money laundering in the electronic banking industry. Furthermore, it highlights the issues and challenges of these approaches in tackling money laundering within the electronic banking sector.

Discussion: This article presents a comprehensive analysis of the existing literature on combating money laundering, focusing on the use of machine learning, deep learning, data mining, and big data techniques. The reviews indicate that the lack of comprehensive data governance prevents the effective utilization of data from various institutions and centers for anti-money laundering purposes. Additionally, multiple graph algorithms, including centrality algorithms and embedded graph algorithms, have been employed to identify money laundering networks and organizations. Not utilizing these algorithms leaves a significant gap. Researchers can enhance the detection of illicit activities in anti-money laundering systems by employing community detection algorithms. Furthermore, the analyses reveal that unsupervised learning techniques can be more efficient in identifying money laundering due to the absence of labeled datasets and imbalanced data. Consequently, unsupervised methods can serve as a suitable tool for anti-money laundering systems.

Keywords: Anti-Money Laundering, Data Mining, Data Governance, Banking Transactions, Machine Learning.

سامانه‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)
انجمن علمی تجارت الکترونیکی ایران
واحد زنجان

مروری بر روش‌های هوشمند داده‌کاوی برای مبارزه با پول‌شویی و استقرار حاکمیت داده در شبکه بانکی

تاریخ دریافت: ۱۷/ ۰۸/ ۱۴۰۳
تاریخ پذیرش: ۲۹/ ۰۹/ ۱۴۰۳

دورهٔ پنجم، زمستان ۱۴۰۳
شمارهٔ چهارم، صص: ۴۷-۵۸

هدایت علیمرادی دوکوهی [۱]، عرفانه نوروزی [۲*]

۱. گروه مهندسی کامپیوتر، واحد قشم، دانشگاه آزاد اسلامی، قشم، ایران. Hedayat.Alimoradi@gmail.com
۲. گروه مهندسی کامپیوتر، واحد قشم، دانشگاه آزاد اسلامی، قشم، ایران. (نویسندهٔ مسئول) NoroziErfaneh@gmail.com

چکیده: با رشد خدمات الکترونیک در حوزه مالی و قدرت‌گرفتن درگاه‌های پرداخت غیرحضوری در دنیا، روش‌های مبارزه با پول‌شویی نیز رشد چشمگیری داشته‌است، به‌نحوی‌که امروزه با نرم‌افزارهای هوشمند، ردگیری تراکنش‌های رمزارزها نیز امکان‌پذیر است. حاکمیت داده جامع یکی از روش‌های سرعت‌بخشیدن به فرآیند مبارزه با پول‌شویی در شبکه بانکی است. در این مقاله برخی از چالش‌های پیاده‌سازی حاکمیت داده و داده‌کاوی در شبکه بانکی به‌منظور مبارزه با پول‌شویی و همچنین روش‌های یادگیری ماشین با نظارت، یادگیری ماشین بدون نظارت و روش‌های پیشرفته هوش مصنوعی یادگیری ماشین و کاستی‌های روش‌های موجود بررسی و پیشنهادهایی برای پژوهشگران ارائه‌خواهدشد. ازآنجاکه پول‌شویی همچنان یک مشکل رایج در اقتصاد جهانی امروزی است، دولت‌ها در سراسر جهان اقدامات سخت‌گیرانه‌ای برای جلوگیری از جرایم مالی اجرامی‌نمایند. این موضوع تقاضای فزاینده‌ای برای سیستم‌های ضدپول‌شویی در صنایع مختلف از جمله بانکداری، بورس، بیمه، خدمات مالی و بازار سرمایه ایجادکرده‌است.

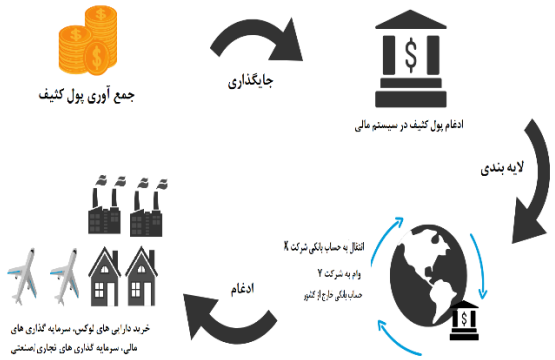
واژه‌های کلیدی: مبارزه با پول‌شویی، داده‌کاوی، حاکمیت داده، تراکنش‌های بانکی، یادگیری ماشین.

۱. مقدمه

پول‌شـــویی به فرآیند پنهان‌کردن منشـــأ غیرقانونی پول‌های کثیف و معتبر جلوه‌دادن آن گفته‌می‌شـــود[۱].پول کثیف، به معنای وجوه جمع‌آوری‌شده از فعالیت‌های مجرمانه یا غیرقانونی از جمله قاچاق مواد مخدر، قاچاق انسـان، رشـوه و فرار مالیاتی تعریف‌می‌شـود. پول‌شـویی می‌تواند به‌عنوان فرآیند پاک‌سازی پول کثیف تعریف‌شود[۲-۳].

کشـف جرایم مالی به یک اولویت مهم برای دولت‌ها تبدیل شـده اسـت و با گسـترش فناوری‌های مدرن و ارتباطات جهانی، روش‌های کلاهبرداری نیز به‌طرز چشـمگیری درحال‌رشـد و تغییر می‌باشـد که منجر به واردشدن زیان‌های قابل‌توجه به مشاغل قانونی شده‌است[۴].

در سال ۲۰۱۲ خبرهای مطبوعاتی متعددی در مورد تسویه‌حساب ۱,۹ میلیارددلاری بانک HSBC به دولت منتشر گردید که به علت عدم توانایی بانک HSBC در ایجاد یک برنامه مؤثر ضـد پول‌شـویی AML[1] بود. برای مدیریت ریسک فعالیت‌های پول‌شویی، در بانک‌ها نیاز شیوه‌ها و کنترل‌های مؤثر ضـدپول‌شـویی وجوددارد که باید اقدامات جدی در برابر هرگونه خطر احتمالی فعالیت های پول‌شـویی انجام‌دهند. این شیوه‌ها و کنترل‌ها باید در برابر هرگونه ادعای آتی که ممکن است برای بانک‌ها و مؤسسات مالی هزینه آفرین شود قابل‌استناد و معتبر باشند تا نگرانی بانک‌ها و مؤسـسـات مالی از متهم شـدن به نداشـتن برنامه ضـدپول‌شـویی مناسـب برطرف‌نماید[۵]. در شـکل (۱) چرخه یک تراکنش کاذب نمایش داده‌می‌شود.



شکل(۱) : مراحل شکل گیری چرخه پولشویی و تمیز نمودن پول کثیف

در چند دهه گذشـــته، یک مدل عملیاتی مبتنی بر قوانین تعبیه شد که به‌علت ساده‌بودن قوانین و کدنویسی آسان بسیار محبوب بود و معمولاً توسط خود مشاوران و کارشناسان این حوزه توسـعه و ارتقامی‌یافت، به همین واسـطه کارشـناسـان قادر بودند تجربه کاری خود را مسـتقیماً در کار پیاده‌سـازی و اجرا نمایند. روش‌های مبارزه با پول‌شـویی که بخشـی از روش‌های کنترل کلاهبرداری هستند باید خودکار انجام‌شوند و به کاهش کاردستی در فرآیند تحقیقات کمک‌کنند. برای اینکه نرم‌افزارها مسـتقل و مشترک برای تحقق اهداف و مقاصد سازمانی عمل‌کنند، ضرورت دارد دانش تجاری مانند قوانین کسـب‌وکار و اسـتراتژی‌های کسب‌وکار از رویه مبارزه با پول شویی استخراج شده و در طراحی عوامل فردی در نرم‌افزارها اعمال‌شوند.

در حال حاضـر اکثر بانک‌ها برای جدا کردن تراکنش‌های مشکوک، به قوانین ایستا و از پیش‌تولیدشده و سیستم‌های مبتنی بر قانون متکی هسـتند. در این روش بدون اطلاع از قوانین کسـب‌وکار و اسـتراتژی‌های کسـب‌وکار اطمینان از مشـروعیت و تشـخیص نیت از یک تراکنش یا چند تراکنش غیرممکن اسـت. پول شویی روزبه‌روز پیچیده‌تر و شامل چندین بانک، مؤسسات مالی، کشـورها و غیره می‌شـود. جهت مبارزه با پول‌شـویی نحوه به‌اشـتراک‌گذاری داده‌ها و دانش بین این نهادهای متعدد در حال تبدیل‌شدن به یک موضوع مهم و ضروری است[۶].

بیشـتر بانک‌ها معتقدند که بدون مقررات دولتی، تلاش آن‌ها برای جلوگیری از پول شویی کافی نخواهدبود و اکثر کارشناسان مبارزه با پول‌شـویی اظهارمی‌دارند که سـرمایه‌گذاری و پرداخت هزینه بانک‌ها در حوزه مبارزه با پول شویی بیشتر باهدف حفاظت از شهرت است[۷].

پول‌شـویی یک موضـوع جهانی بوده و تهدیدی جدی برای اقتصادها و جوامع به شمار می‌رود و دولت‌ها، سازمان‌های نظارتی و نهادهای مالی همگی با تمام ظرفیت خود با آن مبارزه‌می‌کنند، بااین‌حال هزینه‌های میلیارد دلاری مسئولین و شکست عملیات غیرقانونی همچنان خبر ساز است و این نشانه تداوم پول شویی و ضرورت مبارزه با آن است[۸].

۲. مروری بر ادبیات پژوهش

درگذشته بانک‌ها برای مبارزه با جرایم مالی و پیروی از مقررات مبارزه با پول‌شویی، بر سیستم‌های ضدپول‌شویی مبتنی بر قوانین تکیه‌داشتند که می‌توان شناسایی تراکنش‌های نقدی بیش از حدّ مجاز را نمونه‌ای از آن نام‌برد. در حال حاضر تکنیک‌های سنتی کشف و نظارت بر فعالیت‌های غیرقانونی، اگرچه تا حدی بهبودیافته‌اند، اما برای همگامی با سرعت فزاینده فعالیت‌های مجرمانه و حجم داده‌ها و تراکنش‌هایی که در سراسر جهان جریان‌دارند، کافی نیستند. مبارزه مؤثر با جرایم مالی و اطمینان از انطباق با مقررات در محیط پرسرعت دیجیتالی امروزی نیازمند ابزارها و راه‌حل‌های هوشمندتر، سریع‌تر و پویاتر است. این امر منجر به معرفی ابزارهای پیچیده‌تری برای مبارزه با پول‌شویی شده‌است. تکنیک‌های یادگیری ماشین برای مبارزه با پول‌شویی قبلاً ارائه‌شده‌اند، اما هنوز در مراحل اولیه توسعه هستند. روش‌های یادگیری عمیق نیز کشف‌شده‌اند که حتی با مجموعه‌داده‌های عظیم می‌توانند به‌خوبی کار

کنند و فناوری‌های یادگیری ماشین برای ساده‌سازی بیشتر فرآیند مبارزه با پول‌شویی به‌عنوان روشی موفق استفاده‌می‌شود[۸].

پس از بررسی تحقیقات متعدد چندین روش یادگیری ماشین برای شناسایی تراکنش‌های مشکوک که توسط محققان توصیه‌شده معرفی خواهندشد، بااین‌حال به‌ندرت شواهدی دالّ بر کاربرد آن در صنعت وجوددارد و علت آن نیز است که بیشتر تحقیقات بر اساس نمونه‌ای از داده‌های واقعی بسیار قدیمی یا داده‌های مصنوعی بوده‌است.

نبود تجربه عملی پژوهشگران، کسر داده‌های آموزشی (هشدارها، تراکنش‌های مشکوک)، فقدان داده‌های واقعی معاملات پول‌شویی، فقدان داده‌های واقعی فعلی از عوامل مهم عدم‌دستیابی به نتایج کاربردی است. محققان در بررسی خود، انتقادی از سیستم‌های ضدپول‌شویی با تمرکز بر روش‌های یادگیری عمیق انجام‌داده و دریافتند که مدل‌هایی مانند شبکه عصبی کانولوشن[۲]، شبکه عصبی کانولوشن مبتنی بر گراف متغیر، شبکه عصبی کانولوشن مقیاس‌پذیر، شبکه عصبی کانولوشن چندکاناله مبتنی بر پردازش زبان طبیعی، خود رمزگذار[۳] و پرسپترون چندلایه[۴] بیشترین استفاده را دارند.

پژوهشگران همچنین تفسیرپذیری سیستم‌های یادگیری ماشین را در این زمینه بررسی‌کردند که ۵۱ درصد از این سیستم‌ها بدون هوش مصنوعی قابل‌توصیف، غیرقابل‌تفسیر هستند. براین‌اساس، پیشنهاد کردند که تحقیقات آینده باید بر روی استفاده از رویکردهای هوش مصنوعی قابل‌توصیف، روش‌های تحلیل پیوند مانند استخراج نمودار و تجزیه‌وتحلیل شبکه‌های اجتماعی، یادگیری گروهی و روش‌های یادگیری بدون نظارت متمرکز شود[۹].

پژوهشگران دیگری نیز به شناسایی روش‌های مبارزه با پول‌شویی و روش‌های کشف تقلب مالی۵ پرداختند و با استفاده از پایگاه‌های اطلاعاتی SCOPUS و Web of Science، از ادبیات مروری سیستماتیکی برای تحلیل و تحقیق روش‌های مورداستفاده انجام‌داده‌اند. آن‌ها ۴۸ مقاله با موضوع تحقیق یکسان را بررسی‌کرده‌اند که ۲۰ مقاله شامل روش‌های کمی برای راه‌حل روش‌های مبارزه با پول‌شویی و کشف تقلب مالی بودند، ۱۳ مقاله مروری، ۷ مقاله از روش‌های کیفی و ۸ مقاله نیز شامل روش‌های ترکیبی بودند. مطالعه آنان دو شکاف تحقیقاتی را پرمی‌کند: ۱- عدم انجام مطالعات کافی در مورد روش‌های مبارزه با پول‌شویی و روش‌های کشف تقلب مالی در مباحث مالیاتی و ۲- معرفی روش‌های قابل‌استفاده، کمک‌می‌کند[۱۰].

داده‌کاوی فرآیندی برای استخراج دانش از داده‌های موجود است و از داده‌کاوی در بانکداری و تجارت می‌توان به‌عنوان ابزاری برای کشف اطلاعات مفید از داده‌های عملیاتی و داده‌های قدیمی به‌منظور تصمیم‌گیری بهتر استفاده‌کرد.

گروهی در بررسی مقالات داده‌کاوی برای مبارزه با پول‌شویی بیشتر از تکنیک‌های خوشه‌بندی مانند k-Means، الگوریتم CLOPE، و درخت پوشا کمینه[۶] و همچنین روش‌های مبتنی بر قانون[۷] مانند شبکه‌های بیزی[۸] استفاده‌می‌کنند. هستی‌شناسی[۹]، شبکه تابع پایه شعاعی[۱۰]، ماشین بردار پشتیبانی[۱۱]، درخت تصمیم[۱۲] و بر اساس تحلیل شبکه‌های اجتماعی[۱۳] نیز می‌توان استفاده‌نمود[۳].

در یک بررسی سیستماتیک از شناسایی سیستم‌های تراکنش‌های غیرقانونی از جمله سیستم‌های ضدپول‌شویی در زمینه بیت‌کوین در ۲۵ مقاله انتخابی سه گروه به شرح زیر تقسیم‌بندی‌شده‌است[۱۱]:

۱- مطالعات تجزیه و تحلیلی توپولوژی بر اساس الگوریتم‌های گراف.

۲- روش‌های یادگیری بدون نظارت مانند: خوشه‌بندی، تجزیه‌وتحلیل مؤلفه‌های اصلی[۱۴].

۳- روش‌های یادگیری تحت نظارت مانند: جنگل تصادفی[۱۵]، و شبکه‌های عصبی[۱۶].

همچنین پژوهشگران مروری بر سیستم‌های هوش مصنوعی برای مبارزه با پول‌شویی داشته‌اند و مطالعات متعددی از جمله تجزیه‌وتحلیل لینک[۱۷] و سیستم‌های تجزیه‌وتحلیل شبکه[۱۸] که بر الگوریتم‌های مرکزی برای مبارزه با پول‌شویی و کشف ارتباطات درون باندهای پول‌شویی متمرکزند را بررسی و سیستم دسته‌بندی ریسک را ارائه‌کردند که از یادگیری ماشین برای اختصاص امتیاز به معاملات دارای ریسک استفاده‌می‌کند. علاوه بر این، آن‌ها سیستم خود را برای تشخیص پول‌شویی با استفاده از روش‌های پردازش زبان طبیعی (NLP[۱۹]) و یادگیری عمیق[۲۰]، از جمله تجزیه‌وتحلیل احساسات[۲۱]، شناسایی موجودیت نام‌گذاری‌شده[۲۲]، استخراج رابطه، شبکه عصبی کانولوشن و حافظه کوتاه‌مدت[۲۳] ارائه‌می‌دهند. آن‌ها عقیده‌دارند که این سیستم می‌تواند زمان و هزینه تحقیقات را تا حدود ۳۰٪ کاهش دهد[۱۲].

پژوهشگران یک بررسی در مورد مبارزه با پول‌شویی با تمرکز بر حوزه‌های یادگیری ماشینی، یادگیری عمیق، داده‌کاوی و داده‌های حجیم در سال ۲۰۱۷ تا ۲۰۲۳ انجام و دو حوزه الگوریتم‌های یادگیری با نظارت و بدون نظارت را موردتوجه قرارداده‌اند. روش‌ها و پارامترهای ارزیابی دیگر پژوهش‌ها را شناسایی‌کردند[۲۹].

جدول ۱: مروری بر کارهای مرتبط در حوزه پول‌شویی

مرجع	حوزه موضوع	ویژگی تحقیق
[۱]	داده مناسب برای یک برنامه ضدپول‌شویی مجموعه‌داده واقعی یک بانک چندملیتی است	غلبه بر مشکل طراحی پایگاه‌داده و کیفیت داده با به‌کارگیری مجموعه‌داده‌های واقعی مشتریان یک بانک و همچنین حل مسئله مصرف حافظه را برای مقابله با مجموعه‌داده‌های عظیم در حوزه مبارزه با پول‌شویی.
[۲]	تشخیص پول‌شویی بر اساس شباهت ساختاری	از روش‌های کاهش مواردی همچون شناسایی معاملات مشابه و تفکیک حساب‌های مشکوک به پول‌شویی استفاده نموده و نهایتاً با بهره‌گیری از شباهت ساختاری، موفق به شناسایی و گروه‌بندی حساب‌های بالقوه پول‌شویی گردیده‌اند.
[۳]	تکنیک‌های داده‌کاوی برای	داده‌کاوی فرآیندی برای استخراج دانش از داده‌های موجود است و به‌طورکلی در بانکداری و تجارت به‌منظور کشف اطلاعات مفید از داده‌های

	مبارزه با پول‌شویی	عملیاتی و داده‌های قدیمی جهت امکان تصمیم‌گیری بهتر در مواردی همچون زمینه‌های کاربردی مختلف مانند بازاریابی، کشف تقلب، مدیریت ریسک، شناسایی پول‌شویی و سرمایه‌گذاری استفاده می‌کنند. مطالعه مروری بر تحقیقات انجام شده در زمینه داده‌کاوی با تأکید بر کشف پول‌شویی و بررسی کاستی‌های تکنیک‌های داده‌کاوی می‌باشد. باتوجه‌به حجم بالای تراکنش‌های روزانه در بانک‌ها و مؤسسات مالی، امکان سیستم‌های خودکار که بتوانند با داده‌های انبوه تعامل داشته باشند، ضروری است. باتوجه‌به اینکه موارد پول‌شویی در حال تغییر است و پول‌شویی‌ها از روش‌های جدیدتری استفاده می‌کنند، بنابراین، تکنیک‌های داده‌کاوی بدون نظارت برای شناسایی الگوهای جدید پول‌شویی کاربردی‌تر خواهد بود و می‌تواند برای تقویت مدل‌های یادگیری بر اساس روش‌های طبقه‌بندی ضروری باشند.
[۸]	مبارزه با پول‌شویی به‌وسیله یادگیری ماشین	کارشناسان در حال ترکیب فناوری‌های وب معنایی، گراف دانش (KG) و شبکه‌های عصبی گراف (GNN) با یادگیری انتقالی ML/DL هستند تا نتایج بهینه‌تر و محاسبات سریع‌تر را با مجموعه‌داده‌های بسیار بزرگ به‌منظور بهبود عملکرد مبارزه با پول‌شویی و سیستم‌های تحلیل ریسک ارائه دهند.
[۹]	تکنیک‌های یادگیری عمیق و هوش مصنوعی در تشخیص پول‌شویی	نبود تجربه عملی پژوهشگران، کسر داده‌های آموزشی (هشدارها، تراکنش‌های مشکوک)، فقدان داده‌های واقعی معاملات پول‌شویی، فقدان داده‌های واقعی فعلی از عوامل مهم عدم دستیابی به نتایج کاربردی است. پژوهشگران بررسی کردند که درصد بسیاری از روش‌ها از هوش مصنوعی استفاده نکرده و پیشنهاد کردند که تحقیقات آینده باید بر روی استفاده از رویکردهای هوش مصنوعی قابل‌توصیف، روش‌های تحلیل پیوند مانند استخراج نمودار و تجزیه‌وتحلیل شبکه‌های اجتماعی، یادگیری گروهی و روش‌های یادگیری بدون نظارت متمرکز شود.
[۱۰]	مروری بر ادبیات سیستماتیک روش‌های مبارزه با پول‌شویی	از ۴۵ مقاله انتخاب شده در مورد پول‌شویی و کلاهبرداری مالیاتی، ۱۳ مقاله مربوط به بررسی ادبیات، ۷ مقاله مربوط به روش‌های کیفی، ۱۸ مقاله به روش‌های کمی و ۷ مقاله از روش‌های ترکیبی بررسی شده است. مشخص است که مدل‌های کلی برای کشف تقلب مالیاتی و پول‌شویی همچنان کم هستند. بر اساس روش‌های کمی، تشخیص پول‌شویی نمی‌تواند از سه نوع بی‌نظمی فرار کند: (۱) حجم و فراوانی معاملات، (۲) همبستگی تجاری، و (۳) تقلب حسابداری.
[۱۱]	بررسی سیستماتیک تشخیص تراکنش‌های غیرقانونی بیت‌کوین (رمزارزها)	رمزارزها به علت دارابودن ویژگی‌هایی همچون عدم تمرکز، عدم شفافیت و تغییرناپذیری موجب گردیده تعداد کاربران و برنامه‌های مرتبط ارزهای دیجیتال محبوب‌تر شوند. این روند مجرمان را به انجام معاملات غیرقانونی در وب تاریک یا پول‌شویی تشویق می‌کند بااین‌حال ماهیت دفترکل ارزهای دیجیتال دریچه دیگری را به روی مراجع قضایی جهت شناسایی فعالیت‌های غیرقانونی در شبکه مالی بیت‌کوین بازکرده است. در این مقاله، از یک روش عینی و سیستماتیک برای به‌دست‌آوردن ۲۵ اثر ادبی مرتبط با شناسایی فعالیت‌های غیرقانونی در شبکه مالی بیت‌کوین استفاده شده است و مقالات را به سه دسته تقسیم کرده است ۱-یادگیری با نظارت، ۲-یادگیری بدون نظارت و ۳-توپولوژی.
[۱۲]	مبارزه با پول‌شویی به‌وسیله هوش مصنوعی	روش‌های پیشرفته هوش مصنوعی را برای مبارزه با پول‌شویی بررسی شده‌است و با پیشنهاد چارچوبی که از پردازش پیشرفته زبان طبیعی و تکنیک‌های یادگیری عمیق وجوددارد برای تسهیل در فناوری‌های آینده مبارزه با پول‌شویی استفاده می‌نمایند. چارچوب جدید ممکن است در کنار سیستم موجود مبارزه با پول‌شویی بانک مورداستفاده قرارگیرد و به کارشناسان انسانی کمک بیشتری برای تصمیم‌گیری ارائه‌دهد. برخی از رویکردهای یادگیری عمیق عملکردهای رقابتی در حوزه‌های دیگر مانند صنعت را به‌دست آورده‌اند، اما هنوز برای مبارزه با پول‌شویی مورد آزمایش قرار نگرفته‌اند.
[۲۹]	مبارزه با پول‌شویی با استفاده از یادگیری ماشینی	روش‌های یادگیری ماشین برای مبارزه با پول‌شویی بررسی شده است. بازه تحقیق در سال ۲۰۱۷ تا ۲۰۲۳ انتخاب شده است.

۳. سیاست‌های مبارزه با پول‌شویی

گروه ویژه اقدام مالی (FATF)[۲۴]سازمانی است که باهدف مبارزه با پول‌شویی و تأمین مالی تروریسم در سال ۱۹۸۹ ایجادگردید[۱۲]. گروه ویژه اقدام مالی سازمانی است که از عضویت کشورهای مستقل تشکیل-شده‌است و شامل ۳۵ حوزه قضایی عضو و دو سازمان منطقه‌ای می‌باشد. این گروه اقدامات مالی را ملزم به اجرای برنامه‌های مبارزه با پول‌شویی و مقابله با تأمین مالی تروریسم[۲۵] می‌نماید که شامل تجزیه‌وتحلیل داده‌ها و گزارش‌های خاص می‌باشد. یکی از الزامات شناسایی و تأیید مشتریان توسط مؤسسات می‌باش‌د که معمولاً به‌عنوان "مشتری خود را بشناسید" نامیده‌می‌شود. این امر حساب‌های ناشناس و نام‌های صاحب حساب ساختگی را ممنوع می‌کند و از مؤسسات و بانک‌ها می‌خواهد در

هنگام برخورد با مشتریان استعلامات و اقدامات پایه پیشگیرانه را انجام-دهند. الزام دیگر این است که بانک‌ها باید سوابق کلیه تراکنش‌ها را حداقل به مدت پنج سال نگه‌دارند. داده‌ها باید شامل نام مشتریان و یا ذی‌نفعان، آدرس آن‌ها، ماهیت تراکنش‌ها، تاریخ تراکنش‌ها، نوع ارز، مبالغ، انواع حساب‌ها و شماره‌های شناسایی هر حساب باشد.

گروه ویژه اقدام مالی به دو نوع گزارش نیاز دارد:

۱- گزارش تراکنش‌های مشکوک[۲۶] که در واحد اطلاعات مالی ملی ثبت‌می‌شوند.

۲- گزارش تراکنش‌های ارزی[۲۷] که بالاتر از مقدار معین را گزارش‌می‌کند.

۴. تکنیک‌های هوش مصنوعی برای مبارزه با پول‌شویی

مبارزه با پول‌شویی سازوکارهای مختلفی دارد که به مسائل کلان و جزئی در این زمینه می‌پردازد و جهت به‌کارگرفتن هوش مصنوعی در شناسایی مراحل پول‌شویی ابعاد گسترده‌ای را باید درنظرگرفت. تغییر روش‌های سنتی و قدیمی مبارزه با پول‌شویی و حرکت به‌سوی صنعتی نمودن فرآیند مبارزه با پول‌شویی، چالش‌های خاص خود را دارد و تحقیقات پژوهشگران حاکی از ضرورت حرکت به سمت تکنیک‌های هوش مصنوعی می‌باشد که در ادامه به توضیح برخی از آن‌ها خواهیم‌پرداخت.

۱،۴. مراحل پول‌شویی

جای‌گذاری (قراردادن)[۲۸]، لایه‌بندی[۲۹] و یکپارچه‌سازی[۳۰] سه بخش اصلی در طرح‌های پول‌شویی هستند. در فاز قراردادن، درآمدهای حاصل از فعالیت‌های مجرمانه به اسناد مالی تبدیل و یا به‌حساب بانکی واریزمی‌شوند. انتقال وجوه به بانک‌های مختلف و یا افراد دیگر از طریق انتقال وجوه، چک، حواله بانکی و یا روش‌های دیگر را لایه‌بندی گویند. در نهایت، در بخش یکپارچه‌سازی، وجوه به کسب‌وکارهای قانونی منتقل‌شده و یا برای ادامه فعالیت‌های مجرمانه استفاده‌می‌شوند، در این مرحله، پول به‌دست‌آمده غیرقانونی، قسمتی از اقتصاد قانونی می‌شود. رویکردهای هوش مصنوعی می‌توانند برای شناسایی فعالیت‌های پول‌شویی در هر سه‌فاز فوق به‌کاررروند. روش‌های رایج یادگیری ماشین با استفاده از دیتاست‌های بزرگ و برچسب‌گذاری‌شده بانک‌ها می‌توانند برای دسته‌بندی تراکنش‌های مشکوک استفاده‌نمود.

رویکردهای مبتنی بر داده معمولاً برای مراحل جای‌گذاری و لایه‌بندی استفاده‌می‌شوند؛ زیرا داده‌های تراکنش توسط بانک‌ها قابل-نظارت می‌باشند. تشخیص مرحله نهایی ادغام دشوار است؛ زیرا وجوه دارای مکانیسم‌های کشف تقلب نیستند. در این مرحله روش‌های پیشرفته هوش مصنوعی می‌توانند برای مبارزه با پول‌شویی واردشوند و با شناسایی تراکنش‌های مشکوک در فرآیندهای تحلیلی ناظران انسانی را یاری‌نمایند. حجم کار یک ناظر انسانی تا حد زیادی به تعداد تراکنش-های تقلب گزارش‌شده بستگی دارد. رویکردهای پردازش زبان طبیعی[۳۱] تجزیه- تحلیل موجودیت و روابط[۳۲] می‌تواند با امتیازدهی به تراکنش‌های مشکوک بر اساس داده‌های خبری مرتبط و سایر موجودیت‌های بالقوه کلاهبرداری به ناظران انسانی با کاهش بار کاری کمک‌نماید.[۱۲]

۲،۴. راهکارهای صنعتی مبارزه با پول‌شویی

گردش کار صنعتی برای مبارزه با پول‌شویی، مانند یک خط لوله مستقیم است که یک منبع داده را به یک سیستم مبتنی بر قانون متصل‌نماییم. سپس ناظران تحقیقات خود را برای تعیین مشروع یا تقلبی‌بودن معاملات با این منبع داده‌ها ادامه‌می‌دهند. ابتدا با تعیین چارچوب‌هایی مشخص، سیستم داده‌های مرتبط با پول‌شویی را جمع‌آوری و پردازش می‌نمایند و بعد تراکنش‌های جمع‌آوری‌شده را بررسی‌نموده و اگر تراکنش مشکوک تشخیص‌داده‌شود، آن را علامت‌گذاری‌کرده و در اختیار یک ناظر انسانی قرارمی‌دهد و آن فرد درخصوص این که تشخیص سیستم در شناسایی تراکنش مشکوک صحیح بوده یا خیر تصمیم‌می-گیرد. به‌طورکلی، چارچوب‌های مبارزه با پول‌شویی صنعتی را می‌توان در چهارلایه مجزا قرارداد.[۱۲]

- لایه داده[۳۳] که در آن داده‌های مربوطه جمع‌آوری، مدیریت و ذخیره‌می‌شوند. این لایه شامل داده‌های داخلی مؤسسات مالی، بانک‌ها و داده‌های خارجی از منابعی مانند سازمان‌های نظارتی و مراجع قضایی است.
- لایه غربالگری و نظارت[۳۴]، تراکنش‌ها و مشتریان را برای فعالیت مشکوک غربال می‌کند. این لایه عمدتاً توسط مؤسسات مالی، بانک‌ها در یک‌رویه چندمرحله‌ای که اغلب بر اساس قوانین یا تجزیه‌وتحلیل ریسک است، صورت‌می‌پذیرد.
- لایه هشدار و رویداد[۳۵]، اگر فعالیت مشکوکی پیداشود، برای بررسی بیشتر به این لایه ارسال‌می‌شود. این فرآیند شامل تأیید داده‌ها با سوابق قبلی تراکنش‌ها و شواهد لازم برای بررسی تراکنش مشکوک است. در حال حاضر، استفاده از رسانه‌های اجتماعی و محتوای وب برای به‌دست‌آوردن اطلاعات در جهت مبارزه با پول‌شویی به‌خوبی توسعه‌نیافته‌اند و این موضوع تحلیلگران را با کمبود منابع مواجه‌می‌سازد که باعث افزایش ریسک اخذ تصمیمات اشتباه و افزایش زمان برای بررسی صحت تراکنش‌ها می‌شود.
- لایه عملیاتی[۳۶]، پس از تأیید تراکنش مربوط به پول‌شویی، جهت ادامه پیگیری‌های قانونی از جمله مسدودنمودن حساب‌های مرتبط در این لایه صورت‌می‌پذیرد.

۳،۴. تجزیه‌وتحلیل شبکه‌ای برای مبارزه با پول‌شویی

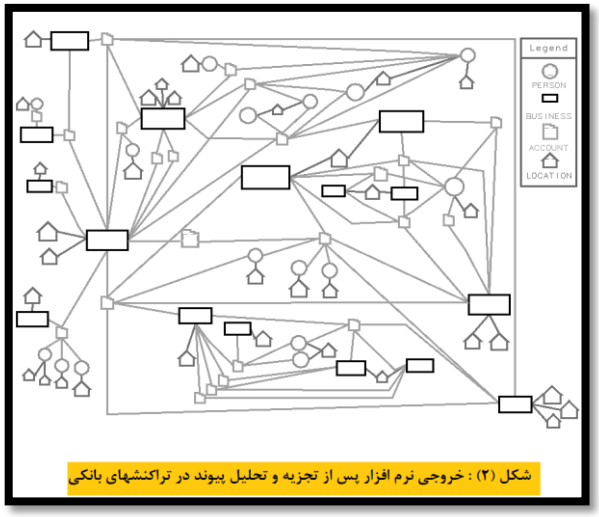
یک روش برای شناسایی فعالیت‌های پول‌شویی تجزیه‌وتحلیل شبکه‌ای است. از تجزیه‌وتحلیل شبکه‌ای می‌توان در داده‌ها رابطه‌ای برای

پیداکردن ارتباطات مستقیم و یا پنهان با یک گره پول‌شویی استفاده‌نمود. از روش‌های اولیه تجزیه‌وتحلیل شبکه‌ای، ارزیابی مرکزیت می‌باشد که برای تعیین مهم‌ترین گره در یک شبکه استفاده‌می‌گردد. سیستم‌های تجزیه‌وتحلیل شبکه متداول شامل متغیرهای زیرند[۱۲]:
درجه مرکزیت[۳۷]، اقتدار، مرکزیت میانی[۳۸]، مرکزیت نزدیک[۳۹]، مرکزیت (قطب)[۴۰] و رتبه صفحه[۴۱].

محققان چندین شبکه برای کار جمعی بر روی مبارزه با پول‌شویی ایجادنموده‌اند از جمله تراکنش‌ها، بخش‌های اقتصادی، مناطق جغرافیایی و شبکه پیوند ضمنی برای جلوگیری از پول‌شویی. آن‌ها از داده‌های واقعی ۱۹ماهه یک شرکت که عمدتاً در ایتالیا فعالیت‌می‌کند استفاده‌کرده و دریافتند که معیارهای شبکه در ارزیابی ریسک تقلب بسیار مفید است.[۱۳]

۴,۴.تجزیه‌وتحلیل پیوند[۴۲]

شبکه اجرای جرایم مالی (FINCEN) [۴۳] دارای سیستم هوش مصنوعی (FAIS) [۴۴] می‌باشد و تراکنش‌های نقدی بزرگ را برای شناسایی پول‌شویی بالقوه با داده‌های مرتبط ارزیابی‌می‌نماید. هدف FAIS کشف سرنخ‌های ناشناخته با داده‌های قدیمی و بالقوه دارای ارزش برای بررسی موارد مشکوک است. FAIS نیروهای انسان‌های و عوامل نرم‌افزاری را در یک کار کشف مشارکتی در فضای داده بسیار بزرگ ادغام‌می‌کند. در شکل ۲ نمونه از خروجی نرم‌افزار پس از تجزیه‌وتحلیل پیوند در تراکنش‌های بانکی آمده‌است[۱۴].



شکل (۲) : خروجی نرم افزار پس از تجزیه و تحلیل پیوند در تراکنشهای بانکی

بسیاری از پایگاه‌های اطلاعاتی جهان از تعداد زیادی تراکنش مستقل تشکیل‌شده‌اند و یکی از روش‌های مناسب جهت یافتن شواهدی از گروه‌های ساختاریافته موجودیت‌ها در این داده‌ها روش تجزیه‌وتحلیل پیوند می‌باشد و با بازسازی پایگاه‌های داده امکان جستجو و تحلیل مؤثر ساختارهای پیوندی پنهان در تراکنش‌های اصلی فراهم‌می‌گردد. بخش دولتی و بخش تجاری مقادیر بسیار زیادی از داده‌های مبادلاتی را تولیدمی‌نمایند که موجب تجزیه‌وتحلیل اضافی می‌شود[۱۵].

این موضوع همچنین در مورد پول‌شویی در روش‌های پرداخت موبایلی اعمال‌شده‌است. آن‌ها نمودارهایی با پیوند مصنوعی (مشابه شبکه‌های اجتماعی) ایجادنموده که می‌توان برای تجسم و شناسایی ارتباطات خاص استفاده‌نمود[۱۶].

همچنین پژوهشگران موقعیتی را درنظرگرفتند که در آن هیچ پیوند صریحی بین موجودیت‌ها در یک گراف پیوندی قابل‌مشاهده نبود و بر اساس همبستگی‌ها به‌عنوان ویژگی برای ایجاد پیوندهای جدید جوامعی را ایجادکردند که روابط آن‌ها هنوز مشخص‌نشده‌است[۱۷].

۵,۴. تشخیص نقاط دورتر[۴۵]

یک راه طبیعی برای تعریف قالب شرح وظایف هوش مصنوعی و داده‌کاوی مربوط به کشف کلاهبرداری یا کشف تقلب، از طریق تشخیص بیرونی است. در این روش، یک تراکنش عادی یا معامله غیرمجاز به‌عنوان یک موضوع درنظرگرفته‌می‌شود و سپس هر معامله‌ای که متفاوت است به‌عنوان معامله پرت شناسایی‌می‌شود و بعد یک گروه همتا تعریف‌می‌شود تا عادات معمولی تراکنش‌های یک مشتری را به تصویر بکشد و ازآنجاکه خوشه‌بندی یک روش استاندارد برای تعریف گروه‌های همتاست در مرحله بعد، فاصله بین تراکنش‌های ورودی و گروه‌های همتا محاسبه‌می‌شود تا رفتار پرت تشخیص‌داده‌شود. روش الگوریتم تشخیص پول‌شویی مبتنی بر رگرسیون از یک محدوده تقسیم‌شده (IQR)[۴۶] یک معیار متغیر را جهت جداسازی تراکنش‌های مشکوک در سیستم‌های مالی آنی ارائه و به‌وضوح پیچیدگی زمانی را همراه با پیچیدگی محاسباتی کاهش می‌دهد. تجزیه‌وتحلیل مقایسه‌ای هر دو مکانیسم در برابر روش‌های موجود از نظر حساسیت، ویژگی، زمان اجرا و دقت قابل‌بررسی است [۱۸].

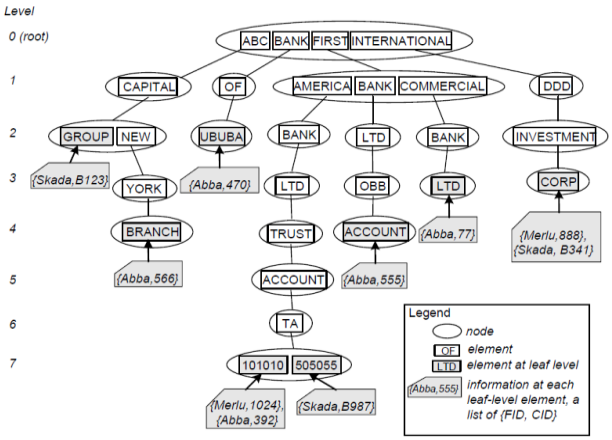
۶,۴. طبقه‌بندی ریسک / امتیازدهی[۴۷]

محققان تعدادی از تکنیک‌های طبقه‌بندی - از جمله جنگل تصادفی، درخت تصمیم، بیز ساده و جدول تصمیم- را برای پیش‌بینی پول‌شویی در برنامه‌های تلفن همراه آزمایش و از شناسه مشتری، مشخصات، تاریخ تراکنش، نوع تراکنش، مبلغ انتقال‌یافته، مکان و سن مشتری برای نمایش هر تراکنش استفاده‌کردند و دریافتند که درخت تصمیم بالاترین عملکرد را دارد. در برخی از پژوهش‌ها لایه غربالگری و مانیتورینگ را به‌عنوان دسته‌بندی‌کننده تراکنش‌های مشکوک تعیین‌می‌کند. به‌دلیل کمبود داده‌های واقعی و یا محدودیت دسترسی به داده‌های واقعی موجب‌شده با مجموعه‌داده‌های شبیه‌سازی‌شده کار شود. علاوه بر این، ازآنجاکه به‌ندرت به مؤسسات مالی اطلاع‌داده‌می‌شود که معامله‌ای به‌عنوان پول‌شویی است، روش‌های موجود اغلب از داده‌های تقلبی ترکیب‌شده استفاده‌شده‌است.[۲۰-۱۹].

۷،۴. یادگیری گراف برای مبارزه با پول‌شویی[۴۸]

یک گره می‌تواند یک حساب واحد را نشان‌دهد که خود نیز نمودار دیگری را در داده‌های عظیم گراف تراکنش‌ها تشکیل‌می‌دهد. در همین حال، مؤسسات مالی میلیون‌ها تراکنش را در ثانیه را پردازش‌می‌کنند. چالش‌های اصلی در یادگیری گراف برای مبارزه با پول‌شویی، سرعت یادگیری/تجزیه گراف و اندازه گراف است. تهیه نقشه داده‌های نموداری با ابعاد بالا و عظیم که میلیاردها رابطه (لبه) بین میلیون‌ها موجودیت (گره) را ترسیم‌می‌کند یک چالش است. در ردیابی تراکنش‌های پول‌شویی، یک موجودیت گره ممکن است یک حساب منفرد یا مجموعه‌ای از حساب‌های مرتبط باشد (شناخته‌شده یا از طریق خوشه‌بندی استنباط‌می‌شود تا به‌عنوان یک حساب کارکند). یک گره همچنین می‌تواند نمودار دیگری از مرحله قبلی در یک سری زمانی باشد. ویژگی‌های شناخته‌شده آن‌هایی هستند که به‌صراحت در داده‌ها تعریف-شده‌اند، مانند اطلاعات جمع‌آوری‌شده در فرآیندهای استاندارد «مشتری خود را بشناسید» (KYC)[۴۹] یا داده‌های چندوجهی جمع‌آوری‌شده و یا از جریان‌های اطلاعات عمومی یا شریک، و همچنین تراکنش‌های قابل‌مشاهده مرتبط ثبت‌شده.[۲۱].

مجموعه‌داده‌های مشتری بر اساس نوع مشتری (حقوقی یا حقیقی) و کشور، گروه‌بندی می‌شوند. طراحی نام شرکت درختی (CN tree)[۵۰] یک توپولوژی درختی پسوندی است. به‌طورکلی، اولین کلمه نام شرکت در سطح ریشه (سطح ۰) و آخرین کلمه آن در سطح برگ ظاهرمی‌شود. درخت CN شامل مجموعه‌ای از گره‌ها می‌باشد که هر گره حاوی یک یا چند عنصر است ویک مسیر از ریشه به برگ را با دنبال‌کردن پیوندهای گره می‌توان ترسیم‌نمود. شکل۳ نمونه‌ای از ارتباطات به شکل درخت است[۱].



شکل شماره (۳) نمونه ای از ارتباطات به شکل درخت میباشد

۸،۴. یادگیری ماشین و یادگیری عمیق مناسب‌ترین روش‌های هوش مصنوعی جهت مبارزه با پول‌شویی

دو نوع اصلی از الگوریتم‌های یادگیری با نظارت[۵۱] و الگوریتم‌های یادگیری بدون نظارت[۵۲] با استفاده از یادگیری ماشین و یادگیری عمیق برای هوش مصنوعی جهت مبارزه با پول‌شویی به شرح زیر پیشنهاد-شده‌اند.

۱،۸،۴. روش‌های نظارت‌شده

یکی از مثال‌های مرسوم در یادگیری با نظارت تشخیص و فیلترکردن هرزنامه‌ها در میان نامه‌ها است. سیستم‌های توصیه‌گر مبتنی بر فیلترینگ مشارکتی یکی دیگر از این کاربردها است [۲۷]. ابتدا تمامی داده‌ها به دو کلاس سالم و هرزنامه‌ها تقسیم‌می‌شوند، سپس ماشین آن‌ها را با مثال‌های موجود می‌آموزد در نهایت از او امتحان گرفته‌می‌شود تا ایمیل جدیدی که تابه‌حال ندیده‌است را به آن بدهید و تشخیص‌دهد سالم است یا هرزنامه. در یادگیری نظارت‌شده باید مجموعه‌ای از ویژگی‌های ورودی و یک مقدار خروجی وجودداشته‌باشد. الگوریتم رابطه بین ورودی و خروجی را از داده‌های تاریخی یادمی‌گیرد و این الگوریتم می‌تواند به یادگیری از داده‌های جدید ادامه‌دهد تا دقت افزایش‌یابد. دو نوع اصلی از الگوریتم‌های یادگیری نظارت‌شده دسته‌بندی[۵۳] و رگرسیون[۵۴] می‌باشد. الگوریتم‌های دسته‌بندی برای پیش‌بینی مقادیر گسسته استفاده‌می‌شوند و الگوریتم‌های رگرسیون روی مقادیر پیوسته پیش‌بینی می‌نمایند. هر دو این الگوریتم‌ها به یک مجموعه آموزشی برچسب‌دار نیاز دارند.

روش‌های نظارتی متعددی برای شناسایی پول‌شویی ایجادشده‌اند که این روش‌ها تشخیص پول‌شویی را به‌عنوان یک موضوع دسته‌بندی دو کلاسه درنظرمی‌گیرند [۲۲]. کیفیت داده‌ها و پاک‌سازی داده‌ها را نیز می‌توان بررسی‌کرد[۲۸].

با استفاده از مجموعه‌داده‌های یک مؤسسه املاک و مستغلات با پنج متغیر مستقل همچون: شخص حقوقی، منشأ مشتری، فعالیت اقتصادی، سابقه کار، و قرارداد تولید محصول در یک مدل درخت رگرسیون برای ارزیابی ریسک پول‌شویی مرتبط با مشتری استفاده‌گردید. کارشناسان داده‌ها را مطابق با استانداردهای ایجادشده توسط وزارت دارایی و اعتبار عمومی مکزیک علامت‌گذاری‌کردند و یافته‌ها نشان‌داد که تنها متغیرهای «محصول قراردادی» و «سابقه کار» دارای اهمیت آماری هستند و سایر متغیرهای مستقل از ساخت درخت رگرسیون حذف‌شدند. با استفاده از آستانه احتمال ۰،۵، درخت رگرسیون مشتریان را به‌عنوان پرخطر یا کم‌خطر طبقه‌بندی‌کردند. نتایج نشان‌داد که ۷۸،۷٪ از کسانی که به‌عنوان پروفایل‌های کم‌خطر پیش‌بینی و ۱۰۰٪ از کسانی که به‌عنوان پروفایل‌های پرخطر طبقه‌بندی‌شده‌بودند، صحیح شناسایی-شدند[۲۳].

محققان نمودارهای تراکنش بیت‌کوین را مشخص و الگوهای پول‌شویی و تراکنش‌های منظم را بر اساس داده‌های جمع‌آوری‌شده در سه سال مطالعه‌نموده و نشان‌دادند که تراکنش‌های پول‌شویی نسبت به تراکنش‌های معمولی نسبت به درجه/خارج از درجه بالاتر، مجموع یکنواخت‌تر، میانگین خروجی‌ها و تعداد کمی از اجزای ضعیف‌تر مرتبط با تراکنش‌های معمولی دارند. نتایج طبقه‌بندی اولیه و پیش‌بینی با استفاده از یک طبقه‌بندی ثابت‌کرد که ما می‌توانیم پول‌شویی را از

تراکنش‌های معمولی متمایزکنیم و نمونه‌های جدید را پیش‌بینی‌کنیم. نتایج همچنین نشان‌داد که عملکرد کلاسی را می‌توان با تکنیک‌های گروهی بهبود بخشید[۲۴].

۲،۸،۴. روش‌های یادگیری بدون نظارت

یادگیری بدون نظارت، همچنین به‌عنوان یادگیری ماشین بدون نظارت شناخته‌می‌شود، از الگوریتم‌های یادگیری ماشین برای تجزیه‌وتحلیل و خوشه‌بندی مجموعه‌داده‌های بدون برچسب استفاده‌می‌کند. این الگوریتم‌ها الگوهای پنهان یا گروه‌بندی داده‌ها را بدون نیاز به دخالت انسان کشف‌می‌نمایند. یادگیری بدون نظارت روشی مناسب برای رفع مشکل برچسب‌گذاری داده‌ها در روش یادگیر با نظارت برای مبارزه با پول‌شویی می‌باشد؛ زیرا نیازی به داده‌های برچسب‌دار ندارد. برخلاف یادگیری تحت‌نظارت، الگوریتم‌های یادگیری بدون‌نظارت مانند خوشه-بندی[۵۵]، تشخیص ناهنجاری[۵۶]، تجزیه‌وتحلیل شبکه[۵۷] و کاهش ابعاد[۵۸] می‌توانند برای شناسایی پول‌شویی استفاده‌شوند.

محققان دو سیستم بدون نظارت که از الگوریتم‌های تشخیص ناهنجاری جنگل جداسازی[۵۹] و ماشین بردار پشتیبان یک کلاسه برای شناسایی تراکنش‌های غیرعادی پول‌شویی استفاده‌نمودند. در پژوهش آنان جنگل جداسازی بهتر از ماشین بردار پشتیبان یک کلاسه عمل‌کرد و به ترتیب ۱۱۸۲۵ و ۱۱۲۲۲ ناهنجاری را تشخیص‌داد. کارشناسان تأییدکردند که تمامی تراکنش‌های طبقه‌بندی‌شده توسط این سامانه پرخطر بوده و ۵۰ مورد به‌وضوح به‌عنوان مظنون شناسایی و ۴۱۴ تراکنش مشکوک و به ۴ گروه پول‌شویی تقسیم‌شده‌اند[۲۵].

یک روش جدید برای شناسایی کل جریان پول‌شویی از مبدأ تا مقصد با استفاده از گراف چندبخشی پیشنهادشده‌است. این رویکرد شامل استخراج زیر گراف‌های مشکوک پول‌شویی با استفاده از یک معیار ناهنجاری جدید بوده که دو معیار اصلی را درنظرمی‌گیرد. ۱- چگالی زیرگراف زیرا پول‌شویی‌ها اغلب تراکنش‌ها با حجم بالا را انجام‌می‌دهند که منجر به زیرگراف‌های متراکم می‌شود. ۲- تعادل بین درجه وزنی و مازاد حساب‌های میانی در زیرگراف مشکوک[۲۶].

محققان یک سیستم فازی سه‌مرحله‌ای را برای شناسایی پول‌شویی با استفاده از مجموعه‌داده‌های یک مؤسسه مالی معرفی‌نموده و در مرحله اول، کارشناسان از منطق فازی برای تخصیص یک امتیاز ریسک و یک سطح عدم‌قطعیت به هر مقدار متغیر، بر اساس گروه ویژه اقدام مالی و واحد اطلاعات مالی[۶۰] که با رویدادهای پول‌شویی و تأمین مالی تروریسم سروکار دارند، استفاده‌کردند. مرحله دوم شامل تشکیل خوشه‌ها با استفاده از روش‌های خوشه‌بندی بود و بهترین روش خوشه‌بندی با استفاده از شاخص (CH) [۶۱] تعیین‌شد که الگوریتم C-Means مؤثرترین بود. در مرحله نهایی، یک شاخص ناهنجاری مبتنی بر واریانس متغیر برای هر تراکنش در پرخطرترین خوشه‌ها اعمال‌شد تا هرگونه رفتار نامنظم که نشان‌دهنده فعالیت‌های مجرمانه باشد، شناسایی‌گردد و اگر از آستانه معینی عبورکند، معامله به‌عنوان ریسک بالا، خوشه‌بندی‌می‌شود و یک هشدار ایجادمی‌نماید[۳۰].

۵. کاستی‌های راه‌حل‌های فعلی

ازآنجاکه هیچ الگوی ثابتی وجودندارد تا تراکنش‌های پول‌شویی را شناسایی‌کند، پول‌شویی را می‌توان به‌راحتی با معاملات قانونی اشتباه-گرفت. الگوهای کلاهبرداری پیوسته در حال تغییر هستند که این مسئله همگام‌شدن سیستم‌ها و سیاست‌های مبتنی بر قانون را دشوار می‌کند. این مشکلات منجر به این می‌شود که مؤسسات بین کارایی و اثربخشی سیستم برای مبارزه با پول‌شویی یکی را انتخاب‌کنند. سیستم کارآمد، سیستمی است که به‌سرعت تقلب را تشخیص‌می‌دهد و کمتر به تحلیل‌گران انسانی متکی است و ریسک بالاتری را برای نادیده‌گرفتن تراکنش‌های متقلبانه ارائه‌می‌کند. یک سیستم با ریسک پایین‌تر ایمن‌تر است؛ زیرا اکثر تراکنش‌ها به‌صورت عمیق بررسی می‌شوند. بااین‌حال، این امر هم برای تحلیلگران و هم برای مؤسسه مالی پرهزینه است. مبادله بین ریسک و هزینه باید توسط مؤسسات در هنگام طراحی سیستم‌های خود درنظرگرفته‌شود. هوش مصنوعی یک روش کلیدی برای رسیدگی به مسائل غربالگری و سازگاری است. تحقیقات در مورد مبارزه با پول‌شویی خودکار به‌دلیل محدودیت‌های قانونی دسترسی به داده‌ها و مسائل فنی دارای سخت و در اکثر مواقع ناممکن می‌نماید و این در حالی است که دسترسی به داده‌ها برای سیستم‌ها امری ضروری و مهم است؛ زیرا داده‌های شبیه‌سازی شده، نمی‌توانند جای خالی داده‌های دنیای واقعی پر نمایند. در حال حاضر، به‌دلیل اهمیت حفظ حریم خصوصی مشتری، هیچ داده منبع‌باز برای تحقیقات پول‌شویی وجود ندارد؛ بنابراین، داده‌ها باید توسط مؤسسات خصوصی ارائه‌شوند و این یک کار دشوار است؛ زیرا انتشار داده‌های مشتری می‌تواند اعتبار یک مؤسسه را به خطر بیندازد و ممکن است با حاکمیت حریم خصوصی داده‌ها مطابقت نداشته‌باشد. مؤسسات به دلیل حجم زیادی داده‌های جمع‌آوری‌شده، برای پردازش آن‌ها، خود در داخل سازمان تلاش جداگانه‌ای می‌نمایند؛ اما باید به این نکته توجه‌داشت که جذب منابع مالی مهم‌ترین هدف مؤسسات مالی است و به‌نوعی با تعارض منافع روبه-رو خواهی شد.

از دیگر مسائل مهم که مؤسسات مالی در اجرای مبارزه با پول‌شویی باید بر آن غلبه‌کنند، توزیع، ذخیره‌سازی و پردازش داده‌های آن‌هاست. در اکثر مؤسسات، اکثر معاملات قانونی هستند و باید پذیرفته‌شوند. هر تراکنشی که توسط تحلیل‌گران جعلی اعلام‌شود، برای ارزیابی بیشتر به مقامات بالاتر ارسال‌می‌شود. تصمیم نهایی در مورد اینکه آیا یک معامله واقعاً تقلبی است لزوماً به عهده مؤسسه مالی نمی‌باشد؛ بنابراین، مؤسسات مالی تعداد زیادی تراکنش مشکوک را به‌دست‌می‌آورند با

زیرمجموعه‌ای از معاملات مشکوک که تحلیل‌گران آن‌ها را تقلبی-می‌دانند، اما هیچ بازخوردی درباره صحت تصمیم‌های خود از سوی مقامات بالاتر دریافت‌نمی‌کنند. این بدان معناست که داده‌هایی که مؤسسات مالی می‌توانند به محققان ارائه‌دهند، اغلب بدون برچسب «تقلب» یا «قانونی» ارائه‌می‌شوند. این امر ساخت مدل‌هایی برای پیش-بینی تراکنش‌های جعلی را دشوار می‌کند. هنگام طراحی راه‌حل‌های هوش مصنوعی برای مبارزه با پول‌شویی، مشارکت با تحلیلگران مهم است، زیرا بازخورد آن‌ها می‌تواند تنها منبع موجود برای درک عملکرد سیستم باشد. تضمین امنیت و مالکیت داده‌ها نیز چالش دیگری است.

مشکل مهم دیگر، کمبود منابع مشترک است. جدا از فهرست‌های نظارتی و توصیه‌های نظارتی خاص، مؤسسات در سراسر جهان از یک مجموعه‌داده مشترک استفاده‌نمی‌کنند که بتوان از آن به نفع تحقیقات برای مبارزه با پول‌شویی استفاده‌کرد. در چنین شرایطی، پیچیدگی اجرای مقررات حفظ حریم خصوصی و مالکیت داده پیشرفت تحقیقات مبارزه با پول‌شویی را کاهش‌می‌دهد. تجزیه‌وتحلیل پیوند، تجزیه‌وتحلیل احساسات و بسیاری دیگر از تکنیک‌های پردازش زبان طبیعی و مبتنی بر دانش اغلب برای کاهش خطا برای مبارزه با پول‌شویی قابل‌استفاده می‌باشند. اجرای چنین مؤلفه‌هایی به‌شدت به داده‌های عمومی بستگی-دارد.

۶. نتیجه‌گیری

در این مقاله تجزیه‌وتحلیل جامعی از ادبیات موجود در مورد مبارزه با پول‌شویی، با تمرکز بر استفاده از یادگیری ماشین، یادگیری عمیق، داده-کاوی و تکنیک‌های کلان‌داده انجام‌پذیرفت. بررسی‌ها نشان‌می‌دهد که فقدان حاکمیت داده جامع موجب عدم امکان استفاده از داده‌های نهادها و مراکز مختلف جهت مبارزه با پول‌شویی است. همچنین الگوریتم‌های گراف چندگانه از جمله: الگوریتم‌های مرکزیت و گراف تعبیه‌شده استفاده‌شدند که قادر به شناسایی باندها و سازمان‌های پول‌شویی هستند و عدم‌استفاده از ان‌ها معضل قابل‌توجهی است.

محققان می‌توانند با استفاده از الگوریتم‌های تشخیص انجمن‌ها در سیستم‌های ضدپول‌شویی برای افزایش تشخیص فعالیت‌های غیرقانونی استفاده‌نمایند. علاوه‌براین، تجزیه‌وتحلیل‌ها نشان‌می‌دهد که تکنیک‌های یادگیری بدون‌نظارت به‌دلیل فقدان مجموعه‌داده‌های برچسب‌گذاری-شده و داده‌های نامتعادل می‌توانند در شناسایی پول‌شویی کارآمدتر باشند؛ بنابراین، روش‌های بدون‌نظارت می‌توانند به‌عنوان ابزاری مناسب برای سیستم‌های ضدپول‌شویی عمل‌نمایند.

۷. کارهای آینده

در آینده، الگوریتم‌های تشخیص انجمن‌ها ممکن است توسط محققان برای بهبود تشخیص فعالیت‌های پول‌شویی استفاده‌شوند. شناسایی این گروه‌ها یا جوامع نزدیک به هم می‌تواند بالقوه شبکه‌ها و سازمان‌های پنهان درگیر در پول‌شویی را آشکارکند. این الگوریتم‌ها همچنین ممکن است به شناسایی اشخاص کلیدی در این گروه‌ها کمک‌کنند و ساختارهای پیچیده عملیات پول‌شویی را روشن‌کنند. به‌طورکلی، ترکیب الگوریتم‌های تشخیص انجمن‌ها می‌تواند بینش‌های ارزشمندی ارائه‌دهد و نقشی حیاتی در مبارزه با فعالیت‌های پول‌شویی ایفا نماید.

References

[1] Le-Khac, N. A., Markos, S., O'Neill, M., Brabazon, A., & Kechadi, T. (2016). An efficient search tool for an anti-money laundering application of a multi-national bank's dataset. arXiv preprint arXiv:1609.02031.

[2] Soltani, R., Nguyen, U. T., Yang, Y., Faghani, M., Yagoub, A., & An, A. (2016, October). A new algorithm for money laundering detection based on structural similarity. In 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 1-7). IEEE.

[3] Salehi, A., Ghazanfari, M., & Fathian, M. (2017). Data mining techniques for anti money laundering. International Journal of Applied Engineering Research, 12(20), 10084-10094.

[4] Kou, Y., Lu, C. T., Sirwongwattana, S., & Huang, Y. P. (2004, March). Survey of fraud detection techniques. In IEEE International Conference on Networking, Sensing and Control, 2004 (Vol. 2, pp. 749-754). IEEE.

[5] Huang, J. Y. (2015). Effectiveness of US anti-money laundering regulations and HSBC case study. Journal of Money Laundering Control, 18(4), 525-532.

[6] Gao, S., Xu, D., Wang, H., & Green, P. (2009). Knowledge-based anti-money laundering: a software agent bank application. Journal of Knowledge Management.

[7] Verhage, A. (2008). Between the hammer and the anvil? The anti-money laundering-complex and its interactions with the compliance industry. Crime, Law and Social Change, 52, 9-32.

[8] Mohammed, H. N., Malami, N. S., Thomas, S., Aiyelabegan, F. A., Imam, F. A., & Ginsau, H. H. (2022, April). Machine Learning Approach to Anti-Money Laundering: A Review. In 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON) (pp. 1-5). IEEE.

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

[10] Goecks, L. S., Korzenowski, A. L., Gonçalves Terra Neto, P., de Souza, D. L., & Mareth, T. (2022). Anti-money laundering and financial fraud detection: A systematic literature review. Intelligent Systems in Accounting, Finance and Management, 29(2), 71-85.

[11] Lin, C. Y., Liao, H. K., & Tsai, F. C. (2022). A Systematic Review of Detecting Illicit Bitcoin Transactions. Procedia Computer Science, 207, 3217-3225.

[12] Han, J., Huang, Y., Liu, S., & Towey, K. (2020). Artificial intelligence for anti-money laundering: a review and extension. Digital Finance, 2(3-4), 211-239.

[13] Drezewski, R., Sepielak, J., & Filipkowski, W. (2015). The application of social network analysis algorithms in a system supporting money laundering detection. Information Scienece, 295, 18–32.

[14] Senator, T. E., Goldberg, H. G., Wooton, J., Cottini, M. A., Khan, A. U., Klinger, C. D., ... & Wong, R. W. (1995). Financial crimes

enforcement network AI system (FAIS) identifying potential money laundering from reports of large cash transactions. AI magazine, 16(4), 21-21.

[15] Goldberg, H. G., & Wong, R. W. (1998, October). Restructuring transactional data for link analysis in the FinCEN AI system. In AAAI Fall Symposium (pp. 38-46).

[16] Lopez-Rojas, E. A., & Axelsson, S. (2012). Money laundering detection using synthetic data. In Annual workshop of the Swedish Artificial Intelligence Society (SAIS). Linköping University Electronic Press, Linköpings universitet.

[17] Zhang, Z., Salerno, J. J., & Yu, P. S. (2003, August). Applying data mining in investigating money laundering crimes. In Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining (pp. 747-752).

[18] Kannan, S., & Somasundaram, K. (2017). Autoregressive-based outlier algorithm to detect money laundering activities. Journal of Money Laundering Control, 20(2), 190–202.

[19] Tang, J., & Yin, J. (2005, August). Developing an intelligent data discriminating system of anti-money laundering based on SVM. In 2005 International conference on machine learning and cybernetics (Vol. 6, pp. 3453-3457). IEEE.

[20] Lopez-Rojas, E. A., & Axelsson, S. (2012). Multi agent based simulation (mabs) of financial transactions for anti money laundering (aml). In Nordic Conference on Secure IT Systems. Blekinge Institute of Technology.

[21] Weber, M., Chen, J., Suzumura, T., Pareja, A., Ma, T., Kanezashi, H., Kaler, T., Leiserson, C.E., & Schardl, T.B. (2018). Scalable graph learning for anti-money laundering: a first look. arXiv:1812.00076.

[22] Alkhalili, M., Qutqut, M. H., & Almasalha, F. (2021). Investigation of applying machine learning for watch-list filtering in anti-money laundering. IEEE Access, 9, 18481-18496.

[23] Martínez-Sánchez, J. F., Cruz-García, S., & Venegas-Martínez, F. (2020). Money laundering control in Mexico: a risk management approach through regression trees (data mining). Journal of Money Laundering Control.

[24] Hu, Y., Seneviratne, S., Thilakarathna, K., Fukuda, K., & Seneviratne, A. (2019). Characterizing and detecting money laundering activities on the bitcoin network. arXiv preprint arXiv:1912.12060.

[25] Shokry, A. M., Rizka, M. A., & Labib, N. M. (2020). Counter terrorism finance by detecting money laundering hidden networks using unsupervised machine learning algorithm. In International Conferences ICT, Society, and Human Beings.

[26] Li, X., Liu, S., Li, Z., Han, X., Shi, C., Hooi, B., ... & Cheng, X. (2020, April). Flowscope: Spotting money laundering based on graphs. In Proceedings of the AAAI conference on artificial intelligence (Vol. 34, No. 04, pp. 4731-4738).

[27] Bazargani, M & Homayounpour, Z. (2020). Presenting a novel method based on collaborative filtering for nearest neighbor detection in recommender systems. Intelligent Multimedia Processing and Communication Systems (IMPCS).1(1),55-64.

[28] Shahnavaz, A., Afzali, Mehdi & Rahimzadeh, s. (2020). A new approach for data cleaning to improve quality of data warehouse. Intelligent Multimedia Processing and Communication Systems (IMPCS).1(2),33-41.

[29] Youssef, B., Bouchra, F., & Brahim, O. (2023). State of the Art Literature on Anti-Money Laundering Using Machine Learning and Deep Learning Techniques. In The International Conference on Artificial Intelligence and Computer Vision (pp. 77-90).

[30] Segovia-Vargas, M. J. (2021). Money laundering and terrorism financing detection using neural networks and an abnormality indicator. Expert Systems with Applications, 169, 114470.

پی‌نوشت

[1] Anti money laundering (AML)
[2] convolution neural network
[3] autoencoder
[4] multilayer perceptron
[5] financial fraud detection
[6] minimum spanning tree
[7] rule-based
[8] bayesian networks
[9] Semantic web
[10] radial basis function network
[11] support vector machine (svm)
[12] decision tree (dt)
[13] social network analysis
[14] principal component analysis (PCA)
[15] random forest
[16] neural networks
[17] link analysis
[18] network analysis systems
[19] natural language processing (NLP)
[20] deep learning
[21] sentiment analysis
[22] named entity recognition
[23] long short-term memory (LSTM)
[24] Financial Action Task Force (FATF)
[25] Counter Terrorist Financing (CTF)
[26] suspicious transaction reports (STRs)
[27] currency transaction reports (CTRs)
[28] placement
[29] layering
[30] integration
[31] natural language processing (NLP)
[32] entity and relationship analysis
[33] data layer
[34] screening and monitoring layer
[35] alert and event layer
[36] operational layer
[37] Degree of Centrality
[38] Betweenness Centrality
[39] Closeness Centrality
[40] Hubness
[41] Page Rank
[42] Link Analysis
[43] Financial Crimes Enforcement Network (FINCEN)
[44] Financial Crimes Enforcement Network AI system (FAIS)
[45] Outlier Detection
[46] inter quartile range (IQR)
[47] risk classification/scoring
[48] graph learning for aml
[49] know your customer (KYC)
[50] Company Name Tree (CN tree)

[51] Supervised learning
[52] Unsupervised learning
[53] Cluster analysis
[54] Regression analysis
[55] clustering
[56] anomaly detection
[57] network analysis
[58] dimensionality reduction
[59] isolation forest
[60] financial intelligence unit
[61] calinski-harabasz