شناسایی تراکنش‌های مشکوک درعملیات ضدپول‌شویی به کمک مدل ترکیبی هوشمند

الهام پاسبان، بانکدار و بانک صادرات ایران، e.paseban@gmail.com
سپهر ظریف‌برگی، معاون شعبه و بانک صادرات ایران،sepehrparnia@gmail.com

چکیده

در چند دهه اخیر، اقتصاد جهانی با پدیده پول‌شویی و آثار مخرب آن بر اقتصاد کشور مواجه بوده است. پول‌شویی یک فرآیند مجرمانه پنهان کردن منشاء غیر قانونی پول کثیف و مشروع جلوه دادن آن می‌باشد. در این سال‌ها با جهانی شدن اقتصاد، آزادسازی جریان‌های سرمایه‌ای بین‌المللی، توسعه بانکداری الکترونیکی و... پول‌شویی نیز تا حدودی تسهیل شده است، به طوری که براساس تخمین صندوق بین‌المللی پول و بانک جهانی درآمدهای نامشروعی که توسط پول‌شویان در چرخه تطهیر و پول‌شویی قرار می‌گیرند، در حدود ۲ تا ۵ درصد تولید ناخالص جهانی است. اکثر موسسات بین‌المللی راه‌حل‌های ضدپول‌شویی متعددی برای برخورد با این تقلب سرمایه‌گذاری انجام داده‌اند. با این حال، روش‌های جستجوی سنتی زمان زیادی می‌برد. اخیراً روش های داده‌کاوی توسعه یافته‌اند و تکنیک‌های مناسب‌تری برای شناسایی پول‌شویی به نظر می‌رسند. در این تحقیق، یک روش ترکیبی هوشمند مبتنی بر خوشه‌بندی شبکه‌های عصبی و فیلترهای رگرسیونی در جهت شناسایی تراکنش‌های مشکوک پیشنهاد کرده‌ایم، بدین صورت که این روش ابتدا با استفاده از شبکه های عصبی تراکنش‌ها را خوشه‌بندی نموده و در قدم بعدی با استفاده از فیلترهای رگرسیونی تراکنش‌ها را طبقه‌بندی و سپس با استفاده از قواعد بیزین تراکنش‌ها را منظم‌تر کرده‌است. نتایج بدست آمده از این پیاده‌سازی روی یک مجموعه داده دستی در بازه زمانی یک‌ماهه و یک مجموعه داده بانکی بدین صورت است که در سه روش رگرسیون برای مجموعه داده دستی خود و برای مجموعه داده بانکی به جز فیلتر رگرسیونی غیرخطی خودکار با در نظر گرفتن پارامترهای خارجی در دو روش دیگر در مقایسه با کار پایه بهینه‌تر می‌باشد.

کلیدواژه: پول‌شویی، تراکنش‌های‌مشکوک، رگرسیون، خوشه‌بندی، طبقه بندی، داده‌کاوی.

مقدمه

پول‌شویی یک فعالیت غیر قانونی است که در طی انجام آن، عواید و درآمدهای ناشی از اعمال خلاف قانون، مشروعیت می‌یابد. مسأله پول‌شویی با نگرش امروزی برای نخستین بار در سال ۱۹۷۹ و با کشف یک چمدان حاوی ششصد میلیون دلار پول نقد در فرودگاه پالرمو، که حاصل فروش مواد مخدر بود، مطرح گردید. کشفی که به تشکیل پرونده ایتالیایی-آمریکایی "ارتباط پیتزا" منجر شد و در سال ۱۹۸۵ محاکمه آن برگزار گردید.[۱۷]بطور کلی پول‌شویی فرآیندی است که طی آن عواید حاصل از فعالیت‌های مجرمانه و غیرقانونی در مجاری قانونی قرار می‌گیرد و طی روندی، به ظاهر تطهیر و پاک می‌شود.

به طور کلی فرآیند پول‌شویی دارای سه مرحله جایگذاری[۱]، لایه‌چینی[۲] و یکپارچه سازی[۳] می‌باشد [۱۹-۱۸].اولین مرحله از فرآیند پول‌شویی جایگذاری یا تزریق عواید حاصل از فعالیتهای مجرمانه به شبکه مالی رسمی با هدف تبدیل عواید مزبور از حالت نقدی به ابزارها و دارایی‌های مالی است. مرحله لایه چینی به جداسازی عواید حاصل ازجرم، از منشاء غیرقانونی آن اختصاص دارد که از طریق ایجاد لایه‌های پیچیده با هدف عدم امکان ردیابی و منشاء مال صورت می‌گیرد. هدف از مرحله یکپارچه سازی فراهم آوردن ظاهری مشروع برای توجیه قانونی عواید حاصل از فعالیت‌های مجرمانه است. در این مرحله وجوه انباشته شده در لایه‌های مختلف صرف خرید دارایی‌های قانونی می‌شود.

با توجه به رشد روزافزون جرایم اقتصادی و غیراقتصادی در کشور، مبارزه با پول‌شویی به منظور ناامن نمودن فضای فعالیت مجرمان و تبه‌کاران و کاهش رفتارهای مجرمان و کمک به مسئولان برای کشف و ردیابی شبکه‌های فساد و اختلاس ضروری است. با اعمال قوانین مبارزه با پول‌شویی، راه‌های فرار مالیاتی کاهش می‌یابد و درآمدهای ناشی از مالیات دولت افزایش خواهد یافت. ایران نیز باید همگام با مسائل روز دنیا، از جمله جهانی شدن اقتصاد، یکسان‌سازی پول کشورهای اروپایی (یورو) و بالتبع، نقل و انتقالات آسان و سریع کالا و خدمات و سرمایه، پیوستن به سازمان تجارت جهانی (WTO) و همچنین، فراگیر شدن عملیات مبارزه با پول‌شویی در سطح دنیا، حرکت کند و شرایط خود را با مقتضیات جهانی تطبیق دهد [۱].

بطور کلی به منظور پیشگیری از کلاهبرداری‌های کلان تجاری و بازگرداندن نقدینگی به چرخه تجارت و ارائه راهکاری در جهت رشد تجاری و امنیت ملی نیاز به انجام تحقیقات مثمر ثمر که به مرحله عملیاتی برسد، به شدت احساس می‌شود. ضرورت مبارزه با پدیده پول‌شویی زمانی به درستی احساس می‌شود که طبق آمار غیررسمی پول‌شویی بعد از تجارت نفت و معاملات ارزی بزرگترین تجارت شناسایی شده است.

یکی از بدترین موارد کلاهبرداری، کلاهبرداری تجاری است و بدتر از آن پول‌شویی است. پول‌شویی مجموعه ای از درآمد مجرمان در دارایی‌هایی است که نمی‌تواند در بستر جرم ردگیری شود، جایی‌که فرآیند منابع مخفی پول به پول‌شویی برمی‌گردد. همانگونه که فعالیت‌های پول‌شویی بطور گسترده در حال رشد می‌باشند، رشد تجاری و امنیت ملی بصورت بحرانی تحت تأثیر قرار گرفته می‌شود. از استراتژی‌های ضدپول‌شویی کنونی قوانین و قواعدی برای ایجاد پیشگیری و توقیف فعالیت‌های پول‌شویی را انتظار می‌رود [۲].

برای مثال، در حد ممکن بانک‌ها اعتبار سنجی مشتری قبل از تجارت بانکی، چک کردن تراکنش‌های نقدی مشکوک خارجی، ردگیری جریان‌های نقدی بزرگ، و حساب‌های مشکوک به پول‌شویی لیست سیاه و غیره را در برمی‌گیرد. با این وجود، روش‌های ضدپول‌شویی موجود به مداخله‌های انسانی پاسخ می‌دهد و کاربرد تکنیک‌های داده‌کاوی جدید هنوز در فاز اول باقی است [۳].

آشکارسازی تراکنش‌های تجاری مشکوک یک شرط قبلی اصلی و جنبهٔ کلیدی ضدپول‌شویی است. روش‌های موجود براساس تعداد تراکنش‌ها است و فرآیند پیاده‌سازی شناسایی به شدت محدود به مکانیزم گزارش‌گیری فعالیت‌های غیرمعمول بانکی است. بنابراین، محدودیت‌های زیادی از تلاش‌های ضدپول‌شویی از قبیل پوشش ضعیف شناسایی، چرخهٔ طولانی کشف سرنخ و تأخیر زیاد وجود دارند [۳].

هدف اصلی این تحقیق بهبود دقت و صحت در شناسایی تراکنش‌های مشکوک به پول‌شویی می‌باشد. بهبود روش‌های گذشته

---

۱. Placement
۲. Layer by layer
۳. Integration

نیز از دیگر اهداف می‌باشد.

در ادامه به مرور ادبیات و کارهای انجام شده در رابطه با تکنیک‌های خوشه‌بندی، الگوریتم ژنتیک[۴]، شبکه عصبی، دسته‌بندی[۵]، الگوهای تکرار[۶]، قواعد انجمنی[۷] و رگرسیون برای تقسیم بندی مشتریان به دسته‌های مشکوک و غیر مشکوک پرداخته می‌شود.

در بخش بعدی ، شرحی بر روش تحقیق و تفصیلی بر الگوریتم پیشنهاد شده مبتنی بر مدل ترکیبی هوشمند جهت کشف تراکنش‌های مشکوک خواهد بود. در بخش چهارم، ارزیابی‌هایی برای تست میزان دقت و صحت روش پیشنهادی با سایر روش‌های مورد مقایسه انجام می‌شود. در نهایت نتیجه‌گیری و پیشنهاداتی برای کارهای آتی بیان می‌گردند.

ادبیات موضوع

در دو دهه اخیر، داده کاوی، شبکه عصبی، الگوریتم ژنتیک و تکنیک‌های هوشمند دیگر به طور گسترده‌ای در فرآیندهای مالی به کار می‌روند. با این وجود، تحقیقات کمی در رابطه با تشخیص الگوهای پول‌شویی با توجه به این تکنیک‌های هوشمند صورت پذیرفته‌است. در ادامه بصورت کاملاً مختصر نمونه‌هایی از کارهای انجام شده در این زمینه را بررسی می‌کنیم.

دابلیو.زینگکی[۸] برای شناسایی تراکنش‌های منجر به پول‌شویی از روش خوشه بندی بر درخت پوشای مینیمم بهبود یافته برای کشف تراکنشهای مشکوک استفاده کرده که درخت پوشای مینیمم یافته براساس معیار عدم شباهت ساخته می‌شود. در این تحقیق از یک مجموعه داده تجاری جهت پیاده‌سازی نتایج استفاده شده است. مزیت این روش ارائه یک پارامتر نامتجانس جهت اندازه‌گیری تفاوت درجات پرت و سپس طراحی الگوریتم کشف پول‌شویی است ولی در محیط واقعی قابل پیاده سازی نیست.[۴]

ام. کچادی[۹] نیز با استفاده از خوشه‌بندی جهت تقسیم بندی اولیه، استفاده از الگوریتم ژنتیک برای تغذیه شبکه عصبی، استفاده از شبکه عصبی جهت آموزش و درخت تصمیم گیری روشی جهت کشف پولشویی ارائه نموده که نتایج بدست آمده نشان می‌دهد که این روش به بهبود کارایی در واحد زمان و در مقایسه با زمان اجرا کمک می‌کند و در داده های خیلی زیاد، سریع تر می‌توان موارد مشکوک را پیدا کرد ولی انواع مشتری را در نظر نمی‌گیرد. در این تحقیق از تراکنش‌های صندوق دولت به کمک بانک CE با تخمین ده میلیون رکورد تراکنش از ده هزار مشتری در چهارده سال اخیر استفاده شده است.[۵]

لوخاک ان[۱۰] و همکاران با استفاده از تکنیک خوشه‌بندی و شبکه عصبی مبتنی بر انتشار رو به عقب و ذخیره نتایج در یک پایگاه‌دانش جهت تصمیم‌گیری سعی در کشف تراکنش‌های مشکوک دارد. این الگوریتم روی یک بانک خاص مورد آزمایش قرار گرفته و نتایج را با نتایج دستی بدست آمده همان بانک مور مقایسه قرار داده و نتیجه گرفته است که روش مناسبی است ولی با کار پایه دیگری نتایجش را مقایسه نکرده است و فرآیند یادگیری آن برای مجموعه پایگاه‌داده های خیلی بزرگ نیز خیلی مناسب نیست.[۶]

---

۴ Genetic Algorithm.
۵ Classification.
۶ Frequent Pattern.
۷ Association Rules.
۸ W.Xingqi.
۹ M.Kechadi.
۱۰ Le-Khac N.

روئی لوئی [11] و همکاران با به‌کارگیری الگوریتم‌های تصمیم‌گیری جهت شناسایی فعالیت‌های پول‌شویی با استفاده از الگوریتم خوشه‌بندی (k-mean, BIRCH) توانسته‌اند بصورت کارآمدتر تراکنش‌های مشکوک را شناسایی کنند بدین ترتیب که برای هر داده مالی از گره تا برگ را جستجو کرده و در برگ، درباره اینکه در گروه بماند یا خیر تصمیم گرفته می‌شود که البته روی دامنه محدودی قابل اجراست.در این تحقیق از یک مجموعه داده خاص جهت پیاده‌سازی و آزمایشات استفاده شده که به نام و منبع آن اشاره‌ای نشده است.[۷]

در مقاله ای.دابلیو.تی.انجیا[12] و همکاران به شکاف‌های بین کشف کلاهبرداری مالی(FDD[13]) و نیازهای صنعت جهت پیشبرد تحقیقات روی موضوعات فراموش شده توجه شده است و تکنیک‌های عمده داده‌کاوی از قبیل: مدل‌های منطقی، شبکه‌های عصبی، درخت تصمیم‌گیری در این مقاله بررسی و استفاده شده است. مشکلی که با FDD وجود دارد حساسیت هزینه است. هزینه طبقه‌بندی نادرست(خطاهای مثبت کاذب و منفی کاذب) متفاوت است، یک خطای منفی کاذب معمولاً از خطای مثبت کاذب کم‌هزینه‌تر است. دامنه تحقیق محدود بوده است. در این تحقیق حدود ۴۹ مجله علمی در این زمینه مرور شده است.[۸]

در مقاله کوثری و همکاران با به‌کارگیری الگوریتم‌های تصمیم‌گیری جهت کشف رفتارهای مشکوک امکان مدل‌سازی رفتار کاربران در پنج دسته مختلف بوجود آمده که با دقت بیشتری نوع رفتار کاربر را پیش‌بینی می‌کند ولی این نظریه در حد تئوریک بوده و عملیاتی نشده است.داده‌های آموزشی این پژوهش به تعداد ۱۰۰،۰۰۰ رکورد اولیه به عنوان نمونه واقعی از یک بانک خصوصی دریافت شده است.[۹]

دانگ خوآ کائو[14]و فوک دو[15]با استفاده از تکنیک‌های خوشه‌بندی و یک آموزش جدید برای تبدیل داده‌های بانکی به داده‌های مناسب جهت به‌کاربردن در الگوریتم CLOPE در کشف پولشویی بهره جسته‌اند. پیاده‌سازی روی مجموعه دادهٔ یکی از بانک‌های ویتنام انجام شده است که با استفاده از الگوریتم CLOPE بدین صورت که برای ورودی‌های جدید یک خوشه ایجاد کرده سپس، با محاسبه بهره‌وری در صورت پیدا نمودن خوشه بهینه آن را به خوشه قبلی اضافه می‌کند در غیر اینصورت این روند تارسیدن به نتیجه تکرار می‌گردد. این روش برای داده‌های بزرگ مقیاس‌پذیر بوده ولی اینکه این سیستم نمی‌تواند به تنهایی اجرا شود و می‌بایست براساس توانایی آنالیز درآنالیز داده‌ها باشد از نقاط ضعف آن می‌باشد.[۱۰]

در مقاله هرمیت کوآر خانوجا[16] و همکاران یک متدلوژی برای بانک‌های خصوصی برای سیستم مانیتورینگ پیوسته به عنوان راهنمای ذخیره بانکی هند(RBI) برای تراکنش‌های مالی پیشنهاد داده‌اند که گزارشات بارزسی پایگاه‌داده‌یشان را بطور مستمر برای نشانه‌گذاری تراکنش‌های مشکوک در هر حالتی چک خواهد کرد. این تراکنش‌ها بطور دقیق با مشاهدات تئوری Dempster Shafer برای تولید گزارشات مشکوک بطور اتوماتیک به عنوان واحد اطلاعات مالی تحلیل و تأیید می‌شود. این مدل روی دیتاست شبیه‌سازی شده از تراکنش‌های بانکی مالی تست و برای ارتقا نتایج نشان داده شده است، این روش یک راه کاربردی برای ترکیب اطلاعات می‌باشد.[۱۱].

---

[11] . Rui Liu
[12] . E.W.T. Ngai
[13] . FDD: Financial Fraud Detection
[14] . Dang Khoa Cao
[15] . Phuc Do
[16] Harmeet Kaur Khanuja

ماهش خاروت[۱۷] و همکاران در تحقیق خود استفاده از تکنیک‌های داده‌کاوی در زمینه بانکداری که مناسب ماهیت و حساسیت داده‌های بانکی و فرآیندهای تصمیم‌گیری پیچیده بلادرنگ است، توصیف می‌کنند. موضوع اصلی برای یک بانک تصمیم‌گیری خوب و به موقع برای به حداقل‌رسانی سطح خطرات مربوط به بانک است. سیستم پیشنهادی در این تحقیق، شامل هفت ماژول (پیش‌پردازش، ورودی داده‌ها، خوشه‌بندی تنظیم دنباله مشکوک، مرئی سازی داده‌ها، آموزش از تصمیم کاربر، تولید پروفایل سازمان، استخراج رفتار) می‌باشد. در پیش‌پردازش و ورودی داده‌ها، داده‌ها را جمع‌آوری و عملیات پیش‌پردازش را روی آن‌ها انجام می‌دهد. از الگوریتم K-means برای خوشه‌بندی داده‌ها استفاده نموده و دنباله‌های مشکوک را می‌یابد. سپس، الگوی تکرار برای یادگیری هدف بکار برده می‌شود. در نهایت رفتار کاربر با استفاده از ترکیب خوشه‌بندی و قواعد انجمنی استخراج می‌شود. از مزایای این روش، به یکپارچه‌سازی وبه کاربردن داده‌ها به عنوان ورودی از منابع متنوع و استفاده از چند تکنیک داده‌کاوی اشاره نمود. ولی اینکه در این تحقیق، به مجموعه داده خاصی اشاره نشده و نتایج بصورت کمی بیان نشده است، از معایب آن به شمار می‌آید [۲۷].

در مقاله زینگرونگ لو[۱۸] با استفاده الگوهای تکرار و قواعد انجمنی برای آشکارسازی فعالیت‌های ضدپول‌شویی(AML) و تمرکز روی کشف تراکنش‌های مشکوک در جریان تراکنش‌های تجاری کار شده است. در این روش، به تراکنش‌های تجاری به عنوان یک جریانی از داده‌ها توجه شده، و یک روش بدست آوردن پویا را برای آشکارسازی الگوهای مشکوک روی جریان تراکنش‌ها بکار برده است. مخصوصاً یک الگوریتم دسته‌بندی(کلاس‌بندی) براساس قوانین ارتباط چند کلاسی روی جریان‌های داده‌ها با ایجاد یک درخت الگوی تکرار[۱۹] برای بهبود زمان و فضای کارآمد و سپس کاهش تکرار قوانین بوسیله حد هاؤفدینگ[۲۰] روی جریان‌های پویای داده‌ها پیشنهاد شده است. از مزایای این روش، مقیاس‌پذیری در مجموعه داده‌های بزرگ می‌باشد. در این تحقیق، به مجموعه داده استفاده شده در پیاده‌سازی الگوریتم اشاره نشده است و همچنین در مقیاس پایین دقت مناسبی ندارد[۱۲].

در مقاله ندا حیدری‌نیا و همکاران که به عنوان مقاله پایه در نظر گرفته شده با مطالعه‌ی پروفایل کاربران تعدادی از ویژگی‌ها شامل معاملات مالی حجیم در مناطق ریسک‌پذیر از دیدگاه پول‌شویی، فعال شدن حساب راکد با مقادیر قابل توجه و غیره استخراج شدند. آموزش شبکه با استفاده از طراحی یک سیستم فازی، توسعه‌ی یک سیستم استنتاج عصبی-فازی وفقی و اضافه کردن بردار ویژگی‌های کاربران به آن انجام شده است. سپس خروجی شبکه می‌تواند میزان ریسک رفتار کاربر را تعیین نماید. این روش ترکیبی با توجه به صحت و سرعت قابل قبول برای مجموعه داده‌های حجیم انتخاب مناسبی خواهد بود. روش پیشنهادی مبتنی بر ANFIS است؛ چراکه ویژگی‌ها و قابلیت‌های مناسبی دارد. سیستم استنتاج عصبی-فازی وفقی، الگوریتم‌های منطق فازی و شبکه عصبی را به کار می‌گیرد تا بین حوزه‌های ورودی و خروجی نگاشت غیر خطی ایجاد کند. با استفاده از قدرت زبان فازی و قدرت عددی شبکه‌های عصبی، ANFIS در مدل‌سازی فرایندهای پیچیده بسیار قدرتمند خواهد بود سیستم فازی با استفاده از ویژگی‌های مستخرج از داده‌ها بانکی و برخی از قواعد فازی، طراحی شده و با استفاده از الگوهای بهینه‌ی ایجاد شده در یک سیستم ANFIS، پول‌شویی هوشمندانه را مشخص می‌کند.دقت ناشی از این سیستم پیشنهادی ۹۶ درصد است. پیاده‌سازی این روش بر روی مجموعه‌داده‌های یک بانک (به نام آن اشاره‌ای نشده است) صورت گرفته است. از مزایای این روش می‌توان به مناسب بودن برای داده‌های حجیم، سرعت قابل قبول و دقت بالا اشاره نمود.[۱۵]

---

[۱۷] Mahesh Kharote .
[۱۸] Xingrong Luo .
[۱۹] FP-Tree.
[۲۰] Hoeffding.

سی اچ.سورش[۲۱] و همکاران یک روش ضد پول‌شویی کارامد ارائه کردند که با استفاده از روش وابستگی مبتنی بر hash قادر است مسیر پیمایش پول‌شویی را شناسایی کند و در شناسایی عامل و مولد در سطوح مختلف پول‌شویی با استفاده از روش نظریه‌ی گراف، موفق باشد سیستم پیشنهادی دو مرحله عمده دارد. در گام اول برای تولید دو مجموعه داده‌ی پرتکرار از روش مبتنی بر هش استفاده شده و در گام دوم شناسایی مسیر تراکنش‌های مشکوک با استفاده از روش نظریه‌ی گراف روش هش کردن بدست آورده شد که روشی کارآمد برای جلوگیری ازاتلاف وقت و پیچیدگی برای شناسایی تراکنش های مشکوک به نظر می‌رسد.[۱۳]

در مقاله ویکاس جایارسی[۲۲] و بالان[۲۳] احتمال سازگاری ریسک در پول‌شویی با استفاده از روش درخت تصمیم اندیس-محور نقشه بیتی (BIDT) مورد بررسی قرار می‌گیرد. در ابتدا برای بدست آوردن درخت دانشی که ریسک پول‌شویی یک شرکت را تعیین کرده و مقیاس‌پذیری را بهبود بخشد از یادگیری درخت تصمیم اندیس-محور نقشه بیتی استفاده شده است. از مزایای این روش می‌توان استفاده برای پایگاه داده های بزرگ بانکی، دقت بالا برای شناسایی دقیق پولشویی تراکنش ها با نرخ تکراربالا را نام برد.[۱۴]

عبدل کی. شیخ و امریل نضیر[۲۴] در مقاله خود مدلی را جهت شناسایی اجتماع و روابط بین تراکنش‌ها و مشتریان با استفاده از تحلیل شبکه‌های اجتماعی ارائه داده‌اند. با کمک این مدل گروه‌ها و باندهای مافیایی که نقش اصلی در فعالیت‌های پول‌شویی را بازی می‌کنند، شناسایی می‌شوند. در این روش یک شبکه اجتماعی با استفاده از گراف شبکه ای معنایی و فعالیت‌های شبکه‌های ازقبیل درجه مرکزیت و خوشه‌بندی و غیره جهت شناسایی مشتریان مشکوک ساخته می‌شود. درجه مرکزیت جهت شناسایی سرشاخه‌ها در گروه‌های اجتماعی کاربرد دارد و هدف از خوشه‌بندی، جداسازی گروه‌هایی با شخصیت‌های مشابه و یا مبنتی بر شاخص‌های ویژه از شاخه‌ها که با دیگر خوشه‌ها نسبت دارند، می‌باشد. شناسایی گروه‌های مشکوک در شبکه‌های اجتماعی از مزایای این روش تلقی می‌شود ولی این مورد که هیچ ارتباط خاصی در تحلیل بین حساب‌های بانکی و عملیات انجام شده دیده نمی‌شود از نکات ضعف این روش می‌باشد.[۱۶]

در جدول ۱ الگوریتم های بیان شده در بخش قبل به همراه تکنیک مورد استفاده در آنها و همچنین مزایا و معایب هریک آورده شده است.

با توجه به مرور انجام شده روی این الگوریتم‌ها، در اکثر آنها از یک تکنیک خوشه‌بندی جهت تقسیم بندی مشتریان به دو دسته مشکوک و غیر مشکوک، با توجه به تعیین پارامترها و خصوصیات تعریف شده استفاده می شود و بعد از آن، تکنیک‌های مختلف دیگر نظیر الگوریتم ژنتیک، شبکه عصبی، دسته‌بندی، الگوهای تکرار و قواعد انجمنی و غیره جهت محدود کردن گروه مشکوک و همچنین یادگیری شبکه مورد استفاده قرار می‌گیرد. مشکلی که در پژوهش‌های زمینه پول‌شویی وجود دارد این است که در اکثر مواقع به دلیل امنیتی بودن موضوع، امکان دسترسی به مجوعه دادهٔ محیط واقعی نداشته و ناگزیر به شبیه‌سازی مجموعه داده در محیط‌های شبیه‌ساز هستند. از معیارهایی که در کشف تراکنش‌های مشکوک در اکثر تحقیقات به عنوان معیارهای اصلی مدنظر قرار می‌گیرند، معیار دقت و زمان شناسایی می‌باشند که این دو مورد در مجموعه پایگاه داده های خیلی بزرگ متفاوت می‌باشند. با توجه به اینکه در روش‌های مرور شده از الگوریتم‌های متفاوتی استفاده شده است،

---

[۲۱] Ch. Suresh .

[۲۲] Vikas Jayasree .

[۲۳] Balan .

[۲۴] Abdul K. Shaikh, Amril Nazir

نمی‌توان از روی مقدار خروجی هریک بهترین یا ضعیف‌ترین الگوریتم را مشخص کرد. ولی بطور کلی در روش‌های مرور شده، مقاله ندا حیدری و همکاران که به دقت ۰,۹۶ درصد رسیده نسبت به دیگر موارد از خروجی بهینه‌تری برخوردار می‌باشد.

جدول ۱. تحلیل ارزیابی الگوریتم‌های انجام شده در زمینه پول‌شویی

ردیف	نویسنده / سال	روش‌های مورد استفاده	مزایا	معایب
۱	W. Xingqiو همکاران(2009)	روش خوشه‌بندی مبتنی بر درخت پوشای مینیمم بهبود یافته	ارائه یک پارامتر نامتجانس جهت اندازه‌گیری تفاوت درجات پرت و سپس طراحی الگوریتم کشف پول‌شویی.	عدم پیاده‌سازی در محیط واقعی.
۲	Le Khac, Nhien An and Kechadi, M(2010)	استفاده از خوشه‌بندی جهت تقسیم بندی اولیه،الگوریتم ژنتیک برای تغذیه شبکه عصبی،شبکه عصبی جهت یادگیری و درخت تصمیم‌گیری	بهبود کارآیی بهتر در واحد زمانی کمتر.	مجزا بودن براساس تراکنش‌های یک مشتری خاص.
۳	Le-Khac, Nhien-An and Markos, Sammer and Kechadi, Mohand-Tahar(2010)	استفاده از تکنیک خوشه‌بندی و شبکه عصبی مبتنی بر انتشار رو به عقب و ذخیره نتایج در یک پایگاه‌دانش جهت تصمیم‌گیری.	این الگوریتم روی یک بانک خاص مورد آزمایش قرار گرفته و نتایج را با نتایج دستی بدست آمده همان بانک مور مقایسه قرار داده و نتیجه گرفته است که روش مناسبی است	ولی با کار پایه دیگری نتایجش را مقایسه نکرده است و پروسه یادگیری آن برای مجموعه پایگاه‌داده های خیلی بزرگ نیز خیلی مناسب نیست.
۴	Rui Liu, Xiao-long Qian Shu Mao, Shuai-zheng Zhu(2011)	به‌کارگیری الگوریتم‌های تصمیم‌گیری جهت شناسایی فعالیت‌های پول‌شویی با استفاده از الگوریتم خوشه‌بندی(k-mean, BIRCH)	شناسایی کارآمدتر تراکنش‌های مشکوک و غیرنرمال به کمک الگوریتم درخت تصمیم‌گیری.	قابل اجرا روی یک دامنه محدود

ردیف	نویسنده / سال	روش‌های مورد استفاده	مزایا	معایب
۵	E.W.T. Ngai , Yong Hu , Y.H. Wong , Yijun Chen , Xin Sun(2011)	تکنیک‌های عمده داده‌کاوی استفاده شده عبارتند از: مدل‌های منطقی، شبکه‌های عصبی، درخت تصمیم‌گیری.	توجه به شکاف‌های بین کشف کلاهبرداری مالی(FDD) و نیازهای صنعت جهت پیشبرد تحقیقات روی موضوعات فراموش شده،	مشکلی که با FDD وجود دارد حساسیت هزینه است. هزینه طبقه‌بندی نادرست(خطاهای مثبت کاذب و منفی کاذب) متفاوت است، یک خطای منفی کاذب معمولاً از خطای مثبت کاذب کم‌هزینه‌تر است. دامنه تحقیق محدود بوده است.
۶	روح الله کوثری لنگری و همکاران(۱۳۹۱-۲۰۱۲)	به‌کارگیری الگوریتم‌های تصمیم‌گیری جهت کشف رفتارهای مشکوک	امکان مدل‌سازی رفتار کاربران در پنج دسته مختلف وجود دارد که با دقت بیشتری نوع رفتار کاربر را پیش‌بینی می‌کند.	در حد تئوریک است و عملیاتی نشده‌است.
۷	Dang Khoa Cao, Phuc (2012)	آشکارسازی پول‌شویی به کمک تکنیک‌های خوشه‌بندی(الگوریتم CLOPE)	این الگوریتم برای مجموعه داده‌های بزرگ نیز مقیاس‌پذیر است.	سیستم در این الگوریتم به تنهایی بطور کامل نمی‌تواند کار کند و می‌بایست مبتنی بر توانایی آنالیز در آنالیزکردن داده‌ها و فراهم آوردن مجموعه‌ای از قوانین جهت تایید خوشه‌ها بعد از خوشه‌بندی است.
۸	Harmeet Kaur وKhanuja همکاران(2014)	ارائه یک متدلوژی جهت تهیه گزارشات بارزسی پایگاه‌داده‌ها بطور مستمر برای نشانه‌گذاری تراکنش‌های مشکوک	یک راه کاربردی برای ترکیب اطلاعات، شواهد فردی می‌تواند برای شواهد قویتر ترکیب شود.	عدم تمرکز روی تکنیک خاصی از تکنیک‌های داده‌کاوی

ردیف	نویسنده / سال	روش‌های مورد استفاده	مزایا	معایب
۹	Mahesh Kharoteو همکاران(2014)	استفاده از تکنیک‌های داده‌کاوی(Clustering, frequnty pattern) در زمینه بانکداری متناسب با ماهیت و حساسیت داده‌های بانکی و فرآیندهای تصمیم‌گیری پیچیده بلادرنگ	بکارگیری داده‌ها به عنوان ورودی از منابع متنوع، یکپارچه‌سازی و سپس عملیات اجرایی روی داده‌ها و استفاده از بیش از یک تکنیک داده‌کاوی	عدم نمایش دقت و سرعت نتایج روی نمودار جهت مقایسه در مقیاسهای پایین و بالا.
۱۰	Luo, Xingrong (2014)	استفاده الگوهای تکرار و قواعد انجمنی برای آشکارسازی فعالیت‌های ضدپول‌شویی(AML) و تمرکز روی کشف تراکنش‌های مشکوک در جریان تراکنش‌های تجاری	این الگوریتم برای مجموعه داده‌های بزرگ نیز مقیاس‌پذیر است.	در مقیاس پایین دقت زیاد مناسب نیست.
۱۱	نداحیدری وهمکاران(۲۰۱۴)	استفاده ازسیستم استنتاجی عصبی-فازی وفقی (ANFIS) برای شناسایی تراکنش‌های مشکوک درپول‌شویی	مناسب برای معاملات مالی حجیم ، داده های عظیم ، سرعت قابل قبول و صحت بالا	-
۱۲	Ch.Sureshو همکاران(2016)	استفاده از روش وابستگی مبتنی برهش برای شناسایی مسیر پیمایش پول‌شویی	روشی کارآمد برای جلوگیری ازاتلاف وقت و پیچیدگی برای شناسایی تراکنش‌های مشکوک	-

ردیف	نویسنده / سال	روش‌های مورد استفاده	مزایا	معایب
۱۳	Jayasree , Balan(2016)	تعیین درخت دانشی که ریسک پول‌شویی را نمایش می دهد با استفاده ازدرخت تصمیم اندیس محور نقشه بیتی	استفاده برای پایگاه داده های بزرگ بانکی، دقت بالا برای شناسایی دقیق پول‌شویی تراکنش‌ها با نرخ تکراربالا	-
۱۴	Abdul K. Shaikh, Amril Nazir(2018)	ساخت یک شبکه اجتماعی با استفاده از گراف شبکه ای معنایی و فعالیت‌های شبکه‌های ازقبیل درجه مرکزیت و خوشه‌بندی و غیره جهت شناسایی مشتریان مشکوک	شناسایی گروه‌های مشکوک در شبکه‌های اجتماعی	عدم وجود ارتباط خاصی در تحلیل بین حساب‌های بانکی و عملیات انجام شده

روش تحقیق

در این تحقیق، به معرفی روشی که خود شامل سه روش می‌باشد(فیلتر رگرسیونی غیرخطی خودکار با در نظر گرفتن پارامترهای خارجی، فیلتر رگرسیونی غیرخطی خودکار، فیلتررگرسیونی غیرخطی ورودی-خروجی)، پرداخته‌ایم. نتایج پیاده‌سازی آن در بخش بعدی ارائه شده است.

در این روش با استفاده از ابزار خوشه‌بندی شبکه‌های عصبی[۲۵] در محیط Matlab طبقه بندی تراکنش‌ها به تراکنش‌های مشکوک وغیرمشکوک پیشنهاد شده است، در این روش برای پیاده‌سازی ابتدا، با توجه به امنیتی بودن موضوع و عدم ارائه مجموعه داده از مراجع ذیصلاح این موضوع و نویسندگان مقالات مرور شده از یک مجموعه داده دستی خود در بازه زمانی یکماهه و یک مجموعه دادهٔ بانکی که بصورت محرمانه توسط یکی از متخصصین در این زمینه ارسال شد، استفاده شد که مراحل پیاده‌سازی روی این دو مجموعه داده انجام شد و نتایج در فصل بعدی ارائه شده است. جهت پیاده‌سازی این روش، با ورود به ابزار خوشه‌بندی شبکه‌های عصبی بصورت زیر عمل نموده ایم:

پس از بارگذاری مجموعه داده با استفاده از شبکه‌های عصبی تراکنش‌ها خوشه‌بندی شده‌اند که این خوشه‌بندی اولیه تراکنش‌ها می‌باشد. در قدم بعدی، با استفاده از فیلتر های رگرسیونی تراکنش‌ها طبقه‌بندی شده‌اند. در این مرحله، با سه فیلتر رگرسیونی مواجه می‌شویم که در این تحقیق، هر سه روش تست و ارزیابی شده‌اند. در هر سه فیلتر در مرحله بعدی، با استفاده از قواعد بیزین تراکنش‌ها را منظم‌تر نموده و در انتها رگرسیون روش ارائه شده را با روش کار پایه می سنجیم. قابل ذکر است در روش ارائه شده ، تراکنش‌ها را به داده های سری -زمانی مدل کرده‌ایم، به این دلیل که هر تراکنش در زمان مشخصی انجام شده است و تراکنش‌ها را مانند یک سری داده مرتبط به هم مورد بررسی قرار داده‌ایم. فلوچارت روش ارائه

[۲۵] Neural Net Clustering .

شده در شکل ۱ آمده است.

محیط و تنظیمات آزمایشات

کلیه آزمایشات در محیط ویندوز ۱۰، cpu cor i7- 2.20GHz، حافظه ۶ گیگا بایت و با نرم افزار Matlab R2015a پیاده‌سازی شده است.

مجموعه داده مورد آزمایش

همانگونه که در فصل قبل اشاره کردیم آزمایشات انجام شده روی یک مجموعه داده دستی که در فاصله زمانی یکماهه(Δt) رصد شده اند و یک مجموعه داده بانکی انجام شده است. با توجه به اینکه از سری‌های زمانی در روش خود استفاده کرده‌ایم.

مجموعه داده بانکی دستی خود دارای ۱۵۰رکورد و مجموعه داده بانکی نیز یک فایل Excel با ۱۵۰۰ رکورد که هر رکورد خود دارای ۷ فیلد(نوع حساب، میانگین گردش حساب بصورت ماهیانه، میانگین تراکنش‌های حساب بصورت ماهیانه، گزارش تراکنش مشکوک[۲۶]، گزارش تراکنش‌های نقدی[۲۷]، استفاده از بانکداری الکترونیک و مبادلات ارزی)می‌باشد. همانگونه که در فصل قبل اشاره شد، این فایل مجموعه داده بانکی بصورت محرمانه توسط یکی از متخصصین در این زمینه ارسال شده است که به نام بانک مورد نظر اشاره‌ای نشده است.

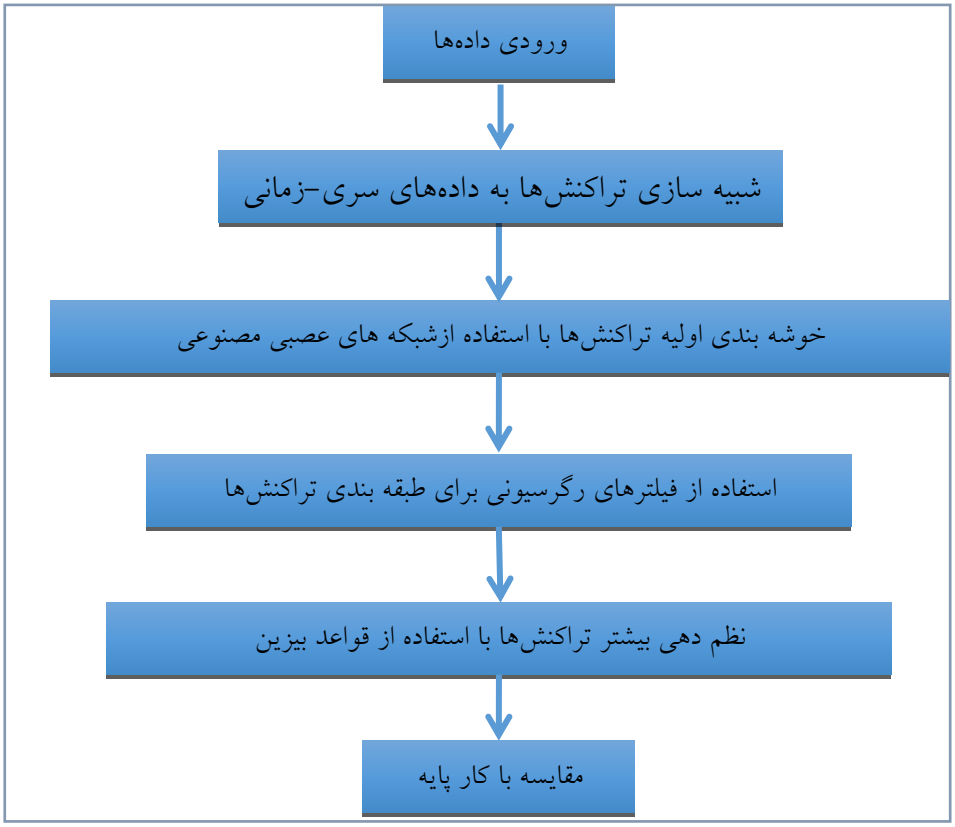
مجموعه داده بانکی که بصورت دستی ایجاد نموده‌ایم بصورت زیر است:

جدول ۲. بخشی از مجموعه داده دستی

نوع	میانگین گردش ماهانه	میانگین تراکنش‌های ماهانه	گزارش تراکنش‌های مشکوک	گزارش تراکنش‌های نقدی بالاتر از سقف مجاز	کاربرد بانکداری الکترونیک	فعالیت‌های ارزی
حقوقی	۲۲۰۷۵۲۰۰۰۰۰۰۰/۰۰	۷۴/۰۰	۰/۰۰	۱/۰۰	۰/۰۰	۰/۰۰
حقوقی	۱۴۶۰۰۰۰۰۰۰۰۰/۰۰	۴۸/۰۰	۱/۰۰	۱/۰۰	۱/۰۰	۱/۰۰
حقیقی	۱۳۳۲۰۰۰۶۴۹۴۴۰/۰۰	۷۷/۰۰	۰/۰۰	۱/۰۰	۱/۰۰	۰/۰۰
حقیقی	۹۸۱۰۰۰۰۰۰۰۰/۰۰	۹۶/۰۰	۰/۰۰	۱/۰۰	۱/۰۰	۱/۰۰
حقیقی	۹۷۱۲۵۰۴۷۳۵۵۰/۰۰	۱۵۰/۰۰	۰/۰۰	۱/۰۰	۰/۰۰	۰/۰۰
حقیقی	۹۴۵۰۰۰۰۰۰۰۰/۰۰	۲۱۰/۰۰	۰/۰۰	۱/۰۰	۰/۰۰	۱/۰۰
حقوقی	۹۴۵۰۰۰۰۰۰۰۰/۰۰	۳۰۲/۰۰	۱/۰۰	۱/۰۰	۰/۰۰	۰/۰۰
حقوقی	۹۰۰۰۰۰۰۰۰۰۰/۰۰	۲۵۸/۰۰	۱/۰۰	۱/۰۰	۱/۰۰	۰/۰۰
حقوقی	۸۰۸۰۱۷۰۰۰۴۸۲/۰۰	۱۰۰/۰۰	۰/۰۰	۱/۰۰	۱/۰۰	۰/۰۰

[۲۶] STR: Suspicious Transaction Report.

[۲۷] CTR: Cash Transaction Report.



شکل۱. فلوچارت روند کاری روش پیشنهادی

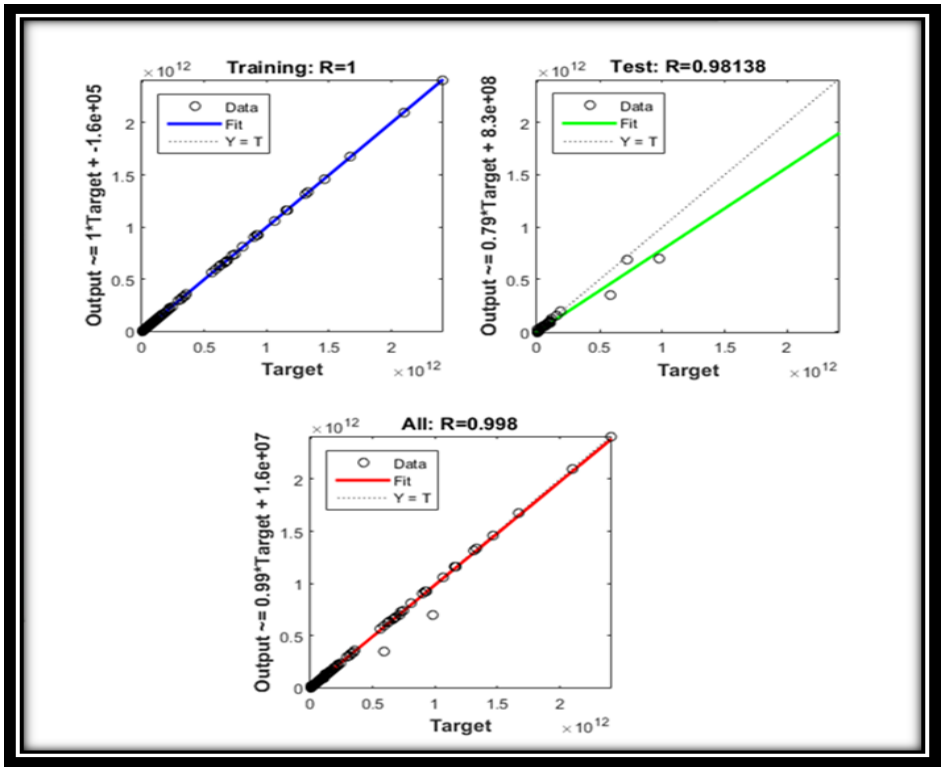
یافته‌ها و نتایج

معماری شبکه عصبی که در هر سه روش عنوان شده، برای مجموعه داده دستی با توجه به تعداد کم رکوردها از همان حالت پیش‌فرض از ۱۰ سلول عصبی[۲۸] مخفی و تعداد ۲ تأخیر زمانی و برای مجموعه داده بانکی نیز از ۲۵ سلول عصبی مخفی و تعداد ۲۵ تأخیر زمانی تشکیل شده است. در هر سه روش در قسمت تقسیم بندی داده‌ها، برای داده‌های آموزش[۲۹] اعتبارسنجی[۳۰] و تست[۳۱] از همان حالت پیش‌فرض نرم‌افزار (آموزش:۷۵٪، اعتبارسنجی:۱۵٪ و تست:۱۵٪)استفاده شده است. منظور از داده‌های آموزش، آن دسته از داده‌هایی است که در حین فرآیند آموزش و برای آموزش شبکه‌های عصبی به هر دوصورت ورودی و خروجی می‌باشد و همه جوانب آن مشخص است.

پس از پیاده‌سازی با مجموعه داده بانکی به نتایجی که در شکل‌های ۲ و ۴ نشان داده شده است، رسیده‌ایم. پس از اجرا با ۱۰۰۰تکرار پس از یک ساعت و بیست و هفت دقیقه و بیست و نه ثانیه (۱:۲۷:۲۹) اجرا خاتمه پیدا کرده است. نتایج و نمودارهای این روش با مجموعه داده بانکی در مقایسه با کارپایه، مطابق به آنچه در شکل ۲ نشان می‌دهد، نشان‌دهنده بهینه‌تر و کاراتر بودن این روش نسبت به کار پایه می‌باشد. در کار پایه مقدار رگرسیون ۰,۹۶۰۸ می‌باشد و در روش

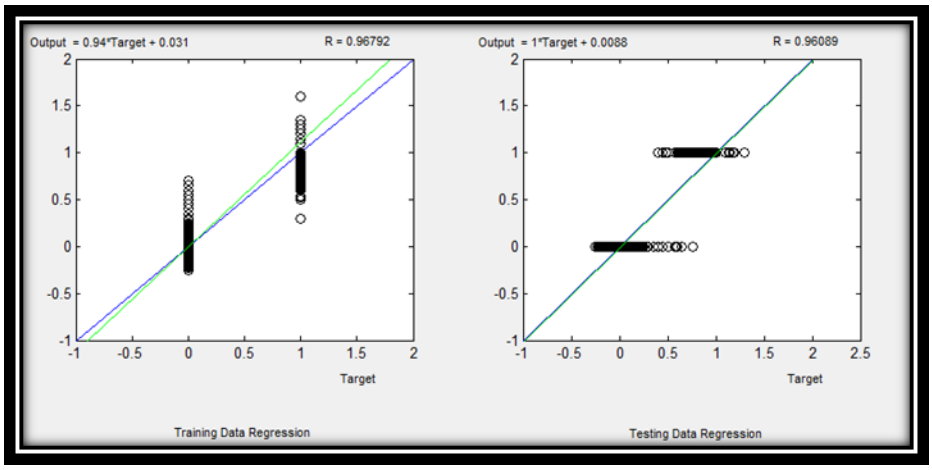
[۲۸] Neuron.
[۲۹] Training.
[۳۰] Validation.
[۳۱] Testing.

پیشنهادی رگرسیون در حالت خروجی وهدف ۰,۹۹۸ می‌باشد.



شکل ۲. نمودارر‌گرسیون مدل غیرخطی خودکار

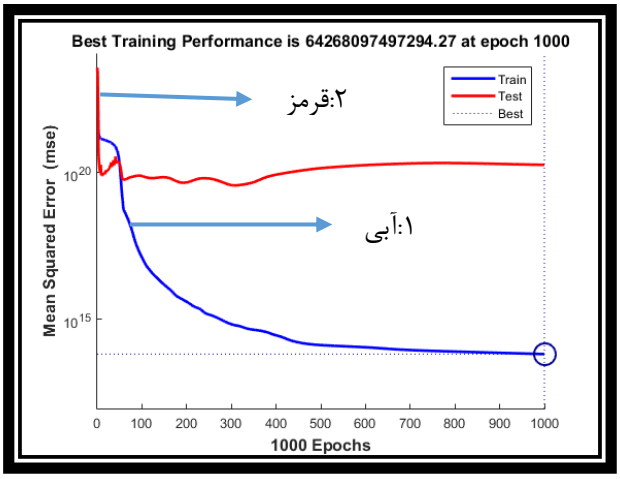
همانگونه که در شکل ۲ نشان داده شده در قسمت‌هایی که تراکم داده‌ها بیشتر است احتمال وقوع تراکنش مشکوک بیشتر می‌باشد و نیز مشاهده می‌شود که تقریبا نمودار رگرسیون نتیجه پیاده‌سازی ما منطبق بر نمودار بهترین حالت می‌باشد. درزیر نمودار رگرسیون کار پایه جهت مقایسه با نتایج خروجی آزمایشات این تحقیق در شکل ۳ آمده است.



شکل ۳. نمودار رگرسیون کار پایه

در شکل ۴ نمودار بهترین کارایی برای روش ارائه شده، نمایش داده شده است. همانگونه که در شکل زیر نمایش داده شده خط چین بهترین حالت، منحنی آبی (منحنی ۱) نتیجه بعد از آموزش و منحنی قرمز (منحنی۲) مربوط به حالت تست

می‌باشد که در این روش حالت بعد از آموزش به بهترین حالت بسیار نزدیکتر می‌باشد و در نتیجه از کارایی خوبی برخوردار است.



شکل۴. نموداربهترین کارایی رگرسیون غیرخطی خودکار

جمع بندی

در این تحقیق سعی بر آن داشتیم که روشی کارآمدی برای شناخت تراکنش‌های مشکوک در پول‌شویی ارائه نمائیم. روش ترکیبی هوشمند ارائه شده مبتنی برشبکه های عصبی مصنوعی و فیلترهای رگرسیون محور می باشد.

قابل ذکر است کار پایه با استفاده ازیک سیستم فازی وشبکه های عصبی ANFIS تراکنش‌های مشکوک را شناسایی کرده است. با مقایسه نمودار رگرسیون روش طراحی شده با روش کار پایه به این نتیجه می رسیم که روش ارائه شده با استفاده از هر دو مجموعه داده کاراتر به دلیل اینکه رگرسیون متغیر میزان مشکوک بودن تراکنش و درست تشخیص دادن آن در مقایسه با کار پایه و روش های ارائه شده کاراتر می باشد.

روش ارائه شده مبتنی بر رگرسیونی غیرخطی خودکار با در نظر گرفتن پارامترهای خارجی با مجموعه داده دستی خود دارای رگرسیون۰,۹۹ ، با فیلتر رگرسیونی غیر خطی خودکار با مجموعه داده دستی دارای رگرسیون ۰,۹۸ و با مجموعه داده بانکی دارای ۰,۹۹ و در نهایت با فیلتر رگرسیونی غیرخطی ورودی-خروجی با مجموعه داده دستی خود دارای رگرسیون ۰,۹۹ و با مجموعه داده بانکی دارای رگرسیون ۰,۹۸ می باشد در حالیکه روش ارائه شده در کار پایه دارای رگرسیون ۰,۹۶ می‌باشد که نشان دهنده بهبود روش عنوان شده ما می‌باشد. فقط در روش فیلتر رگرسیونی غیرخطی خودکار با درنظر گرفتن پاراکترهای خارجی دارای رگرسیون پایین‌تری نسبت به رگرسیون کار پایه می باشد که از روش ارائه شده در کار پایه کاراتر نمی‌باشد.

در زیر به سه مورد از کارهایی که در این زمینه می‌توان تحقیق کرد، ذکر شده است:

- ارائه الگوریتمی مبتنی بر مدل مخفی مارکوف[۳۲] جهت کشف تراکنش‌های مشکوک.
- پیاده سازی روش اول همین تحقیق که از نظر تئوریک بررسی شد.
- کشف تراکنش‌های مشکوک به کمک SVM[۳۳]

[۳۲] Hidden Moarkov Model .

منابع

[1] nashriyat.ir. Available from: http://marifat.nashriyat.ir/node/478.

[2] Luo, Xingrong. "Suspicious Transaction Detection for Anti-Money Laundering." International Journal of Security and Its Applications (2014).

[3] fumblog.um.ac.ir. Available from: http://fumblog.um.ac.ir/fumindex.php?op=ViewArticle&articleId=7127&blogId=552.

[4] Wang, X. and G. Dong. Research on money laundering detection based on improved minimum spanning tree clustering and its application. in 2009 Second International Symposium on Knowledge Acquisition and Modeling. 2009. IEEE.

[5] Le Khac, N.A. and M. Kechadi. Application of data mining for anti-money laundering detection: A case study. in Data Mining Workshops (ICDMW), 2010 IEEE International Conference on. 2010. IEEE.

[6] Le-Khac, N.-A., S. Markos, and M.-T. Kechadi, Towards a new data mining-based approach for anti-money laundering in an international investment bank, in Digital Forensics and Cyber Crime. 2009, Springer. p. 77-84

[7] Liu, R., et al. Research on anti-money laundering based on core decision tree algorithm. in Control and Decision Conference (CCDC), 2011 Chinese. 2011. IEEE.

[8] Ngai, E., et al., The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 2011. 50(3): p. 559-569.

[9] R. Kosari Langari, e.a., Introducing a Model for Suspicious Behaviors Detectio in Electronic Banking by Using Decision Tree Algorithms. Spring, 2013. 28(3): p. 577-584

[10] Cao, D.K. and P. Do, Applying data mining in money laundering detection for the vietnamese banking industry, in Intelligent Information and Database Systems. 2012, Springer. p. 207-216.

[11] Tang, J. and J. Yin. Developing an intelligent data discriminating system of anti money laundering based on SVM. in Machine Learning and Cybernetics, 2005. Proceeding of 2005 International Conference on. 2005. IEEE.

[12] Luo, Xingrong. "Suspicious Transaction Detection for Anti-Money Laundering." International Journal of Security and Its Applications (2014).

[13] Suresh, C., K.T. Reddy, and N. Sweta, A Hybrid Approach for Detecting Suspicious Accounts in Money Laundering Using Data Mining Techniques. International Journal of Information Technology and Computer Science (IJITCS), 2016. 8(5): p. 37.

[14] Jayasree, V. and R.S. Balan, Money laundering regulatory risk evaluation using Bitmap Index-based Decision Tree. Journal of the Association of Arab Universities for Bas and Applied Sciences, 2016.

[۳۳] *Support Vector Machine*.

[15] Heidarinia, Neda, Ali Harounabadi, and Mehdi Sadeghzadeh. "An Intelligent Anti-Money Laundering Method for Detecting Risky Users in the Banking Systems." International Journal of Computer Applications 97.22 (2014).

[16] Shaikh, Abdul K., and Amril Nazir. "A Model for Identifying Relationships of Suspicious Customers in Money Laundering using Social Network Functions." Proceedings of the World Congress on Engineering. Vol. 1. 2018

[۱۷] تذهیبی. فریده،"پول‌شویی و روش‌های مبارزه با آن"، انتشارات جنگل، چاپ اول،۱۳۸۹

[۱۸] حسابرس, م.; Available from: مجله حسابرس شماره ۶۰ شهریور ۱۳۹۱.

[۱۹] جزایری.مینا، "پول‌شویی و مؤسسات مالی، مؤسسه عالی آموزش بانک‌داری ایران"،۱۳۸۷