فصلنامه مطالعات نوین بانکی

شماره مجوز: ۸۳۲۸۹ ((شماره بیست و دوم-بهار۱۴۰۳)) ISSN : 5420-2645

تحلیل و شناسایی موارد مشکوک به پولشویی و تامین مالی تروریسم مبتنی بر داده کاوی و هوش مصنوعی

(تاریخ دریافت ۱۴۰۳/۰۳/۰۲ تاریخ تصویب ۱۴۰۳/۰۳/۲۷)

سحر شعبانی چافجیری

کارشناسی ارشد، مدیریت کسب و کار، گروه مدیریت، واحد تهران‌غرب، دانشگاه آزاداسلامی، تهران، ایران

دکترمحمد حسین درویش متولی[۱]

استادیار، گروه مدیریت صنعتی، واحد تهران‌غرب، دانشگاه آزاد اسلامی، تهران، ایران

چکیده

امروزه سازمان‌های فعال حوزه پولشویی همواره در تلاش هستند به گونه ای رفتار نمایند که معاملات نامشروع خود را مشروع جلوه دهند. لذا بانک‌ها در مواجه با این سازمان‌ها با ریسک‌های قابل توجه و پیچیده ای همراه هستند. هدف اصلی از انجام این پژوهش استفاده از روش داده‌کاوی و هوش مصنوعی در تحلیل و شناسایی موارد مشکوک به پولشویی و تامین مالی تروریسم می‌باشد. این پژوهش از نظر هدف و نتایج کاربردی و از نظر ماهیت اجرا توصیفی است. نمونه آماری این پژوهش ۱۲۳۷ نفر از مشتریان بانکهای تجاری ایران درسال۱۳۹۹ می‌باشد. نتایج نشان داد که بیشتر موارد پولشویی در شهرهای پرخطر و فقط نیمی از موارد مشکوک مربوط به افراد با سابقه کیفری می‌باشد.

واژگان کلیدی: داده کاوی, هوش مصنوعی, پولشویی, تامین مالی تروریسم

---

[۱] نویسنده مسئول

مقدمه

امروزه دورنمای رقابت در صنعت بانکداری به طور قابل توجهی تغییر یافته است. توسعه فناوریهای جدید راه‌های زیادی را برای متقلبان و مجرمان بازکرده که بتوانند مرتکب تقلب شوند. ایجاد یک سیستم‌اطلاعاتی جدید و تکنیک‌های شناسایی تقلب علاوه برآنکه تقلب‌ها و کلاهبرداری‌های صورت گرفته در یک سازمان را شناسایی کرده و مورد تجزیه و تحلیل قرار می‌دهد به نوعی با شناخت رفتار کاربران یا مشتریان سعی در پیشبینی رفتار آتی آنها داشته و ریسک انجام تقلب‌ها را کاهش می‌دهد (سرلک، ولی و همکاران، ۱۳۹۵). پول شویی[۱]، فرآیند پنهان سازی و قانونی جلوه دادن منشأ پول کثیف[۲] و یا به عبارتی قانونی جلوه دادن عواید مالی حاصل از جرم و جنایت می‌باشد و بعد از بانکداری و صنعت خودرو، سومین کسب و کار[۳] بزرگ دنیاست (لوپز و اکسلسون، ۲۰۱۲) (رابینسون، ۱۹۹۶). پولشویی جرمی سازمان یافته‌ی فراملی است که بسیاری از کشورها به خصوص کشورهای در حال توسعه به شکلی گسترده با آن دست به گریبان هستند. عواملی مانند نظام اداری ناسالم و غیرکارآمد، نظام ناسالم اقتصادی، نظام مالی غیر شفاف و فاقد سیستم نظارتی قوی و ضعف دولت، بسترهایی مناسب برای عملیات پولشویی هستند. پولشویی دارای اثرات گسترده نامطلوب و زیان باری است که موجب فرار مالیاتی، فرار سرمایه از کشور، اختلال در بازارهای مالی، تورم و...می‌گردد (عیسی آبادی، ابوالقاسم ۱۴۰۲). شاید در نگاه نخست، پولشویی به عنوان یک جرم بدون قربانی درنظر آید و هیچ یک از حالت های ناخوشایند مانند احساس بی اطمینانی یا ترس ناشی از جرایم دیگر از قبیل قتل، سرقت و ...درباره پولشویی در میان مردم وجود نداشته

---

۱. Money Laundering
۲ Dirty Money
۳ Business

باشد اما هرگاه توجه شود که پولشویی عارضه‌ای ثانویه و متناظر با یک جرم مانند قاچاق مواد مخدر است، مشخص می شود که عدم اطلاع کافی از علت و ماهیت پولشویی، این جرم را در افکار عمومی چنین ناشناخته و بی پاسخ گذاشته است.(سلیمان فلاح، امیرحسین ۱۴۰۲) . امروزه یکی از مهمترین موانع استفاده از خدمات بانکداری الکترونیکی نبود امنیت و برخی سوء استفاده ها در مسیر انجام مبادلات مالی است. به همین دلیل استفاده از روش‌هایی برای تحلیل و شناسایی موارد مشکوک به پولشویی و تامین مالی تروریسم از مسائل مهم در مؤسسات مالی و بانکهاست. در این پژوهش سعی می‌شود با استفاده از تکنولوژی داده کاوی و روش هوش مصنوعی روشی نوین در کشف تقلب ارائه شود. هر چند آمار دقیقی از تقلب در کارتهای بانکی معتبر کشور وجود ندارد ولی به نظر می‌رسد همزمان با توسعه بانکداری الکترونیک تقلب در کارتهای بانکی رو به رشد بوده و در آینده ای نه چندان دور به یکی از معضلات سیستم بانکی کشور تبدیل خواهد شد. بدین روی در این پژوهش پس از مصاحبه با خبرگان در زمینه شناسایی انواع تقلب های رایج در زمینه موارد مشکوک به پولشویی از طریق اعمال تغییرات معنادار روی داده ها برای تهیه تراکنش‌های متقلبانه با بهره گیری از روش دسته بندی در داده کاوی و تکنیک هوش مصنوعی بهره برده‌ایم که در مقالات پیشین این دو روش بکار برده نشده است.

پژوهش حاضر از نظر هدف کاربردی است و از نظر روش و ماهیت اجرا، توصیفی و پیمایشی است، جامعه آماری این پژوهش، مشتریان بانک های قرض الحسنه مهر ایران ، ملت و رسالت تهران برای سال ۱۳۹۹ می باشد و برای تعیین میزان حجم نمونه از ۱۲۳۷ مشتری فعال بانکی استفاده شده است در این تحقیق، با استفاده از ابزار پرسشنامه اقدام به گردآوری اطلاعات از

جامعه آماری مورد مطالعه شده و پس از جمع آوری اطلاعات به منظور تجزیه و تحلیل داده ها از نرم افزارهای SPSS و neurosolutions استفاده می شود.

در این تحقیق به منظور شناسایی موارد مشکوک به پولشویی و تامین مالی تروریسم از روش داده کاوی و هوش مصنوعی استفاده می شود، مراحل کار به صورت زیر است:

- خوشه بندی مشتریان بانک بر مبنای ویژگی های دستورالعمل بانک مرکزی و الگوریتم داده کاوی K-means
- تفکیک مشتریان بانک به دو دسته مشتریان مشکوک به پولشویی و مشتریان عادی با استفاده از نتایج الگوریتم K-means
- طبقه بندی مشتریان بانک با استفاده از تکنیک های هوش مصنوعی به ویژه شبکه عصبی مصنوعی(ANN
- بررسی میزان صحت الگوریتم پیشنهادی

بخش اول: روش k-means

روش خوشه بندی K-Means علی‌رغم سادگی آن یک روش پایه برای بسیاری از روش‌های خوشه‌بندی دیگر محسوب می‌شود. این روش، روشی انحصاری و مسطح محسوب می‌شود. برای این الگوریتم شکل های مختلفی بیان شده است. ولی همه آنها دارای روالی تکراری هستند که برای تعدادی ثابت از خوشه‌ها سعی در تخمین موارد زیر دارند:

۱- به دست آوردن نقاطی به عنوان مراکز خوشه‌ها. این نقاط در واقع همان میانگین نقاط متعلق به هر خوشه هستند.

۲- نسبت دادن هر نمونه داده به یک خوشه که آن داده کمترین فاصله تا مرکز آن خوشه را دارا باشد.

تابع زیر به عنوان تابع هدف مطرح است.

$$J = \sum_{j=1}^{k} \sum_{i=1}^{n} \left\| x_i^{(j)} - c_j \right\|^2$$

که در آن || || معیار فاصله بین نقطه i ام با مرکز خوشه j ام است.

الگوریتم روش k-means به شرح زیر است:

در ابتدا k نقطه به عنوان نقاط مراکز خوشه ها انتخاب شوند.

هر نمونه داده ها به خوشه ای که مرکز آن خوشه کمترین فاصله تا آن داده را دارا است نسبت داده می شود.

پس تعلق تمام داده ها به یکی از خوشه ها برای هر خوشه یک نقطه جدید به عنوان مرکز محاسبه می شود.

مراحل تکرار می شوند تا زمانی که دیگر هیچ تغییری در مراکز خوشه‌ها حاصل نشود.

شبکه عصبی مصنوعی: شبکه‌های عصبی مصنوعی(ANN)، شبکه‌هایی گسترده، قابل انطباق و عموماً یک ماشین یادگیری غیرخطی است که با الهام از طرز کار مغز بشر ساخته شده و قادر است به سادگی ارتباطات پنهان میان داده‌ها (حتی داده‌هایی که دارای ارتباطات غیرخطی، توزیعی، موازی، غیررقومی (آنالوگ) و غیرالگوریتمی هستند) را کشف نماید.

یکی از نتایج طراحی شبکه‌های عصبی مصنوعی یکسان نمودن برنامه سیستماتیک(یک الگوی آموزش) برای تنظیم نمودن وزنها و همچنین برای تدقیق طبقه‌بندی است. دقت این کار با توجه به پارامترهای اندازه‌گیری خطا تعیین می‌شود. تمامی شبکه‌های عصبی در سه مولفه اصلی مشترک هستند:

۱- نورون یا گره(PE)

۲- وزنهای ارتباطی(Wij)

۳- لایه های مجزایی که شامل نورونها هستند و توسط وزنها به هم مرتبط می‌شوند.

بخش دوم: تحلیل داده ها

هدف اصلی در این پژوهش یافتن پارامترهایی است که در کشف الگوی مشکوک پولشویی بیان شده در قانون مبارزه با پولشویی مناسب باشند. در واقع، این پژوهش به دنبال رسیدن به اهداف زیر است:

۱- شناخت موارد مشکوک به پولشویی و تامین مالی تروریسم

۲- کشف موارد مشکوک به پولشویی و تامین مالی تروریسم براساس هوش مصنوعی

برای رسیدن به اهداف فوق، ابتدا از معیارهای جمعیت شناسی مشخص شده توسط بانک مرکزی استفاده و مشتریان بانک مورد مطالعه را با روش k-means به دو دسته مشتریان مشکوک به پولشویی و مشتریان عادی دسته بندی می کنیم. در واقع با این روش موارد مشکوک به پولشویی شناسایی می شود. در ادامه از تکنیک های هوش مصنوعی استفاده و یک الگو برای کشف موارد مشکوک به پولشویی ارائه خواهیم نمود. ابتدا زیر مجموعه

هدف را مشخص می کنیم. طبق موارد بیان شده در قانون برای کشف موارد مشکوک، دو نکته حائز اهمیت است:

۱- بدیهی‌ترین عملکرد این است که در ابتدای ایجاد رابطه بین مشتری و بانک، مشتریان بر اساس ریسک احتمالی دسته بندی می‌شوند تا بتوان اقدامات کنترلی مناسب را درباره آنان در نظر گرفت و در ادامه، این گروه از مشتریان را با دقت بیشتری مورد توجه قرار داد.

۲- پولشویی در اغلب موارد در طولانی مدت و با شیوه های پیچیده صورت می‌پذیرد تا کشف الگوی پولشویی در آنها کار ساده ای نباشد. بنابراین نکته مهم، رصد دقیق فعالیت‌های مستمر حساب ها در طولانی مدت است که می‌تواند به کشف الگوهای پنهان پولشویی منجر شود. طبق ماده ۴ دستورالعمل چگونگی شناسایی مشتریان ایرانی موسسات اعتباری، "موسسات اعتباری و بانک‌ها موظف هستند مشتریان خود را با توجه به ریسکی که احتمال می‌دهد از ناحیه آنها و به واسطه عواملی همچون موقعیت اجتماعی و شغلی، وضعیت مالی، نوع و ماهیت فعالیت حرفه ای، پیشینه مشتری، موطن اصلی، حساب های مرتبط یا دیگر شاخص های موثر (به تشخیص موسسه اعتباری) که متوجه موسسه می‌شود؛ طبقه بندی نماید"۱ تا نسبت به افراد هر طبقه اقدامات مناسب را انجام دهد. به عنوان مثال درمورد حساب های در معرض ریسک بیشتر، موسسه اعتباری موظف است سیستمی ایجاد کند که حساب های یاد شده به طور ادواری نیز تحت پایش قرار گیرند. هر بانک می‌بایست برای چنین حساب هایی، اقدام به ایجاد علائم هشدار دهنده کلیدی نماید. برای نیل به این هدف باید اطلاعات لازم در دسترس باشد. در مرحله اول باید به شناسایی عوامل موثر بر پولشویی و تامین مالی تروریسم پرداخت. برای این کار با مطالعات اولیه مبانی نظری و قوانین بانک مرکزی عوامل شناسایی شدند. با توجه به دستور العمل‌های ده گانه بانک مرکزی برای مبارزه با پولشویی اطلاعات مورد نیاز در هنگام

افتتاح حساب برای هر شخص به دقت مشخص و ثبت می‌شود. از میان این اطلاعات، زیرمجموعه هدف برای پوشش موارد مشکوک بیان شده در قانون طبق جدول (۱) است:

جدول (۱) عوامل موثر بر شناسایی پولشویی طبق قوانین بانک مرکزی

معرف دارد	Introduction
مجوز دارد	License
جز کدام نوع از مشتریان است	Type
سابقه کیفری دارد	Penal
جز افراد با ریسک بالا است	High-risk
شهر محل سکونت وی پرخطر است	High-risk city
تقاضای کارت اعتباری	Credit card
شهر محل سکونت با شهر مورد تقاضا برای کارت اعتباری متفاوت است	Same city
صاحب این حساب دارای حساب های دیگری هم است	More account
حساب های با آدرس های یکسان	Same address

بعد از مشخص شدن عوامل موثر بر پولشویی در مرحله بعد به جمع آوری داده های مشتریان پرداخته می شود. داده های تحقیق مربوط به مشتریان بانک های تجاری در ایران برای سال ۱۳۹۹ می باشد. در اینجا از اطلاعات ۱۲۳۷ مشتری این بانک استفاده می‌شود. برای تجزیه و تحلیل داده ها، باید بتوان الگوریتم‌های داده کاوی را برای بدست آوردن افراد و الگوهای مشکوک به کار گرفت. برای این منظور از الگوریتم خوشه بندی k-means استفاده می‌شود. در این الگوریتم، اعضای یک خوشه تا حد امکان به یکدیگر شبیه بوده و با اعضای دیگر خوشه ها، متفاوت می‌باشند. با توجه به این خاصیت حساب ها را به ۳ خوشه تقسیم کنیم و انتظار می‌رود حساب های با میزان ریسک مشابه در یک خوشه قرار گیرند. در میان این ۳ خوشه، خوشه‌ی ای مورد توجه ماست که افراد مشکوک و با میزان ریسک بالا را در خود جای داده است. بنابراین هنگام درج حساب جدید، اطلاعات لازم برای حساب، محاسبه می‌شود و میزان شباهت حساب با مراکز هر سه خوشه بدست می‌آید، سپس حساب با توجه با میزان شباهت به یکی از این خوشه‌ها نسبت داده می‌شوند، اگر فرد به خوشه خطرناک تعلق گرفت باید برای بررسی‌های بیشتر گزاش داده شود.

شکل (۱) به عنوان مثال خوشه بندی گفته شده را نشان می‌دهد همانطور که می‌بینید داده ها به ۳ خوشه تبدیل شده اند. مراکز هر خوشه در واقع میانگین اعضای آن خوشه هستند.

Final Cluster Centers

	Cluster		
	۱	۲	۳
Introduction	۰	۱	۰
Licence	۰	۰	۱
Type	۰	۱	۳
Highrisk	۰	۰	۰
Highriskcity	۰	۰	۱
Penal	۰	۱	۰
Creditcard	۱	۰	۱
Notsamecity	۰	۰	۰
Moreaccount	۰	۰	۰
Sameaddress	۰	۰	۰

Number of Cases in each Cluster

Cluster	۱	۳۹۷.۰۰۰
	۲	۳۸۱.۰۰۰
	۳	۳۹۸.۰۰۰
Valid		۱۱۷۶۳
Missing		۶۱.۰۰۰

شکل (۱) مراکز خوشه‌ها در خوشه بندی حساب ها

برای تشخیص خوشه خطرناک در میان سه خوشه، راه حل پیشنهادی محاسبه عبارت زیر برای هر خوشه است:

X=Type+ penal+ high-risk+ high-risk city+ credit card+ same address+more account+ same city- (introduce+ license)

حاصل عبارت فوق برای هر کدام از خوشه‌ها که بیشتر بود آن خوشه، خوشه‌ی مشکوک به پولشویی محسوب می‌شود.

$x_۱ = ۱$, $x_۲ = ۱$, $x_۳ = ۴$

بنابراین همانطور که ملاحظه می‌کنید خوشه ۳ خوشه‌ی خطرناک است و افراد متعلق به این خوشه جزو افرادی هستند که دارای ریسک احتمالی بالاتری برای پولشویی هستند و فعالیت‌های آنان باید با دقت بیشتری رصد شود.

همانطور که پیشتر بیان شد، بانک‌ها نه تنها باید هویت مشتریان خود را احراز نمایند بلکه لازم است بر فعالیت حساب آنها نیز نظارت مستمر داشته باشند. تا بدین وسیله به تعیین آن دسته از مبادلاتی بپردازند که با وضع معمول یا مورد انتظار آن مشتریان یا نوع حساب آنها همخوانی ندارند.

طبق ماده ۹ دستورالعمل نحوه تعیین سطح فعالیت مورد انتظار مشتری در موسسات اعتباری، "موسسه اعتباری موظف است نرم افزارهای رایانه ای خود را به گونه ای طراحی نماید که امکان شناسایی و گزارش تراکنش‌های نامتناسب با سطح فعالیت تعیین شده (به عنوان مثال نقل و انتقال حجم قابل ملاحظه وجه نقد بر خلاف سوابق و رویه‌های معمول فعالیت مشتری یا گردش غیرمتعارف حساب وی) را داشته باشد. همچنین نرم افزارهای مزبور باید از قابلیت به روزرسانی سطح فعالیت مشتریان برخوردار باشند."

مورد مهمی که در قانون بر آن تاکید بسیار شده، تناسب میان فعالیت یک حساب و میزان فعالیت مورد انتظار برای آن است، هنگام افتتاح حساب با توجه به نکاتی مانند شغل و میزان درآمد و... سطح فعالیت و گردش مورد انتظار برای هر حساب مشخص می‌شود. اما اگر در عمل، فعالیت حساب بیش از سطح فعالیت مورد انتظار باشد یک مورد مشکوک خواهد بود که باید برای پیگیری بیشتر گزارش داده شود. برای کشف چنین حالتی می‌توان از داده کاوی استفاده کرد.

ابتدا زیر مجموعه هدف را برای پوشش این الگو پولشویی مشخص می‌کنیم. سطح فعالیت هر حساب به فراوانی تعداد تراکنش و مبالغ جابه‌جا شده توسط آن در طول دوره خاصی بستگی دارد. بنابراین زیرمجموعه هدف طبق جدول (۲) تعداد و مبلغ تراکنش‌ها در یک دوره ی زمانی مشخص خواهد بود.

جدول(۲) پارامترهای مورد استفاده در خوشه بندی تراکنش‌های حساب

تعداد تراکنش‌های یک حساب در طول مدت مشخص	Count
مبلغ تراکنش‌های یک حساب در طول مدت مشخص	Sum

سپس نوبت به اعمال الگوریتم داده کاوی می‌رسد. که در اینجا نیز می‌توانیم از خصوصیات الگوریتم خوشه بندی k-means به نحو مطلوبی بهره برد. برای این منظور، حساب ها را با توجه به تعداد تراکنش‌ها و مبالغ آن در دوره زمانی خاص، به دو خوشه تقسیم می‌کنیم. هر نمونه داده به یک خوشه که آن داده کمترین فاصله تا مرکز آن خوشه را دارا باشد نسبت داده می‌شود. در پایان مراکز هر خوشه به عنوان خروجی الگوریتم مشخص می‌شود. حساب هایی با تعداد تراکنش و مبالغ مشابه در یک خوشه قرار می‌گیرند، بر این اساس حساب ها به دو سطح تقسیم می‌شوند.

Final Cluster Centers

	Cluster	
	۱	۲
count	۵۶	۶۵
sum	۳۰۰۰۰۰۰۰	۷
	۰	۰۰۰۰۰۰۰۰

Number of Cases

in each Cluster

Cluster		
	۱	۳۹۷.۰۰۰
	۲	۱.۰۰۰
	Valid	۳۹۸.۰۰۰
	Missing	.۰۰۰

شکل (۲) مراکز خوشه ها در خوشه بندی تراکنش های هر حساب

شکل (۲) به عنوان مثال خوشه بندی تراکنش‌ها برای هر حساب را نشان می‌دهد. همانطور که می‌بینید داده ها به خوشه تبدیل شده اند، مراکز هر خوشه در واقع میانگین اعضای آن خوشه هستند. سعی می‌کنیم با توجه به پارامتر ها، به هر خوشه یک سطح فعالیت نسبت دهیم. برای تعیین سطح فعالیت هر خوشه، راه حل پیشنهادی محاسبه عبارت زیر برای هر خوشه است:

$$y = Sum + Count$$

حاصل عبارت فوق برای هر کدام از خوشه‌ها که بیشتر بود آن خوشه، سطح بالاتری خواهد داشت.

$$y_1 = ۳۰۰۰۰۰۰۵۶ \quad , \quad y_2 = ۷۰۰۰۰۰۰۰۶۵$$

با توجه به مقادیر می‌توان به افراد متعلق به خوشه‌ی یک، سطح فعالیت ۱ و به افراد خوشه‌ی دو، سطح فعالیت ۲ را نسبت داد. حال با توجه به اینکه در هنگام افتتاح حساب نیز به هر حساب یک سطح مورد انتظار برای فعالیت مشخص شده، اگر سطح نسبت داده شده در الگوریتم با سطح فعالیت مورد انتظار، متفاوت بود به این معنی است که شخص فعالیتی خارج از سطح مورد انتظار انجام داده و این مسئله برای بررسی بیشتر باید گزارش داده شود.. در این مرحله از تحقیق با استفاده از تکنیک داده کاوی k-means مشتریان بانک را در دو دسته مشتریان مشکوک به پولشویی و مشتریان عادی طبقه بندی نمودیم. به این صورت مشتریان مربوط به خوشه ۳ شامل ۳۹۷ مشتری به عنوان موارد مشتری های مشکوک به پولشویی شناخته شدند. همچنین مشتری های خوشه ۱، ۲ که شامل ۸۴۰ مشتری هستند به عنوان مشتریان عادی در نظر گرفته می‌شوند.

بخش سوم: کشف موارد مشکوک به پولشویی و تامین مالی تروریسم با استفاده از روش شبکه عصبی

در بخش قبل مشتریان بانک تجاری مورد مطالعه در سه خوشه دسته بندی شدند و مشتریان خوشه ۳ دارای ریسک بالای برای پولشویی بودند. در این بخش مشتریان خوشه ۳ را به عنوان مشتریان مشکوک به پولشویی و خوشه ۱ و ۲ را مشتریان عادی در نظر گرفته می شود و به یافتن الگویی برای کشف موارد مشکوک به پولشویی و تامین مالی تروریسم با استفاده از روش شبکه عصبی پرداخته می شود. به اینصورت که طبقه مشتریان (تعیین شده در بخش قبل) را به عنوان خروجی و شاخص های ۱۰ گانه بانک مرکزی را به عنوان ورودی ها در این الگوریتم ها در نظر گرفته می شوند. تمامی این الگوریتم ها توسط نرم افزار Nero solutions بر روی مجموعه مشتریان اجرای می شوند. به منظور مقایسه عملکرد الگوریتم های شبکه عصبی از دو روش رایج استفاده می شود. روش اول مبتنی بر بررسی ضریب تبیین می باشد که رابطه زیر شیوه محاسبه آن را نشان می دهد(زینوزیان[۱]، ۲۰۱۱).

$$R^2 = 1 - \left[\frac{\sum_{i=1}^{n} \left(p_{ANN,i} - p_{\exp,\, i} \right)^2}{\sum_{i=1}^{n} \left(\overline{p}_{ANN,i} - p_{\mathrm{ANN},\, i} \right)^2} \right]$$

P_{ANN} = مقدار پیش بینی برای پارامترهای خروجی از شبکه

P_E = عبارتست ازمقادیر داده های تجربی حاصل از آزمایش است.

[۱] Zenoozian

روش دوم بررسی میانگین مجذور خطا است که دقت و اعتبار دسته های آموزشی و آزمونی را اندازه گیری می نماید و از طریق رابطه زیر محاسبه می شود.

$$MSE = \frac{\sum_{i=1}^{N} \left(p_{ANN,i} - p_{\exp,\, i} \right)^2}{N}$$

همچنین برای ارزیابی مدل های شبکه های عصبی از مدل‌های ضریب همبستگی(R) و میانگین خطای مطلق(MAE) و بعنوان یک معیار کمی برای سنجش دقت مدل‌های شبکه های عصبی استفاده می‌شود(فقیه،۱۳۸۹). ضریب همبستگی میزان همبستگی بین مقادیر برآورده شده توسط مدل و مقادیر واقعی می باشدو مقدار این ضریب همواره بین صفر ویک قرار داشته و هرچه مقدار آن به یک نزدیکتر باشد، نشان دهنده عملکرد بهتر مدل شبکه عصبی می باشد و از طریق رابطه زیر محاسبه می شود.

$$R = \frac{\sum_{i=1}^{n} (x_i - x^-)(N_i - N^-)}{\sqrt{\sum_{i-1}^{n} (x_i - x^-)^2} \ \sqrt{\sum_{i=1}^{n} (N_i - N^-)^2}}$$

مقدار میانگین خطای مطلق از صفر تا بینهایت تغییر می کند و هرچه مقدار میانگین خطای مطلق کمتر و به صفر نزدیک باشد، نشان دهنده عملکرد بهتر مدل شبکه عصبی می باشد و از طریق رابطه زیر محاسبه می شود:

$$MAE = \frac{\sum_{i=1}^{n} \left| (y_{est})_i - (y_{obs})_i \right|}{n}$$

با استفاده از معیار های فوق الگوریتم بهینه برای شناسایی موارد مشکوک به پولشویی ارائه می شود. در اینجا نرون خروجی را خوشه مشتری (خوشه ۱، ۲ و ۳) و نرون ورودی را معیارهای ده گانه تشکیل می دهد. ماتریس ورودی در ابعاد ۱۲۳۷*۱۰ و ماتریس خروجی در ابعاد ۱۲۳۷*۱ می باشد. برای تصمیم‌گیری در مورد زمان متوقف ساختن آموزش، داده‌ها به صورت تصادفی به سه مجموعه تقسیم شد، ۷۰ درصد داده های مورد نظر برای آموزش شبکه، ۱۵ درصد برای صحت سنجی شبکه و ۱۵ درصد بقیه نیز برای آزمایش شبکه تحصیص داده شد. در این قسمت مشتریان توسط شبکه های عصبی مصنوعی پرسپترون چند لایه (MLP)، توابع شعاعی پایه (RBF)، نگاشت خود سازمانده (SOM) و بردار ماشین پشتیبان (SVM) با نرم افزار Neuro Solutions و با الگوریتم های آموزشی مومنتوم، گرایان نزولی و لورنبرگ-مارکوارت با تابع انتقال سیگموئید و هایپربولیک با یک مخفی و با نرون های متفاوت آموزش و آزمایش شد و پس از اعمال الگوهای مختلف و آموزش شبکه بهترین الگو از میان الگوها انتخاب شد. معیار انتخاب، شبکه‌ای است که بهترین آموزش را دیده ، کمترین میانگین مجذور خطا (MSE) را داشته و نتایج قابل قبولی ارائه داده باشد. البته در انتخاب شبکه باید به وقوع پدیده بیش پردازش نیز دقت داشته باشیم زیرا در آزمون هایی که خطا به مقدار زیادی به صفر نزدیک شود شبکه تعمیم دهی قابل قبولی نخواهد داشت.

در ابتدا ماتریس داده ها، توسط شبکه عصبی پرسپترون چند لایه با مقدار epochs =۱۰۰۰ ، با توابع انتقال تانژانت هایپربولیک و سیگموئید و با قانون آموزشی ممنتم که برای تعیین مناسب‌ترین مقدار ممنتم مدل های مختلف شبکه عصبی، که در آنها مقدار ممنتم (۰.۱و۰.۲و۰.۳و۰.۴و۰.۵و۰.۶و۰.۷و۰.۸و۰.۹) در نظر گرفته شده و همچنین با گرایان نزولی و لورنبرگ-مارکوارت مورد آزمایش و آموزش قرار گرفت، که نتایج این تحلیل در ادامه آورده شده است. ابتدا به انتخاب بهترین ساختار در پرسپترون چند لایه می پردازیم، که مقادیر به دست آمده برای آن در جدول (۳) آورده شده است.

جدول (۳) آزمون سعی و خطا برای انتخاب بهترین ساختار برای پرسپترون چند لایه

ساختار	نوع شبکه	تابع انتقال	قانون آموزش	مقدار ممنتم	Test			
					MSE	سطح اطمینان	MAE	R
R۱	MLP	TAN	ممنتم	۰/۱	۰/۰۵۸۹۸۰۶۴	۰/۹۴۱۰۱۹۳۶	۰/۲۱۶۱۱۶٤٦	۰/۰۲۷۷۰۸۳۷
R۲		TAN		۰/۲	۰/۰۵۳۳۹۲۱۲	۰/۹۴۶۶۰۷۸۸	۰/۲۰۳٦۹٦۹٦	۰/۱۹۲٦٦۷۰۹
R۳		TAN		۰/۳	۰/۰۵۸۶۴۲۱۷	۰/۹۴۱۳۵۷۸۳	۰/۲۱۰۸۹٤۱۹	۰/۰۷۰۱۳۱۸۸
R٤		TAN		۰/۴	۰/۰۵۸۶۴۷۷۸	۰/۹۴۱۳۵۲۲۲	۰/۲۱۳٤۰۳٦	۰/۰٤۷۸۳٤٦۷
R٥		TAN		۰/۵	۰/۰۵۶۵۳۵۴۲	۰/۹۴۳۴۶۴۵۸	۰/۲۰۸۸۸۹۷۸	۰/۰٥٥٥۷۳۸۱
R٦		TAN		۰/۶	۰/۰۵۹۷۵۷۷۸	۰/۹۴۰۲۴۲۲۲	۰/۲۱۷۲۳٤٥۹	۰/۰٤۱۲۸۲٤
R۷		TAN		۰/۷	۰/۰۵۵۰۹۰۶۳	۰/۹۴۴۹۰۹۳۷	۰/۲۰٥۱۹۹۷۱	۰/۱۰۷٦۸۰٦٥
R۸		TAN		۰/۸	۰/۰۵۴۰۶۹۲	۰/۹۴۵۹۳۰۸	۰/۲۰٥۷۹۱٦٥	۰/۱۹٦۰۳٥۹٤

R۹		TAN		۰/۹	۰/۰۵۴۳۶۹۱۷	۰/۹۴۵۶۳۰۸۳	۰/۲۰۶۳۵۱۸۳	۰/۱۸۳۰۷۵۸۲
R۱۰		TAN	گرادیان نزولی		۰/۰۵۴۲۶۱۵۲	۰/۹۴۵۷۳۸۴۸	۰/۱۹۸۹۸۹۰۷	۰/۰۵۸۶۵۰۸۲
R۱۱		TAN	لورنبرگ و مارکوات		۰/۰۵۹۸۳۲۲۵	۰/۹۴۰۱۶۷۷۵	۰/۲۱۵۸۸۲۵٤	۰/۲۱۷٦۹٤۲۵
R۱۲		SIG	ممنتم	۰/۱	۰/۱۰۷۶۳۴۹۸	۰/۸۹۲۳۶۵۰۲	۰/۲۹٦۲۱۸۲۱	۰/۲٤٦۲۱۱۸٤
R۱۳		SIG		۰/۲	۰/۱۰۵۲۱۷۶۳	۰/۸۹۴۷۸۲۳۷	۰/۲۹۲۹۱۹۳۲	۰/۲۳۷۷۳۲٤۸
R۱٤		SIG		۰/۳	۰/۰۶۹۰۸۶۸۵	۰/۹۳۰۹۱۳۱۵	۰/۲۳٤٤۳٤۵۸	۰/۱۲۵٦۰۹۵۳
R۱۵		SIG		۰/۴	۰/۰۵۶۷۱۳۳۸	۰/۹۴۳۲۸۶۶۲	۰/۲۱۱۹۵۲۷۵	۰/۲۸۷۹۰۰۲٤
R۱٦		SIG		۰/۵	۰/۰۵۵۲۹۱۶۹	۰/۹۴۴۷۰۸۳۱	۰/۲۰۸٦۲۳۳۹	۰/۲۸۵٦۸۷۹۱
R۱۷		SIG		۰/۶	۰/۰۵۵۵۶۵۶۸	۰/۹۴۴۴۳۴۳۲	۰/۲۰۹۵۳۲۰۵	۰/۳۰۹۲۷٤۷۸
R۱۸		SIG		۰/۷	۰/۰۵۲۵۲۵۷۲	۰/۹۴۷۴۷۴۲۸	۰/۲۰۲۲۰۱۲۹	۰/۳۰۹۳٦۱۱۳
R۱۹		SIG		۰/۸	۰/۰۵۰۱۳۷۴۶	۰/۹۴۹۸۶۲۵۴	۰/۱۹۵۵۱۲۲۵	۰/۳۱٦۵۷۲۸۱
R۲۰		SIG		۰/۹	۰/۰۵۱۲۸۹۶	۰/۹۴۸۷۱۰۴	۰/۱۹۷۹۹۷٤۹	۰/۲۸۱٤٤۷۰۳
R۲۱		SIG	گرادیان نزولی		۰/۰۵۵۵۴۷۵۶	۰/۹۴۴۴۵۲۴۴	۰/۲۰٦۹٤۸۲۹	۰/۱۱۲۲۵۷٦۷
R۲۲		SIG	لورنبرگ و مارکوات		۰/۰۵۵۷۹۰۷۷	۰/۹٤٤۲۰۹۲۳	۰/۲۰۷۱٦۰۹٤	۰/۱۲۳٦۱۳۲۱

بهترین ساختار برای شبکه عصبی زمانی است که مجذر توان دوم خطا یعنی MSE آن کمترین مقدار یا سطح اطمینان آن بالاترین مقدار باشد، که با توجه به جدول فوق این ساختار مربوط R۱۹ با تابع انتقال سیگموید با قانون آموزش ممنتم ۰/۸ و با مقدار MSE=۰,۰۵۰۱۳۷٤٦ و با سطح اطمینان ۰/۹۴۹ و همچنین با ضریب همبستگی۰.۳۱۶ =R و میانگین قدر مطلق خطا MAE=۰,۱۹۵ است.

در ادامه از شبکه عصبی تابع شعاعی پایه (RBF) با مقدار epochs =۱۰۰۰، با توابع انتقال تانژانت هایپربولیک و سیگموئید و با قانون آموزشی ممنتم (۰.۱و۰.۲و۰.۳و۰.۴و۰.۵و۰.۶و۰.۷و۰.۸و۰.۹)، گرایان نزولی و لورنبرگ-مارکوارت مورد آزمایش و آموزش قرار گرفت، که مقادیر به دست آمده برای آن در جدول (۴) آورده شده است.

جدول (۴) آزمون سعی و خطا برای انتخاب بهترین ساختار برای تابع شعاعی پایه

ساختار	نوع شبکه	تابع انتقال	قانون آموزش	مقدار ممنتم	Test			
					MSE	سطح اطمینان	MAE	R
R۱	RBF	TAN	ممنتم	۰/۱	۰/۰۵۱۰۳۹۹۲	۰/۹۴۸۹۶۰۰۸	۰/۱۹۲۸۹۴۲۳	۰/۶۵۶۲۱۸۴۹
R۲		TAN		۰/۲	۰/۰۴۹۷۵۹۲۹	۰/۹۵۰۲۴۰۷۱	۰/۱۹۰۵۱۸۰۶	۰/۶۷۱۶۴۹۱۵
R۳		TAN		۰/۳	۰/۰۵۱۱۴۵۰۱	۰/۹۴۸۸۵۴۹۹	۰/۱۹۱۵۸۲۸۲	۰/۶۹۳۹۹۱۶۳
R٤		TAN		۰/۴	۰/۰۵۲۸۲۶۵۷	۰/۹۴۷۱۷۳۴۳	۰/۱۹۵۹۹۰۴	۰/۶۴۷۸۱۵۸۷
R٥		TAN		۰/۵	۰/۰۴۹۸۱۹۷۵	۰/۹۵۰۱۸۰۲۵	۰/۱۸۵۰۳۸۹۴	۰/۵۹۰۴۰۳۳۹
R٦		TAN		۰/۶	۰/۰۴۹۸۸۴۱۳	۰/۹۵۰۱۱۵۸۷	۰/۱۹۲۰۵۲۸۵	۰/۶۳۱۵۲۱۲۹

R۷		TAN		۰/۷	۰/۰۴۶۰۶۴۶۱	۰/۹۵۳۹۳۵۳۹	۰/۱۷۳۵۰۱۸۱	۰/۶۰۳۱۵۲۹۲
R۸		TAN		۰/۸	۰/۰۵۱۷۳۹۹۴	۰/۹۴۸۲۶۰۰۶	۰/۱۹۳۰۶۳۸۹	۰/۶۵۹۴۴۴۳۲
R۹		TAN		۰/۹	۰/۰۴۸۲۲۷۵۵	۰/۹۵۱۷۷۲۴۵	۰/۱۸۴۸۸۷۴۹	۰/۶۹۱۸۹۸۷
R۱۰		TAN	گرادیان نزولی		۰/۰۴۹۳۲۹۸۹	۰/۹۵۰۶۷۰۱۱	۰/۱۹۱۴۶۳۲۲	۰/۲۸۵۴۱۷۲
R۱۱		TAN	لورنبرگ و مارکوات		۰/۰۶۱۹۸۱۷۶	۰/۹۳۸۰۱۸۲۴	۰/۲۲۲۷۵۵۲۳	-۰/۰۲۲۶۹۶۷۴
R۱۲		SIG		۰/۱	۰/۰۷۲۱۰۸۶۳	۰/۹۲۷۸۹۱۳۷	۰/۲۳۶۴۶۷۹۳	-۰/۳۶۲۶۸۹۹۷
R۱۳		SIG		۰/۲	۰/۰۷۲۳۹۴۰۸	۰/۹۲۷۶۰۵۹۲	۰/۲۳۷۱۴۰۱۴	-۰/۵۸۰۳۲۸۰۵
R۱٤		SIG		۰/۳	۰/۰۷۱۲۱۵۰۳	۰/۹۲۸۷۸۴۹۷	۰/۲۳۴۸۶۹۴۴	۰/۶۱۷۴۴۵۹۶
R۱۵		SIG		۰/۴	۰/۰۷۱۷۸۱۰۱	۰/۹۲۸۲۱۸۹۹	۰/۲۳۵۷۲۵۹۳	۰/۴۲۹۴۹۳۷
R۱٦		SIG	ممنتم	۰/۵	۰/۰۷۲۲۱۸۸۲	۰/۹۲۷۷۸۱۱۸	۰/۲۳۶۴۹۶۳۵	-۰/۲۷۷۵۵۱۲۲
R۱۷		SIG		۰/۶	۰/۰۷۲۴۵۲۷۵	۰/۹۲۷۵۴۷۲۵	۰/۲۳۷۳۶۸۱۵	-۰/۴۹۰۵۷۷۰۸
R۱۸		SIG		۰/۷	۰/۰۷۱۴۰۳۵۲	۰/۹۲۸۵۹۶۴۸	۰/۲۳۵۰۷۱۴۴	۰/۷۱۵۰۲۷۹۲
R۱۹		SIG		۰/۸	۰/۰۷۱۶۶۱۹۲	۰/۹۲۸۳۳۸۰۸	۰/۲۳۵۷۸۳۹۶	-۰/۲۳۴۹۸۱۰۹
R۲۰		SIG		۰/۹	۰/۰۷۵۴۲۶۶۶	۰/۹۲۴۵۷۳۳۴	۰/۲۳۶۶۳۰۶۴	۰/۳۰۰۱۰۷۹۳
R۲۱		SIG	گرادیان نزولی		۰/۰۵۶۵۳۵۷	۰/۹۴۳۴۶۴۳	۰/۲۰۴۷۱۸۰۹	۰/۱۲۹۶۴۶۹۲
R۲۲		SIG	لورنبرگ و مارکوات		۰/۰۵۸۸۳۷۹۱	۰/۹۴۱۱۶۲۰۹	۰/۲۱۰۷۳۱۲	۰/۱۲۳۲۴۶۸۹

با توجه به جدول (۴) بهترین ساختار برای تابع شعاعی پایه مربوط به RV با تابع انتقال تانژانت هایپربولیک با آموزش ممنتم ۰/۷ می باشد که در آن میانگین مجذور خطا برابر MSE=۰/۰٤٦۰٦٤٦۱ و سطح اطمینان ۰/۹۵۳ و همچنین با ضریب همبستگی۰.۶۰۳ =R و میانگین قدر مطلق خطا MAE=۰,۱۷۳ می باشد.

توابع انتقال تانژانت هایپربولیک و سیگموئید و با قانون آموزشی ممنتم (۰.۱و۰.۲و۰.۳و۰.۴و۰.۵و۰.۶و۰.۷و۰.۸و۰.۹)، گرایان نزولی و لورنبرگ- مارکوارت مورد آزمایش و آموزش قرار گرفت، که نتایج آن در جدول (۶) آورده شده است. با توجه به جدول (۵) بهترین ساختار برای شبکه عصبی نگاشت خودسازمانده(SOM) مربوط به ساختار R۹ می باشد که در آن تابع انتقال، تانژانت هایپربولیک و قاعده آموزش ممنتم ۰/۹ می باشد و همچنین میانگین مجذور خطا برابر MSE=۰/۰٤۲۱۷٤٦۳ ، سطح اطمینان ۰/۹۵۷ ، ضریب همبستگی۰.۶۵۴ =R و میانگین قدر مطلق خطا MAE=۰,۱۷۱ می باشد.

جدول (۵) آزمون سعی و خطا برای انتخاب بهترین ساختار برای نگاشت خودسازمانده

ساختار	نوع شبکه	تابع انتقال	قانون آموزش	مقدار ممنتم	Test			
					MSE	سطح اطمینان	MAE	R
R۱	SOM	TAN	ممنتم	۰/۱	۰/۰۴۹۸۸۴۹۹	۰/۹۵۰۱۱۵۰۱	۰/۱۹۱۵۳۵۶۳	۰/۶۶۸۷۲۲۸۹
R۲		TAN		۰/۲	۰/۰۵۴۱۱۳۵	۰/۹۴۵۸۸۶۵	۰/۱۹۷۳۹۵۶۱	۰/۵۳۳۲۷۳۹۹
R۳		TAN		۰/۳	۰/۰۵۷۰۱۱۳۲	۰/۹۴۲۹۸۸۶۸	۰/۲۰۷۳۶۸۶۴	۰/۶۱۳۷۷۱۳۳
R٤		TAN		۰/۴	۰/۰۵۷۱۶۵۳۷	۰/۹۴۲۸۳۴۶۳	۰/۲۰۶۰۴۳۴۶	۰/۵۳۵۹۷۸۹۱
R٥		TAN		۰/۵	۰/۰۴۶۳۲۸۷۷	۰/۹۵۳۶۷۱۲۳	۰/۱۸۳۵۲۰۲۷	۰/۶۵۹۵۶۹۷۴
R٦		TAN		۰/۶	۰/۰۴۹۶۶۵۱۶	۰/۹۵۰۳۳۴۸۴	۰/۱۸۷۳۰۹۶۷	۰/۶۱۵۰۱۴۴
R۷		TAN		۰/۷	۰/۰۵۸۲۰۲۰۱	۰/۹۴۱۷۹۷۹۹	۰/۲۰۷۷۹۷۸۵	۰/۴۹۹۹۱۸۲۱
R۸		TAN		۰/۸	۰/۰۵۹۹۰۶۱۴	۰/۹۴۰۰۹۳۸۶	۰/۲۱۱۹۰۸۶۱	۰/۴۴۸۷۲۷۱۳
R۹		TAN		۰/۹	۰/۰۴۲۱۷۴	۰/۹۵۷۸۲۵	۰/۱۷۱۱۹۹	۰/۶۵۴۵۳۲۴
R۱۰		TAN	گرادیان نزولی		۰/۰۶۶۴۸۱۵۷	۰/۹۳۳۵۱۸۴۳	۰/۲۲۵۷۹۴۱۵	-۰/۱۲۳۶۱۵۸۲
R۱۱		TAN	لورنبرگ و مارکوات		۰/۰۷۶۶۸۴۷۴	۰/۹۲۳۳۱۵۲۶	۰/۲۴۹۹۸۵۷۸	-۰/۰۱۴۴۲۷۷۹
R۱۲		SIG	ممنتم	۰/۱	۰/۰۶۹۶۹۵۲۱	۰/۹۳۰۳۰۴۷۹	۰/۲۳۱۶۶۳۸۸	۰/۵۳۷۶۹۹۷۷
R۱۳		SIG		۰/۲	۰/۰۵۹۱۳۵۲۶	۰/۹۴۰۸۶۴۷۴	۰/۲۱۱۷۴۵۱۲	۰/۶۹۵۰۲۷۴۲
R۱٤		SIG		۰/۳	۰/۰۵۴۷۱۱۰۱	۰/۹۴۵۲۸۸۹۹	۰/۲۰۱۸۴۱۳۴	۰/۶۸۶۵۵۷۳۷
R۱٥		SIG		۰/۴	۰/۰۵۲۱۵۲۸۶	۰/۹۴۷۸۴۷۱۴	۰/۱۹۵۸۶۵۲۴	۰/۶۸۳۸۴۸۷۲
R۱٦		SIG		۰/۵	۰/۰۵۵۹۵۱۱۲	۰/۹۴۴۰۴۸۸۸	۰/۲۰۴۲۲۱۳۸	۰/۶۸۲۹۲۰۲۸

R۱۷		SIG		۰/۶	۰/۰۵۱۱۳۷۵۱	۰/۹۴۸۸۶۲۴۹	۰/۱۹۴۰۴۲۲	۰/۶۸۹۸۲۰۵۷
R۱۸		SIG		۰/۷	۰/۰۵۰۷۹۶۶۳	۰/۹۴۹۲۰۳۳۷	۰/۱۹۳۴۷۵۳۶	۰/۶۹۰۶۵۴۰۶
R۱۹		SIG		۰/۸	۰/۰۵۱۳۹۱۱۵	۰/۹۴۸۶۰۸۸۵	۰/۱۹۴۶۸۷۵۶	۰/۶۷۹۸۰۶۲
R۲۰		SIG		۰/۹	۰/۰۵۲۰۵۹۱۸	۰/۹۴۷۹۴۰۸۲	۰/۱۹۷۱۷۸۲۹	۰/۶۵۶۳۴۸۷۸
R۲۱		SIG	گرادیان نزولی		۰/۰۶۴۲۱۶۰۷	۰/۹۳۵۷۸۳۹۳	۰/۲۲۳۸۷۴۱۶	-۰/۲۶۳۲۶۸۰۵
R۲۲		SIG	لورنبرگ و مارکوات		۰/۰۵۷۷۹۹۱۳	۰/۹۴۲۲۰۰۸۷	۰/۲۱۲۶۱۰۵۶	-۰/۰۳۰۶۲۲۳۵

همچنین تحلیل مشابهی برای شبکه عصبی بردار ماشین پشتیبان (SVM) با مقدار epochs ۱۰۰۰= مورد آزمایش و آموزش قرار گرفت، که نتایج آن در جدول (۶) آورده شده است.

جدول (۶) آزمون سعی و خطا برای انتخاب بهترین ساختار برای بردار ماشین پشتیبان

ساختار	نوع شبکه	Test			
		MSE	سطح اطمینان	MAE	R
R۱	SVM	۰/۰۶۱۲۹۲۷۳	۰/۹۳۸۷۰۷۲۷	۰/۲۰۷۱۱۲۹۹	۰/۰۸۹۳۵۲۶۲

با توجه به جدول (۶) برای روش ماشین بردار پشتیبان(SVM) مقدارمیانگین مجذور خطا برابر MSE=۰,۰۶۱۲۹۲۷۳ ، سطح اطمینان برابر ۰/۹۳۸ ، ضریب همبستگی۰.۰۸۹۳ =R و میانگین قدر مطلق خطا MAE=۰, ۲۰۷ می باشد.

در نهایت با توجه به نتایج به دست آمده از انواع شبکه ها، بهترین ساختار شبکه به عنوان شبکه عصبی بهینه انتخاب می شود. این شبکه باید کمترین مجذر توان دوم خطا یعنی MSE را داشته، یا سطح اطمینان آن بیشترین باشد. با توجه به نتایج این جدول ها شبکه عصبی نگاشت خودسازمانده با تابع انتقال تانژانت هیپربولیک و با قاعده آموزشی ممنتم ۰/۹ در تدوین مدل‌ها

عملکرد بهتری نسبت به تابع سیگموئید داشت.شبکه عصبی نگاشت خودسازمانده با تابع انتقال تانژانت هیپربولیک و با مقادیر میانگین مجذور خطا برابر MSE=۰/۰٤۲۱۷٤٦۳ ، سطح اطمینان ۰/۹۵۷ ، ضریب همبستگی R= ۰.۶۵۴ و میانگین قدر مطلق خطا MAE=۰,۱۷۱ به عنوان بهینه‌ترین الگوریتم هوش مصنوعی برای شناسایی موارد مشکوک به پولشویی استفاده می شود که در جدول(۷) ارائه شده است.

جدول (۷) بهینه‌ترین الگوریتم هوش مصنوعی جهت شناسایی موارد مشکوک به پولشویی

ساختار	نوع شبکه	تابع انتقال	قانون آموزش	مقدار ممنتم	Test			
					MSE	سطح اطمینان	MAE	R
R۹	SOM	TAN	ممنتم	۰/۹	۰/۰۴۲۱۷۴۶۳	۰/۹۵۷۸۲۵	۰/۱۷۱۱۹۹	۰/۶۵۴۵۳۲۴

همانطور که از جدول(۷) می بینید، نتایج به دست آمده از روش پیشنهادی دارای صحت اجرای بالای ۹۵ درصد می باشد. با این اوصاف یک الگو برای کشف موارد مشکوک به پولشویی وتامین مالی تروریسم ارائه گردید. به اینصورت که برای کشف موارد مشکوک به پولشویی از الگوریتم بهینه شبکه عصبی نگاشت خودسازمانده با تابع انتقال تانژانت هیپربولیک استفاده می شود. زیرا در تشخیص موارد مشکوک به پولشویی بالاترین صحت تشخیص را دارد.

بحث و نتیجه گیری

در این پژوهش با تلفیق دو تکنیک داده کاوی و هوش مصنوعی به تحلیل و شناسایی موارد مشکوک به پولشویی و تامین مالی تروریسم پرداخته شد. ابتدا به کمک تکنیک داده کاوی، مشتریان بانک در جامعه آماری مورد مطالعه در سه خوشه دسته بندی شدند و مشتریان خوشه ای که دارای ریسک بالای پولشویی بود به عنوان موارد مشکوک به پولشویی و تامین مالی تروریسم شناسایی نمودیم در ادامه از تکنیک هوش مصنوعی استفاده شد و نشان دادیم الگوریتم شبکه عصبی نگاشت خودسازمانده با تابع انتقال تانژانت هیپربولیک بهترین روش برای کشف موارد مشکوک به پولشویی و تامین مالی تروریسم است. همچنین صحت اجرای الگوریتم شبکه عصبی نگاشت خودسازمانده با تابع انتقال تانژانت هیپربولیک برابر ٪۹۵/۷۸ بوده که به نسبت مقدار بالایی می باشد. در ادامه از تکنیک داده کاوی به ویژه روش k-means استفاده و مشتریان بانک در سه خوشه دسته بندی شد. خوشه سوم دارای بالاترین ریسک پولشویی نسبت به خوشه های دیگر است. مشتریان این خوشه به عنوان موارد مشکوک به پولشویی و تامین مالی تروریسم شناسایی شدند.

روش های شبکه عصبی مورد استفاده در این تحقیق جز روش های یادگیری می باشند. به اینصورت که باید داده های اولیه موجود باشد تا با آموزش به وسیله داده های موجود بتوان الگو طبقه بندی را کشف نمود. پس در این تحقیق از بین ۱۲۳۷ مشتری مورد مطالعه تعداد ۳۹۷ مشتری به عنوان موارد مشتری های مشکوک به پولشویی وتعداد ۸۴۰ مشتری به عنوان مشتری عادی در نظر گرفته شدند. در ادامه از روش های هوش مصنوعی به ویژه از الگوریتم های پرسپترون چندلایه(MLP)، تابع شعاعی پایه ای(RBF)، نگاشت خودسازمانده (SOM) و ماشین بردار پشتیبان (SVM) استفاده و موارد مشکوک به پولشویی و تامین مالی تروریسم را

شناسایی نمودند. بعد از آموزش و آزمایش این الگوریتم ها، نگاشت خودسازمانده با تابع انتقال تانژانت هیپربولیک و با قاعده آموزش ممنتم ۰/۹ نسبت به سایر الگوریتم های مورد بررسی بوده نتایج درست تری ارائه نمود به طوریکه این الگوریتم در سطح اطمینان ۷۸٪/۹۵ موارد مشکوک به پولشویی را تشخیص داد.

پژوهشگرانی در سالهای گذشته بر موضوعات مشابه ای تحقیقاتی انجام داده اند که به تعدادی از آنها و نتایج بدست آمده اشاره می کنیم. فرخیان و چاله چاله (۱۳۹۸) در تحقیقی با عنوان "کشف تراکنش های مشکوک به پولشویی بر اساس الگوی بافتاریِ حسابهای بانکی" به تشخیص تراکنش های مشکوک به پول شویی پرداختند. جامعه آماری تحقیق شامل ۱/۸ میلیون تراکنشِ ۱۰۰۸ نفر، طی مدت ۶ سال از ۴۸ بافت مختلف می باشد که به روش شبیه سازی رایانه ای ایجاد شده است. نتایج تحقیق آن ها نشان می دهد که بیانگر نرخ ۱۰۰ ٪ پیش بینی درستِ تراکنش های مشکوک به پولشویی و نرخ ۱/۱۴ ٪ پیش بینی غلطِ تراکنش های عادی به عنوان مشکوک به پولشویی می باشد. حقی و همکاران (۱۴۰۰) در تحقیقی با عنوان " عوامل زیرساختی مدیریت چالش‌های مبارزه با پولشویی در نظام بانکی ایران و برآورد الگوی مبتنی بر رهنمودهای بین‌المللی" به شناسایی مجموعه‌ای از عوامل زیرساختی در مبارزه با پولشویی در ایران پرداختند. یافته‌های پژوهش آن ها حاکی از این است که به کارگیری نظام‌مند الگوی زیرساختی برمبنای رهنمودهای بین‌المللی شامل ابعاد کارکردی، زمینه‌ای و ساختاری موجب بهبود کارایی سیستم مبارزه با پولشویی و مدیریت بهینه چالش‌های مبارزه با پولشویی در بانک‌ها می‌گردد. لک، جمشید و همکاران(۱۴۰۲) در تحقیقی با عنوان " ارائه مدل احتمال وقوع پولشویی بر مبنای ویژگی های کیفی گزارشگری مالی" به بررسی تاثیر کیفیت گزارشگری مالی بر احتمال وقوع پولشویی در شرکتهای تولیدی پذیرفته شده در

بورس اوراق بهادار تهران پرداختند. نتایج بررسی ها نشان داد که افزایش کیفیت گزارشگری مالی موجب کاهش احتمال وقوع پولشویی می شود همچنین مشخص شد که ویژگی های کیفیت گزارشگری مالی شامل ارائه مفید اطلاعات موجبات کاهش احتمال وقوع پولشویی را فراهم می نمایند . کاظمی و همکاران (۱۴۰۱) در تحقیقی با عنوان "شناسایی فعالیت های پولشویی در معاملات مالی با استفاده از روش های داده کاوی، قانون بنفورد و الگوریتم GANs" از الگوریتم های داده کاوی به منظور کشف موارد مشکوک به پول شویی با استفاده از داده های واقعی تراکنش های بانکی یک بانک تجاری پرداختند. از دو رویکرد برای پیش بینی استفده نمودند. رویکرد اول حساب هایی که در تراکنش های آن ها موارد پرت(پولشویی) وجود دارد را با دقتی حدود ۹۳٪ درصد، و رویکرد دوم حساب های مشکوکی که در پنهان نمودن ارقام ساختگی در تراکنش های آن ها، از روش های حرفه ای استفاده نشده است را با دقتی حدود ۶۰٪ به درستی تشخیص دهد. اما در این تحقیق ابتدا با استفاده از دستورالعمل های بانک مرکزی برای شناسایی موارد مشکوک به پولشویی و تکنیک داده کاوی مشتریان بانک در نمونه آماری مورد مطالعه را در سه خوشه طیقه بندی نموده که یک خوشه به عنوان مشتریان مشکوک به پولشویی و دو خوشه دیگر به عنوان مشتریان عادی در نظر گرفته شدند. در مرحله بعد از روش هوش مصنوعی به ویژه پرسپترون چندلایه(MLP)، تابع شعاعی پایه ای(RBF)، نگاشت خودسازمانده (SOM) و ماشین بردار پشتیبان (SVM) به شناسایی موارد مشکوک به پولشویی و تامین مالی تروریسم پرداخته شد که بهینه ترین روش با درستی ۹۵/۷۸ درصد به تشخیص موارد می پردازد که به نسبت درصد قابل توجهی است. چه از روش اجرا و نمونه آماری مورد مطالعه نتایج تحقیق حاضر با نتایج تحقیقات قبلی متفاوت می باشد.

تمامی موارد مشکوک به پولشویی در این تحقیق در شهرهای پرخطر و افراد پرخطر از دیدگاه بانک می باشد، پس این موارد آیتمی مهم برای تشخیص موارد مشکوک به پولشویی می باشد. فقط نیمی از مشتریان بانک در طبقه مشکوک به پولشویی شامل دو معیار سابقه کیفری و مجوز افتتاح حساب بودند. پس این موارد تاثیری بر شناسایی موارد مشکوک به پولشویی ندارند همچنین تمامی موارد مشکوک به پولشویی در پژوهش حاضر دارای معرف بوده اند و این نشان می دهد که داشتن معرف تاثیری برای شناسایی موارد مشکوک به پولشویی ندارد. پیشنهاد می شود از سایر الگوریتم های داده کاوی و هوش مصنوعی برای مبارزه با پولشویی پرداخته و نتایج آن را با نتایج تحقیق حاضر مقایسه نمایند. همچنین برای مبارزه با پولشویی از روش های سری های زمانی برای تشخیص موارد پرت در داده استفاده و سپس از تکنیک داده کاوی و هوش مصنوعی استفاده نمود. روش تلفیقی داده کاوی و شبکه عصبی استفاده شده در تحقیق حاضر به منظور پولشویی الکترونیکی می تواند مورد استفاده قرار گردد. می توان برای کشف الگوهای رفتاری پولشویی و تامین مالی تروریسم از تحلیل شبکه و یادگیری ماشین استفاده کرد . می توان در تحقیقی به بررسی آثار و پیامدهای پولشویی در حسابهای بانک های ایران و به بررسی پولشویی و تامین مالی تروریسم بر سلامت رشد اقتصادی در ایران پرداخته شود. همچنین تاثیر بانکداری الکترونیک در شفافیت مالی تخصیص منابع، مقابله با پولشویی و تامین مالی تروریسم بررسی شود و نقش حسابرسی داخلی مبتنی بر ریسک در پیشگیری و مبارزه با پولشویی در شرکت های پذیرفته شده در بورس بررسی شود و در نهایت تحقیقی با عنوان شناسایی و اولویت بندی عوامل تاثیرگذار بر پولشویی با رویکرد تحلیل سلسله مراتبی انجام شود. در فرایند پژوهش با محدودیت هایی مواجه بودیم که می توان به مواردی همچون فقدان پایگاه اطلاعاتی قابل اتکا و معتبر در زمینه پولشویی در ایران به عنوان

عمده ترین محدودیت این پژوهش اشاره کرد همچنین ممکن است اگر ابزار جمع آوری اطلاعات و بازه زمانی تحقیق تغییر کند، نتایج بدست آمده دستخوش مغایرت شود.

منابع و مآخذ

الف) منابع فارسی

۱. حقی، حسین علی و همکاران؛ (۱۴۰۰) عوامل زیرساختی مدیریت چالشهای مبارزه با پولشویی در نظام بانکی ایران و برآورد الگوی مبتنی بر رهنمودهای بین المللی، پژوهش‌های اقتصادی ایران، انتشارات دانشگاه علامه طباطبایی، دوره ۲۶

۲. سلیمان فلاح، امیرحسین؛ (۱۴۰۲) مبانی و اصول مبارزه بانکها و موسسات مالی و اعتباری با پولشویی در ایران. فصلنامه علمی مطالعات نوین بانکی. دوره ششم

۳. سرلک، ولی و همکاران؛ (۱۳۹۵) روشها و راهکارهای شناسایی تقلب مالی در بانکداری الکترونیک بااستفاده از داده کاوی، همایش ملی دانش و فن‌آوری مهندسی برق، کامپیوتر و مکانیک، ایران، تهران

٤. علی‌رمضانی، محمد؛ (۱۴۰۰) مطالعه و تحلیل جرم تامین مالی تروریسم و ارتباط آن با جرم پولشویی، دانشگاه آزاد اسلامی واحد رفسنجان

٥. عیسی‌آبادی، ابوالقاسم؛ (۱۴۰۲) بررسی پولشویی در نظام بانکی از منظر حقوق ایران و بین الملل

٦. فرخیان، علی و چاله چاله، عبداله؛ (۱۳۹۸) کشف تراکنشهای مشکوک به پولشویی بر اساس الگوی بافتاری حسابهای بانکی، دانش حسابرسی، سال نوزدهم، شماره ۷۴

۷. کاظمی، عالیه و همکاران (۱۴۰۱) شناسایی فعالیتهای پولشویی در تراکنشهای مالی با استفاده از روشهای داده کاوی، قانون بنفورد و الگوریتم GANs . اقتصاد پولی مالی

ب) منابع لاتین

۱. *Alhajeri, R., & Alhashem, A. (2023). Using Artificial Intelligence to Combat Money Laundering. Intelligent Information Management, 15(4), 284-305.*

۲. *Bakhos Douaihy, H., & Rowe, F. (2023). Institutional pressures and RegTech challenges for banking: The case of money laundering and terrorist financing in Lebanon. Journal of Information Technology, 02683962231152968*

۳. *Lopez-Rojas, E. A., & Axelsson, S. (۲۰۱۲). Multi agent based simulation (mabs) of financial transactions for anti money laundering (aml). In Nordic Conference on Secure IT Systems. Blekinge Institute of Technology.*

٤. *Mullo, J. I. H., & Baculima, V. H. Q. (2023). Comparative Study on Money Laundering and Terrorism Financing in Ecuador and Uruguay: A Critical Review. Remittances Review, 8(4)*

٥. *Prisznyák, A. (2022). Bankrobotics: Artificial Intelligence and Machine Learning Powered Banking Risk Management: Prevention of Money Laundering and Terrorist Financing. PÉNZÜGYI SZEMLE/PUBLIC FINANCE QUARTERLY, ٦٧(٢), ٢٨٨-٣٠٣.*

۶. *Robinson, J. (1996). The Laundrymen: inside money laundering, the world's third-largest business. Arcade Pub.*

۷. *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*