



هفتمین همایش سالانه
بانکداری الکترونیک
و نظام‌های پرداخت

تهران، مرکز همایش‌های بین‌المللی برج میلاد - ۲۰ و ۲۱ بهمن ۱۳۹۶

7th Annual Conference
on Electronic Banking
and Payment Systems

نواوری، بازیگران جدید و کارایی در کسب و کار مالی



طراحی سیستم کشف پولشویی

اعظم احمدیان

هیأت علمی گروه بانکداری، پژوهشکده پولی و بانکی

Azam_ahmadyan@yahoo.com

چکیده

امروزه با گسترش فن‌آوری اطلاعات در شبکه بانکی دنیا، جرم در این صنعت به صورت چشمگیری در حال افزایش است و هزینه‌های زیادی را به کسب و کارها تحمیل می‌کند. در نتیجه شناسایی جرم به مسأله بسیار مهمی تبدیل شده است. یکی از جرم‌هایی که منجر به ایجاد اختلال در عملکرد بانکها می‌شود، جرم پول‌شویی است. در واقع پدیده پول‌شویی مشهورترین تقلب در سطح بین‌المللی است که تلاش‌های گسترده‌ای در سطح بین‌الملل جهت کشف آن در حال انجام است. مبارزه با پدیده پول‌شویی در صنعت بانکداری بر اساس تجزیه و تحلیل و پردازش اظهارات در مورد معاملات مشکوک در سطح بانک‌های دنیا در حال انجام است. با وجود اینکه ممکن است، تعداد بسیار محدودی از معاملات در فرآیند پول‌شویی قرار گرفته باشند، اما تجزیه و تحلیل عملیات بانکی جهت کشف تقلب پول‌شویی توسط مؤسسات مالی نیاز به زمان طولانی دارند.

در همین راستا طراحی مکانیسمی که قادر به شناسایی جرم پول‌شویی باشد، دارای اهمیت است. تکنیک‌های شناسایی جرم پولشویی، علاوه بر آنکه تقلب‌ها و کلاهبرداری‌های صورت‌گرفته 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 تقلب در زمینه پول‌شویی را کاهش می‌دهد.

با توجه به اهمیت موضوع در این مقاله سعی شده است، بر اساس ضوابط بین‌المللی، مکانیسمی جهت شناسایی جرم پول‌شویی در شبکه بانکی کشور طراحی گردد. طراحی این مکانیسم بانکها را قادر خواهد ساخت قبل از وقوع جرم، احتمال وقوع آن را شناسایی کرده و مانع از رخداد پدیده پول‌شویی شوند.

کلمات کلیدی: جرم پولشویی، بانکداری الکترونیک، مکانیسم ضد پولشویی

۱. مقدمه

پدیده پولشویی فرآیندی است که در آن پول کثیف به صورت قانونی به پول تمیز تبدیل می‌شود. به واسطه پولشویی مجرمین سعی می‌کند پول‌هایی را که از فعالیت‌های مجرمانه بدست می‌آورند، با روش‌های قانونی به پول تمیز تبدیل کنند. امروزه فرآیند پولشویی سومین و بزرگترین تجارت در جهان بعد از مبادله ارزی و صنعت خودرو است. بنابراین شناسایی و پیش‌بینی آن دارای اهمیت است [1].



گسترش فناوری اطلاعات و توسعه ابزارهای الکترونیکی نقل و انتقال وجوه، رخداد پدیده پولشویی را برای مجرمین سهل‌تر نموده است. مؤسسات فنوری فناورانه‌های مالی با ریسک‌های مختلفی نظیر ریسک شهرت، ریسک عملیاتی و ریسک تمرکز و ریسک مقررات مواجه هستند. بکارگیری ابزارهای نوین بانکی، آنها را با ریسک پولشویی نیز مواجه ساخته است. همین امر موجب شده است، دولت‌ها نهاد‌های مالی را ملزم به شناسایی و کشف آن کنند. در این میان طراحی سیستم ضد پولشویی می‌تواند ضمن کشف پولشویی به ثبات مالی و امنیت بانک‌ها در سطح بین‌الملل کمک نماید. برای کشف پدیده پولشویی می‌توان از روش سنتی یا روش هوشمند استفاده نمود. روش سنتی فرآیند ضد پولشویی یک روش مبتنی بر انسان است که در این روش پدیده پولشویی کشف و شناسایی شده و از رخداد آن ممانعت می‌شود [2]. در مقابل ارزش داده‌های بانکی و تراکنش‌های بانکی با روش‌های مختلف افزایش یافته است و بکارگیری روش‌های سنتی برای کشف پولشویی زمان‌بر و پرهزینه بوده و گاهی اوقات غیر ممکن است. بنابراین روش‌هایی نیاز است که به صورت اتوماتیکی جرم پولشویی را کشف نماید [3].

در همین راستا دولت‌ها و مجامع بین‌المللی نیز تأکید بر طراحی مکانیسم کشف پولشویی در نهاد‌های مالی دارند. بر اساس توصیه شماره ۱۵ از توصیه‌های چهارگانه گروه ویژه اقدام مالی ۱، کشورها و مؤسسات مالی ملزم به شناسایی و ارزیابی ریسک‌های پولشویی و تأمین مالی تروریسم بوده و باید برای مدیریت و کاهش این‌گونه ریسک‌ها، از فناوری‌های نوین بهره‌مند شوند. بر اساس ماده ۳۸ آیین‌نامه اجرایی مبارزه با پولشویی کشور نیز، واحد اطلاعات مالی موظف به جمع‌آوری و اخذ اطلاعات مشکوک، ارزیابی، بررسی و تحلیل اطلاعات گزارش‌ها و معاملات مشکوک و طراحی نرم‌افزارهای مورد نیاز برای مبارزه با پولشویی است.

با توجه به اهمیت موضوع در این مقاله سعی شده است با توجه به ادبیات نظری و تجربی موجود در زمینه کشف پولشویی، مکانیسم کشف پولشویی طراحی شود. در همین راستا در بخش دوم مقاله، ادبیات نظری و تجربی پدیده پولشویی و طراحی مکانیسم ضد پولشویی بیان شده و در بخش سوم ضرورت کشف پولشویی در شبکه بانکی کشور بیان شده و در آخر نیز مکانیسم ضد پولشویی طراحی شده برای کشور بیان شده است.

۲. ادبیات نظری و تجربی طراحی مکانیسم کشف پولشویی

۲-۱. پولشویی

فرآیند پولشویی، فرایندی است که در آن درآمدهای نامشروع، مشروع شده و مجرمین سعی می‌کنند که پول‌هایی که از روش‌های نامشروع به دست می‌آورند را پاک نمایند. عمده‌تاً فرآیند پولشویی دارای سه مرحله است که در شکل ۱ نشان داده شده است. جایابی ۲: اولی مرحله و پرخطرترین مرحله این است که مجرم زمانی که پول زیادی دریافت می‌کند یا آن را در یک حساب یا در چند حساب وارد می‌کند. لایه‌بندی ۳: در واقع لایه گذاری مرحله ای از پولشویی است که معطوف به جدا سازی عواید حاصل از جرم، از منشأ غیر قانونی آن است. این عمل از طریق ایجاد لایه‌های پیچیده ناشی از معاملات چندگانه با هدف مبهم ساختن زنجیره عطف حسابرسی و عدم امکان ردیابی منشأ مال صورت می‌پذیرد و این امر متضمن انجام دادن عملیاتی مانند حواله وجه سپرده شده نزد یک مؤسسه مالی به مؤسسه مالی دیگر یا تبدیل سپرده نقدی به اسناد پولی دیگر (اوراق بهادار، سهام و چک‌های مسافرتی است. مرحله سوم تلفیق یا یکپارچه‌سازی ۴ است که در آن پوشش و ظاهری مشروع

¹ Financial Action Task Force (FATF)

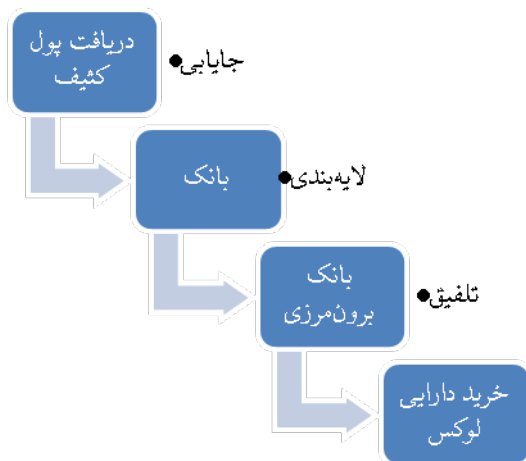
² placement

³ Layering

⁴ integration



برای توجیه قانونی عواید حاصل از فعالیت‌های مجرمانه است. به عنوان مثال پول در فرآیند پولشویی به خرید یک دارایی لوکس اختصاص می‌یابد و به این ترتیب پول قانونی می‌شود [4].



شکل ۱- فرآیند هندسی پولشویی

فراهم بودن امکان انجام عملیات بانکی گوناگون و گسترده برای مشتریان، بدون حضور فیزیکی و به طور شبانه روزی در بانکداری الکترونیکی، این امکان را برای پولشویان نیز فراهم می‌کند تا بدون این که هویت آنها شناسایی شود، بتوانند به اهداف مجرمانه خود برسند. در عین حال، زمان رسیدن به هدف را نیز برای آنها کم کرده و شستشوی پول را آسان تر می‌کند. در واقع پولشویان می‌توانند بدون نگرانی از الزامات قانون گذاری و حسابرسی‌های مالی، آزادانه‌تر به فعالیت‌های خود ادامه دهند.

در روش پولشویی الکترونیکی، تراکنش‌های چهره به چهره حذف شده و مجرمان با اختفای هویت، انجام فعالیت می‌نمایند. بنابراین، پولشویی در فضای الکترونیکی نسبت به روش سنتی آن مزایایی دارد که برخی از مهمترین آنها عبارتند از:

- می‌تواند سبب افزایش سرعت در انجام مراحل سه‌گانه پولشویی و تطهیر اموال نامشروع شده و پولشویان با صرف هزینه کمتر به بالاترین منفعت مالی برسند.
- استفاده از تراکنش‌های الکترونیکی در فضای مجازی، باعث گمنامی و اختفای هویت آنها می‌شود. جرم پولشویی می‌تواند در فضای جغرافیایی گسترده‌تری در سطح ملی و جهانی انجام گیرد.
- کاهش حضور فیزیکی افراد در شعب و انجام نقل و انتقالات پولی به صورت الکترونیکی، می‌تواند باعث کم شدن نسبت جرایمی مانند جعل اسناد به منظور مخفی نگه داشتن هویت و دادن رشوه به افراد، توسط پولشویان در مؤسسات مالی و بانکی شود.
- استفاده از فضای مجازی در بانکداری الکترونیکی و کاهش حضور فیزیکی افراد در شعب می‌تواند موجب کاهش ریسک خطر شناسایی افراد مجرم در مراحل پولشویی شود.

بنابراین، از آنجا که با پیشرفت بانکداری الکترونیکی، پولشویی الکترونیکی نیز گسترش یافته و مجرمان به روش‌های جدیدتری برای مخفی کردن فعالیت‌های غیر قانونی خود دست یافته‌اند، لازم است که بانکها نیز با دقت بیشتری به شناسایی این افراد و فالیتهای آنها بپردازند. در بانکداری الکترونیک با استفاده از فناوری الکترونیکی و نرم افزارها، تشخیص عملیات



مشکوک به پولشویی نسبت به بانکداری سنتی سریع‌تر امکان‌پذیر بوده و می‌توان با داشتن سامانه یکپارچه بانکی به کشف رفتارهای پولشویی و استخراج پیشینه اقدام نمود[5].

۲-۲. سیستم‌های ضد پولشویی ۱ هوشمند

بسیاری از نهادهای مالی، در تلاش برای مبارزه با پولشویی، سیستم‌های ضد پولشویی را بسط داده‌اند و برای پیاده‌سازی آن برنامه‌ریزی کرده‌اند. در ادامه سیستم ضد پولشویی بر مبنای قاعده، سیستم ضد پولشویی چند عاملی، سیستم ضد پولشویی تحلیل جریان تراکنش و سیستم ضد پولشویی لینک بیان می‌شود.

برای پیاده‌سازی سیستم ضد پولشویی بر مبنای قاعده، نهادهای مالی سعی کرده‌اند، معیارهایی را برای شناسایی معاملات مشکوک بکار گیرند که به این نوع سیستم‌ها، سیستم‌های بر پایه قاعده ۲ می‌گویند. مشخصه‌های کلی این نوع سیستم‌ها عبارت هستند از [6]:

- این سیستم‌ها ناتوان از شناسایی پولشویی در مواردی که مبالغ معاملات کوچک است، هستند.
 - در این نوع سیستم‌ها، مسئله اشتباه مثبت ۳ رخ می‌دهد. به این مفهوم که معاملات تحت مجموعه محدود که به عنوان معاملات مشکوک ثبت می‌شوند، ممکن است هیچ نوع ریسکی را برای نهاد مالی نداشته باشند.
 - اگرچه سیستم‌های بر مبنای قاعده ظرفیت بسط و بهبود را دارند، اما این سیستم‌ها، جهان شمول نیستند و فقط برای موارد خاصی که طراحی می‌شوند، قابل کاربرد هستند.
- با توجه به کاستی‌های سیستم‌های کشف پولشویی بر مبنای قاعده، نهادهای هوشمند بر مبنای عامل و سیستم‌های چند نهادی ایجاد و بسط یافته است. مشخصه‌های اصلی این سیستم‌ها عبارت هستند از [7]:
- یک سیستم هوشمند بر مبنای عامل، یک سیستم کامپیوتری است که در یک فضای هوشمند قادر است به اهداف طراحی شده دست‌یابد.
 - این سیستم‌ها برای فعالیت نیاز به نیروی انسانی و سیستم‌های دیگر نداشته و به صورت درونی کنترل می‌شوند.
 - یک سیستم هوشمند بر مبنای عامل در مقابل اهدافی که برای آن تعریف شده است، انعطاف‌پذیر است. به طوری که با تغییر شرایط محیطی بازهم کارآ و اثربخش خواهد بود.
 - سیستم‌های هوشمند بر مبنای عامل ۴ در مقایسه با سیستم‌های هوشمند بر مبنای قاعده، انعطاف‌پذیری و کارایی بیشتری داشته و می‌توانند به صورت غیر متمرکز نیز اثربخش باشند.
 - این سیستم برای دستیابی به اهداف، نیاز به استفاده از دانش محیطی و رفتارهای سیستم‌های دیگر برای برنامه‌ریزی دارد.
 - رابطه بین عوامل در یک فضای هوشمند نظیر فضای اینترنت صورت می‌گیرد.
 - این سیستم‌ها برای شناسایی ریسک‌های پیش روی نهادهای مالی با هر میزان معامله (چه کوچک چه بزرگ) مناسب بوده و بکارگیری آنها باعث بهبود فضای کسب و کار می‌شود.
- برای طراحی ساختار یک سیستم ضد پولشویی چند عاملی، فرآیند ضد پولشویی در چند زیر مجموعه طراحی می‌شود [8] هر عامل وظیفه خاصی برعهده داشته و با دیگر عوامل نیز برای دستیابی به هدف کل سیستم همکاری دارد.

¹ Anti money laundering system

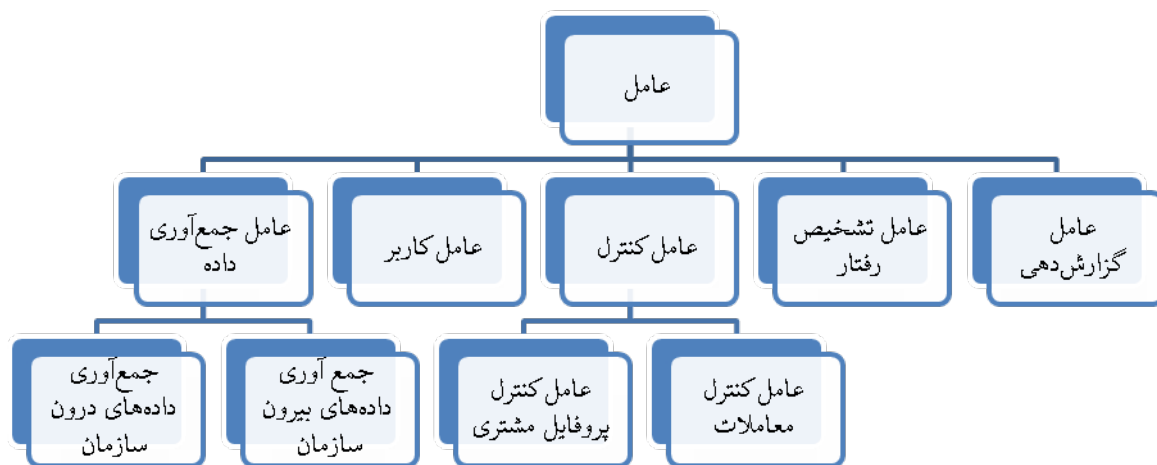
² Rule- based Systems

³ Problem of false positive

⁴ Agent-based



فرآیند ضد پولشویی چند عاملی مجموعاً شامل عامل جمع‌آوری داده ۱، عامل کاربر ۲، عامل کنترل ریسک پولشویی ۳، عامل تشخیص رفتار ۴ و عامل گزارش‌دهی ۵ است. عامل جمع‌آوری داده مشتمل بر جمع‌آوری داده‌های درون و بیرون از سازمان مالی است. کنترل پولشویی شامل ارزیابی پروفایل مشتریان و اندازه‌گیری ریسک معاملات است. در شکل (۲) چارچوب کلی یک سیستم ضد پولشویی هوشمند بر مبنای عامل نشان داده شده است.



شکل ۲- ساختار سیستم هوشمند چند عاملی

عامل کاربر، کاربران را قادر می‌سازد، وضعیت جاری معاملات مالی، کنترل پولشویی، تشخیص و فرآیند گزارش‌دهی را انجام دهند و آنها را برای قضاوت و کشف پولشویی در سایر بخش‌های مالی بکار برند. عامل جمع‌آوری داده، سیستم را قادر به جمع‌آوری داده از درون و بیرون سازمان می‌سازد. عامل کنترل، داده‌ها را از عامل جمع‌آوری داده، دریافت نموده و آن را ارزیابی می‌کند، این عامل مشتمل بر دو عامل است. عامل کنترل پروفایل مشتریان و عامل کنترل معاملات. عامل کنترل پروفایل مشتریان، اطلاعات مربوط به حساب مشتریان را ارزیابی می‌کند و زمانی کاربرد دارد که حساب مشتری باز و در جریان باشد. عامل کنترل معاملات، معاملات مشکوک به پولشویی را شناسایی می‌کند. عامل گزارش‌دهی، زمانی که رفتار مشکوک به پولشویی مشاهده شد، به‌صورت خودکار گزارش پولشویی را تهیه نموده و به عامل کاربر هشدار می‌دهد تا فعالیت‌ها را مدیریت نماید.

در این قسمت سیستم ضد پولشویی به روش تحلیل جریان تراکنش بیان می‌شود. کشف پولشویی به روش تحلیل جریان تراکنش توسط اومادیو و دیویا (۲۰۱۲) [4] بیان شده است. این سیستم امکان تبدیل داده‌های کمی به صورت

¹ Data Connecting Agent

² User agent

³ Monitoring agent

⁴ Behavior Diagnosing agent

⁵ Reporting agent



هفتمین همایش سالانه
بانکداری الکترونیک
و نظام‌های پرداخت

تهران، مرکز همایش‌های بین‌المللی برج المیلاد - ۲ و ۳ بهمن ۱۳۹۶

7th Annual Conference
on Electronic Banking
and Payment Systems

نواوری، بازیگران جدید و کارایی در کسب و کار مالی



گزارش‌هایی فراهم می‌کند. ساختار این سیستم مشتمل بر ۷ بخش است که عبارت هستند از: مرحله قبل از پردازش ۱، ورود دیتا ۲، خوشه‌بندی و شناسایی وضعیت مشکوک ۳، نمایش داده ۴، یادگیری از تصمیم کاربر ۵، ایجاد پروفایل بانک ۶، استخراج رفتار ۷. مرحله قبل از پردازش داده‌ها، دارای دو زیر مجموعه است. مجموعه پیش از انتقال داده ۸ و مجموعه انتقال داده ۹. این مرحله داده‌های خام را دریافت نموده و آن را برای واردکننده داده آماده می‌سازد. هدف اصلی این مرحله، دریافت داده‌ها از منابع مختلف و آماده‌سازی آنها به فرصتی که برای واردکننده داده قابل کاربرد باشد، تبدیل می‌کند. داده‌های مورد نیاز برای داده‌کاوی، صرفاً از یک منبع و با یک فرمت خاص قابل دسترسی نیست. در این مرحله داده‌ها از منابع مختلف دریافت شده و آنها را به فرمت مورد نیاز ترکیب می‌کند. داده‌های منسجم ممکن است که دوبار ثبت شوند. بعد از ترکیب داده‌ها، عملیات پاکسازی داده صورت می‌گیرد، تا داده‌های دوبار ثبت شده را از پایگاه داده پاک می‌کند و داده‌ها برای واحد تبدیل داده ۱۰ آماده شوند. واحد تبدیل داده، داده‌ها را از واحد قبل از تبدیل داده، دریافت می‌کند. داده‌ها را به فرمتی تبدیل می‌کند که مورد نیاز است. واردکننده داده، داده‌ها را دریافت می‌کند. در این مرحله داده‌ها فراخوانی شده و به فرمت خاص مورد نیاز سیستم تبدیل می‌شود. مرحله خوشه‌بندی، داده‌های وارد شده را برای الگوریتم خوشه‌بندی استفاده می‌کند. در طرف محصول، خوشه‌بندی‌هایی را ایجاد می‌کند که ورودی الگوریتم داده‌کاوی هستند. مرحله شناسایی موقعیت‌های مشکوک، با استفاده از روش الگوریتم داده‌کاوی، خوشه‌بندی‌ها را تحلیل می‌کند و در نهایت موقعیت‌های مشکوک را شناسایی می‌کند. مرحله نمایش داده، نتایج را به صورت خطی نمایش می‌دهد. مرحله ایجاد پروفایل به طور اتوماتیک، پروفایلی از تراکنش‌های مشکوک گزارش می‌کند که در این پروفایل، ساعت و روز جریان وجوه، فردی که وجوه را انتقال داده، مقدار انتقال داده شده و ... وجود دارد. از طرفی پروفایل بانک ممکن است در طول فرآیند تحلیل داده فیلتر شود و در نتیجه این مرحله ایجاد پروفایلی از فعالیت‌های مشکوک بانک است. مرحله یادگیری از تصمیم کاربران، مرتبط با کاربران بوده و از تصمیمات آنها در تحلیل انتقالات مشکوک استفاده می‌کند. سپس پروفایل کاربر ساخته شده، برای فیلتر کردن بر اساس تصمیمات گذشته کاربر استفاده شود. در نتیجه یک مدل با تصمیمات کاربران طراحی می‌شود. در مرحله استخراج رفتار مشتری، پروفایل کاربر تحلیل شده و با پروفایل یک کاربر نرمال مقایسه شده و سپس وضعیت مشکوک شناسایی شده و نوع پولشویی و ساعت پولشویی استخراج می‌شود.

سورش و ردی (۲۰۱۵) [9] سیستمی را طراحی کرده‌اند که از تحلیل لینک برای کشف تقلب در حساب‌های بانکی، استفاده می‌شود. در این مقاله یک رویکرد پایه اکتشافی ۱۱ طراحی شده است که از قواعد تصمیم برای تحلیل لینک با پذیرش تکنیک جدول چند پیوندی ۱۲ استفاده می‌کند. این روش زمان ارزیابی را کاهش داده و مواردی که تراکنش‌ها مورد ارزیابی قرار می‌گیرند را افزایش می‌دهد و می‌تواند گزارش‌های مختلفی را ارائه دهد. وقتی که ارزش تراکنش‌ها بزرگ باشد، این سیستم برای شناسایی پولشویی مناسب است. در روش سیستم پیشنهادی هر بانک به صورت انفرادی تراکنش‌های مربوط به حساب مشتریان را کنترل می‌کند و تراکنش‌های مشکوک را شناسایی می‌کند. این سیستم دارای سه مرحله است. گزارش

¹ preprocessing

² Data importer

³ Clustering and suspected

⁴ Data visualization

⁵ Learning from the user decision

⁶ Company/organization profile generation

⁷ Extracting behavior

⁸ Pre data transform unit(pre-DTU)

⁹ Data transform unit

¹⁰ Data transform unit

¹¹ heuristic base approach

¹² Multi table joins



هفتمین همایش سالانه
بانکداری الکترونیک
و نظام‌های پرداخت

تهران، مرکز همایش‌های بین‌المللی برج میلاد - ۲۰ و ۲۱ بهمن ۱۳۹۶

7th Annual Conference
on Electronic Banking
and Payment Systems

نواوری، بازیگران جدید و کارایی در کسب و کار مالی



معاملات مشکوک به واحد اطلاعات مالی ۱، پردازش داده‌ها و تحلیل لینک که هر مرحله در ادامه توضیح داده می‌شود. در مرحله گزارش به واحد اطلاعات مالی، تراکنش‌های مشکوک به واحد اطلاعات مالی گزارش می‌شود. شناسایی تراکنش‌های مشکوک به وسیله قواعد و مقررات بانکی صورت می‌گیرد. شناسایی تراکنش‌های مشکوک بر مبنای ارزش تراکنش‌ها و تاریخچه تراکنش‌ها صورت می‌گیرد. در این سیستم هر تراکنشی که بزرگ باشد، مبلغ بزرگی وارد حساب شود و سریع از حساب خارج شود، به عنوان تراکنش مشکوک شناسایی می‌شود. تکرار تراکنش‌ها در یک دوره یک هفته‌ای نیز می‌تواند به عنوان یک معیار برای شناسایی عملیات مشکوک به کار رود. در مرحله قبل از پردازش داده، تراکنش‌هایی که به عنوان تراکنش‌های مشکوک شناسایی می‌شوند به واحد اطلاعات مالی گزارش می‌شوند. گزارش‌هایی که به این واحد ارائه می‌شوند، مشتمل بر تراکنش‌های متعدد از واحدهای مختلف بانک درباره یک مشتری است. برای پردازش داده فقط بخش اندکی از تراکنش‌ها نیاز است. در داده‌های قبل از پردازش، تراکنش‌های مشکوک از تراکنش‌های ناکامل و سایر تراکنش‌ها متمایز می‌شوند. برای دستیابی به داده‌های با کیفیت نیاز است، داده‌ها قبل از پردازش آماده شوند. به این ترتیب در پایگاه داده‌ای، تراکنش‌های با اطلاعات بی‌ربط با الزام معیارهای مشخص برای شناسایی معاملات مشکوک کنار گذاشته می‌شوند. به عنوان مثال جزئیاتی نظیر مقدار ۲، مشخصه تراکنش ۳، از کدام حساب ۴، به کدام حساب ۵ و تکرار ۶ برداشت‌ها و واریزها، برای شناسایی تراکنش‌های مشکوک به کار می‌روند. در مرحله تحلیل لینک، کاربر بررسی می‌کند، چطور یک حساب به یک حساب مشکوک وصل می‌شود. به این ترتیب ارتباط بین تراکنش‌های حساب‌های مختلف بررسی شده و صحت تراکنش‌ها سؤال می‌شود. به عنوان مثال در مورد پولشویی مشکوک، پول از یک حساب به حساب‌های مختلف وارد شده و دوباره به یک حساب وارد می‌شود. اغلب این حساب‌ها ویژگی مشترک دارند. مانند شماره تلفن یا آدرس شغل کاربر. تحلیل لینک با استفاده از ارتباط بین حساب‌ها می‌تواند تراکنش‌های مشکوک را شناسایی نماید. این ارتباط بین تراکنش‌ها، مطالعه مشخصه‌های مشترک تراکنش‌ها را تسهیل می‌سازد. فهرست تراکنش‌های دریافت شده در واحد اطلاعات مالی با تراکنش‌هایی که در ارتباط با فعالیت پولشویی اتفاق می‌افتند، تطبیق داده می‌شوند. هر تراکنش در پایگاه داده‌ای به عنوان یک گره ۷ استفاده می‌شود. هر گره با تراکنش‌های قبلی مرتبط شده و با کنترل کردن سایر تراکنش‌ها با حساب‌های مشکوک مرتبط می‌شوند. قواعدی نظیر وجود چند حساب، مشخصه‌های مشتری، سابقه مشتری در زمینه پولشویی و تقلب، ماهیت تراکنش و ارزش تراکنش می‌تواند در مرحله لینک به شناسایی تراکنش‌های مشکوک به پولشویی کمک نماید.

۳-۲. داده‌کاوی در بانکها و نهادهای مالی

امروزه نهادهای مالی آمارهای بانکی بزرگ و بسیاری از مجموعه‌های داده‌ها را به صورت روزانه مدیریت و ثبت می‌کنند. رشد داده‌های مالی جمع‌آوری شده باعث شده است که اثربخشی نیروی انسانی در مدیریت و تحلیل آنها به روش سنتی ناکارآمد باشد. رقابت جهانی و پویایی‌های بازار و افزایش سریع در ابداعات تکنولوژی چالشی مهم برای این نهادهای مالی است. نهادهای مالی نیاز دارند که از روش‌های هوشمند استفاده کنند زیرا که روش‌های آماری سنتی ظرفیت کافی برای تحلیل مجموعه آماری بزرگ ندارند.

¹ Financial intelligence unit

² amount

³ Transaction-id

⁴ From account

⁵ To account

⁶ frequency

⁷ node



هفتمین همایش سالانه
بانکداری الکترونیک
و نظام‌های پرداخت

تهران، مرکز همایش‌های بین‌المللی برج میلاد - ۲ و ۳ بهمن ۱۳۹۶

7th Annual Conference
on Electronic Banking
and Payment Systems

نواوری، بازیگران جدید و کارایی در کسب و کار مالی



در بانکداری و مالی از روش داده‌کاوی برای حل مسائل تجاری در یافتن مسائل مالی استفاده می‌کنند. روش داده‌کاوی می‌تواند در ابتدا برای تحلیل حجم بزرگی از داده‌ها و برای ساختن پروفایل مشتریان استفاده شود. روش داده‌کاوی می‌تواند قواعدی ایجاد کرده و مدل‌هایی بسازد که قادر به درک عملکرد کسب و کار، ایجاد بازار جدید و تحلیل ریسک و تحلیل سیاست مشتریان باشد. کاربرد دیگر داده‌کاوی در بخش بانکی و مالی، قدرت پیش‌بینی آن است. نتایج حاصل از داده‌کاوی در پیش‌بینی روند خدمات و عامل ریسک بر اساس رفتار گذشته بنا شده است.

با توجه به اینکه نهاد مالی در کشف پدیده پولشویی با حجم بزرگی از داده‌ها مواجه بوده و استخراج پولشویی از میان حجم عظیم داده‌ها، به روش سنتی امکان‌پذیر نیست، بکارگیری روش داده‌کاوی در مجموعه داده‌های بزرگ جهت شناسایی و کشف فعالیت‌های مشکوک به پولشویی مناسب است [10].

۳-۴. روش‌های مرسوم داده‌کاوی در فرآیند ضد پولشویی

برای طراحی تکنیک داده‌کاوی کارا نیاز است که آن متناسب با کشف پولشویی طراحی شود. یک چارچوب داده‌کاوی باید با چهار سطح سازگار باشد. با تراکنش‌های مالی، حساب‌ها، یک مؤسسه و چند مؤسسه. در این میان تراکنش‌های مالی از همه مهمتر هستند. در یک سطح تراکنش‌های مربوط به یک حساب بررسی شده و در سطح دوم تراکنش‌های چندگانه مرتبط با چند حساب بررسی می‌شوند. بررسی مجموعه تراکنش‌ها مرتبط با حساب‌های یک نفر، یک دید کلی از این حسابها در مورد فعالیت مالی آنها می‌دهد. در بررسی تراکنش‌های چندگانه، میزان ارتباط بین حساب‌های مختلف مبتنی بر تکرار تراکنش‌های آنها نشان داده می‌شود. در سطح یک بانک ممکن است یک مشتری چند حساب داشته باشد یا حساب‌های چندگانه با افراد مختلف در یک بانک وجود داشته باشد که در این صورت عملیات مالی آن مشکوک به پولشویی خواهد بود. در سطح آخر روش داده‌کاوی، جستجوی پولشویی در شرکت‌های چندگانه، بانک‌ها و مشتریان چندگانه است. در این شرایط یک سیستم ضد پولشویی بر مبنای داده‌کاوی پیشنهاد شده، ترکیبی از سه واحد است. واحد فیلتر کردن داده‌ها^۱، واحد یکپارچه‌سازی^۲ و واحد تحلیل^۳. روش‌های آماری برای فیلتر کردن به کار می‌رود. یکپارچه‌سازی از طریق برقراری ارتباط بین حساب‌های مختلف و تعیین رتبه مشکوک به پولشویی اجرا می‌شود. واحد تحلیل، نتایج را مورد بررسی قرار می‌دهد [11].

در میان روش‌های مختلف داده‌کاوی، مهمترین روش‌های مورد استفاده در کشف پولشویی، روش خوشه‌بندی، روش ماشین بردار و روش فازی است. خوشه‌بندی فرآیندی است که داده‌ها بر حسب تشابه در خوشه‌های مختلف دسته‌بندی می‌شوند. در حوزه طراحی مکانیسم ضد پولشویی خوشه‌بندی برای گروه‌بندی معاملات و حسابها بر حسب تشابهات آنها صورت می‌گیرد. این تکنیک به شناسایی معاملات مشکوک و کشف ریسک مشتریان یا ریسک حسابها کمک می‌کند. یکی از مهمترین چالش‌های خوشه‌بندی در داده‌های مالی اندازه آنها است. این تکنیک میلیونها تراکنش را در هزاران زمان مورد بررسی قرار می‌دهد [12].

در این روش مشتریان و زمان تراکنش به $n+2$ فضای اقلیدسی تقسیم می‌شوند به طوری که n مشتری به l زمان و l تراکنش تقسیم می‌شوند. در این روش ابتدا کل زمان به فاصله‌های زمانی مختلف تقسیم می‌شود. بنابراین هر تراکنش به عنوان یک ورودی در فضای زمان در نظر گرفته می‌شود. این روش همه تراکنش‌های مشتریان را در طول زمان به صورت هیستوگرام ترسیم نموده و آن را خوشه‌بندی می‌کند. این روش برای تحلیل رفتار فردی بیشتر از تحلیل رفتار گروهی برای کشف تقلب در تراکنش‌ها مناسب است. بنابراین محقق مجبور نخواهد بود، تعداد زیادی از مشتریان و تعداد زیادی از

¹ Filtering

² Integrating

³ analyzing



تراکنش‌های مالی با مقادیر مختلف را برای دوره زمانی طولانی تحلیل نماید. در این شرایط کشف پولشویی سخت است به خصوص مواردی که هیچ نوع قله برجسته‌ای در هیستوگرام وجود نداشته باشد یا قله برجسته اندک باشد. در این شرایط تحلیل‌های عمومی دیگر، نظیر انطباق رفتار مشتریان و تراکنش‌های مالی با معیارهای وجود پدیده پولشویی در ابتدا نیاز است و پس از آن، از این روش خوشه‌بندی برای تحلیل‌های بیشتر استفاده می‌شود [13].

روش دیگر داده‌کاوی برای کشف پدیده پولشویی، ماشین بردار پشتیبان است که از جمله روش‌های آماری است که برای دسته‌بندی و رگرسیون استفاده می‌شود. ابزار ضد پولشویی شامل کشف رفتار غیر معمولی همه موارد نظیر تراکنش‌ها، حساب‌ها و انواع خروجی‌ها است. بنابراین مسئله پولشویی زمانی کشف می‌شود که داده‌های گروه‌بندی شده به دو دسته مجموعه‌های نرمال و غیر نرمال تقسیم می‌شوند. برای سنجش اعتبار مدل طراحی شده بر مبنای ماشین بردار پشتیبان، باید داده‌ها به دو گروه آموزش و یادگیری تقسیم شوند. به عبارت دیگر نتایج دسته‌بندی بستگی به قوت مجموعه آموزش دارد. در این روش مجموعه آموزش باید به اندازه کافی بزرگ باشد تا نتایج باثباتی را ارائه دهد. با این وجود در زمینه پولشویی یافتن مجموعه داده‌ها برای آموزش یک چالش است. در برخی از مؤسسات مالی فقط یک یا دو تراکنش مشکوک در هر ماه در مقایسه با هزاران تراکنش تمیز در هر روز قابل شناسایی است. بنابراین ماشین بردار پشتیبان که بر اساس مجموعه داده کوچک بنا شده است، برای دسته‌بندی داده‌ها به نرمال و غیر نرمال مناسب است. ماشین بردار پشتیبان، به اختلالاتی که در مجموعه داده‌های مالی معمول است، حساس نیست [14]. ماشین بردار پشتیبان با یک روش آموزش نظارت شده، داده‌های مورد نیاز برای آموزش را ایجاد می‌کند تا بتواند قوانین دسته‌بندی را ایجاد نماید. ماشین بردار یک طبقه‌ای نظارت نشده برای کشف داده‌های خارج از محدوده ۲ به کار می‌رود که برای مجموعه آموزش پولشویی مناسب است [15]. به این ترتیب که مجرمین پولشویی که تلاش می‌کنند، فعالیت خود را مخفی کنند، با تحلیل داده‌های خارج از محدوده، قابل شناسایی می‌شوند. در نهایت آنچه مهم است این است که داده‌های مالی ناهمگن هستند. بنابراین به همراه ماشین بردار پشتیبان باید از تکنیک‌های تکمیلی نیز برای تحلیل داده‌های مالی ناهمگن استفاده شود [11].

یکی از مهمترین تکنیک‌های داده‌کاوی که در سال‌های اخیر برای کشف پولشویی به کار گرفته شده است، تکنیک منطق فازی است. تکنیک منطق فازی دارای دو کاربرد کنترل و کشف می‌باشد. کنترل و بررسی داده‌ها، نخستین گام در کشف پدیده پولشویی است. اگر موارد خاص در فرآیند نظارت و کنترل کشف شد، گام بعدی در منطق فازی، اطمینان از وجود پدیده پولشویی است. در پایان نیز یک استراتژی کنترلی برای مدیریت مسائل مورد نیاز است [16]. در منطق فازی به طور معمول عبارتها و گزاره‌ها به صورت اگر و آنگاه بیان می‌شوند. این عبارتها را قاعده‌های زبانی ۳ یا قاعده‌های گفتاری می‌نامند. یک قاعده گفتاری، گزاره شرطی اگر و آنگاه متکی به متغیرهای گفتاری است. چنانچه بجای عبارت گفتاری از یک تابع خاصی استفاده شود، سیستم فازی ایجاد شده را سیستم فازی تاکاگی-سوگنو-کانگ ۴ می‌نامند. سیستم‌های فازی که در آن عبارتهای گفتاری به جای توابع خطی استفاده می‌شود، سیستم‌های فازی ممدانی ۵ می‌نامند [17].

در طراحی سیستم کشف پولشویی با استفاده از روش منطق فازی، ابتدا باید از منابع مختلف داده‌های مورد نیاز را جمع‌آوری کرد. منابع اصلی که برای تحلیل داده‌ها مورد نیاز است، عبارت هستند از: مدل‌های موجود برای کشف تقلب که داده‌های مشکوک به تقلب را از سایر داده‌ها متمایز می‌کنند. دوم از نمایشگرهای خدمات مشتری که حساب‌ها را نشان داده و در ارتباط با مشتری هستند. سوم از طریق تحلیل پروفایل مشتری و چهارم از طریق حسابی که مشتریان با آنها در ارتباط

1 One class SVM

2 outlier

3 Linguistic Rules

4 Takagi-sugeno-kang

5 Mamdani Fuzzy System



هستند. پس از جمع‌آوری داده، قواعد با استفاده از معیارهایی که مشخص‌کننده پدیده پولشویی هستند، به صورت اگر و آنگاه تعریف شده و در پایان نیز استنتاج فازی برای کشف پدیده پولشویی صورت می‌گیرد [16].
در این مقاله سعی شده است، از روش منطق فازی برای کشف پدیده پولشویی استفاده شود.

۳. مقررات پولشویی در کشور و نحوه شناسایی آن

بر اساس ادبیات نظری جرم پولشویی، فرآیندی است که مجرمین درآمدهای ناشی از عملیات مجرمانه را به روش‌های قانونی به درآمدهای تمیز تبدیل می‌کنند. بر اساس قانون مبارزه با پولشویی کشور مصوب سال ۱۳۸۶ و آیین‌نامه اجرایی مبارزه با پولشویی کشور مصوب مورخ سال ۱۳۸۷، جرم پولشویی عبارت است از:

الف- تحصیل، تملک، نگهداری یا استفاده از عواید حاصل از فعالیت‌های غیرقانونی با علم به اینکه به‌طور مستقیم یا غیر مستقیم در نتیجه ارتکاب جرم به‌دست آمده باشد.

ب- تبدیل، مبادله یا انتقال عوایدی به منظور پنهان کردن منشأ غیر قانونی آن با علم به اینکه به‌طور مستقیم یا غیر مستقیم ناشی از ارتکاب جرم بوده یا کمک به مرتکب به‌نحوی که وی مشمول آثار و تبعات قانونی ارتکاب آن جرم نگردد.

ج- اخفاء یا پنهان کردن ماهیت واقعی، منشأ، منبع، محل، نقل و انتقال، جابه‌جایی یا مالکیت عوایدی که به‌طور مستقیم و غیرمستقیم در نتیجه جرم تحصیل شده باشد.

برای شناسایی پدیده پولشویی نیاز است که معیارهایی برای کشف آن در هر کشور تعریف شود. بر اساس مطالعات مختلف معیارهایی برای کشف پولشویی در نظر گرفته شده است.

داشتن حساب‌های چندگانه توسط فرد

انجام گردش مالی بالا در مدت زمان کوتاه (بین یک تا سه روز کاری)، نظیر بازکردن حساب، ارسال وجوه، بستن حساب، بازکردن مجدد حساب، دریافت وجوه، خارج کردن وجوه و بستن حساب.

گردش مالی بالا بدون ارتباط با فضای کسب و کار

نسبت تفاوت مبالغ وارد شده و خارج شده از حساب به مبلغ وارد شده که هر چه به یک نزدیک باشد، احتمال رویداد

پولشویی بیشتر است [16].

- فعال شدن ناگهانی حسابهای راکد و کم کار
- تبدیل مکرر وجه نقد بیش از سقف مقرر به ارزهای دیگر
- تقاضای انتقال وجه به حساب‌های متفاوت با توجه به عدم همخوانی با شغل مشتری
- افزایش غیر عادی موجودی حساب‌های بانکی اشخاص
- واریز وجوه کمتر از سقف مکرر به حسابهای مشخص به دفعات زیاد
- بازپرداخت وام یا اعتبار سررسید گذشته، معوق و یا مشکوک الوصول، با این هدف که بانک وثیقه منقول یا غیر منقولی را که منشأ غیر قانونی دارد، تملیک کند.
- استفاده از اسامی مخفف و مجهول در خصوص افراد ذینفع
- ایجاد گردش نابهنگام حساب به صورت صوری با مبالغ بالا بدون انطباق با شغل افراد
- نقل و انتقال با مبالغ بالا به حسابهایی که صاحبان آنها آدرس و تلفن مشابه ای به بانک ارائه داده‌اند [18].



در مقررات مربوط به مبارزه با پولشویی در کشور ما نیز معیارهایی به این شرح برای کشف پدیده پولشویی تعریف شده است. بر اساس فصل اول آیین‌نامه اجرایی مبارزه با پولشویی، تعاریف، تبصره موجود در ماده ۱، معاملات مشکوک تعریف شده است. بر این اساس:

- معاملات و عملیات مالی مربوط به ارباب رجوع که بیش از سطح فعالیت مورد انتظار وی باشد.
- کشف جعل، کذب و یا گزارش خلاف واقع از سوی ارباب رجوع قبل یا بعد از آنکه معامله‌ای صورت گیرد و نیز در زمان اخذ خدمات پایه.
- معاملاتی که به هر ترتیب مشخص شود ذینفع واقعی حداقل یکی از متعاملین ظاهری آن شخص یا اشخاص دیگری بوده‌اند.
- معاملات تجاری بیش از سقف مقرر که با موضوع فعالیت ارباب رجوع و اهداف تجاری شناخته شده از وی مغایر باشد.
- معاملاتی که اقامتگاه قانونی طرف معامله در مناطق پر خطر (از نظر پولشویی) واقع شده باشد.
- معاملات بیش از سقف مقرر که ارباب رجوع، قبل یا حین معامله از انجام آن انصراف داده و یا بعد از انجام معامله بدون دلیل منطقی نسبت به فسخ قرار داد اقدام نماید.
- معاملات که طبق عرف کاری اشخاص مشمول، پیچیده، غیر معمول و بدون اهداف اقتصادی واضح می‌باشد.
- سقف مقرر: مبلغ یکصد و پنجاه میلیون ریال وجه نقد یا معادل آن به سایر ارزها و کالای گرانبها هیئت وزیران در صورت نیاز، سقف مذکور را با توجه به شرایط اقتصادی کشور تعدیل خواهد نمود.

اگرچه این تبصره بسیاری از موارد را در زمینه جرم پولشویی در نظر گرفته است، اما به نظر می‌رسد با در نظر گرفتن برخی موارد دیگر نیز می‌توان شناسایی جرم را بهبود بخشید. در برخی از کشورها، زمان معامله (اینکه در شب باشد)، تعداد دفعات واریز و برداشت در مدت زمان کوتاه (مدت زمان بین یک تا ۳ روز)، تفاوت بین برداشت و واریز وجوه نیز به عنوان علائم جرم پولشویی در نظر گرفته شده‌اند. به نظر می‌رسد با بررسی جامع‌تر در این حوزه می‌توان این بند را بهبود بخشید و به شناسایی دقیق‌تر جرم پولشویی کمک نمود.

با توجه به اهمیت موضوع کشف پولشویی در مجامع بین‌المللی نیز برای کشف پدیده پولشویی به خصوص در حوزه بانکداری الکترونیک توصیه‌هایی بیان شده است. توصیه شماره ۱۶، از توصیه‌های چهل‌گانه FATF، کشورها باید اطمینان دهند که مؤسسات مالی، اطلاعات ضروری و دقیق در مورد فرستنده وجوه و اطلاعات ضروری مربوط به ذینفع (دریافت‌کننده وجوه) را در فرآیند نقل و انتقالات الکترونیکی و پیام‌های مربوط، درج کرده و این اطلاعات در سراسر زنجیره پرداخت و در فرآیند نقل و انتقال و پیام‌های مرتبط باقی می‌مانند.

در راستای اجرای این توصیه، دستورالعملی با عنوان دستورالعمل رعایت مقررات مبارزه با پولشویی در حوزه نظام‌های پرداخت و بانکداری الکترونیک در کشور بیان شده است که بر اساس آن ضوابط مربوط به ابزارهای انجام تراکنش، ضوابط مربوط به روش‌های انجام تراکنش، ضوابط مربوط به مشخصات تراکنش‌های الکترونیکی بیان شده است. اگر چه این آیین‌نامه معیارهایی برای کشف پولشویی از طریق بانکداری الکترونیک را ارائه می‌دهد اما حلقه مفقوده آن، طراحی مکانیسمی هوشمند برای کشف پولشویی است.

۴. مکانیسم پیشنهادی برای کشف پولشویی در شبکه بانکی کشور

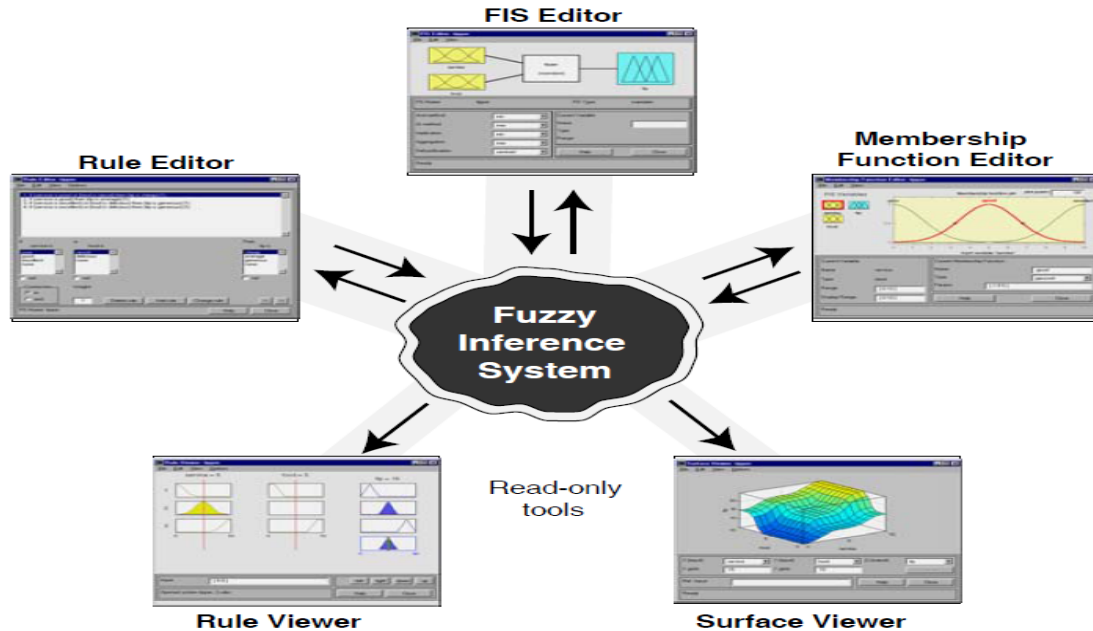
هدف از این مقاله طراحی یک مکانیسم منطق فازی برای کشف پولشویی است. به همین منظور ابتدا بر اساس مقررات موجود در کشور و بر اساس ادبیات نظری، معیارهایی برای کشف پدیده پولشویی استفاده شده است. سپس تابع عضویت سیستم فازی



تعریف شده و در پایان نیز استنتاج فازی صورت گرفته است. باتوجه به قانون مبارزه با پولشویی مهمترین معیارهای شناسایی پولشویی، عدم رعایت سقف مقرر و سپرده‌گذاری به دفعات و برداشت یکجا و عمده است. در هنگام انجام تراکنش یکی از موضوعات قابل توجه عبور از سقف مقرر است که باید گزارش داده شود و همچنین اطلاعات مربوط به آن ثبت شود تا در صورت نیاز بتوان آن را گزارش داد.

همچنین معاملات نقدی کمتر از سقف مقرر به صورت مداوم و مستمر، احتمالاً به منظور ممانعت از گزارش‌دهی، یکی از شگردهای پولشویی است، که تقریباً از معمولترین و پر تکرارترین الگوهای پولشویی به حساب می‌آید و سیستم باید نسبت به آن حساس بوده و اینگونه الگوها را تشخیص دهد. برای طراحی این سیستم با بهره‌گیری از نرم‌افزار MATLAB2015 از ۱۵۰۰ حساب در یک بانک خصوصی در یک دوره سه ماهه استفاده شده است.

به طور کلی سیستم استنتاج فازی ۱ شامل ۵ عنصر است که سیستم طراحی شده در این مقاله نیز در این چارچوب طراحی شده است. ویرایشگر استنتاج فازی ۲ بیان می‌کند چه تعداد ورودی وجود داشته و نام آنها چیست؟ این سیستم محدودیتی در تعداد ورودی‌ها ندارد. ویرایشگر تابع عضویت ۳ برای تعریف توابع عضویت مرتبط با هر متغیر به کار می‌رود. ویرایشگر قواعد ۴ برای ویرایش فهرست قواعدی که رفتار سیستم را تعریف می‌کند، بکار می‌رود. ناظر قواعد ۵ برای مشاهده نمودار فازی بکار می‌رود. ناظر قواعد نشان می‌دهد کدامیک از قواعد فعال بوده و چطور توابع عضویت نتایج را تحت تأثیر قرار می‌دهد. نمایشگر سطح ۶ برای مشاهده وابستگی خروجی‌ها با ورودی‌ها را نشان داده و سطح خروجی سیستم را ترسیم می‌کند.



شکل ۳- چارچوب استنتاج فازی

¹ Fuzzy Inference System

² Fuzzy Inference System Editor

³ Membership Function Editor

⁴ Rule Editor

⁵ Rule Viewer

⁶ Surface Viewer



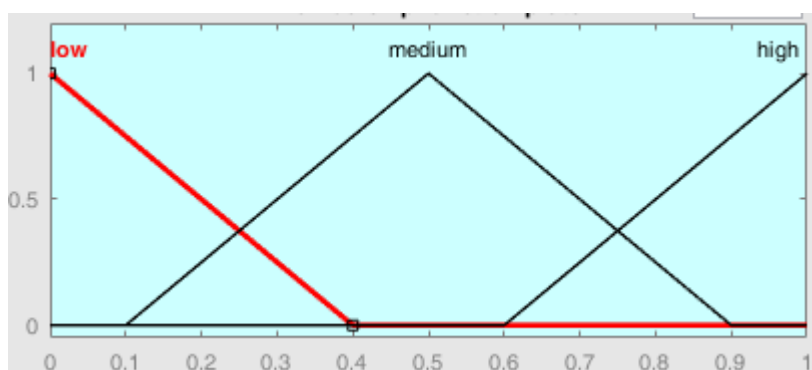
سیستم طراحی شده در این مقاله نیز در چارچوب استنتاج فازی بوده و نوع منطق فازی، روش ممدانی^۱ است. برای فازی سازی متغیرها نیز از تابع مثلثی استفاده شده است.

در سیستم مدنظر این مقاله، دو ورودی و یک خروجی وجود دارد. سقف برداشت از حساب بانکی بر اساس قانون پولشویی نباید از ۵۰۰ میلیون ریال و ۵۰ میلیون تومان بیشتر باشد و تراکنش بانکی نیز نباید از ۱۵ میلیون تومان در یک روز بیشتر باشد. یکی از ورودی‌های این مدل، برداشت از سپرده (v5) بیش از سقف مقرر در نظر گرفته شد. همچنین برای کمی کردن برداشت و واریز مکرر در مدت زمان کوتاه، فرض شده است، اگر فاصله واریز وجوه و برداشت وجوه (v9) کمتر از ۳ روز باشد، تراکنش مالی به عنوان تراکنش مشکوک شناسایی می‌شود. بنابراین ورودی دیگر فاصله بین روزهای واریز و برداشت وجوه در نظر گرفته شد. خروجی این نرم‌افزار، شناسایی تقلب پولشویی (v1) است. برای هر یک از ورودی‌ها و خروجی‌ها سه حالت کم، متوسط و زیاد در نظر گرفته شد. در جدول زیر معیارها تعریف شده‌اند.

جدول ۱- معیارهای کشف پولشویی در مکانیسم طراحی شده

معیارهای شناسایی پولشویی	کم (low(L))	متوسط (medium(m))	زیاد (high(h))
برداشت از سپرده بر حسب سقف مقرر (v5)	بین صفر تا ۱۵۰۰۰۰۰۰۰ میلیون ریال	بین ۱۵۰۰۰۰۰۰۰ تا ۵۰۰۰۰۰۰۰۰ میلیون ریال	بیش از ۵۰۰۰۰۰۰۰۰
فاصله زمانی بین برداشت و واریز وجوه (v9)	بیش از سه روز	بین دو تا سه روز	بین یک تا دو روز

متغیرهای زبانی برای خروجی سیستم که متغیر شناسایی تقلب پولشویی است، مطابق شکل (۴) در نظر گرفته شده‌اند. به این معنا که نتیجه استنتاج سیستم فازی، تخصیص حساب‌ها به یکی از سه گروه خواهد بود. همانطور که مشاهده می‌شود، شدت غیر معمول بودن حساب‌ها، از کم به زیاد، افزایشی است.



شکل ۴- تابع عضویت متغیر خروجی

پس از فازی سازی ورودی‌ها و تعیین درجه عضویت، نوبت به ساختار قواعد سیستم فازی می‌رسد. با توجه به اینکه دو ورودی و سه گزینه برای هر یک تعریف شده است، تعداد ۹ قاعده قابل تعریف است. مهمترین قواعد این نرم‌افزار این است که

¹ mamdani



اگر مبلغ برداشت از سپرده بین صفر تا ۱۵ میلیون تومان باشد و دوره زمانی بیش از ۳ روز باشد، احتمال رخداد تقلب پولشویی بسیار کم است. اگر مبلغ برداشت از سپرده بین ۱۵ تا ۵۰ میلیون تومان باشد و دوره زمانی بین واریز و برداشت سپرده بین دو تا سه روز باشد، احتمال رخداد تقلب پولشویی متوسط است و اگر مبلغ برداشت از سپرده بیش از ۵۰ میلیون تومان باشد و دوره زمانی بین واریز و برداشت سپرده بین یک تا دو روز باشد، احتمال رخداد تقلب پولشویی بسیار زیاد است. به صورت خلاصه قواعد این نرم‌افزار در جدول ۲ نشان داده شده است.

جدول ۲- قواعد فازی مورد نظر این مقاله

H(high)	M(medium)	L(low)	V5/v9
VH	H	M	H(high)
H	M	L	M(medium)
M	L	VL	L(low)

پس از انتخاب قواعد، استنتاج فازی صورت می‌گیرد. روش‌های متفاوتی برای استنتاج در سیستم‌های فازی وجود دارد که از تفاوت در سه عملگر فازی ۱ در قسمت فرض، دلالت بر فرض نتیجه ۲ و تجمیع ۳ نتایج ناشی می‌شود. در نهایت با توجه به انتخاب نوع عملگرها، روش استنتاج سیستم فازی این مقاله، سیستم فازی ممدانی، یکی از پرکاربردترین روش‌های استنتاج فازی در هوش مصنوعی، انتخاب شد. مشخصات عملگرهای مذکور روش ممدانی در جدول (۳) مشاهده می‌شود.

جدول ۳- مشخصات سیستم فازی ممدانی

Name=money laundering detection	AndMethod= μ_{\min}
Type= μ_{mamdani}	OrMethod= μ_{\max}
NumInputs=2	ImpMethod= μ_{\min}
NumOutput=1	AggMethod= μ_{\max}
NumRules=9	DefuzzMethod= ζ_{centroid}

پس از طراحی سیستم منطق فازی، ضروری است سیستم طراحی شده اعتبار سنجی شود. به همین منظور از سیستم فازی عصبی تطبیقی ۴ استفاده شده است. برای اجرای این سیستم نیاز است که داده‌ها برای آموزش و یادگیری آماده شوند. به همین منظور به صورت تصادفی ۷۰ درصد داده‌ها برای آموزش و ۳۰ درصد برای یادگیری انتخاب می‌شود. در سیستم فازی عصبی تطبیقی، پارامترهای تابع عضویت به صورت اتوماتیکی انتخاب می‌شوند. به این ترتیب که از روش گراداینت ۵ و حداقل مربعات برای شناسایی پارامترهای تابع عضویت استفاده می‌شود. بنابراین سیستم ANFIS طراحی شده یک شبکه عصبی چند لایه با روش یادگیری گراداینت است که این روش برای تعیین پارامترها در لایحه پنهان به کار می‌رود. پارامترهای لایه خروجی به وسیله روش حداقل مربعات معمولی تعریف می‌شوند. ساختار عمومی ANFIS نیز شامل دو ورودی و یک خروجی است. برای ایجاد ANFIS به این ترتیب عمل می‌شود که ابتدا یک سیستم منطق فازی با نوع SUGeno و با نوشتن دستور

¹ Fuzzy operator

² Implication

³ Aggregation

⁴ Adaptive Neuro fuzzy inference (ANFIS)

⁵ Gradient



genfis1 در صفحه دستور متلب، ایجاد می‌شود. پارامترهای تعداد دوره‌ها (epoch)، خطای تحمل (Tolerance Error) و تعداد تابع عضویت مشخص می‌شود. بر اساس پیش فرض نرم‌افزار تعداد epoch معادل ده و Tolerance Error معادل صفر در نظر گرفته می‌شود. سپس فرآیند یادگیری با استفاده از دستور anfis آغاز می‌شود. زمانی که دور تکرار کامل شد، فرآیند یادگیری نیز به پایان می‌رسد. برای آزمون صحت دریافت نتایج از خروجی، از آماره RMSE استفاده می‌شود که برای مدل طراحی شده در این مقاله مقدار RMSE به دست آمده برابر با ۰,۰۸۵۹۶ که مقدار بسیار کوچکی است به دست می‌آید که بیانگر مناسب بودن مدل طراحی شده برای کشف تقلب پولشویی است. از طرف دیگر با استفاده از دستور evalfis می‌توان مقدار عددی خروجی حاصل از اجرای سیستم منطق فازی را به دست آورد. خروجی این نرم افزار، کشف تقلب پولشویی است که مقدار عددی آن برابر با ۰,۱۴۷۰ شده است. با توجه به اینکه مقدار عددی خروجی در دامنه صفر و یک تعریف شده بود و مقدار عددی کمتر از ۰,۵ بیانگر کم بودن احتمال رخداد تقلب پولشویی است، بنابراین مقدار عددی ۰,۱۴۷۰ بیانگر کم بودن احتمال رخداد پولشویی است.

۵. نتیجه‌گیری و جمع‌بندی

این مقاله به طراحی و ارائه سیستم منطق فازی با روش استنتاج ممدانی برای کشف تقلب پولشویی پرداخت. داده‌های به کار رفته در این مقاله در قالب متغیرهای کلامی جمع‌آوری شده است. از این رو از تئوری منطق فازی در طراحی سیستم استفاده شد. خروجی سیستم مد نظر متغیر شناسایی تقلب پولشویی است. سیستم فازی طراحی شده می‌تواند تمام حساب‌های کاربران را پس از شناسایی، در قالب سه گروه کم، متوسط و زیاد دسته‌بندی کند. ادعای پولشویی که در گروه کم قرار می‌گیرد، می‌تواند مورد چشم‌پوشی قرار گیرد. مواردی که در گروه متوسط قرار می‌گیرند، نیازمند بررسی مشخصات مشتری صاحب حساب در چارچوب مقررات شناسایی مشتریان است و آن دسته از مواردی که در گروه زیاد قرار می‌گیرند، نیازمند ارائه گزارش به واحد پولشویی جهت رسیدگی بیشتر است. نتایج حاصل از اعتبارسنجی سیستم پیشنهادی، بیانگر صحت و اعتبار بالای سیستم پیشنهادی است. مشخصه‌های اصلی سیستم پیشنهاد شده عبارت هستند از:

- این سیستم نه تنها می‌تواند به‌طور مستقل پولشویی را تشخیص دهد، بلکه می‌تواند از محیط نیز آموزش دیده و تغییرات محیطی را پذیرفته و تصمیم‌گیری نماید. به‌طوری‌که تصمیمات توسط انسان قابل تفسیر باشد.
- بواسطه عامل کاربر، سیستم ضد پولشویی طراحی شده می‌تواند با برنامه مالی هماهنگ باشد.
- اضافه کردن و کم کردن و حذف کردن قواعد کسب و کار و سناریوهای پولشویی در آن راحت است.
- این روش می‌تواند، برای کسب و کار مناسب باشد، به دلیل اینکه هزینه‌های کشف پولشویی را کاهش داده و بهره‌وری واحد کشف پولشویی را افزایش دهد.

در پایان پیشنهاد می‌شود، هر بانک سیستم ضد پولشویی هوشمند طراحی نماید که این سیستم قادر به دریافت اطلاعات از واحد اطلاعات مالی و تجزیه و تحلیل پروفایل مشتریان و تجزیه و تحلیل حساب‌های مشتریان بدون نیاز به هویت آنها باشد.



در پایان پیشنهاد می‌شود، هر بانک سیستم ضد پولشویی هوشمند طراحی نماید که این سیستم قادر به دریافت اطلاعات از واحد اطلاعات مالی و تجزیه و تحلیل پروفایل مشتریان و تجزیه و تحلیل حساب‌های مشتریان بدون نیاز به هویت آنها باشد. کارکنان بانک‌ها نیز می‌بایست در انجام کارهای روزمره خود، طبق دستورالعمل‌های بانکی به مواردی از قبیل شناخت هویت و ماهیت کار مشتری، تغییرات ناگهانی فعالیت مالی با توجه به شغل مشتریان و تحقیق از امور مشتری در صورت هر گونه شک و تردید، توجه و دقت لازم را داشته باشند.

۶. مراجع

1. Sammer ,M., O'Neill.M., Brahazon.A., and Kechadi,. M-tahar,. 2011. An Investigation into Data mining approaches for Anti Money Laundering,. International Conference an computer Engineering and Applications, IPCSIT, Vo, 2(2011).
2. Wat kins, R.C. et al.2003. Exploring Data mining tehнологies as tool to investigate money laundering ., Journal of policing practice and Research: An International Journal. Vol, 4. No.2, January 2003, PP:163-178.
3. Han, J and Kamber,M. 2005. Data Mining: Concept and Techniques. Morgan Kaufmann Publishers, 2nd EDs., Nov, 2005
4. Umadevi, P., Divya, E,. 2012. Money Laundering detection using TFA System. ICEMA,. International Conference on digital object Identifier.
۵. پیرسرایی، زربخش و اسداله شاه بهرامی، (۱۳۹۳). ضرورت استفاده از سیستمهای تشخیص پولشویی در بانکداری الکترونیکی. فصلنامه روند سال بیست و یکم، شماره ۶۸، زمستان ۱۳۹۳، صفحات ۱۷۹-۲۱۲.
6. Horobin,I. 2001. Applying technology to fight moey laundering. Money laundering Bulletin, Apr, 2001.
7. Wicks. T,. 2001. Intelligent Systems for money laundering prevention. Money laundering Bulletin, App, 2001.
8. Menon,R. and Kuman,S. 2005. Understanding the role of technology in Anti money Laundering Complianc., Infosys Technology Ltd, Jan, 2005.
9. Suresh,Ch,. Thammi Reddy,T,.2015. A Method to enhance money laundering Detection using Link Analysis., International Journal of advanced Research in computer Science and software engineering,. Vol. 5. Issue 11, November 2015.
10. Kingdon, J.2004. AI Fights Money Laundering, IEEE Transactions on Intelligent Systems, 2004, PP. 87-89.
11. Tang, J.2005. A Framework on developing an Intelligent discriminating system of anti money laundering., International Conference on Financial and banking , CZECH Rep,. 2005.
12. Zang,Z,. J.Salcrmo, J,. and YU,P.S.2003. Applying Data Mining in Investigating money laundering crimes,. SIG KDD,03, August 2003, Washington DC, USA. PP:747-752.
13. Jain,R,. Kasturi, R,. and Schunk, B.G.1995. Machine vision. Published by McGraw-Hill, INC., ISBN 0-07-032018-7



هفتمین همایش سالانه
بانکداری الکترونیک
و نظام‌های پرداخت

تهران، مرکز همایش‌های بین‌المللی برج میلاد - ۲ و ۳ بهمن ۱۳۹۶

7th Annual Conference
on Electronic Banking
and Payment Systems

نوآوری، بازیگران جدید و کارایی در کسب و کار مالی



14. Vapnik, V., 1995. The nature of statistical learning theory., Springer verlag, new York.
15. Scholkopf, B., 2000. A Short Tutorial on Kernels, Microsoft Research, Rech Rep: MSR-TR-200-6t, 2000.
16. Chen, Yu-To, Mathe John., 2011. Fuzzy computing applications for Anti-money laundering and distributed storage system load monitoring., World conference on soft computing (2011)

۱۷. صادقی، حسین ، عباس عصارى وحدى شقاقى شهرى. ۱۳۸۹ . اندازه گیری فساد مالی در ایران با استفاده از منطق

فازی. پژوهشنامه اقتصادی سال دهم شماره چهارم زمستان ۱۳۸۹

۱۸. احمدی نژاد منفرد، مریم.(۱۳۸۸). پولشویی و سیستم مالی شامل آثار اقتصادی، اجتماعی، فرهنگی. مجله توسعه

صادرات، سال سیزدهم، شماره ۷۸، صص ۳۸-۴۱.