**فصلنامه سیاست‌های مالی و اقتصادی**

سال ششم، شماره ۲۱، بهار ۱۳۹۷، صفحات ۱۳۳ – ۱۰۹

# پیشنهاد یک متدولوژی برای کشف پول‌شویی (با به‌کارگیری روش منطق فازی)

**اعظم احمدیان**

عضو هیئت علمی گروه بانکداری، پژوهشکده پولی و بانکی، بانک مرکزی ایران (نویسنده مسئول)

Azam_ahmadyan@yahoo.com

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 کسب‌وکارها تحمیل می‌کند. درنتیجه شناسایی جرم به مسئله بسیار مهمی تبدیل شده است. یکی از جرم‌هایی که منجر به ایجاد اختلال در عملکرد بانک‌ها می‌شود، جرم پول‌شویی است که تلاش‌های گسترده‌ای در سطح بین‌الملل جهت کشف آن در حال انجام است. 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 تجزیه‌وتحلیل قرار می‌دهد، به نوعی با شناخت رفتار کاربران یا مشتریان سعی در پیش‌بینی رفتار آتی آن‌ها داشته و ریسک انجام 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 شود. 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. آزمون اعتبار مدل بیانگر RMSE=0.08 است. نتیجه حاصل، بیانگر مناسب بودن مدل برای کشف پول‌شویی است.

طبقه‌بندی C54, C87, G21:JEL

واژگان کلیدی: جرم پول‌شویی، بانکداری الکترونیک، مکانیسم ضد پول‌شویی.

* تاریخ دریافت: ۱۳۹۶/۴/۲۳ تاریخ پذیرش: ۱۳۹۶/۹/۱۳

[ Downloaded from qjfep.ir on 2026-11-24 ]

## ۱. مقدمه

پدیده پول‌شویی فرایندی 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 به دست می‌آورند، با روش‌های قانونی به پول تمیز تبدیل کنند. امروزه فرایند پول‌شویی سومین و بزرگ ترین تجارت در جهان بعد از مبادله ارزی و صنعت خودرو است. بنابراین شناسایی و پیش‌بینی آن دارای اهمیت است.[1]

گسترش فن آوری اطلاعات و توسعه ابزارهای الکترونیکی نقل و انتقال وجوه، رخداد پدیده پول‌شویی را برای مجرمین سهل‌تر کرده است. همین امر موجب شده است که 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 کند. برای کشف پدیده پول شویی می توان از روش سنتی یا روش هوشمند استفاده کرد. روش سنتی فرایند ضد پول‌شویی یک روش مبتنی بر انسان است که در این روش پدیده پول‌شویی کشف و شناسایی شده و از رخ دادن آن ممانعت می‌شود[2]. در مقابل، ارزش داده‌های بانکی و تراکنش‌های بانکی با روش‌های مختلف افزایش یافته است و به‌کارگیری روش‌های سنتی برای کشف پول‌شویی زمان‌بر و پرهزینه بوده و گاهی اوقات غیرممکن است. بنابراین روش‌هایی نیاز است که به‌صورت اتوماتیکی جرم پول‌شویی را کشف کند[3].

در برهه کنونی شبکه بانکی کشور در تلاش برای پیوستن به شبکه بانکی بین‌المللی است، بنابراین ضرورت دارد موانع موجود در این زمینه در شبکه بانکی شناسایی و قبل از هر نوع برقراری رابطه با بانک‌های بین‌المللی رفع شود. یکی از مهم‌ترین گزینه‌ها برای بانک‌های بین‌المللی عدم وجود پدیده پول‌شویی در بانک‌های طرف ارتباط است. این موضوع ضرورت

1. Sammer et al. 2011.
2. Wat kins et al.2003.
3. Han and Kamber.2005.

[ Downloaded from qjfep.ir on 2026-11-24 ]

طراحی مکانیسمی که بتواند پول شویی را کشف کند، برجسته ساخته است. هدف از این تحقیق طراحی مکانیسمی که هم به بانکداران و هم به سیاست گذاران و هم به ناظران بانکی کمک کند که بهتر بتوانند فرایند مالی موجود در بانک خود را کنترل کنند و هرگونه تراکنش مشکوک را با دقت بررسی کرده و در صورت وجود احتمال بالای پول شویی، از تحقق آن ممانعت به عمل آورند.

به دلیل اهمیت موضوع، در این مقاله سعی شده است با توجه به ادبیات نظری و تجربی موجود در زمینه کشف پول شویی، مکانیسم هوشمندی طراحی شود. این مکانیسم صرفاً احتمال رخداد پدیده پول شویی را نشان می‌دهد و درواقع یک مکانیسم هشدار برای کشف پول شویی است و دقت مدل طراحی‌شده به منزله وجود پول شویی در بانک مورد بررسی نیست. در همین راستا در بخش دوم مقاله، ادبیات نظری و تجربی پدیده پول‌شویی و طراحی مکانیسم ضد پول‌شویی و در بخش سوم ،مکانیسم ضد پول‌شویی طراحی‌شده برای کشور و در پایان نیز جمع‌بندی مقاله بیان شده است.

## ۲. ادبیات نظری و تجربی طراحی مکانیسم کشف پول‌شویی

### ۲-۱. سیستم‌های ضد پول‌شویی[1] هوشمند

فرایند پول شویی، فرایندی است که در آن درآمدهای نامشروع، مشروع شده و مجرمین سعی می‌کنند که پول‌هایی که از روش‌های نامشروع به دست می‌آورند را پاک کنند. فراهم بودن امکان انجام عملیات بانکی گوناگون و گسترده برای مشتریان، بدون حضور فیزیکی و به طور شبانه‌روزی در بانکداری الکترونیکی، این امکان را برای پول‌شویان فراهم می‌کند تا بدون اینکه 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 آسان‌تر می‌کند. فرایند پول‌شویی می‌تواند آثار منفی بر فعالیت‌های مالی اقتصادی داشته باشد. بنابراین شناسایی و پیش‌بینی آن دارای اهمیت است. با توجه

1. Anti money laundering system

[ Downloaded from qjfep.ir on 2026-11-24 ]

به اهمیت موضوع، بسیاری از نهادهای مالی در تلاش برای مبارزه با پول‌شویی، سیستم‌های ضد پول‌شویی را بسط داده‌اند و برای پیاده‌سازی آن برنامه‌ریزی کرده‌اند. چهار نوع سیستم ضد پول‌شویی در کشورهای مختلف در حال پیاده‌سازی است که عبارتند از: سیستم ضد پول‌شویی بر مبنای قاعده، سیستم ضد پول‌شویی چندعاملی، سیستم ضد پول‌شویی تحلیل جریان تراکنش و سیستم ضد پول‌شویی لینک. در سیستم ضد پول‌شویی بر مبنای قاعده، کشورها بر اساس قوانین موجود در کشور خود و همچنین بر اساس قواعد بین‌المللی، معیارهایی را برای شناسایی تراکنش‌های مشکوک تعریف می‌کنند. سپس بر اساس آن معیارها به کشف پول‌شویی می‌پردازند. در سیستم ضد پول‌شویی چندعاملی، چندین عامل در شناسایی پول‌شویی دخیل بوده و وظایف خاص خود را دارند. عامل‌ها در تعامل با یکدیگر و با تجزیه‌وتحلیل پروفایل مشتریان و اندازه‌گیری ریسک معاملات به کشف پول‌شویی می‌پردازند. در سیستم تحلیل جریان تراکنش، تراکنش‌های بانکی با به‌کارگیری روش داده‌کاوی به دو گروه سالم و مشکوک تقسیم می‌شوند. سپس با تجزیه‌وتحلیل تراکنش‌های مشکوک و پروفایل مشتریان مربوط به تراکنش‌های مشکوک، پول‌شویی کشف می‌شود. در سه روش قبلی امکان کشف پول‌شویی برای داده‌های بزرگ وجود ندارد. اما در سال‌های اخیر با به‌کارگیری روش big data سیستمی تحت عنوان سیستم لینک طراحی شده است که به صورت هم‌زمان به تجزیه‌وتحلیل تراکنش‌ها و پروفایل مشتریان می‌پردازد و بر اساس قواعد تصمیم، پدیده پول‌شویی کشف می‌شود. با توجه به اهمیت موضوع شناسایی سیستم‌های مختلف ضد پول‌شویی، در ادامه چهار سیستم معرفی شده در سطوح بالا به صورت مشروح بیان می‌شوند.

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 چندعاملی، سیستم ضد پول‌شویی تحلیل جریان تراکنش و سیستم ضد پول‌شویی لینک بیان می‌شود.

[ Downloaded from qjfep.ir on 2026-11-24 ]

برای پیاده‌سازی سیستم ضد پول‌شویی بر مبنای قاعده، نهادهای مالی سعی کرده‌اند، معیارهایی را برای شناسایی معاملات مشکوک به کار گیرند که به این نوع سیستم‌ها، سیستم‌های بر پایه قاعده[1] می‌گویند. مشخصه‌های کلی این نوع سیستم‌ها عبارتند از[2]:

- این سیستم‌ها ناتوان از شناسایی پول‌شویی در مواردی هستند که مبالغ معاملات کوچک است.
- در این نوع سیستم‌ها، مسئله اشتباه مثبت[3] 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، جهان‌شمول 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 چندعاملی ایجاد و بسط یافته است. مشخصه‌های اصلی این سیستم‌ها عبارتند از[4]:

- یک سیستم هوشمند بر مبنای عامل، یک سیستم کامپیوتری است که در یک فضای هوشمند قادر است به اهداف طراحی شده دست یابد.
- 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، انعطاف‌پذیر است. به‌طوری‌که با تغییر شرایط محیطی باز هم کارا و اثربخش خواهد بود.
- سیستم‌های هوشمند بر مبنای عامل[1] در مقایسه با سیستم‌های هوشمند بر مبنای قاعده، انعطاف‌پذیری و کارایی بیشتری داشته و می‌توانند به صورت غیرمتمرکز نیز اثربخش باشند.

1. Rule- based Systems
2. Horobin,. 2001.
3. Problem of false positive
4. Wicks,T. 2001.

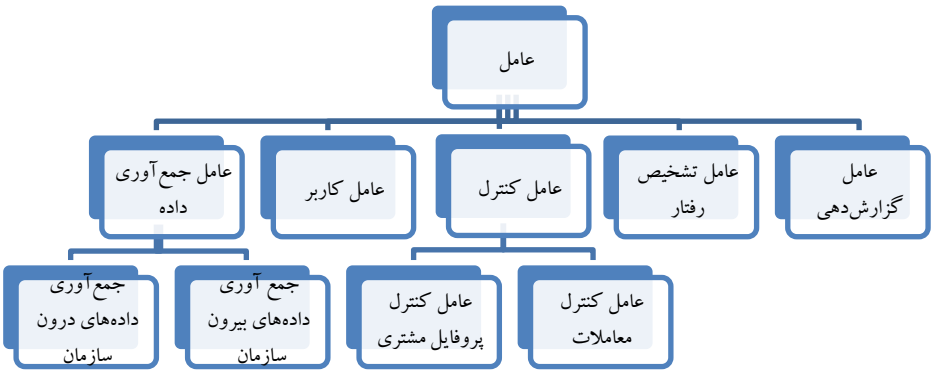
[ Downloaded from qjfep.ir on 2026-11-24 ]

- این سیستم برای دستیابی به اهداف، نیاز به استفاده از دانش محیطی و رفتارهای سیستم های دیگر برای برنامه‌ریزی دارد.
- رابطه بین عوامل در یک فضای هوشمند نظیر فضای اینترنت صورت می گیرد.
- این سیستم‌ها برای شناسایی ریسک‌های پیش روی نهادهای مالی با هر میزان معامله (چه کوچک چه بزرگ) مناسب بوده و به‌کارگیری آن‌ها باعث بهبود فضای کسب‌وکار می‌شود.

برای طراحی ساختار یک سیستم ضد پول‌شویی چندعاملی، فرایند ضد پول‌شویی در چند زیرمجموعه طراحی می شود[۲]. هر عامل وظیفه خاصی بر عهده داشته و با دیگر عوامل نیز برای دستیابی به هدف کل سیستم همکاری دارد. فرایند ضد پول شویی چندعاملی مجموعاً شامل عامل جمع آوری داده[۳]، عامل کاربر[۴]، عامل کنترل ریسک پول‌شویی[۵]، عامل تشخیص رفتار[۶] و عامل گزارش‌دهی[۷] 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 (۱) چارچوب کلی یک سیستم ضد پول‌شویی هوشمند بر مبنای عامل نشان داده شده است.

1. Agent-based
2. Menon,R. and Kuman,S. 2005.
3. Data Connecting Agent
4. User agent
5. Monitoring agent
6. Behavior Diagnosing agent
7. Reporting agent

[ Downloaded from qjfep.ir on 2026-11-24 ]




مأخذ: ویکس، ۲۰۰۱

شکل ۱. ساختار سیستم هوشمند چندعاملی

عامل کاربر، کاربران را قادر می‌سازد، وضعیت جاری معاملات مالی، کنترل پول‌شویی، تشخیص و فرایند گزارش‌دهی را انجام دهند و آن‌ها را برای قضاوت و کشف پول‌شویی در سایر بخش‌های مالی به کار ببرند. عامل جمع‌آوری داده، سیستم را قادر به جمع‌آوری داده از درون و بیرون سازمان می‌سازد. عامل کنترل، داده‌ها را از عامل جمع‌آوری داده، دریافت کرده 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 کرده و به عامل کاربر هشدار می‌دهد تا فعالیت‌ها را مدیریت کند.

[ Downloaded from qjfep.ir on 2026-11-24 ]

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)[1] بیان شده است. این سیستم امکان تبدیل داده‌های کمی به صورت گزارش‌هایی فراهم می‌کند. ساختار این سیستم مشتمل بر ۷ بخش است که عبارتند از: مرحله قبل از پردازش[2]، ورودی داده[3]، خوشه‌بندی و شناسایی وضعیت مشکوک[4]، نمایش داده[5]، یادگیری از تصمیم کاربر[6]، ایجاد پروفایل بانک[7]، استخراج رفتار[8]. مرحله قبل از پردازش داده‌ها، دارای دو زیرمجموعه است. مجموعه پیش از انتقال داده[9] و مجموعه انتقال داده[10]. این مرحله داده های خام را دریافت کرده 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 دو بار ثبت شوند. بعد از ترکیب داده‌ها، عملیات پاک‌سازی داده صورت می‌گیرد تا داده‌های دو بار ثبت‌شده را از پایگاه داده پاک می‌کند و داده‌ها برای واحد تبدیل داده[11] 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

1. Umadevi and Divya(2012).
2. preprocessing
3. Data importer
4. Clustering and suspected
5. Data visualization
6. Learning from the user decision
7. Company/organization profile generation
8. Extracting behavior
9. Pre data transform unit(pre-DTU)
10. Data transform unit
11. Data transform unit

[ Downloaded from qjfep.ir on 2026-11-24 ]

واردشده 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 درنهایت 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 داده‌شده و ... وجود دارد. از طرفی پروفایل بانک ممکن است در طول فرایند تحلیل داده فیلتر شود و درنتیجه 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. درنتیجه 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)[1] سیستمی را طراحی کرده‌اند که از تحلیل لینک برای کشف تقلب در حساب‌های بانکی استفاده می‌شود. در این مقاله یک رویکرد پایه اکتشافی[2] طراحی شده است که از قواعد تصمیم برای تحلیل لینک با پذیرش تکنیک جدول چند پیوندی[3] 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

1. Suresh,Ch,. Thammi Reddy,T,.2015.
2. heuristic base approach
3. Multi table joins

[ Downloaded from qjfep.ir on 2026-11-24 ]

شناسایی می‌کند. این سیستم دارای سه مرحله است. گزارش معاملات مشکوک به واحد اطلاعات مالی[1]، 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 یک‌هفته‌ای 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 باکیفیت 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 می شوند. به عنوان مثال جزئیاتی نظیر مقدار[2]، مشخصه تراکنش[3]، از کدام حساب[4]، به کدام حساب[5] و تکرار[6] 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

1. Financial intelligence unit
2. amount
3. Transaction-id
4. From account
5. To account
6. frequency

[ Downloaded from qjfep.ir on 2026-11-24 ]

پول شویی مشکوک، پول از یک حساب به حساب های مختلف وارد شده و دوباره به یک حساب وارد می شود. 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 کند. این ارتباط بین تراکنش‌ها، مطالعه مشخصه‌های مشترک تراکنش‌ها را تسهیل می‌سازد. فهرست تراکنش های دریافت شده در واحد اطلاعات مالی با تراکنش هایی که در ارتباط با فعالیت پول‌شویی اتفاق می‌افتند، تطبیق داده می‌شوند. هر تراکنش در پایگاه داده‌ای به عنوان یک گره[1] استفاده می شود. هر گره با تراکنش های قبلی مرتبط شده و با کنترل کردن سایر تراکنش‌ها با حساب های مشکوک مرتبط می شوند. قواعدی نظیر وجود چند حساب، مشخصه‌های مشتری، سابقه مشتری در زمینه پول شویی و تقلب، ماهیت تراکنش و ارزش تراکنش می تواند در مرحله لینک به شناسایی تراکنش‌های مشکوک به پول‌شویی کمک کند.

کلاییدو و جاوو (۲۰۱۶)[2]، با استفاده از روش چندعاملی و پروفایل مشتریان به طراحی مکانیسم هوشمند برای کشف پدیده پول شویی در کشور پرتغال پرداخته‌اند. به همین منظور ابتدا ساختار کلی مدل و سپس عناصر مرتبط با آن بیان شده است. در این راستا ابتدا پروفایل مشتریان بر اساس قواعد مشخص خوشه‌بندی شده و تراکنش‌های مشکوک کشف شده است. قواعد بر اساس مقررات موجود در این کشور طراحی شده است.

کاروته و شیرساگر (۲۰۱۴)[3]، با استفاده از طراحی سیستم بر مبنای تحلیل جریان تراکنش، به طراحی مکانیسم کشف پول شویی در کشور هند پرداخته‌اند. به همین منظور از تحلیل رفتار مشتریان بانک‌ها با استفاده از خوشه‌بندی مشتریان برای کشف پول‌شویی استفاده شده است. بنابراین برای خوشه‌بندی از سوابق الگوریتم خوشه‌بندی استفاده شده و برای استخراج الگو از سوابق و یادگیری الگوی تصمیمی کاربر، معماری مکرر الگو استفاده شده است. حداقل آستانه

1. node
2. Claudio and Joao,. 2016.
3. Kharote, and Kshirasagar. 2014.

[ Downloaded from qjfep.ir on 2026-11-24 ]

مناسب برای انتقال از یک حساب یا توسط فرد در یک حساب مشخص به صورت پیش‌فرض تعیین شده است. دقت بالای ۹۰ درصد در این مکانیسم حاکی از مناسب بودن مدل برای کشف پول‌شویی بوده است.

هلمی و همکاران (۲۰۱۴)[1] از سه روش کشف پول‌شویی بر مبنای قاعده، خوشه‌بندی و تحلیل لینک برای کشف پول‌شویی در کشور مصر استفاده کرده‌اند. در این مقاله با توجه به نتایج حاصل از طراحی سیستم‌های مختلف، سیستم لینک برای کشف پول‌شویی استفاده شده است. این سیستم با دو سیستم بر مبنای قاعده و بر مبنای ریسک تجزیه‌وتحلیل شده است. روش بر مبنای ریسک از پروفایل مشتریان و تراکنش‌ها استفاده می‌کند. سیستم بر مبنای قاعده نیز از چارچوب کشف پول‌شویی در قوانین موجود در کشور مصر استفاده می‌کند.

پیرسرایی و شاه بهرامی (۱۳۹۳)، به بررسی و مطالعه سیستم‌های تشخیص پول‌شویی در جهت پیشنهاد یک سیستم مناسب برای بانک ملی پرداخته است. افزون بر این، با توجه به مجموعه مقررات و قوانین بانک مرکزی و سیستم بانکی کشور و تجربه مؤلف در بانک ملی یک سیستم هوشمند ضد پول‌شویی برای بانکداری الکترونیکی مورد تجزیه‌وتحلیل و طراحی قرار گرفته است و نشان داده شده است که با پیاده‌سازی این سیستم می‌توان عملیات ضد پول‌شویی را در فضای الکترونیکی مؤثرتر انجام داد. در این مقاله برای طراحی سیستم ضد پول شویی، از یک مدل چندعاملی استفاده شده است.

خدادی (۱۳۹۲)، به بررسی تأثیر قوانین و دستورالعمل‌های مبارزه با پول‌شویی به عنوان دو عامل اصلی شناسایی‌شده برای مبارزه با پول‌شویی در کشور بر میزان موفقیت آن در بخش بین‌الملل بانک ملت می‌پردازد. در این مقاله پس از شناسایی عوامل با استفاده از تحلیل عاملی اکتشافی و با چرخش واریماکس و تعیین دو عامل مهم تأثیرگذار، برای سنجش تأثیر قوانین و دستورالعمل‌های موجود بر مبارزه با پول‌شویی، از دو فاکتور قوانین مبارزه با پول‌شویی و

1. Helmy et al. 2014.

[ Downloaded from qjfep.ir on 2026-11-24 ]

دستورالعمل‌های دقیق و شفاف در این زمینه استفاده شده و تأثیر آن بر مبارزه با پول‌شویی سنجیده شده است. نتایج حاکی از این است که قوانین و دستورالعمل های مربوطه بر میزان موفقیت بانک ها در مبارزه با پول‌شویی تأثیر مستقیم داشته و ارتباط معنی‌دار بین اجرای این قوانین و دستورالعمل‌ها بر کاهش اثرات مخرب این جرم بر جامعه وجود دارد.

## ۲-۲. روش‌های مرسوم داده‌کاوی در فرایند ضد پول‌شویی

برای طراحی تکنیک داده‌کاوی کارا که قادر به کشف پول‌شویی باشد، نیاز است که آن متناسب با کشف پول‌شویی طراحی شود[1]. در میان روش‌های مختلف داده‌کاوی، مهم‌ترین روش‌های مورد استفاده در کشف پول‌شویی، روش خوشه‌بندی، روش ماشین بردار و روش فازی است. خوشه‌بندی فرایندی 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[2].

در این روش مشتریان و زمان تراکنش به n+2 فضای اقلیدسی تقسیم می‌شوند به‌طوری‌که n مشتری به l زمان و l تراکنش تقسیم می‌شوند. در این روش ابتدا کل زمان به فاصله‌های زمانی مختلف تقسیم می شود. 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 کرده و آن را خوشه‌بندی می‌کند. 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 تراکنش های مالی با مقادیر مختلف را برای دوره زمانی طولانی تحلیل نماید. در

1. Tang, J.2005.
2. Zang,Z,. J.Salcrmo, J,. and YU,P.S.2003.

[ Downloaded from qjfep.ir on 2026-11-24 ]

این شرایط کشف پول‌شویی سخت است به‌خصوص مواردی که هیچ نوع قله برجسته‌ای در هیستوگرام وجود نداشته باشد یا قله برجسته اندک باشد. بنابراین تحلیل های 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[1].

روش دیگر داده‌کاوی برای کشف پدیده پول‌شویی، ماشین بردار پشتیبان است که ازجمله روش‌های آماری است که برای دسته‌بندی و رگرسیون استفاده می‌شود. ابزار ضد پول‌شویی شامل کشف رفتار غیرمعمولی همه موارد نظیر تراکنش‌ها، حساب‌ها و انواع خروجی‌ها است. بنابراین مسئله پول‌شویی زمانی کشف می‌شود که داده‌های گروه‌بندی‌شده به دو دسته مجموعه‌های نرمال و غیر نرمال تقسیم می‌شوند. برای سنجش اعتبار مدل طراحی‌شده 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 داده های مالی معمول است، حساس نیست[2]. ماشین بردار پشتیبان با یک روش آموزش نظارت‌شده، داده‌های مورد نیاز برای آموزش را ایجاد می‌کند تا بتواند قوانین دسته‌بندی را ایجاد نماید. ماشین بردار یک طبقه‌ای[3] نظارت‌نشده برای کشف داده‌های خارج از محدوده[4] به کار می‌رود که برای مجموعه آموزش پول‌شویی مناسب

1. Jain,R,. Kasturi, R,. and Schunk, B.G.1995.
2. Vapnik,V.1995.
3. One class SVM
4. outlier

[ Downloaded from qjfep.ir on 2026-11-24 ]

است[۱]. به این ترتیب که مجرمین پول شویی که تلاش می کنند، فعالیت خود را مخفی کنند، با تحلیل داده‌های خارج از محدوده، قابل شناسایی می شوند. درنهایت آنچه مهم است این است که داده های مالی ناهمگن هستند. بنابراین به همراه ماشین بردار پشتیبان باید از تکنیک های تکمیلی نیز برای تحلیل داده‌های مالی ناهمگن استفاده شود[۲].

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 است. کنترل و بررسی داده‌ها، نخستین گام در کشف پدیده پول‌شویی است. اگر موارد خاص در فرایند نظارت و کنترل کشف شد، گام بعدی در منطق فازی، اطمینان از وجود پدیده پول شویی است. در پایان نیز یک استراتژی کنترلی برای مدیریت مسائل مورد نیاز است.[۳] در منطق فازی به طور معمول عبارت‌ها و گزاره‌ها به صورت اگر و آنگاه بیان می‌شوند. این عبارت‌ها را قاعده‌های زبانی[۴] یا قاعده‌های گفتاری می‌نامند. یک قاعده گفتاری، گزاره شرطی اگر و آنگاه متکی به متغیرهای گفتاری است. چنانچه به جای عبارت گفتاری از یک تابع خاصی استفاده شود، سیستم فازی ایجادشده را سیستم فازی تاکاگی- سوگنو- کانگ[۵] می‌نامند. سیستم‌های فازی که در آن عبارت‌های گفتاری به جای توابع خطی استفاده می‌شود، سیستم‌های فازی ممدانی[۶] می‌نامند[۷].

در طراحی سیستم کشف پول شویی با استفاده از روش منطق فازی، ابتدا باید از منابع مختلف، داده‌های مورد نیاز را جمع آوری کرد. منابع اصلی که برای تحلیل داده‌ها مورد نیاز است، عبارتند از: مدل‌های موجود برای کشف تقلب که داده‌های مشکوک به تقلب را از سایر داده‌ها متمایز

1. Scholkopf, B, 2000.
2. Tang, J,2005.
3. Chen, Yu-To, Mathe John,. 2011.
4. Linguistic Rules
5. Takagi-sugeno-kang
6. Mamdani Fuzzy System

۷. صادقی و عصاری وحدی شقاقی شهری، ۱۳۸۹.

[ Downloaded from qjfep.ir on 2026-11-24 ]

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 هستند. پس از جمع آوری داده، قواعد با استفاده از معیارهایی که مشخص کننده پدیده پول‌شویی هستند، به صورت اگر و آنگاه تعریف شده و در پایان نیز استنتاج فازی برای کشف پدیده پول‌شویی صورت می‌گیرد[1].

در این مقاله سعی شده است از روش منطق فازی برای کشف پدیده پول‌شویی استفاده شود.

## ۳. مکانیسم پیشنهادی برای کشف پول‌شویی در شبکه بانکی کشور

در این مقاله سعی شد ابتدا با استفاده از روش‌های خوشه‌بندی، ماشین بردار، شبکه عصبی و مکانیسم منطق فازی، مکانیسم کشف پول شویی طراحی شود. سپس با به کارگیری معیارهای مناسب، مدل مناسب برای طراحی مکانیسم کشف پول شویی انتخاب شود. به همین منظور ابتدا بر اساس مقررات موجود در کشور و بر اساس ادبیات نظری، معیارهایی برای کشف پدیده پول شویی استفاده شده است. سپس تابع عضویت سیستم فازی تعریف شده و در پایان نیز استنتاج فازی صورت گرفته است. با توجه به قانون مبارزه با پول‌شویی مهم‌ترین معیارهای شناسایی پول‌شویی، عدم رعایت سقف مقرر و سپرده گذاری 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 پرتکرارترین الگوهای پول‌شویی به حساب می‌آید و سیستم باید نسبت به آن حساس بوده و این گونه الگوها را تشخیص دهد. برای طراحی این سیستم با بهره گیری از نرم‌افزار MATLAB2015 از ۱۵۰۰ حساب در یک بانک در یک دوره سه‌ماهه استفاده شده است.

1. Chen, Yu-To, Mathe John,. 2011.

[ Downloaded from qjfep.ir on 2026-11-24 ]

برای انتخاب سیستم مناسب برای کشف پدیده پول شویی، از چهار شاخص خطای نوع اول، خطای نوع دوم، دقت کلی مدل و معیار خطای جذر میانگین مربعات[1] استفاده شده است. در این پژوهش فرض صفر، بیانگر وجود علائم مشکوک به پول‌شویی است. خطای نوع اول احتمال رد فرض صفر به شرط درست بودن آن و خطای نوع دوم احتمال قبول فرض صفر به شرط غلط بودن آن است.

در تحلیل اعتبار[2]، اگر یک حساب مستعد پول شویی به صورت سالم دسته‌بندی شود، خطای نوع اول به معنی عدم هشدار به آن بانک و ادامه همان روند اشتباه از سوی آن بانک است، اما خطای نوع دوم که نتیجه دسته‌بندی یک حساب سالم در زمره حساب های مشکوک است منجر به توجه بیشتر به معیارهای کشف پدیده پول‌شویی در مورد آن حساب می‌شود. به همین دلیل خطای نوع اول هزینه بیشتری نسبت به خطای نوع دوم دارد و از این رو از اهمیت بیشتری برخوردار است.

در این پژوهش، از هر چهار معیار معرفی‌شده، برای ارزیابی مدل استفاده شده است. نتایج در جدول زیر مشخص شده است. همان‌طور که مشاهده می‌شود، روش منطق فازی با دقت ۹۷/۲۰٪ و با کمترین مقدار خطای جذر میانگین مربعات، بهترین روش برای شناسایی پدیده پول‌شویی شناسایی شده است. بنابراین در این مقاله یک مکانیسم منطق فازی برای کشف پول شویی طراحی است، که در ادامه به‌صورت مشروح این مکانیسم تشریح می‌شود.

جدول ۱. نتایج حاصل از مدل‌سازی از طریق روش‌های داده‌کاوی

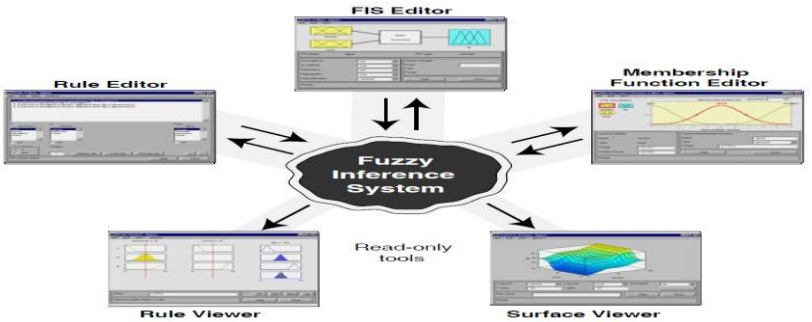
| | خوشه‌بندی | ماشین بردار | شبکه عصبی | منطق فازی |
|---|---|---|---|---|
| معیار خطای جذر میانگین مربعات | ۰/۰۸۹۷۸ | ۰/۰۹۰۲۴ | ۰/۰۸۷۶۵ | ۰/۰۸۵۹۶ |
| دقت کلی مدل | ٪۹۰/۸۹ | ٪۸۷/۲۵ | ٪۹۵/۱۳ | ٪۹۷/۲۰ |
| خطای نوع اول | ٪۵/۵۷ | ٪۱۴/۳۳ | ٪۰/۰۲ | ٪۰/۰۰۰ |
| خطای نوع دوم | ٪۱۵/۳۷ | ٪۶۷/۱۴ | ٪۴۵/۸۶ | ٪۱۶/۵۶ |

مأخذ: یافته‌های تحقیق

1. root-mean-square error (RMSE)
2. Credit Analysis

[ Downloaded from qjfep.ir on 2026-11-24 ]

به طور کلی سیستم استنتاج فازی[1] شامل ۵ عنصر است که سیستم طراحی شده در این مقاله نیز در این چارچوب طراحی شده است. ویرایشگر استنتاج فازی[2] بیان می کند چه تعداد ورودی وجود داشته و نام آن‌ها چیست؟ این سیستم محدودیتی در تعداد ورودی‌ها ندارد. ویرایشگر تابع عضویت[3] برای تعریف توابع عضویت مرتبط با هر متغیر به کار می‌رود. ویرایشگر قواعد[4] برای ویرایش فهرست قواعدی که رفتار سیستم را تعریف می کند، به کار می‌رود. ناظر قواعد[5] برای مشاهده نمودار فازی به کار می‌رود. ناظر قواعد نشان می‌دهد کدام‌یک از قواعد فعال بوده و چطور توابع عضویت نتایج را تحت تأثیر قرار می‌دهد. نمایشگر سطح[6] برای مشاهده وابستگی خروجی‌ها با ورودی‌ها را نشان داده و سطح خروجی سیستم را ترسیم می کند.




مأخذ: یافته‌های تحقیق

شکل ۲. چارچوب استنتاج فازی

سیستم طراحی‌شده در این مقاله نیز در چارچوب استنتاج فازی بوده و نوع منطق فازی، روش ممدانی[7] است. برای فازی‌سازی متغیرها نیز از تابع مثلثی استفاده شده است.

1. Fuzzy Inference System
2. Fuzzy Inference System Editor
3. Membership Function Editor
4. Rule Editor
5. Rule Viewer
6. Surface Viewer
7. Mamdani

[ Downloaded from qjfep.ir on 2026-11-24 ]

در سیستم مدنظر این مقاله، دو ورودی و یک خروجی وجود دارد. سقف برداشت از حساب بانکی بر اساس قانون پول شویی 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 نرم افزار، احتمال رخداد 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.

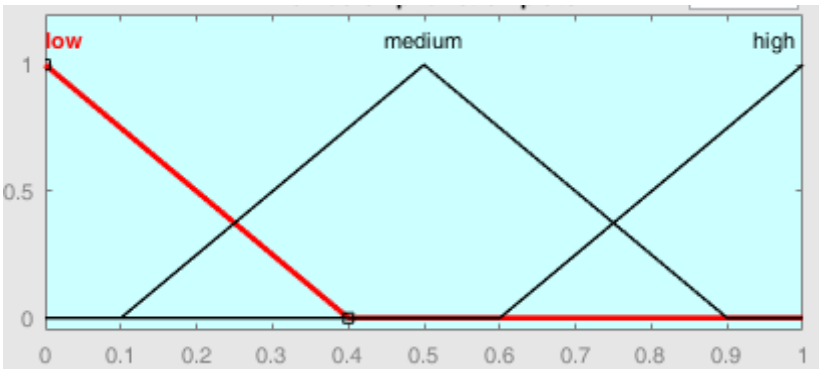
جدول ۲. معیارهای کشف پول‌شویی در مکانیسم طراحی‌شده

| معیارهای شناسایی پول‌شویی | کم | متوسط | زیاد |
|---|---|---|---|
| برداشت از سپرده بر حسب سقف مقرر (v5) | بین صفر تا ۱۵۰۰۰۰۰۰۰ ریال | بین ۱۵۰۰۰۰۰۰۰ تا ۵۰۰۰۰۰۰۰۰ ریال | بیش از ۵۰۰۰۰۰۰۰۰ ریال |
| فاصله زمانی بین برداشت و واریز وجوه (v9) | بیش از سه روز | بین دو تا سه روز | بین یک تا دو روز |

مأخذ: نتایج تحقیق

متغیرهای زبانی برای خروجی سیستم که متغیر شناسایی تقلب پول شویی 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 غیرمعمول بودن حساب‌ها، از کم به زیاد، افزایشی است.

[ Downloaded from qjfep.ir on 2026-11-24 ]




مأخذ: نتایج تحقیق

شکل ۳. تابع عضویت متغیر خروجی

پس از فازی سازی ورودی ها و تعیین درجه عضویت، نوبت به ساختار قواعد سیستم فازی می رسد. 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 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 پول شویی بسیار زیاد است. به صورت خلاصه قواعد این نرم‌افزار در جدول ۲ نشان داده شده است.

جدول ۳. 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) |

مأخذ: نتایج تحقیق

[ Downloaded from qjfep.ir on 2026-11-24 ]

پس از انتخاب قواعد، استنتاج فازی صورت می‌گیرد. روش‌های متفاوتی برای استنتاج در سیستم‌های فازی وجود دارد که از تفاوت در سه عملگر فازی[1] در قسمت فرض، دلالت بر فرض نتیجه[2] و تجمیع[3] نتایج ناشی می‌شود. درنهایت 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 (۴) مشاهده می‌شود.

جدول ۴. مشخصات سیستم فازی ممدانی

| | |
|---|---|
| Name=money laundering detection | AndMethod='min' |
| Type='mamdani' | OrMethod='max' |
| NumInputs=2 | ImpMethod='min' |
| NumOutput=1 | AggMethod='max' |
| NumRules=9 | DefuzzMethod='centroid |

مأخذ: نتایج تحقیق

پس از طراحی سیستم منطق فازی، ضروری است سیستم طراحی‌شده اعتبارسنجی شود. به همین منظور از سیستم فازی عصبی تطبیقی[4] استفاده شده است. برای اجرای این سیستم نیاز است که داده ها 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 گرادیانت[5] و حداقل مربعات برای شناسایی پارامترهای تابع عضویت استفاده می شود. بنابراین سیستم ANFIS طراحی‌شده یک شبکه عصبی چندلایه با روش یادگیری گرادیانت است که این روش برای تعیین پارامترها در لایحه پنهان به کار می‌رود. پارامترهای لایه خروجی به‌وسیله روش حداقل مربعات معمولی تعریف می‌شوند. ساختار عمومی ANFIS نیز شامل دو ورودی و یک

1. Fuzzy operator
2. Implication
3. Aggregation
4. Adaptive Neuro fuzzy inference(ANFIS)
5. Gradient

[ Downloaded from qjfep.ir on 2026-11-24 ]

خروجی است. برای ایجاد ANFIS به این ترتیب عمل می شود که ابتدا یک سیستم منطق فازی با نوع SUgeno و با نوشتن دستور genfis1 در صفحه دستور متلب، ایجاد می شود. پارامترهای تعداد دوره‌ها (epoch)، خطای تحمل (Tolerance Error) و تعداد تابع عضویت مشخص می‌شود. بر اساس پیش‌فرض نرم‌افزار تعداد epoch معادل ده و Tolerance Error معادل صفر در نظر گرفته می شود. سپس فرایند یادگیری با استفاده از دستور anfis آغاز می شود. زمانی که دور تکرار کامل شد، فرایند یادگیری نیز به پایان می رسد. برای آزمون صحت دریافت نتایج از خروجی، از آماره RMSE[1] استفاده می‌شود که برای مدل طراحی‌شده در این مقاله مقدار RMSE به‌دست‌آمده برابر با ۰/۰۸۵۹۶ که مقدار بسیار کوچکی است به دست می‌آید که بیانگر مناسب بودن مدل طراحی‌شده برای کشف تقلب پول شویی است. از طرف دیگر با استفاده از دستور evalfis می توان مقدار عددی خروجی حاصل از اجرای سیستم منطق فازی را به دست آورد. خروجی این نرم‌افزار، کشف تقلب پول شویی 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 پول شویی است، بنابراین مقدار عددی ۰/۱۴۷۰ بیانگر کم بودن احتمال رخداد پول‌شویی است.

## ٤. نتیجه‌گیری و جمع‌بندی

این مقاله به طراحی و ارائه سیستم منطق فازی با روش استنتاج ممدانی برای کشف تقلب پول شویی پرداخت. داده‌های به کاررفته در این مقاله در قالب متغیرهای کلامی جمع آوری شده است. از این رو از تئوری منطق فازی در طراحی سیستم استفاده شد. خروجی سیستم مدنظر متغیر شناسایی تقلب پول‌شویی است. سیستم فازی طراحی‌شده می‌تواند تمام حساب‌های کاربران را پس از شناسایی، در قالب سه گروه کم، متوسط و زیاد دسته بندی کند. ادعای پول شویی که در گروه کم قرار می گیرد، می تواند مورد چشم‌پوشی قرار گیرد. مواردی که در گروه متوسط قرار می گیرند،

1. Root-mean-square deviation

[ Downloaded from qjfep.ir on 2026-11-24 ]

نیازمند بررسی مشخصات مشتری صاحب حساب در چارچوب مقررات شناسایی مشتریان است و آن دسته از مواردی که در گروه زیاد قرار می گیرند، نیازمند ارائه گزارش به واحد پول شویی جهت رسیدگی بیشتر است. نتایج حاصل از اعتبارسنجی سیستم پیشنهادی، بیانگر صحت و اعتبار بالای سیستم پیشنهادی است. مشخصه‌های اصلی سیستم پیشنهادشده عبارتند از:

- این سیستم نه تنها می‌تواند به‌طور مستقل پول‌شویی را تشخیص دهد، بلکه می‌تواند از محیط نیز آموزش‌دیده و تغییرات محیطی را پذیرفته و تصمیم‌گیری کند. به طوری که تصمیمات توسط انسان قابل‌تفسیر باشد.
- به‌واسطه عامل کاربر، سیستم ضد پول‌شویی طراحی‌شده می‌تواند با برنامه مالی هماهنگ باشد.
- اضافه کردن و کم کردن و حذف کردن قواعد کسب‌وکار و سناریوهای پول‌شویی در آن راحت است.
- این روش می‌تواند برای کسب‌وکار مناسب باشد، به دلیل اینکه هزینه‌های کشف پول‌شویی را کاهش داده و بهره‌وری واحد کشف پول‌شویی را افزایش دهد.
- در پایان پیشنهاد می شود، هر بانک سیستم ضد پول‌شویی هوشمند طراحی کند که این سیستم قادر به دریافت اطلاعات از واحد اطلاعات مالی و تجزیه‌وتحلیل پروفایل مشتریان و تجزیه‌وتحلیل 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 هرگونه شک و تردید، توجه و دقت لازم را داشته باشند.

[ Downloaded from qjfep.ir on 2026-11-24 ]

## منابع

**احمدی‌نژاد منفرد، مریم** (۱۳۸۸). «پول‌شویی و سیستم مالی شامل آثار اقتصادی، اجتماعی، فرهنگی». *مجله توسعه صادرات*. سال سیزدهم. شماره ۷۸. صص ۳۸-۴۱.

**پیرسرایی، زربخش و اسداله شاه بهرامی** (۱۳۹۳). «ضرورت استفاده از سیستم های تشخیص پول‌شویی در بانکداری الکترونیکی». *فصلنامه روند*. سال بیست و یکم. شماره ۶۸. زمستان ۱۳۹۳. صص ۱۷۹-۲۱۲.

**خدادی، اکبر** (۱۳۹۲). «بررسی نقش و تأثیر عوامل قانونی در فرایند مبارزه با پول‌شویی در بخش بین‌الملل بانک‌ها (مطالعه موردی بانک ملت)». *دانش ارزیابی*. سال پنجم. شماره ۱۶.

**صادقی، حسین، عصاری، عباس و وحدی شقاقی شهری** (۱۳۸۹). «اندازه‌گیری فساد مالی در ایران با استفاده از منطق فازی». *پژوهشنامه اقتصادی*. سال دهم. شماره چهارم.

**Chen, Yu-To, Mathe John**, (2011). "Fuzzy computing applications for Anti-money laundering and distributed storage system load monitoring", World conference on soft computing.

**Claudio, Alexandre and Joao, Balsa (**2016). "Client profiling for and Anti-Money Laundering System". arXiv:1510.00878, vol. 2 [cs.LG] 11.

**Han, J and Kamber, M**, (2005). *Data Mining: Concept and Techniques*. Morgan Kaufmann Publishers, 2nd EDs.

**Helmy,T; Abd-ELMegied, Mohamed Zaki; S, Tarek S; S. K. Mahmoud** (2014). "Design of a Monitor for Detecting Money Laundering and Terrorist Financing". *International Journal of Computer Networks and Applications*, Vol. 1, I. 1.

**Horobin, I.** (2001). "Applying technology to fight moey laundering". Money laundering Bulletin.

**Kharote, Mahesh and Kshirasagar, V.P.** (2014). "Data Mining Model for Money Laundering Detection in Financial Domain". *International Journal of Computer Applications*, Vol. 85, No. 16.

**Kingdon, J** (2004). "Al Fights Money Laundering", *IEEE Transactions on Intelligent Systems*, PP. 87-89.

**Jain,R,. Kasturi, R,. and Schunk, B.G**. (1995). *Machine vision*. Published by McGraw-Hill.

**Menon, R. and Kuman, S**. (2005). "Understanding the role of technology in Anti – money Laundering Complianc", Infosys Technology Ltd.

**Sammer,M., O'Neill. M,. Brahazon. A,. Kechadi, M-tahar.** (2011). "An Investigation into Data mining approaches for Anti Money Laundering", *International Conference an computer Engineering and Applications*, Vol. 2.

**Scholkopf, B.** (2000). *A Short Tutorial on Kernels, Microsoft Research*, Rech Rep: MSR-TR-200-6t.

[ Downloaded from qjfep.ir on 2026-11-24 ]

**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. I. 11.

**Tang, J. (**2005). "A Framework on developing an Intelligent discriminating system of anti money laundering", *International Conference on Financial and banking*, CZECH Rep.

**Umadevi, P,. Divya, E,.** (2012). "Money Laundering detection using TFA System". ICEMA,. *International Conference on digital object Identifier*.

**Vapnik, V. (**1995). *The nature of statistical learning theory*, Springer verlag, New York.

**Wat kins, R.C. et al. (**2003). "Exploring Data mining tehnologies as tool to investigate money laundering", *Journal of policing practice and Research: An International Journal*, Vol. 4, No. 2, PP. 163-178.

**Wicks. T,.** (2001). "Intelligent Systems for money laundering prevention". Money laundering Bulletin.

**Zang, Z,. J. Salcrmo, J,. and YU, P. S** (2003). "Applying Data Mining in Investigating money laundering crimes",. SIG KDD'03, Washington DC, USA. PP. 747-752.

[ Downloaded from qjfep.ir on 2026-11-24 ]

[ Downloaded from qjfep.ir on 2026-11-24 ]

فصلنامه سیاست‌های مالی و اقتصادی

[ Downloaded from qjfep.ir on 2026-11-24 ]