DOI: http://dx.doi.org/10.22059/jitm.2015.51912

مدیریت فناوری اطلاعات
دانشکدهٔ مدیریت دانشگاه تهران

دورهٔ ۶، شمارهٔ ۴
زمستان ۱۳۹۳
ص. ۷۴۶- ۷۲۱

شناسایی تقلب در کارت‌های بانکی با استفاده از شبکه‌های عصبی مصنوعی

ملیحه وثوق[۱]، محمدتقی تقوی‌فرد[۲]، محمود البرزی[۳]

چکیده: هرچند آمار دقیقی از تقلب در کارت‌های بانکی معتبرِ کشور وجود ندارد، به نظر می‌رسد تقلب در کارت‌های بانکی روند رو به رشدی دارد و می‌تواند در آیندهٔ نه‌چندان دور به یکی از معضلات سیستم بانکی کشور تبدیل شود. متأسفانه هنوز در کشورمان تحقیقات مناسبی در این خصوص صورت نگرفته و سیستم بانکی مدل یا مدل‌هایی کارا نیاز دارد که بتواند امنیت استفاده از کارت‌های بانکی را تضمین کند. لذا در این پژوهش، پس از شناسایی انواع تقلب‌های رایج در زمینهٔ کارت‌های بانکی و شبیه‌سازی تراکنش‌های متقلبانه، با بهره‌گیری از شبکه‌های عصبی مصنوعی، مدلی برای طبقه‌بندی تراکنش‌ها به تراکنش‌های سالم و متقلبانه (مشکوک به تقلب) ایجاد شد. این مدل که از نوع شبکهٔ عصبی پرسپترون چندلایه است، علاوه‌بر اینکه مبتنی بر سیستم بانکی داخلی کشور است، توانسته است با دقت ۹۹درصد، عملکرد نسبتاً خوبی در طبقه‌بندی مزبور داشته باشد. با مقایسهٔ معیارهای ارزیابی عملکرد محاسبه‌شدهٔ این پژوهش و نتایج مدل‌های ارائه‌شده در مطالعات دیگر، مشخص شد معیارهای ارزیابی عملکرد پژوهش حاضر از روایی و پایایی مناسبی برخوردارند.

واژه‌های کلیدی: *پرسپترون چندلایه، تقلب، شبکهٔ عصبی، کارت‌های بانکی.*

۱. کارشناس‌ارشد مدیریت فناوری اطلاعات، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، تهران، ایران
۲. استادیار گروه مدیریت صنعتی، دانشگاه علامه طباطبائی، تهران، ایران
۳. استادیار گروه مدیریت صنعتی، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، تهران، ایران

تاریخ دریافت مقاله: ۱۳۹۲/۰۷/۰۶
تاریخ پذیرش نهایی مقاله: ۱۳۹۳/۰۴/۰۸
نویسندهٔ مسئول مقاله: ملیحه وثوق
E-mail: m.vosough@cbi.ir

مقدمه

طی دهه‌های اخیر، اهمیت تجارت الکترونیک[1] به‌طور چشمگیری افزایش‌یافته و همچنان رو به افزایش است. امروزه استفاده از تجارت الکترونیک و سرویس‌های ارتباطی و اطلاعاتی برای دسترسی بهتر و بیشتر مشتریان، به‌طور فزاینده‌ای رواج یافته است. بسیاری از شرکت‌ها و مؤسسه‌ها بخشی از کسب‌وکار خود (یا تمامی آن) را به سمت خدمات برخط[2] سوق داده‌اند. صنعت بانکداری نیز از این فناوری‌ها بی‌بهره نمانده است و با ایجاد خدمات الکترونیکی و نظام‌های پرداخت[3]، موجب کاهش تعاملات فیزیکی در محیط اداری بانک‌ها شده و استفاده از خدمات بانک‌ها را به سمت منازل و محیط کار افراد سوق داده است. یکی از خدمات بانک‌های ایرانی در سال‌های اخیر که با استقبال زیاد مشتریان بانک‌ها روبه‌رو شد، استفاده از کارت‌های بانکی در سطوح گسترده‌ای از تعاملات تجاری است.

هرچند تحولات یادشده گامی بزرگ در جهت کارایی، سهولت دسترسی و سودآوری است، معایبی نیز دارد که مهم‌ترین آنها آسیب‌پذیری نسبت به تهدیدهاست؛ چرا که بسیاری از تخلف‌های نظام بانکی و فعالیت‌های متقلبانه، به سیستم‌های بانکداری الکترونیکی بازمی‌گردد. کارت‌های بانکی، یکی از دلایل عمدهٔ رشد بانکداری الکترونیک، اکنون به پراستفاده‌ترین ابزار بانکداری تبدیل شده است، لذا بخش عمده‌ای از فعالیت‌های متقلبانه، معطوف به تراکنش با این کارت‌هاست. لذا بخش عمده‌ای از فعالیت‌های متقلبانه، معطوف به تراکنش با این کارت‌هاست. اشخاص حقوقی، حقیقی و همچنین بانک‌ها، سالانه مبالغ هنگفتی را به‌واسطهٔ تقلب و متقلبانی از دست می‌دهند که دائم به‌دنبال راه‌های جدیدی برای اقدامات غیرقانونی با استفاده از این کارت‌ها هستند. نتایج پژوهشی در حوزهٔ اتحادیهٔ اروپا نشان داد، از سال ۲۰۰۱ تا ۲۰۰۹ با وجود تمهیدات مختلف و بودجه‌های هزینه‌شده برای جلوگیری از تقلب در کارت‌های بانکی، همگام با افزایش تعداد کارت‌ها و حجم تراکنش‌های بانکی با استفاده از آنها، میزان تقلب‌ها نیز از حدود ۳ میلیارد یورو به حدود ۵ میلیارد یورو افزایش یافته است و پیش‌بینی شده است که این رقم تا سال ۲۰۱۵ به ۱۰ میلیارد یورو برسد (گولاپالی، کالی و ویجی، ۲۰۱۲).

یکی از حساس‌ترین، چالش‌برانگیزترین و دشوارترین وظایف بانک‌ها، به‌ویژه بانک‌های مرکزی، نظارت بر صحت و سلامت تراکنش‌های انجام‌گرفته روی حساب‌ها، به‌منظور حفظ امنیت مشتریان بانک‌ها و همچنین خود بانک‌ها است. از این رو ایجاد سیستمی توسط بانک‌ها و

---

1. e-Commerce
2. Online
3. Payment Systems

بانک مرکزی ـ که ناظر بر عملکرد نظام‌های پرداخت باشد ـ به‌منظور شناسایی تقلب در تراکنش‌های موجود در کارت‌های بانکی، ضروری به نظر می‌رسد. یکی از اصلی‌ترین زیرساخت‌های ایجاد چنین سیستمی، تدوین روشی مناسب برای شناسایی الگوهای موجود در تراکنش‌ها و تعیین تراکنش‌های غیرعادی (مشکوک به تقلب) است.

با توجه به حجم گستردهٔ تراکنش‌های بانکی روزانه و نیاز به تشخیص به‌موقع تقلب‌ها و جلوگیری از وقوع آنها، درعمل شناسایی دستی امکان‌پذیر نیست و مستلزم صرف زمان و نیروی انسانی بسیاری خواهد بود. لذا مهم‌ترین ضرورت، ایجاد روشی مناسب برای شناسایی تقلب، شناسایی رایانه‌ای دقیق و سریع تقلب‌های صورت پذیرفته در تراکنش‌های بانکیِ مبتنی بر کارت‌های بانکی است.

بیان مسئله

تا کنون در سیستم بانکی کشور سازوکار و برنامهٔ جامعی برای شناسایی و جلوگیری از تقلب‌های مربوط به تراکنش‌های مبتنی بر کارت وجود نداشته است (نوبرزاد، ۱۳۹۱؛ حاتمی‌راد و شهریاری، ۱۳۹۰)؛ به‌طوری که اغلب به‌دلیل نداشتن سیستم مناسب، تقلب‌های زیادی ناشناخته باقی مانده‌اند. در سایر کشورها نیز به‌دلیل گستردگی استفاده از کارت‌های اعتباری[1]، پژوهش‌های انجام‌گرفته به‌طور عمده بر این کارت‌ها تمرکز کرده‌اند؛ در حالیکه استفاده از این نوع کارت‌ها در کشورمان هنوز رواج پیدا نکرده است و کمابیش همهٔ تراکنش‌های به‌وسیلهٔ کارت‌های نقدی (ازپیش پرداخت‌شده[2]) صورت می‌گیرد. همچنین با توجه به ملاحظات امنیتی، مطالعات صورت‌گرفته به‌طور کامل منتشر نمی‌شوند و نمی‌توان از آنها بهره‌ای برد. بنابراین بهره‌گیری از مدل‌های طراحی‌شده در ادبیات سایر کشورها چندان مقدور نیست. کارت‌های بانکی که یکی از دلایل عمدهٔ رشد بانکداری الکترونیک محسوب می‌شود، اکنون به پراستفاده‌ترین ابزار بانکداری تبدیل شده است، لذا بخش عمده‌ای از فعالیت‌های متقلبانه معطوف به تراکنش با این کارت‌هاست. با توجه به حجم گستردهٔ تراکنش‌های بانکی روزانه و نیاز به تشخیص به‌موقع تقلب‌ها و جلوگیری از وقوع آنها، درعمل شناسایی دستی امکان‌پذیر نیست و مستلزم صرف زمان و نیروی انسانی بسیاری خواهد بود. بنابراین با توجه به نبود سازوکاری برای شناسایی تقلب در کارت‌های سیستم بانکی کشور، مسئلهٔ اصلی این پژوهش، ایجاد چارچوبی برای شناسایی تقلب در کارت‌های بانکی، هنگام تراکنش یا به فاصلهٔ کوتاهی پس از آن است. بدین منظور از روش شبکهٔ عصبی مصنوعی استفاده شده است. بیشترین دلیل استفاده از شبکه‌های عصبی، وجود

1. Credit Card
2. Prepaid

مسائل بسیار زیاد حل‌نشدنی توسط الگوریتم‌های حل مدل‌های غیرخطی است. مزیت استفاده از شبکهٔ عصبی این است که محقق نیازی به دانستن نوع ارتباط بین متغیرهای مستقل و وابسته ندارد (طلوعی اشلقی و حق‌دوست، ۱۳۸۶). استفاده از کارت توسط مشتری مشخص، معمولاً از الگوهای مشخصی تبعیت می‌کند که شبکهٔ عصبی با استفاده از بازشناسی الگو می‌تواند شناسایی این الگوها و تقلب‌های مربوط به آن را امکان‌پذیر کند (پاتیدار و شارما، ۲۰۱۱). بنابراین سؤال اصلی پژوهش حاضر این‌گونه مطرح می‌شود، چگونه می‌توان با استفاده از شبکه‌های عصبی مصنوعی و با توجه به تقلب‌های شناخته‌شدهٔ پیشین، تراکنش‌های متقلبانه را شناسایی کرد.

پیشینهٔ پژوهش

پیشینهٔ نظری

در مقاله‌ها و منابع علمی، تقلب در کارت‌های بانکی به روش‌های گوناگونی تعریف شده است که چکیدهٔ این تعاریف را می‌توان این‌گونه جمع‌بندی کرد: تقلب در کارت‌های بانکی به کلاهبرداری یا تقلب به‌وسیلهٔ کارت بانکی یا هرگونه سازوکار پرداخت مشابه اطلاق می‌شود که از منبع متقلبانه در تراکنش انجام می‌شود (دلامیر، عبدو و پوینتون، ۲۰۰۹؛ پاتیدار و شارما، ۲۰۱۱؛ فوا، لی، اسمیت و گایلر، ۲۰۱۰).

به‌دلیل کمبودهای امنیتی سیستم پردازش کارت‌های بانکی مرسوم، تقلب در آنها روند افزایشی دارد و سالانه میلیاردها دلار از دست می‌رود. تقلب در کارت‌های بانکی به یکی از منابع جذاب کسب درآمد برای مجرمان تبدیل شده است. مجرمان روش‌های بسیار پیچیده و ماهرانه‌ای دارند و در سراسر جهان فعالیت می‌کنند. به همین دلیل مسئلهٔ تقلب برای بانک‌ها و مؤسسه‌ها اهمیت ویژه‌ای دارد (نصیری و مینایی، ۱۳۸۹). پیشگیری و شناسایی تقلب بخش مهمی از مدیریت ریسک در بانک‌ها است. هدف از شناسایی سریع تقلب، متوقف‌کردن آن در کوتاه‌ترین فاصلهٔ زمانی ممکن پس از رخ‌دادن است. برخی از انواع تقلب که تا کنون شناسایی‌شده، شامل تقلب‌های فروشنده (تبانی فروشنده[1]، تقلب سه‌جانبه[2])، تقلب‌های اینترنتی (شبیه‌سازی سایت، سایت فروشندهٔ دروغین، تولیدکننده‌های کارت اعتباری[3]، فیشینگ[4])، کارت‌های گم‌شده یا ربوده‌شده، در اختیار گرفتن حساب، بدون استفاده از کارت، دریافت‌نکردن

1. Merchant Collusion
2. Triangulation
3. Credit Card Generators
4. Phishing

کارت، جست‌وجو در سطل زباله، کارت‌های جعلی (پاک‌کردن نوار مغناطیسی[1]، ایجاد کارت تقلبی، ضبط‌کردن[2]، کارت سفید)، سرقت پستی، افشای اطلاعات در محل کار یا منزل، شبکه‌های اجتماعی، تقلب ورشکستگی[3]، تقلب در دستگاه‌های خودپرداز (حلقهٔ لبنانی[4]، دست‌خوانی[5]) و غصب‌کردن[6] (دلامیر، عبدو و پوینتون، ۲۰۰۹؛ پاش، ۲۰۰۸؛ پاتیدار و شارما، ۲۰۱۱؛ ساخاروا، ۲۰۱۲) است. به‌طور مسلم روش‌های تقلب به موارد اشاره‌شده محدود نمی‌شود و متخلفان از روش‌های دیگری نیز استفاده می‌کنند. هرچه تمهیدات امنیتی بانک‌ها برای جلوگیری از تقلب افزایش می‌یابد، متقلبان روش‌های جدیدتری به‌کار می‌برند. نکتهٔ مثبت اینکه تقلب معمولاً با الگوهای مشخصی صورت می‌پذیرد که امکان شناسایی این الگوها و تقلب‌های مربوط به آن الگوها وجود دارد.

پیشینهٔ تجربی

هرچند شناسایی تقلب آسان نیست، روش‌های گوناگونی برای شناسایی تقلب کارت‌های بانکی به‌کار گرفته می‌شود. اغلب روش‌های استفاده‌شده در ادبیات موضوع، مبتنی بر داده‌کاوی است. روش‌های داده‌کاوی به‌عنوان یکی از اصلی‌ترین ابزارهای شناسایی تقلب در کارت‌های بانکی استفاده می‌شود (بولتن و هند، ۲۰۰۲). داده‌کاوی، فرایند کشف روابط ناشناخته و الگوی درون‌داده‌هاست، درواقع فعالیتی است که به‌طور اساسی با آمار و تحلیل دقیق داده‌ها انطباق دارد (آذر، احمدی و سبط، ۱۳۸۹). هرچه حجم داده‌ها بیشتر و روابط میان آنها پیچیده‌تر باشد، دسترسی به اطلاعات نهفته در داده‌ها مشکل‌تر می‌شود، لذا نقش داده‌کاوی به‌مثابهٔ یکی از روش‌های کشف دانش، روشن‌تر می‌شود (شهرابی، ۱۳۹۲).

راهبردهای کلان مسائل شناسایی تقلب در حوزهٔ کارت‌های بانکی را نیز می‌توان منطبق با راهبردهای داده‌کاوی دانست. دو راهبرد کلان برای فرایند داده‌کاوی وجود دارد: ۱. یادگیری نظارت‌شده[7] و ۲. یادگیری نظارت‌نشده[8]. روش‌های نظارت‌شده، از یک پایگاه داده شامل موارد متقلبانه و غیرمتقلبانهٔ ساختاریافته استفاده می‌کنند و در موارد جدید مشکوک به تقلب به‌کار می‌روند. یادگیری نظارت‌شده از داده‌های گذشته یاد می‌گیرد و دانش آموخته‌شده را در موارد

---

1. Erasing the magnetic Stripe
2. Skimming
3. Bankruptcy Fraud
4. Lebanese Loop
5. Shoulder Surfing
6. Imposters
7. Supervised Learning
8. Unsupervised Learning

بعدی به‌کار می‌برد. این فرایند تلاش می‌کند الگوهای از پیش تعریف‌شدهٔ معین از فعالیت تراکنش‌هایی را شناسایی کند که برای مطابقت‌دادن با فعالیت‌های متقلبانه به‌کار می‌روند.

در روش نظارت‌نشده، سیستم بدون در اختیارداشتن داده‌های خروجی و بدون کمک خارجی، درستی یا نادرستی سیگنال‌های خروجی خود را مشخص می‌کند (پاش، ۲۰۰۸: ۲۵). بُلتن و هند در سال ۲۰۰۲ روش‌ها و مدل‌های استفاده‌شده برای کشف تقلب را بررسی کردند. آنها مدل‌های کشف تقلب در حوزهٔ کارت‌های اعتباری را با دو رویکرد نظارت‌شده و نظارت‌نشده طبقه‌بندی کردند و برای کشف تقلب در کارت‌های بانکی، روش خوشه‌بندی را به‌کار بردند. به‌کمک این روش، حساب‌هایی که در یک بازهٔ زمانی مشخص الگوی رفتاری متفاوتی از خود نشان می‌دهند، شناسایی می‌شوند (بولتن و هند، ۲۰۰۲).

درخت‌های تصمیم‌گیری، یکی از روش‌های داده‌کاوی با قابلیت فهم زیاد و سرعت مناسب در یادگیری الگو است (البرزی، محمدپورزرندی و خان‌بابایی، ۱۳۸۹). فان و همکارانش به‌منظور بنا کردن یک سیستم شناسایی سرزده برای انواع تقلب، روی درخت‌های تصمیم به‌ویژه درخت تصمیم استقرایی[1] کار کردند (فَن، میلر، استولفو، لی و چان، ۲۰۰۴). همچنین شِن و همکارانش علاوه‌بر سایر چارچوب‌های ارائه‌شده، درخت تصمیم را نیز آزمودند و با سایر مطالعات مقایسه کردند (شِن، تُنگ و دِنگ، ۲۰۰۷). درخت تصمیم یکی از روش‌های طبقه‌بندی است. هر تراکنش دارای مجموعه مشخصاتی است که بر اساس مقادیر آنها، تراکنش به یک طبقه تعلق می‌گیرد، پس هدف از طبقه‌بندی، ساختن تابعی است که هر تراکنش را بر اساس مقادیر مشخصاتش به یکی از چندین گروه از پیش‌تعیین‌شده، نگاشت کند. در پژوهش دیگری که روی پورتفولیوی بزرگ بانکی و به‌منظور تعیین تقلب در کارت‌های اعتباری ایتالیا صورت گرفته، از روش‌های آماری استفاده شده است (پولینا و پابا، ۲۰۱۰). روش‌های آماری برمبنای این فرض اساسی بنا شده‌اند که «احتمال رخداد داده‌های نمونهٔ نرمال در یک مدل تصادفی، بیشتر از احتمال رخداد داده‌های نمونهٔ غیر نرمال است». بیشتر روش‌های آماری شناسایی تقلب، یک مدل احتمال توزیع داده‌ای می‌سازند و آن را برای هر تراکنش ارزیابی می‌کنند. درنتیجه تراکنش‌های با احتمال کم غیر نرمال هستند (نصیری و مینایی، ۱۳۸۹). پژوهشی دیگر، مدل مارکف مخفی[2] را به‌کار برده است که در آن تراکنش‌های کارت اعتباری با استفاده از این مدل آزمون شده است؛ به‌طوری که اگر با احتمال زیاد پذیرفته نشود، تقلب محسوب می‌شود (سریواستاوا، کُندو و سورال، ۲۰۰۸). لئونارد از سیستم خبرهٔ مبتنی بر قوانین، برای شناسایی تقلب کارت اعتباری استفاده کرده

1. Induction
2. Hidden Markov Model

است (لئونارد، ۱۹۹۵). پژوهشی دیگر، دو نظریهٔ داده‌کاوی پیشرفتهٔ ماشین بردار پشتیبان[1] و جنگل‌های تصادفی[2] را با استفاده از رگرسیون لجستیک[3] ارزیابی کرده است. پژوهش مزبور بر اساس داده‌های واقعی تراکنش‌های بین‌المللی کارت اعتباری انجام گرفته است (باتاچاریا، ژا، ثاراکونل و وستلند، ۲۰۱۱). در سال ۲۰۱۱ مدلی مبتنی بر قوانین برای شناسایی و مقابله با تراکنش‌های متقلبانه (برای تقلب‌های بدون استفاده از کارت) در سیستم‌های پرداخت الکترونیکی ارائه شده است. در این روش، با تعریف الگوریتم یادگیری مبتنی بر قوانین، به طبقه‌بندی تراکنش‌ها به تراکنش‌های «سالم» و «متقلبانه» پرداخته شده است (الخطیب، ۲۰۱۱).

استفاده از شبکه‌های عصبی مصنوعی برای طبقه‌بندی در بسیاری از زمینه‌ها، کاربرد فراوانی دارد که یکی از ویژگی‌های آنها، خاصیت یادگیری نظارت نشده است (قاسمی و اصغری‌زاده، ۱۳۹۳). شبکه‌های عصبی مصنوعی نیز یکی از روش‌هایی است که برای شناسایی تقلب در کارت‌های بانکی استفاده می‌شود. برتری شبکه‌های عصبی نسبت به روش‌های دیگر این است که می‌تواند از تراکنش‌های گذشته بیاموزد و با گذشت زمان نتایج را بهبود دهد. همچنین می‌تواند قوانین را استخراج کند و رفتار آینده را براساس وضعیت فعلی پیش‌بینی کند (نصیری و مینایی، ۱۳۸۹). آگوئلکا برنامهٔ شبکهٔ عصبی مصنوعی کاربردی‌ای برای خوشه‌بندی طراحی کرد، این برنامه می‌تواند از حجم بزرگی از داده‌های تراکنش‌ها استفاده کند. در پژوهش مزبور از چهار خوشهٔ با ریسک زیاد، متوسط، پایین و کم‌ریسک شده است استفاده شده است، به این شکل که تراکنش‌های پردازش‌شده در یکی از این خوشه‌ها قرار خواهد گرفت، چنانچه تراکنش مشکوک باشد به پایگاه داده برمی‌گردد (آگوئلکا، ۲۰۱۱). در پژوهشی دیگر، از شبکهٔ عصبی P-RCE به‌منظور شناسایی تقلب در کارت‌های اعتباری استفاده شده است. P-RCE یکی از زیرمجموعه‌های شبکه‌های توابع پایهٔ شعاعی[4] است، شبکهٔ پس‌انتشار[5] سه‌لایه دارد و به‌منظور شناسایی الگوها به‌کار می‌رود. هدف این محققان، رسیدن به شبکهٔ آموزش‌دیده‌ای بود که بتواند به تقلب‌ها امتیاز دهد و تراکنش‌های کارت اعتباری را رتبه‌بندی کند (قوش و رایلی، ۱۹۹۴: ۶۲۳). پاتیدار و شارما نیز مطالعات خود را در زمینهٔ شناسایی تراکنش‌های متقلبانهٔ کارت اعتباری با استفاده از شبکه‌های عصبی و الگوریتم ژنتیک انجام دادند (پاتیدار و شارما، ۲۰۱۱).

---

1. Support Vector Machine
2. Random Forests
3. Logistic Regression
4. Radial Basis FunctionNetworks
5. Feed Forward Network

تمام روش‌های شناسایی تقلب در کارت‌های اعتباری منحصر به روش‌های داده‌کاوی نیست و روش‌های ابتکاری دیگری نیز در نوشتارهای علمی برای شناسایی تقلب در کارت‌های اعتباری استفاده شده است. برای مثال، بنتلی و همکاران نیز از دو روش الگوریتم ژنتیک و منطق فازی استفاده کردند. هدف آنها ایجاد قوانین منطقی مناسب برای طبقه‌بندی تراکنش‌های کارت اعتباری به طبقه‌های مشکوک و غیرمشکوک با استفاده از روش فازی دارویی بوده است. اساساً این روش فرایند امتیازدهی را دنبال می‌کند. در آزمایش شرح داده شده در این پژوهش، پایگاه داده از ۴۰۰۰ تراکنش با ۶۲ فیلد ساخته شده است و انواع مختلف قوانین به‌وسیلهٔ فیلدهای متفاوتی آزمایش شده‌اند. آنها معتقد بودند بهترین قانون، قانونی است که بالاترین پیش‌بینی را انجام دهد (بِنتلی، کیم، جوانگ و چوی، ۲۰۰۰). همچنین چان و همکارانش الگوریتمی را به‌منظور پیش‌بینی رفتار مشکوک ایجاد کردند. در حالیکه مطالعات دیگر از ارزیابی مبتنی بر درصد پیش‌بینی، درصد مثبت درست و درصد منفی نادرست استفاده می‌کنند، اساس این پژوهش ارزیابی به‌کمک مدل هزینه است (چان، فَن، پرودرومیدیس و استولفو، ۱۹۹۹). گادی و همکارانش از جست‌وجوی جامع و الگوریتم ژنتیک برای انتخاب مجموعه پارامترهای بهینه‌ای استفاده کردند که هزینهٔ تقلب برای پایگاه دادهٔ کارت اعتباری توسط صادرکنندگان کارت برزیلی را کمینه کند (گادی، وانگ، پِریرا و لاگو، ۲۰۰۸). نوبرزاد نیز در پایان‌نامهٔ کارشناسی ارشد خود، از روش جست‌وجوی پراکنده و الگوریتم ژنتیک برای شناسایی تقلب در کارت‌های بانکی استفاده کرد (نوبرزاد، ۱۳۹۱).

روش‌های دیگری نیز برای شناسایی تقلب کارت اعتباری استفاده شده است، از جمله نظریهٔ دمپستر- شفر، نظریهٔ یادگیری بیزین[1] (پانیگراهی، کُندو، سورال و مَجومدار، ۲۰۰۹) و پیوندزنی[2] (کُندو، پانیگراهی، سورال و مَجومدار، ۲۰۰۹؛ هوانگ، توفیق و نَگَر، ۲۰۱۰؛ کریفکو، ۲۰۱۰). در مطالعهٔ دیگری محقر و همکارانش، روش‌های کشف تقلب در بانکداری را به دو دستهٔ اصلیِ «روش‌های آماری» و «روش‌های هوش مصنوعی» تقسیم کردند و به بررسی امکان استفاده از روش مبتنی بر هوش کسب‌وکار پرداختند (محقر، لوکس، حسینی و منشی، ۱۳۸۷). در دسته‌بندی این روش‌ها، مرزبندی چندان دقیقی وجود ندارد؛ چرا که هریک از این روش‌ها فقط شکلی از یک روش علمی است و برخی از آنها می‌توانند به یکدیگر تبدیل شوند. یادآوری می‌شود، هیچ‌یک از این روش‌ها به‌تنهایی نمی‌توانند تقلب را حذف کنند، درواقع هر روش توانایی یک سیستم را در شناسایی تقلب افزایش می‌دهد.

---

1. Bayesian Learning
2. Hybridization

مدل مفهومی

مدل مفهومی، توصیف غیرنرم‌افزاری خاصی از مدل است که اهداف، ورودی‌ها، خروجی‌ها، محتوی و فرضیه‌های مدل را تشریح می‌کند (رابینسون، ۲۰۰۴: ۶۳-۷۴). به‌طور خلاصه پس از تعیین هدف اصلی پژوهش با عنوان ایجاد مدلی با قابلیت اطمینان مناسب به‌منظور شناسایی تقلب در کارت‌های بانکی، نحوهٔ جمع‌آوری، پردازش و آماده‌سازی داده‌ها برای ایجاد مدل، تشریح می‌شود و داده‌های تقلب (تراکنش‌های متقلبانه یا مشکوک به تقلب) که به‌کمک دانش خبرگان و ادبیات موضوع شبیه‌سازی شده است، برای مدل‌سازی آماده خواهد شد. سپس متغیرهای مستقل و وابستهٔ مدل تعیین می‌شوند و در مدل شبکهٔ عصبی پرسپترون چندلایه، به‌منزلهٔ مدل اصلی پژوهش برای طبقه‌بندی تراکنش‌ها به «سالم» و «متقلبانه یا مشکوک به تقلب» وارد خواهند شد.

با استفاده از درصدی از داده‌ها به‌صورت تصادفی، مدل شبکهٔ عصبی پرسپترون چندلایه آموزش داده شد و مشخصات شبکهٔ عصبی شناسایی تقلب در کارت‌های بانکی به‌دست آمد. شکل ۱، مدل مفهومی پژوهش حاضر را در قالب نمودار جریان منطقی نمایش می‌دهد.

شکل ۱. مدل مفهومی پژوهش

روش‌شناسی پژوهش

در این بخش به چگونگی جمع‌آوری اطلاعات پژوهش، تشریح و بررسی کیفیت داده‌ها، نحوهٔ انتخاب داده‌ها برای تدوین چارچوب و پاکسازی داده‌ها پرداخته می‌شود و پس از ایجاد داده‌های

متقلبانه (مشکوک به تقلب)، به طراحی چارچوبی برای شناسایی تقلب در کارت‌های بانکی اقدام خواهد شد.

جمع‌آوری و آماده‌سازی داده‌ها

داده‌های اصلی پژوهش از تراکنش‌های ثبت‌شدهٔ کارت‌های بانکی در پایگاه دادهٔ یکی از بانک‌های غیردولتی داخلی با رعایت ملاحظات اخلاقی و با اخذ مجوز از آن بانک، به‌دست آمد و از آن برای طراحی چارچوب شناسایی تقلب در کارت‌های بانکی بهره‌جویی شد. لذا تراکنش‌های حدود ۱۲۰ هزار کارت در بازهٔ زمانی تقریبی دو سال از تاریخ افتتاح بانک یادشده با حدود بیش از ۱۰ میلیون تراکنش استخراج شده است. با توجه به تعدد فیلدهای اطلاعاتی و کاربردی‌نبودن برخی از آنها برای این پژوهش، پس از تحلیل آنها به‌کمک خبرگان و در نظرگرفتن تقلب‌های صورت‌گرفته و شناسایی فیلدهای تحت تأثیر تقلب‌های مختلف، پارامترهای مؤثر در طراحی چارچوب پژوهش استخراج شد و فیلدهای ناکارا از پایگاه اطلاعاتی کنار گذاشته شد.

به‌دلیل حجم زیاد داده‌های ذخیره‌شده در پایگاه اطلاعاتی بانک (حدود ۱۰ میلیون تراکنش) و محدودیت نرم‌افزارها در پردازش حجم زیاد داده‌ها، تعدادی از مجموعه تراکنش‌های ذکرشده، نماینده‌هایی از کل تراکنش‌های موجود در نظر گرفته شدند. بدین ترتیب درنهایت ۱۱۱,۳۴۹ تعداد تراکنش مختص به ۶۴۱ دارندهٔ کارت برای ادامهٔ پژوهش در نظر گرفته شد. گروه‌های هدف یا کارت‌هایی که در معرض ریسک بیشتری قرار دارند و پتانسیل سوء استفاده از آنها زیاد است، متشکل از سه گروه تراکنش زیر است:

گروه ۱: به تراکنش‌های ۱۲۰ کارتی اختصاص دارد که از لحاظ حجم تراکنش، پرتراکنش‌ترین کارت‌ها هستند. در مجموع ۷۸,۳۱۳ رکورد در گروه اول جای گرفت. دلیل انتخاب این گروه قرار داشتن در معرض ریسک بیشتر بوده است.

گروه ۲: به تراکنش‌های ۳۷۱ کارتی اختصاص دارد که از لحاظ حجم تراکنش در گروه کم‌تراکنش‌ترین کارت‌ها قرار دارند. در مجموع ۶۰۱۲ رکورد در گروه دوم جای گرفت که اغلب آنها مختص به کارت‌های صادر شده برای افراد مسن و سالخورده است که تراکنش‌های محدودی انجام می‌دهند.

گروه ۳: تراکنش‌های مربوط به ۱۵۰ کارتی است که به‌صورت تصادفی انتخاب شدند. در مجموع برای گروه سوم ۲۷,۰۲۴ رکورد با استفاده از توزیع برنولی با احتمال ۰/۳ درصد از تراکنش‌هایی که در گروه‌های قبلی جای ندارند، به‌دست آمده است.

همان‌طور که اشاره شد، گروه‌های اول و دوم، گروه‌هایی هستند که متقلبان بیشتر به آنها توجه می‌کنند و گروه سوم، بخشی تصادفی از سایر کارت‌های موجود است.

از آنجاکه برای این پژوهش داده‌های متقلبانه وجود ندارد، با بهره‌گیری از دو منبع مصاحبه و ادبیات موضوع، اقدام به ایجاد داده‌های متقلبانه برای استفاده در مدل‌سازی شد. فوا و همکارانش اعتقاد دارند که داده‌های مصنوعی می‌توانند یک سیستم را آموزش دهند. انواع مختلف تقلب‌های شناخته‌شده و جدید را می‌توان به‌صورت مصنوعی ایجاد کرد (فوا، لی، اسمیت و گایلر، ۲۰۰۵). از این رو سازوکار تهیهٔ تراکنش‌های مشکوک به تقلب در این پژوهش، از طریق اعمال تغییرات معنادار روی داده‌های گردآوری‌شده از طریق پرونده‌های موجود درخصوص تراکنش‌های متقلبانه یا موارد مشکوک گزارش‌شده، مصاحبه با کارشناسان، خبرگان و صاحب‌نظران، ادبیات موضوع در خصوص تقلب‌های ممکن در کارت‌های بانکی و همچنین تحلیل و شبیه‌سازی اطلاعات بوده است. درمجموع حدود ۰/۲ درصد (۲۱۲ تراکنش) از کل داده‌های استفاده‌شده در این پژوهش را داده‌های تقلب تشکیل داده است.

متغیرهای مدل

متغیرهای ورودی شبکهٔ عصبی شامل ۱۵ متغیر مستقلی است که در تعیین رفتار دارندهٔ کارت نقش دارند. برای متغیر خروجی در سیستم نیز یک پارامتر تعیین شده است. ۱۵ متغیر ورودی را فیلدهای اطلاعاتی منتخب از میان تمامی فیلدهای مربوط به تراکنش‌های ثبت‌شده در سیستم بانکی تشکیل می‌دهند. این فیلدها از انواع مختلفی مانند عددی، رشته‌ای، تاریخ، زمان و غیره هستند که برای تبدیل به متغیرهای قابل استفاده در مدل‌سازی باید به نوع عددی تبدیل شوند. لذا برای هر یک از متغیرها، روشی لحاظ شد تا به نوع عددی تبدیل شود.

متغیر وابستهٔ مدل (Fraud-Detector)، به‌شکل یک متغیر طبقه‌ای تعریف شده است؛ به‌صورتی که این متغیر با پردازش متغیرهای مستقل، یکی از مقادیر «سالم» یا «متقلبانه (مشکوک به تقلب)» را به خود می‌گیرد. از آنجا که برای ایجاد مدل‌های پژوهش حاضر مقادیر عددی استفاده می‌شود، برای تراکنش‌های سالم مقدار متغیر وابسته صفر (طبقهٔ منفی) و برای تراکنش‌های متقلبانه (یا مشکوک به تقلب)، مقدار یک (طبقهٔ مثبت) لحاظ شده است؛ بدین ترتیب مقادیر رشته‌ای ذکرشده به عدد تبدیل شدند.

ایجاد مدل شبکهٔ عصبی پرسپترون چندلایه

اغلب محققان شبکه‌های عصبی چندلایهٔ پیشخور، به‌ویژه شبکه‌های پرسپترون چندلایه را تقریب‌زننده‌های جهانی معرفی می‌کنند و معتقدند این شبکه‌ها در صورت وجود لایه و تعداد نورون کافی در لایه‌های خود، می‌توانند هر نگاشت غیر خطی را با هر تقریب دلخواه برآورد کنند. شبکه‌های زیادی برای استفاده در طبقه‌بندی و پیش‌بینی پیشنهاد شده است، ولی این شبکه

یکی از موفق‌ترین شبکه‌های طبقه‌بندی و پیش‌بینی است (نوریگا، ۲۰۰۵). لذا در این پژوهش از این نوع شبکهٔ عصبی مصنوعی برای طبقه‌بندی تراکنش‌ها به طبقات سالم و متقلبانه استفاده شده است. شبکهٔ پرسپترون از قاعدهٔ «پس‌انتشار خطا[1]» استفاده می‌کند که الگوریتم تعمیم‌یافتهٔ «حداقل مربعات خطا» است. شبکه‌های پرسپترون به دو نوع تک‌لایه و چندلایه تقسیم می‌شوند. در نوع چندلایه که تعمیم نوع تک‌لایه است، هر نورون در هر لایه به تمام نورون‌های لایهٔ قبل، متصل است.

برای ایجاد شبکهٔ عصبی پرسپترون چندلایه به‌منظور شناسایی تقلب در کارت‌های بانکی، پس از آزمایش حالت‌های مختلف ایجادشده برای شبکهٔ عصبی (تعداد لایه‌های مختلف، تعداد گره‌های مختلف در هر لایه و توابع تبدیل مختلف)، بهترین حالت انتخاب شده است. این کار با مقایسهٔ میانگین مربعات خطا (MSE)[2] در هریک از حالات و در نظر گرفتن اصل امساک[3] به‌کمک نرم‌افزار انجام گرفته است. شبکهٔ مد نظر باید بتواند متغیرهای مستقل را دریافت کند و پس از پردازش آنها با استفاده از قابلیت بازشناسی الگو[4]، مقدار متغیر وابسته (مقدار یکی از طبقات) را برآورد کند. در طراحی شبکهٔ عصبی، از متغیرهای مستقل و وابستهٔ پیش‌گفته استفاده شده است؛ به این معنا که متغیرهای مستقل، واحدهای (نورون‌ها) مربوط به لایهٔ ورودی شبکه و متغیر وابسته، واحد(های) مربوط به لایهٔ خروجی شبکه را تشکیل می‌دهند.

از آنجا که شبکهٔ عصبی می‌تواند تأثیرات متقابل متغیرها (روابط بین متغیرها) را شناسایی کند، از واردکردن عبارت‌های مربوط به تأثیرات متقابل خودداری شده است. در ضمن با توجه به قابلیت یادشده، به تعریف متغیرهایی که تلفیق شده‌اند یا منتج از متغیرهای دیگرند، نیازی نیست.

برای ایجاد مدل شناسایی تقلب در کارت‌های بانکی، یک متغیر افراز[5] ایجاد شد تا بتوان داده‌ها را به دو بخش آموزش و اعتبارسنجی تقسیم‌بندی کرد. استفاده از داده‌های آزمایش در ایجاد مدل الزامی نیست؛ زیرا اگر داده‌ای برای آزمایش در نظر گرفته نشود، از داده‌های آموزش برای پیگیری خطاها استفاده می‌شود. این موضوع تنها زمان آموزش شبکه را افزایش می‌دهد. در این پژوهش، به‌دلیل محدودبودن تعداد داده‌های تقلب و استفاده از حداکثر این داده‌ها در فرایند آموزش شبکه، از تخصیص داده‌های آزمایش خودداری شده است. به‌واسطهٔ تعریف متغیر افراز و انتخاب داده‌هایی که برای آموزش و اعتبارسنجی استفاده خواهند شد، از مجموع ۱۱۱,۳۴۹ داده، ۶۶,۶۴۸ داده (۶۰ درصد) برای آموزش و ایجاد مدل اختصاص یافت و ۴۴,۶۹۸ داده (۴۰ درصد)

---

1. Error back propagation
2. Mean Square Error
3. Parsimony
4. Pattern recognition
5. Partition variable

برای اعتبارسنجی مدل به‌صورت تصادفی تخصیص داده شد. برای تخصیص تصادفی داده‌ها به مجموعه‌های یادشده، از توزیع برنولی با احتمال ۶۰ درصد برای متغیر افراز استفاده شده است.

تابع تبدیل انتخاب و استفاده شده برای تمامی نورون‌های لایه‌های پنهان، تابع تانژانت هیپربولیک[1] است. رابطهٔ ۱، تابع تبدیل یادشده را نشان می‌دهد. این تابع، مقادیر حقیقی را پس از دریافت به مقداری در بازهٔ (۱،۱) تبدیل می‌کند.

$$Y(c) = \tanh(c) = \frac{e^{c} - e^{-c}}{e^{c} + e^{-c}} \qquad \text{رابطهٔ ۱)}$$

تابع تبدیل Softmax برای واحدهای لایهٔ خروجی انتخاب شده است. این تابع تبدیل، برداری از المان‌هایی با مقدار حقیقی را دریافت می‌کند و به برداری که هر یک از المان‌هایش در بازهٔ (۰،۱) قرار می‌گیرد و مجموع المان‌هایش برابر یک می‌شود، تبدیل می‌کند. تابع تبدیل Softmax به‌صورت رابطهٔ ۲ است. تابع Softmax زمانی برای نورون‌های لایهٔ خروجی استفاده می‌شود که تمامی متغیرهای وابسته از نوع طبقه‌ای باشند. به همین دلیل در این پژوهش که متغیر وابسته از نوع طبقه‌ای است، تابع Softmax، تابع تبدیل واحدهای لایهٔ خروجی انتخاب شده است.

$$Y(c_k) = \text{Softmax}(c_k) = \frac{\exp(c_k)}{\sum_j \exp(c_j)} \qquad \text{رابطهٔ ۲)}$$

در این پژوهش با توجه به اینکه تعداد داده‌های متقلبانه (متغیر وابسته با مقدار یک) محدود است، تلاش بر این بوده است که هیچ‌یک از داده‌های متقلبانه از فرایند آموزش حذف نشود. به همین منظور از روش گروهی[2] برای آموزش شبکه بهره‌جویی شده است. الگوریتم بهینه‌سازی[3] برای برآورد وزن‌های سیناپسی استفاده می‌شود. الگوریتم بهینه‌سازی از نوع «گرادیان همجوار مقیاس‌بندی‌شده»[4] انتخاب شده است که گونه‌ای از الگوریتم پس‌انتشار خطا شمرده می‌شود. همان‌طور که پیش از این هم اشاره شد، الگوریتم پس‌انتشار خطا، نوعی از الگوریتم حداقل مربعات خطا است. این روش برای نوع آموزش گروهی مناسب است و برای آموزش لحظه‌ای و نیمه‌گروهی مناسب نیست. قواعد اختتام آموزش، به‌ترتیب «یک مرحله بدون کاهش در خطا» و

---

1. Hyperbolic tangent
2. Batch training
3. Optimization algorithm
4. Scaled Conjugate Gradient (SCG)

«حداکثر ۵۰۰ دوره[1] آموزش (عبور داده‌ها)» انتخاب شده است. این قواعد می‌توانند از مسئلهٔ انطباق بیش از حد[2] جلوگیری کنند.

خروجی یک مدل طبقه‌بندی می‌تواند یک مقدار حقیقی باشد. سیستم طبقه‌بندی، این مقادیر حقیقی (شبه‌احتمال) را برای هر مورد با آستانهٔ افتراق[3] (مقدار برش)[4] می‌سنجد و در صورت بزرگتر بودن از مقدار برش، آن مورد را در طبقهٔ مثبت قرار می‌دهد.

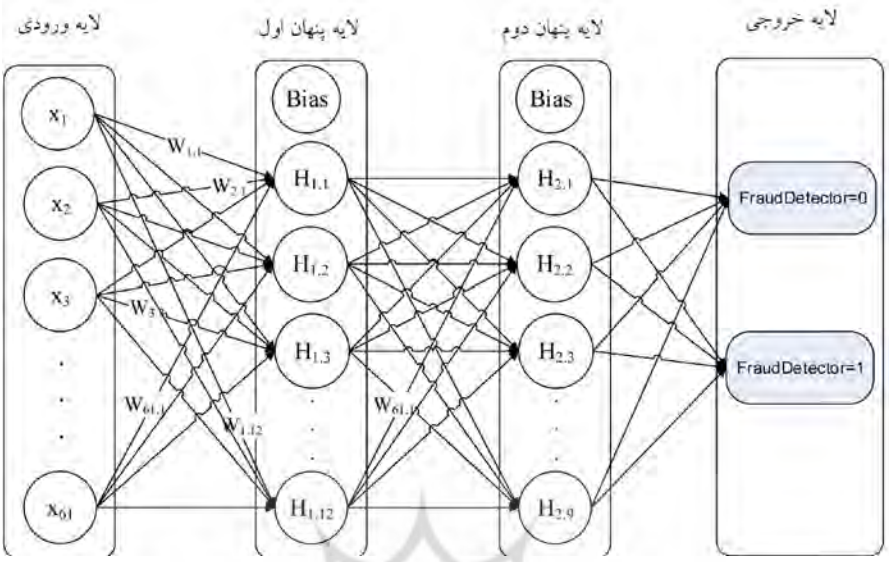
توضیح اینکه برای هر طبقهٔ متغیر(های) وابستهٔ طبقه‌ای با تابع تبدیل Softmax و خطای Cross-Entropy، مقداری توسط شبکه محاسبه می‌شود که این مقدار، احتمال این است که یک رکورد به یک طبقه تعلق دارد یا خیر.

همان‌طور که پیش از این نیز اشاره شد، هدف از ایجاد شبکهٔ عصبی پرسپترون چندلایه، طبقه‌بندی تراکنش‌های کارت‌های بانکی به دو طبقهٔ سالم و متقلبانه است که این کار را با محاسبهٔ یک شبه‌احتمال برای هر طبقه در هر تراکنش انجام می‌دهد. مقدار پیش‌فرض برای حد آستانه ۰/۵ فرض شده است که می‌توان این حد آستانه را تغییر داد. بنابراین مقادیر شبه‌احتمال بزرگتر از ۰/۵، متعلق به طبقهٔ مربوطه است. از این رو بهترین شبکهٔ عصبی پرسپترون انتخاب‌شده برای این پژوهش، شبکه‌ای با دو لایهٔ پنهان است. لایهٔ ورودی (لایهٔ اول) این شبکه، ۶۱ گره یا نورون (بدون در نظر گرفتن بایاس[5]) دارد که از ۱۵ متغیر مستقل به‌دست آمده است. شبکه، هریک از طبقه‌های متغیرهای طبقه‌ای را یک نورون در نظر می‌گیرد. به همین دلیل تعداد نورون‌های لایهٔ ورودی به جای ۱۵ واحد، ۶۱ واحد است.

شبکهٔ منتخب دارای ۱۲ گره (نورون) و یک بایاس در لایهٔ پنهان اول (لایهٔ دوم شبکه) و ۹ گره (نورون) و یک بایاس در لایهٔ پنهان دوم (لایهٔ سوم شبکه) است. لایهٔ آخر (خروجی شبکه)، دو گره دارد (دو طبقه مربوط به متغیر وابسته) که پس از تأثیر تابع تبدیل Softmax، برداری شامل مؤلفه‌هایی با مقدار شبه‌احتمال هر طبقه برآورد می‌کند. با توجه به توضیحاتی که بیان شد، شبکهٔ حاصل را می‌توان به‌صورت $MLP^{۶۱-۱۲-۹-۲}$ بیان کرد. توضیح اینکه تمامی گره‌های هر لایه به تمامی گره‌های لایه‌های قبل متصل است. این اتصال‌ها به‌منزلهٔ وزن هر یک از عناصر شبکه است (شکل ۲).

---

1. Epoch
2. Over fitting
3. Discrimination threshold
4. Cutoff Value
5. Bias



شکل ۲. شبکهٔ عصبی پرسپترون چندلایه برای شناسایی تقلب در کارت‌های بانکی

یافته‌های پژوهش

از آنجا که مدل‌های ارائه‌شدهٔ این پژوهش به‌منظور طبقه‌بندی طراحی شده‌اند، باید با معیارهای خاص طبقه‌بندی ارزیابی شوند. برای ارزیابی عملکرد مدل شبکهٔ عصبی پرسپترون چندلایه، باید طبقه‌بندی واقعی تراکنش‌های کارت‌های بانکی را با طبقه‌بندی انجام‌شدهٔ شبکهٔ عصبی مقایسه کرد و توانایی مدل را در شناسایی تراکنش‌های متقلبانه (یا مشکوک به تقلب) آزمود. معیارهای مندرج در جدول ۱ برای ارزیابی عملکرد سیستم طبقه‌بندی استفاده شده است (برادرسِن، اُنگ، استفان و بوهمان، ۲۰۱۰). در روابط جدول ۱، TP تعداد مثبت‌های درست؛ FP تعداد مثبت‌های نادرست؛ TN تعداد منفی‌های درست و FN تعداد منفی‌های نادرست است.

زمانی که تعداد منفی‌ها بسیار بیشتر از تعداد مثبت‌هاست (مانند پژوهش حاضر)، ممکن است که معیار دقت طبقه‌بندی، معیار مناسبی برای ارزیابی عملکرد نباشد. بنابراین معیارهای دیگری مانند میانگین‌های هندسی (g-mean)[1] (تانگ، ژانگ، چاولا و کراس، ۲۰۰۲) و همچنین معیارهای F و F_β (پاورز، ۲۰۱۱ و تانگ و همکاران، ۲۰۰۲) را برای ارزیابی عملکرد سیستم طبقه‌بندی می‌توان در نظر گرفت که با اضافه کردن TP به معادلات، محاسبه می‌شوند. در محاسبهٔ F_β، مؤلفهٔ β مقداری بین صفر و بی‌نهایت دارد و برای کنترل وزن تخصیص داده شده

1. Geometric Mean

به TP و P استفاده می‌شود؛ بدین ترتیب که هرچه β بزرگتر باشد، به همان نسبت اهمیت بیشتری برای TPR (حساسیت) قائل شده‌ایم تا P (صحت).

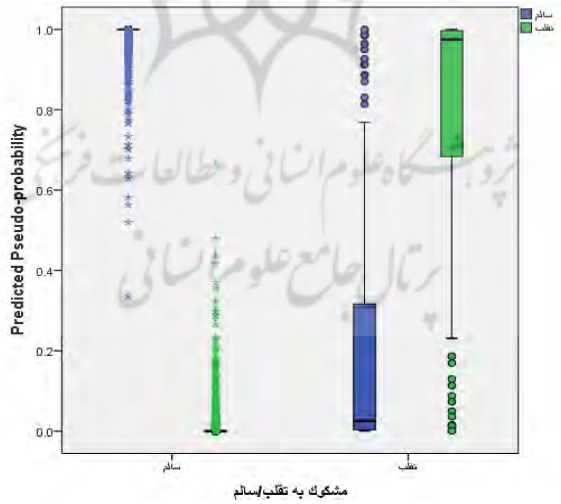
جدول ۱. معیارهای ارزیابی عملکرد طبقه‌بندی

نام معیار	نام جایگزین	توضیح	فرمول محاسبه
نسبت مثبت درست[1]	حساسیت[2] یا فراخوانی[3]	نسبت موارد مثبتی است که به درستی طبقه‌بندی شده‌اند.	$TPR = \frac{TP}{TP + FN}$
نسبت مثبت نادرست[4]	خطای نوع اول	نسبت موارد منفی است که به نادرست، مثبت طبقه‌بندی شده‌اند.	$FPR = \frac{FP}{FP + TN}$
نسبت منفی درست[5]	ویژگی[6]	نسبت موارد منفی است که به درستی طبقه‌بندی شده‌اند.	$TNR = \frac{TN}{TN + FP}$
نسبت منفی نادرست	خطای نوع دوم	نسبت موارد مثبتی است که به نادرست منفی طبقه‌بندی شده‌اند.	$FNR = \frac{FN}{FN + TP}$
دقت[7] طبقه‌بندی	--	نسبت نتایج درست (هم مثبت درست و هم منفی درست) به کل جامعه	$\mathrm{AC} = \frac{TP + TN}{TP + TN + FP + FN}$
صحت[8] طبقه‌بندی		نسبت تعداد مثبت‌های درست به کل نتایج مثبت (هم مثبت‌های درست و هم مثبت‌های نادرست)	$\mathrm{P} = \frac{TP}{TP + FP}$
میانگین هندسی یک	g-mean_1	--	$\sqrt{TPR \times P}$
میانگین هندسی دو	g-mean_2	--	$\sqrt{TPR \times TNR}$
--	F	--	$2 \times \frac{P \times TPR}{P + TPR}$
--	F_β	--	$\frac{(\beta^2 + 1) \times P \times TPR}{\beta^2 \times P + TPR}$

1. True Positive Ratio
2. Sensitivity
3. Recall
4. False Positive Ratio
5. True Negative Ratio
6. Specificity
7. Accuracy
8. Precision

با توجه به هدف اصلی پژوهش که شناسایی بهتر تراکنش‌های متقلبانه از میان تراکنش‌ها است، چهار معیار TPR، FNR، $g\text{-mean}_2$ و F_β از میان معیارهای موجود برای معیارهای اصلی سنجش عملکرد مدل‌های شبکهٔ عصبی پرسپترون چندلایه انتخاب شدند. در ادامه به تحلیل معیارهای عملکرد مدل‌های ایجاد شده پرداخته خواهد شد.

پس از ارزیابی مدل با استفاده از معیارهای اشاره‌شده در جدول ۱، نتایج نشان دادند که با انتخاب مقدار برش معادل ۰/۵، شبکهٔ عصبی پرسپترون با دقت ۹۹/۹ درصد توانسته است تراکنش‌ها را به دو دستهٔ سالم و متقلبانه طبقه‌بندی کند؛ این در حالی است که این شبکه با دقت تقریباً ۱۰۰ درصد، تراکنش‌های سالم و با دقت ۷۰/۴ درصد، تراکنش‌های متقلبانه را به درستی طبقه‌بندی کرده است. مقادیر مربوط به معیارهای اصلی $g\text{-mean}_2$ و F_β به‌ترتیب برابر ۸۳/۹ درصد و ۷۰/۸ درصد محاسبه شده است (توضیح اینکه با توجه به هدف اصلی پژوهش که عملکرد مناسب مدل در شناسایی تراکنش‌های متقلبانه است، برای محاسبهٔ F_β، مقدار β برابر با ۵ در نظر گرفته شده است). با توجه به نمودار پیش‌بینی ـ واقعی (شکل ۳) می‌توان دریافت که با انتخاب مقدار برش ۰/۳، می‌توان با کمترین هزینه در شناسایی تراکنش‌های سالم، شناسایی تراکنش‌های متقلبانه را بهبود بخشید. در این حالت با دقت ۹۹/۹۵ درصد تراکنش‌های سالم و با دقت ۷۵/۳ درصد تراکنش‌های متقلبانه شناسایی شدند و مقادیر معیارهای $g\text{-mean}_2$ و F_β به‌ترتیب برابر ۸۶/۸ درصد و ۷۵/۲ درصد به‌دست آمد.



شکل ۳. نمودار پیش‌بینی ـ واقعی برای شبکهٔ عصبی پرسپترون چندلایه

با وجود اینکه مقدار برش ۰/۳، مقدار بهینه برای آستانه افتراق است، می‌توان با توجه به هدف اصلی پژوهش که کاهش خطای نوع دوم است، مقدار برش را کاهش داد. همواره کاهش خطای نوع دوم، سبب افزایش خطای نوع اول خواهد شد. از آنجاکه این کار ریسک کمی دارد و رویکرد سخت‌گیرانه‌تری را نسبت به تقلب اتخاذ می‌کند، مقدار برش از ۰/۳ به ۰/۰۱ کاهش یافت. درنتیجهٔ این کاهش، دقت شناسایی تراکنش‌های سالم به ۹۹/۵ درصد رسید و بر دقت شناسایی تراکنش‌های متقلبانه به مقدار ۸۷/۷ درصد افزوده شد. مقادیر معیارهای $g\text{-}mean_2$ و F_β به‌ترتیب برابر ۹۳/۴ درصد و ۷۹/۱ درصد به‌دست آمد.

جدول ۲، ماتریس درهم‌ریختگی[1] طبقه‌بندی را با مقدار برش ۰/۱ توسط شبکهٔ عصبی پرسپترون نمایش می‌دهد.

جدول ۲. ماتریس درهم‌ریختگی شبکهٔ عصبی پرسپترون با مقدار برش ۰/۰۱

نمونه	مشاهدات	پیش‌بینی		
		سالم	تقلب	درصد صحیح
آموزش	سالم	۶۶۱۵۸	۳۵۹	٪ ۹۹/۴۶
	تقلب	۲	۱۲۹	٪ ۹۸/۴۷
اعتبارسنجی	سالم	TN =۴۴۳۸۱	FP = ۲۳۸	٪ ۹۹/۴۷
	تقلب	FN = ۱۰	TP = ۷۱	٪ ۸۷/۶۵

با توجه به جدول ۲، معیارهای عملکرد مدل شبکهٔ عصبی در طبقه‌بندی تراکنش‌ها با مقدار برش ۰/۰۱، به‌صورت زیر محاسبه شده است.

رابطهٔ ۳) $TP = ۷۱, \quad FP = ۲۳۸, \quad TN = ۴۴۳۸۱, \quad FN = ۱۰$

رابطهٔ ۴) $$TPR = \frac{TP}{TP + FN} = \frac{۷۱}{۷۱ + ۱۰} = ۰/۸۷۷$$

رابطهٔ ۵) $$FPR = \frac{FP}{FP + TN} = \frac{۲۳۸}{۲۳۸ + ۴۴۳۸۱} = ۰/۰۰۵۳۳۴$$

1. Confusion matrix

رابطهٔ ۶) $$\mathrm{TNR} = \frac{TN}{TN + FP} = \frac{۴۴۳۸۱}{۴۴۳۸۱ + ۲۳۸} = ۰/۹۹۵$$

رابطهٔ ۷) $$\mathrm{FNR} = \frac{\mathrm{FN}}{\mathrm{FN} + \mathrm{TP}} = \frac{۱۰}{۱۰ + ۷۱} = ۰/۱۲۳$$

رابطهٔ ۸) $$\mathrm{AC} = \frac{TP + TN}{TP + TN + FP + FN} = \frac{۷۱ + ۴۴۳۸۱}{۷۱ + ۴۴۳۸۱ + ۲۳۸ + ۱۰} = ۰/۹۹۴$$

رابطهٔ ۹) $$\mathrm{P} = \frac{TP}{TP + FP} = \frac{۷۱}{۷۱ + ۲۳۸} = ۰/۲۳۰$$

نتایج به این معناست که مدل شبکهٔ عصبی پرسپترون توانسته است ۸۷/۷ درصد از تقلب‌ها و تقریباً ۹۹/۵ درصد از تراکنش‌های سالم را به درستی شناسایی کند و تقریباً ۱۲/۳درصد از تقلب‌ها را نتوانسته است به درستی شناسایی کند. بنابراین مدل شبکهٔ عصبی پرسپترون به‌طور کلی می‌تواند در ۹۹/۴ درصد از موارد، طبقهٔ مربوط به هر تراکنش را به درستی شناسایی کند.

معیارهای میانگین هندسی و همچنین معیارهای F و F_β به‌صورت زیر محاسبه می‌شود:

رابطهٔ ۱۰) $$g - mean_۱ = \sqrt{TPR \times P} = \sqrt{۰/۸۷۷ \times ۰/۲۳۰} = ۰/۴۴۹$$

رابطهٔ ۱۱) $$g - mean_۲ = \sqrt{TPR \times TNR} = \sqrt{۰/۸۷۷ \times ۰/۹۹۵} = ۰/۹۳۴$$

رابطهٔ ۱۲) $$F = ۲ \times \frac{P \times TPR}{P + TPR} = ۲ \times \frac{۰/۲۳۰ \times ۰/۸۷۷}{۰/۲۳۰ + ۰/۸۷۷} = ۰/۳۶۴$$

رابطهٔ ۱۳) $$F_۵ = \frac{(۵^۲+۱) \times ۰/۷۱۸ \times ۰/۷۵۳}{۵^۲ \times ۰/۷۱۸ + ۰/۷۵۳} = ۰/۷۹۱$$

با تغییر مقدار برش از ۰/۳ به ۰/۰۱ مشاهده می‌شود که معیارهای اصلی مد نظر این پژوهش مانند TPR، FNR، $g\text{-mean}_۲$ و F_β بهبود یافته‌اند. جدول ۳ مقایسه‌ای از نتایج طبقه‌بندی برای مقدار برش‌های مختلف را نشان داده است.

جدول ۳. بهبود عملکرد مدل شبکهٔ عصبی با تغییر مقدار برش

مقدار برش	TNR	TPR	FPR	FNR	$g\text{-mean}_2$	$F_\beta(\beta = ۵)$
۰/۵	٪ ۹۹/۹۷	٪ ۷۰/۴	٪ ۰/۰۲۷	٪ ۲۹/۶	٪ ۸۳/۹	٪ ۷۰/۸
۰/۳	٪ ۹۹/۹۵	٪ ۷۵/۳	٪ ۰/۰۴۹	٪ ۲۴/۷	٪ ۸۶/۸	٪ ۷۵/۲
۰/۰۱	٪ ۹۹/۵	٪ ۸۷/۷	٪ ۰/۵۳۳	٪ ۱۲/۳	٪ ۹۳/۴	٪ ۷۹/۱

با تعریف مقدار برش ۰/۰۱ برای رگرسیون لجستیک، دقت شناسایی تراکنش‌های سالم، ۹۷/۵ درصد و دقت شناسایی تراکنش‌های متقلبانه، ۷۷ درصد برآورد شده است. جدول ۴ معیارهای عملکرد مدل رگرسیون لجستیک را با مدل شبکهٔ عصبی ایجاد شدهٔ این پژوهش مقایسه می‌کند. همان‌گونه که مشاهده می‌شود، مدل شبکهٔ عصبی قابلیت طبقه‌بندی بسیار بهتری نسبت به رگرسیون لجستیک دارد که دلیل اصلی آن توانایی شبکهٔ عصبی در بازشناسی الگو است.

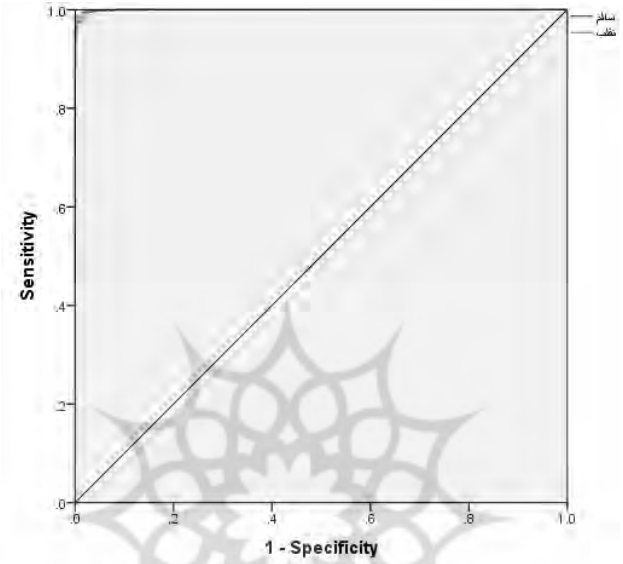
جدول ٤. مقایسهٔ عملکرد مدل‌های شبکهٔ عصبی و رگرسیون لجستیک در شناسایی تقلب

مدل	TNR	TPR	FPR	FNR	$g\text{-mean}_2$	$F_\beta(\beta = ۵)$
شبکهٔ عصبی	٪ ۹۹/۵	٪ ۸۷/۷	٪ ۰/۵۳۳	٪ ۱۲/۳	٪ ۹۳/۴	٪ ۷۹/۱
رگرسیون لجستیک	٪ ۹۷/۵	٪ ۷۷	٪ ۲/۵	٪ ۲۳	٪ ۸۶/۸	٪ ۷۵/۲

نمودار شکل ۴، منحنی ROC[1] مربوط به شبکهٔ عصبی پرسپترون را نمایش می‌دهد. منحنی ROC، نموداری گرافیکی است که عملکرد یک سیستم طبقه‌بندی را با آستانه‌های افتراق متفاوت نمایش می‌دهد. این نمودار با ترسیم نسبت مثبت‌های درست در مقابل نسبت مثبت‌های نادرست با مقادیر برش مختلف، به‌دست می‌آید. در این نمودار، نقطهٔ (۱ , ۰) مختص به بهترین طبقه‌بندی‌کننده‌ای است که می‌تواند تمام موارد مثبت و موارد منفی را به‌درستی طبقه‌بندی کند. در بیشتر مواردِ استفاده از منحنی ROC، سطح زیر نمودار ROC معیار اصلی ارزیابی عملکرد طبقه‌بندی در نظر گرفته می‌شود (فاوسِت، ۲۰۰۳؛ مرزبان، ۲۰۰۴). سطح زیر نمودار ROC برای

1. Receiver Operating Characteristic

مدل پژوهش حاضر برابر با ۰/۹۹۹ محاسبه شده است. نزدیک‌بودن نقاط منحنی به نقطهٔ (۱ , ۰) و نزدیک‌بودن مقدار سطح زیر نمودار ROC به عدد یک، نمایانگر این است که مدل ایجادشده توانایی زیادی در طبقه‌بندی تراکنش‌ها به طبقات سالم و متقلبانه دارد.



شکل ٤. منحنی ROC مدل شبکهٔ عصبی پرسپترون چندلایه

نتیجه‌گیری و پیشنهادها

حاصل پژوهش انجام‌گرفته، مدل‌های شناسایی تقلب در کارت‌های بانکی بوده است که عملکرد آنها در طبقه‌بندی، نسبتاً مناسب به نظر می‌رسد. مدل اصلی این پژوهش، شبکهٔ عصبی پرسپترون چندلایه بوده است که به‌دلیل قابلیت بالای آن در بازشناسی الگو، توانسته است با دقت نسبتاً زیادی هدف پژوهش را برآورده کند. این قابلیت اطمینان، به مدل امکان می‌دهد به‌راحتی تجاری شود و با اتصال به سیستم بانکداری الکترونیک، به‌صورت برخط یا برون‌خطی[1]، اقدامات متقلبانه در تراکنش‌های بانکی را شناسایی کند. یکی از تصمیمات ضروری برای بانک‌ها، نحوهٔ عملیاتی‌کردن مدل‌های شناسایی تقلب است. برای مثال، بانک‌ها باید تصمیم بگیرند که مدل شناسایی تقلب را به‌صورت برخط استفاده کنند یا خیر. در صورت استفادهٔ برخط از مدل‌های شناسایی تقلب، از انجام تراکنش‌های مشکوک به تقلب جلوگیری می‌شود و حتی

1. Offline

کارتی که تراکنش مشکوک با آن انجام گرفته است، باطل می‌شود. لذا این ریسک وجود دارد که نارضایتی بعضی از مشتریان خوبی را شاهد باشیم که مدل به نادرست تراکنش آنها را مشکوک شناسایی کرده است. از سوی دیگر، چنانچه مدل به‌صورت برخط استفاده نشود، این ریسک وجود دارد که تراکنش‌های متقلبانهٔ انجام‌گرفته، برگشت‌پذیر نباشند.

در طبقه‌بندی تراکنش‌های کارت‌های بانکی به گروه‌های سالم و مشکوک به تقلب، سیاست بانک نقش تعیین‌کننده‌ای دارد؛ به‌طوری‌که این سیاست مشخص می‌کند از چه روشی با چه میزان دقت استفاده شود. بنابراین روش استفاده شده در این پژوهش را می‌توان بسته به نیاز بانک‌ها تغییر داد. در پژوهش‌های آتی می‌توان متغیر وابسته‌ای با طبقات چندگانه تعریف کرد. برای مثال می‌توان متغیر وابسته را با طبقات «تراکنش سالم»، «تراکنش با ریسک کم»، «تراکنش با ریسک بالا» و «تراکنش متقلبانه» تعریف کرد و تراکنش‌ها را بر اساس این متغیر وابسته طبقه‌بندی کرد. این امر کمک می‌کند تا تراکنش‌های متقلبانه به‌طور مستقیم مسدود شود و تراکنش‌های با ریسک کمتر را به‌صورت دستی تحت بررسی کارشناسان قرار گیرد.

طی مصاحبه با کارشناسان امنیتِ سیستم بانکداری، این نتیجه به‌دست آمد که تقریباً تمام تراکنش‌های متقلبانه، ظاهری کاملاً قانونی دارند و چنانچه هریک از این تراکنش‌ها را تک‌به‌تک بررسی کنیم، هیچ نشانهٔ مشکوکی در آنها دیده نمی‌شود، درحالیکه این تراکنش‌ها با سایر تراکنش‌های مربوط به کارت مد نظر همزمان بررسی شود، امکان شناسایی موارد مشکوک بیشتر می‌شود. ظاهر قانونی تراکنش‌های متقلبانه، ضمن اینکه شبیه‌سازی داده‌های تقلب را سخت‌تر می‌کند، موجب می‌شود که ایجاد مدل‌های شناسایی تقلب در کارت‌های بانکی پیچیدگی‌های خاص خود را داشته باشد.

References

Alborzi, M., Mohammad Pourzarandi, M. E., Khanbabayi, M. (2010). Using Genetic Algorithm in optimizing decision trees for credit scoring of banks customers. *Journal of Information Technology Management*, 2(4): 23-38. (*in Persian*)

Al-Khatib, A. (2011). Detect CNP fraudulent transactions.*World of Computer Science and Information Technology Journal*, 1(8):326-332.

Azar, A., Ahmadi, P., & Sabt M. V. (2010). Model design for personnel selection with data mining approach (Case Study: A commerce bank of Iran). *Journal of Information Technology Management*, 2(4): 3-22. (*in Persian*)

Bentley, P., Kim, J., Jung, G., & Choi, J. (2000). Fuzzy Darwinian detection of credit card fraud. *Proceedings of 14th Annual Fall Symposium of the Korean Information Processing Society*, Seoul.

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J., C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*. 50(3): 602-613.

Bolton, R. & Hand, D. (2002). Statistical fraud detection: Areview (with discussion). *Statistical Science*, 17(3): 235-255.

Brodersen, K. H., Ong, C. S., Stephan, K. E., & Buhmann, J. M. (2010). The balanced accuracy and its posterior distribution. *Proceedings of 20th International Conference on Pattern Recognition*, 3121-3124.

Chan, P., Fan, W., Prodromidis, A., & Stolfo, S. (1999). Distributed datamining in credit card fraud detection. *IEEE Intelligent Systems*, 14: 67-74.

Delamaire, L., Abdou H., & Pointon J. (2009). Credit card fraud and detection techniques: a review. *Banks and Bank Systems*, 4(2):57-68.

Fan, W., Miller, M., Stolfo, S., Lee, W. & Chan, P. (2004). Using artificial anomalies to detect unknown and known network intrusions. *Knowledge and Information Systems*, 6 (5): 507-527.

Fawcett, T. (2003). *ROC Graphs: Notes and practical considerations for data mining researchers*. CA: Intelligent Enterprise Technologies Laboratory of Hewlett-Packard Company.

Gadi, M. F. A., Wang, X., Pereira, A. & Lago, D. (2008). Credit card fraud detection with artificial immune system. *Lecture Notes in Computer Science*, 5132: 119-131.

Ghasemi, A. R. & Asgharizadeh, E. (2014). Presenting a hybrid ANN-MADM Method to Define Excellence Level of Iranian Petrochemical Companies. *Journal of Information Technology Management*, 6(2): 267-284. (*in Persian*)

Ghosh, S. & Reilly, D. (1994). Credit card fraud detection with a neural-network. *Proceedings of 27th Hawaii International Conference on System Sciences*, 3:621-630.

Gullapalli, V., Kalli, S., & Vijay, A. (2012).*Credit card transaction fraud and mitigating trends: Latest credit card fraud trends and mitigation methodologies*. Retrieved from http://www.capgemini.com/sites/default/

files/resource/pdf/Credit_Card_Transaction_Fraud_and_Mitigation_Trends.pdf.

Hatami Rad, A. & Shahriari, H. R. (2012). E-Banking fraud detection methods and solutions.*Journal of Economics News*, 134: 219-228. (*in Persian*)

Huang, R., Tawfik, H., Nagar, A.K. (2010). A novel hybrid artificial immune inspired approach for online break-in fraud detection. *Procedia Computer Science*,1(1): 2733-2742.

Krivko, M. (2010). A hybrid model for plastic card fraud detection system. *Expert System with Application*, 37(8): 6070-6076.

Kundu, A., Panigrahi, S., Sural, S. & Majumdar, A. K. (2009). BLAST-SSAHA hybridization for credit card fraud detection. *IEEE Transactions on Dependable and Secure Computing*, 6(4): 309-315.

Leonard, K. J. (1995). The development of a rule based expert system model for fraud alert in consumer credit.*European Journal of Operational Research*, 80(2): 350-356.

Marzban, C.(2004).The ROC curve and the area under it as performance measures. *Weather and Forecasting*, 19(6): 1106-1114.

Mohaghar, A., Lucas, C., Hoseini, F., & Monshi, A. A. (2009). Use of business intelligence as a strategic information technology in banking: fraud discovery & detection. *Journal of Information Technology Management*, 1(1): 105-120. (*in Persian*)

Nasiri, N. & Minayi, B. (2011). Data mining methods for credit card fraud detection. *1st International conference on E-Citizen & Cellphone*, 28-29 Feb., Tehran. (*in Persian*)

Nobarzad, A. R. (2013). *Bank card fraud detection using Genetic Algorithm and Scatter Search*. Iran Banking Institute, Tehran. (*in Persian*)

Noriega, L. (2005).*Multilayer Perceptron tutorial*. School of Computing, Staffordshire University, UK.

Ogwueleka, F. N. (2011). Datamining application in credit card fraud detection system. *Journal of Engineering Science and Technology*, 6(3): 311-322.

Paasch, C. A. W. (2008). *Credit card fraud detection using artificial neural network tuned by genetic algorithms* (Doctoral dissertation). Retrieved from the HKUST Institutional Repository (Thesis ISMT 2008 Paasch).

Panigrahi, S., Kundu, A., Sural, S., & Majumdar, A., K.(2009). Credit card fraud detection: A fusion approach using Dempster-Shafer theory and Bayesian learning. *Information Fusion*. 10(4): 354-363.

Patidar, R. & Sharma L. (2011). Credit card fraud detection using neural network. *International Journal of Soft Computing and Engineering*, 1 (NCAI2011): 2231-2307.

Phua, C., Lee, V., Smith, K., & Gayler, R. (2005). A comprehensive survey of data mining-based fraud detection research. *Artificial Intelligence Review*.

Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. *Computing Research Repository*, abs/1009. 6119.

Powers, D. (2011). Evaluation: From Precision, Recall and F-Factor to ROC, Informedness, Markedness & Correlation. *Journal of Machine Learning Technologies*, 2(1): 37-63.

Pulina, M. & Paba, A. (2010). *A discrete choice approach to model credit card fraud*. (No. 20019). University Library of Munich: MPRA.

Robinson S. (2004). *Simulation: The practice of model development and use*. England: John Wiley & Sons.

Sakharova, I. (2012). Payment card fraud: Challenges and solutions. *Proceedings of IEEE International Conference on Intelligence and Security Informatics (ISI)*, 227-234.

Shahrabi, J. (2013). *Data Mining*. Tehran, Amirkabir University Branch of Iranian Academic Center for Education Culture and Research. (*in Persian*)

Shen, A., Tong, R. & Deng, Y. (2007). Application of classification model on credit card fraud detection. *Proceedings of International Conference on Services Systems and Services Management (ICSSSM)*. 9-11 June 2007, Chengdu.

Srivastava, A., Kundu, A. & Sural, S. (2008). Credit card fraud detection using hidden markov model. *IEEE Transactions on Dependable and Secure Computing*, 5(1): 37-48.

Tang, Y., Zhang, Y.Q., Chawla, N.V. & Krasse, S. (2002). SVMs modeling for highly imbalanced classification. *Journal of Latex Class Files*, 1(11):1-9.

Toloie Eshlaghi, A. & Haghdoust, Sh. (2007). Stock price prediction modelling using neural networks and comparison with mathematical prediction methods. *Journal of Economic Research,* 25: 237-252. (*in Persian*)