دومین کنفرانس بین المللی پژوهش های دانش بنیان در
مهندسی کامپیوتر و فناوری اطلاعات
با مجوز به شماره ۱۶/۲۸۰۷۳۸ از وزارت علوم، تحقیقات و فناوری
2nd International Conference on Knowledge-Based Research in Computer Engineering & Information Technology
شهریور ماه ۹۶، تهران، ایران

کشف تقلب در سامانه‌های پرداخت الکترونیک با استفاده از یادگیری عمیق

شیما اشرفی[۱]، محمد طهرانی[۲]، بابک مجیدی[۳]

۱- دانشجوی کارشناسی ارشد رشته کامپیوتر (نرم افزار)، دانشگاه خاتم، تهران، ایران

۲ - استادیار گروه کامپیوتر، دانشگاه خاتم، تهران، ایران

۳- استادیار گروه کامپیوتر، دانشگاه خاتم، تهران، ایران

نویسنده مسئول: m.tehrani@khatam.ac.ir

خلاصه

یکی از مهم‌ترین موانع برای استفاده از بانکداری الکترونیک، عدم امنیت تراکنش‌ها و بروز تقلب در مسیر انجام مبالات مالی است. با توجه به رشد روزافزون تقلب که باعث از دست دادن سرمایه‌های زیادی در سطح جهان و ایران شده و نظر به اینکه از یک سو روش‌های زیادی برای کشف تقلب ارائه شده است ولی روش‌های تقلب هم مدرن‌تر شده و در حوزه‌های مختلف در حال رشد هستند و از سوی دیگر حجم بالای داده و شباهت زیاد بین آن‌ها باعث می شود طبقه بندی داده به متقلبانه و سالم کار بسیار دشواری باشد و نیز یکی از مشکلات در تشخیص تقلب، تنوع و تغییر مداوم شیوه‌های تقلب است و موفقیت در پیشگیری و یا تشخیص یک نوع تقلب باعث به وجود آمدن روشی دیگر می‌شود. بنابراین در این مقاله بر آن شد که روشی برای کشف تقلب در حوزه پرداخت با کارت‌های اعتباری ارائه شود و در این حوزه تمرکز را بر روی تقلب‌هایی که از سوی پذیرنده صورت می گیرد قرار داده شد. در این پژوهش برای شناسایی تقلب از روش ترکیبی یادگیری عمیق با شبکه های عصبی (ANN)[۱] به همراه متد خودرمزگذار[۲] به شناسایی ناهنجاری‌ها در مجموعه داده پرداخته شد که با دقت بالایی تراکنش‌ها به دو دسته متقلبانه و مجاز طبقه بندی شد.

کلمات کلیدی: تشخیص تقلب، شبکه عصبی، یادگیری عمیق، خودرمزگذارها

۱. مقدمه

با پیشرفت روزافزون فناوری‌های نوین در علوم کامپیوتری، بانک‌ها و موسسات مالی و اعتباری نیز دستخوش این پیشرفت ها شده‌اند. هر آنچه این فناوری‌ها باعث سهولت در کارها و مدیریت بهتر فرآیندها شده‌اند ولی مشکلاتی به همراه داشته‌اند، که از آن جمله می توان به بروز تقلب در تراکنش‌های مالی و الکترونیکی اشاره کرد که سالانه هزینه‌ها و خسارات زیادی را برای بانک و موسسات دربرداشته است.[ ]

در سال‌های اخیر پیشرفت زیادی در استفاده از بانکداری الکترونیک و سامانه‌های مدرن بانکی در ایران دیده می‌شود. در نتیجه بروز تقلب و سوء استفاده‌های مالی نیز افزایش می‌یابد و از آنجا که حجم این داده‌ها و تراکنش‌ها بسیار بالا است پیدا کردن ناهنجاری و تقلب در این حجم بالای داده کار بسیار مشکلی است که با به میدان آمدن روش‌های داده کاوی و هوش عملیاتی، روش‌هایی برای کشف تقلب به صورت خودکار پیاده‌سازی شده است.[ ]

[1] Artificial Neural Network
[2] .Autoencoder

در سیستم‌های بانکی کشور، سیستم جامعی برای کشف تقلب تراکنش‌های مبتنی بر کارت به صورت برخط وجود ندارد و به همین دلیل شیوه‌هایی از تقلب‌ها شناسایی نمی‌شوند و متقلبان سال‌های زیادی از این روش‌ها استفاده می‌کنند[]. از این رو بر آن شد که به شناسایی تقلب در تراکنش‌های بانکی مبتنی بر کارت که از سوی پذیرنده صورت می‌گیرد پرداخته‌شود. اگر بتوان به صورت برخط، شناسایی تقلب‌های صورت گرفته از سوی پذیرنده را افزایش داد، می‌توان در بالا بردن اعتماد مشتریان و میزان رضایت آنان نقش بسزایی داشت که این یکی از اهداف و چشم‌اندازهای هر سیستم خدمت‌گذار می‌تواند باشد. بنابراین مهم‌ترین بخش تحقق این آرمان شناسایی ناهنجاری‌ها در این حجم بالای داده و طبقه‌بندی داده در دو بخش مجاز و متقلبانه است. البته باید به این موضوع هم توجه داشت که اگر یک تراکنش سالم هم متقلبانه تشخیص داده شود باعث می شود اعتماد به سیستم کم شده و رضایت مشتریان پایین بیاید. پس کار بسیار دقیق و حساسی باید صورت گیرد تا داده ها به درستی طبقه‌بندی شوند. تراکنش‌های زیادی توسط دستگاه‌های POS در ساعت مختلف روز به سمت سوئیچ‌های بانکی سرازیز می‌شود به همین دلیل به زیرساخت بسیار قوی نیاز است تا با حداقل زمان ممکن تراکنش‌های غیر مجاز شناسایی و به کاربران اخطار داده شود[].

در این مقاله از شبکه عصبی عمیق برای آموزش و طبقه بندی داده‌ها استفاده شده است، و برای کاهش اندازه داده از متد خودرمزگذار استفاده شد که پس از ساخت مدل و پردازش آن با دقت بالغ بر ۸۳٪ موارد تقلب و تقریبا ۱۰۰٪ موارد غیر تقلب را شناسایی شد.

در ادامه به بیان موضوع و لزوم انجام کار پرداخته و کارهای پیشین انجام شده مورد بررسی قرار گرفته است و بعد از آن شبکه عصبی عمیق و الگوریتم‌های خودرمزگذار توضیح داده شده و در انتها مدل پیشنهادی ارائه داده شده و نتیجه بدست آمده، شرح داده می‌شود.

۲. کارهای انجام شده در زمینه کشف تقلب با استفاده از شبکه‌ی عصبی عمیق

وثوق و همکارانش در سال ۱۳۹۳ در پژوهش خود برای تشخیص تقلب در تراکنش‌های بانکی از مدل شبکه‌های عصبی مصنوعی پرسپترون چندلایه‌ی جلورونده استفاده کرده اند. آن‌ها از داده‌های یکی از بانک‌های داخلی استفاده کردند، و با دقت نسبتا خوبی توانستند داده‌ها را طبقه بندی کنند.

اولزووسکی (۲۰۱۴) برای تشخیص تقلب روشی براساس نقشه‌های خود سازمان‌ده و شبکه عصبی پیشنهاد کرده است. او با کمک شبکه عصبی خودسازمان‌ده (SOM[1]) و یک روش آستانه تشخیص بر اساس ماتریس UOM سیستمی پیشنهاد داده و اثربخشی روش پیشنهادی را تایید می کند.[]

فهیمه قبادی و همکاران (۱۳۹۵) در پژوهش خود یک مدل تشخیص تقلب کارت‌های اعتباری مبتنی بر شبکه های عصبی مصنوعی و چند هزینه‌ای برای کاهش ریسک و خطر از دست دادن داده‌های واقعی ارائه دادند و با توجه به ماهیت نامتعادل داده (موارد تقلب و غیر تقلب)، شناسایی معاملات جعلی بسیار دشوار بوده و برای مقابله با مشکل داده‌های نامتعادل، به مدل خود روش چند هزینه را اضافه کرده‌اند. مدل پیشنهادی که شبکه عصبی حساس به هزینه (CSNN[2]) نامیده می شود، مبتنی بر روش تشخیص سوء استفاده است. در این مدل در مقایسه با مدل مبتنی بر سیستم ایمنی مصنوعی (AIS[3])، صرفه جویی در هزینه و افزایش میزان تشخیص نشان داده شده است. درخصوص کشف ناهنجاری در بزرگ داده‌ها، نیز می توان به کار سلطانی حلوایی و اکبری (۲۰۱۴) با استفاده از سیستم‌های ایمنی مصنوعی و مدل نگاشت کاهش در محیط پردازش ابری به کشف ناهنجاری در بزرگ داده پرداخته است اشاره کرد.

[1] . Self Organization Map
[2] . Cost Sensitive Neural Network
[3] . Artificial Immune System

سلیک و همکاران (۲۰۱۷) معتقدن نرمال بودن داده ها برای استفاده در شبکه های عصبی مصنوعی اغلب نیاز به تجزیه و تحلیل آماری گسترده دارد و یک بررسی اولیه از یک مطالعه موردی شامل شناسایی تقلب کارت اعتباری، که در آن تجزیه خوشه ای به منظور نرمال بودن استفاده شده است، ارائه داده‌اند. نتایج حاصل از استفاده‌ی شبکه‌های عصبی مصنوعی و تجزیه و تحلیل خوشه‌ای در شناسایی تقلب در پژوهش آن‌ها نشان می‌دهد که ورودی‌های عصبی توسط ویژگی‌های خوشه‌ای کاهش می‌یابد.[۴]

تمام کارهای قبلی در زمینه‌ی کشف تقلب، بر روی یادگیری ماشین و شبکه‌ی عصبی با یادگیری نظارت شده (با سرپرست) بوده است. اما بر آن شد که از یادگیری ماشین بدون سرپرست یا ناظر استفاده شود. به‌عنوان مثال برای خوشه‌بندی و کاهش (غیر خطی) اندازه‌ی داده از خودرمزگذارها و در تشخیص ناهنجاری‌ها از یادگیری عمیق ماشین، برای تجزیه و تحلیل تقلب استفاده شد.

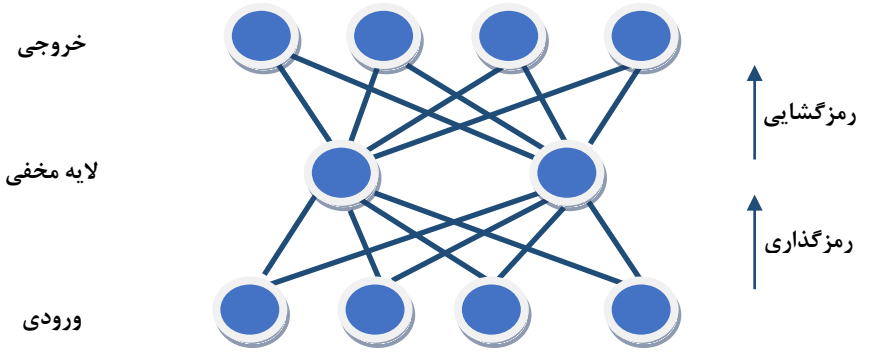
شبکه‌ی عصبی مصنوعی در سال ۱۹۴۰ با الگو گرفتن از عملکرد مدل نورون‌های عصبی مغز انسان مطرح شده است و داده‌ها به اجزایی به نام نورون تقسیم می‌شود و اطلاعات بین نورون‌ها رد و بدل می‌شود و هر یک از این رابطه‌ها دارای وزنی می‌باشند که به مرور آموزش داده می‌شوند و وزن‌ها در شبکه تنظیم می‌شود.

در پایین، نشان داده می‌شود که چگونه می‌توان از خودرمزگذارها در تشخیص ناهنجاری‌ها استفاده نمود. تا قبل از آموزش یک مدل، با استفاده از خودرمزگذارها طبقه بندی و نحوه عملکرد مدل در داده‌های نامتعادل را اندازه‌گیری کنید. خودرمزگذارها، شبکه‌های عصبی مصنوعی با یادگیری عمیق هستند که برای رمزگذاری داده‌ها در شبکه از آن‌ها استفاده می‌شود تا اندازه داده‌ها را کاهش دهند و برای داده‌ها با حجم بالا به کار برده می شود[۲] .

در شبکه‌ی خودرمزگذار حداقل سه لایه وجود دارد که در صورت داشتن تعداد بیشتری لایه فقط می‌توان لایه‌های میانی (پنهان) را افزایش داد. ترتیب لایه ها به صورت زیر می‌باشد.

- لایه ورودی (یک لایه)
- لایه (ها) ی پنهان (یک یا تعداد بیشتر)
- لایه خروجی (یک لایه)

همانطور که در شکل ۱ نشان داده شده است نورون‌های ورودی رمزگذاری می‌شوند و لایه‌های میانی را تشکیل می‌دهند و لایه‌های مخفی میانی هم رمزگشایی می‌شوند تا خروجی را بسازند.



شکل ۱ – نحوه کارکرد شبکه های خودرمزگذار

شبکه‌ی چند لایه هنگام کار در حالت خودرمزگذار، گاهی اوقات یک انتخاب عالی برای انجام فشرده‌سازی داده‌ها یا کاهش ابعاد فضای ویژگی در برنامه‌های پردازش اطلاعات می‌باشد و نشان می‌دهد که برای ارتباط خودکار، غیرخطی بودن واحدهای پنهان بی‌فایده است [].

۳. یادگیری عمیق برای تشخیص تخلف بانکی

داده‌های اصلی پژوهش از تراکنش‌های ثبت شده‌ی کارت‌های بانکی در پایگاه داده‌ی یکی از بانک‌های خصوصی داخلی کشور و با رعایت ملاحظات اخلاقی و با اخذ مجوز از آن بانک، به دست آمد و از آن برای طراحی مدل شناسایی تقلب در کارت‌های بانکی بهره‌جویی شد. لذا تراکنش‌های حدود ۸۶ هزار کارت در بازه‌ی زمانی تقریبی یک ماه، با حدود بیش از ۲۵۰ هزار تراکنش استخراج شده است. با توجه به تعدد فیلدهای اطلاعاتی و کاربردی نبودن برخی از آن‌ها برای این پژوهش، پس از تحلیل آن‌ها به کمک خبرگان و در نظرگرفتن تقلب‌های صورت‌گرفته و شناسایی فیلدهای تحت تأثیر تقلب‌های مختلف، پارامترهای مؤثر در طراحی مدل پژوهش استخراج شد و فیلدهای ناکارا از پایگاه اطلاعاتی کنار گذاشته شد.

مجموعه‌ی داده‌ها حدود ۲۵۰،۰۰۰ مورد از تراکنش‌های کارت‌های اعتباری را ارائه می‌دهد و برای هر تراکنش می‌توان مشخص نمود که آیا تراکنش جعلی است یا نه. داده‌های مجموعه‌ای مانند این، هنگام انجام یادگیری ماشین دارای رفتار خاصی هستند، زیرا آن‌ها به شدت ناسازگار و نامتقارن می‌باشند. در این مورد مطالعه، فقط ٪۰,۱۰۱ از همه‌ی معاملات جعلی بوده و برچسب گذاری شدند.

هنگام برخورد با چنین عدم تعادل شدید در پایگاه داده در زمان اندازه‌گیری عملکرد مدل، باید مراقب بود تا اشتباه نشود. از آنجا که فقط تعداد بسیار اندکی از موارد، متقلبانه هستند، مدلی که با دقت بالای ٪۹۹ تراکنش‌های مجاز را شناسایی کند، با وجود دقت بالای آن، چنین مدلی لزوما به ما کمک نمی کند که موارد جعلی را با دقت بالا پیدا کنیم .

برای ایجاد شبکه‌ی عصبی چندلایه به منظور شناسایی تقلب در کارت‌های بانکی، پس از آزمایش حالت‌های مختلف ایجادشده برای شبکه‌ی عصبی (تعداد لایه‌های مختلف، تعداد گره‌های مختلف در هر لایه و توابع تبدیل مختلف)، بهترین حالت انتخاب شد. این کار با مقایسه‌ی میانگین مربعات خطا (MSE) در هریک از حالات انجام گرفت.

برای بررسی داده‌ها و متغیرهای مدل، متغیرهای ورودی شبکه‌ی عصبی، شامل ۶ متغیر مستقلی است که در تعیین رفتار دارنده‌ی کارت و ترمینال پذیرنده‌ی کارت نقش دارند. برای متغیر خروجی در سیستم نیز یک پارامتر تعیین شده است. شش متغیر ورودی را فیلدهای اطلاعاتی انتخابی از میان تمامی فیلدهای مربوط به تراکنش‌های ثبت شده 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. یک مدل شبکه عمیق عصبی با استفاده از فرم‌های تشکیل شده برای شبکه‌ی عصبی چند عاملی روبه جلو با لایه‌های مخفی به سایز (۱۰,۲,۱۰) ساخته شده است.

برای ایجاد مدل شناسایی تقلب در تراکنش‌های کارت‌های اعتباری بانکی، یک متغیر افراز ایجاد شد تا بتوان داده‌ها را به دو بخش آموزش و اعتبارسنجی تقسیم‌بندی کرد. به واسطه‌ی تعریف متغیر افراز و انتخاب داده‌هایی که برای آموزش و آزمون استفاده خواهند شد، از مجموع ۲۵۶,۵۵۹ داده، ۲۰۵,۲۴۶ داده (۸۰ درصد) برای آموزش و ایجاد مدل اختصاص یافت و ۵۱,۳۱۳ داده (۲۰ درصد) برای اعتبارسنجی مدل به صورت تصادفی تخصیص داده شد. از مجموع

[1] . Mean Square Error

۲۰۵,۲۴۶ داده‌های آموزشی که به دو قسمت مساوی (۱۰۲,۶۲۳) تقسیم شد،۴۰ درصد از کل داده برای داده آموزشی با ناظر (سرپرست) و ۴۰ درصد باقی مانده از کل داده، داده آموزشی بدون ناظر تعیین شد.

تابع تبدیل انتخاب برای تمامی نورون‌های لایه‌های پنهان، تابع تانژانت هیپربولیک است. رابطه‌ی ۱، تابع تبدیل استفاده شده را نشان می‌دهد. این تابع، مقادیر وزن‌ها را پس از دریافت به مقداری در بازه‌ی (۱,۱) تبدیل می‌کند.

$$\tanh(x) = 2\partial(2x) - 1 \quad (1)$$

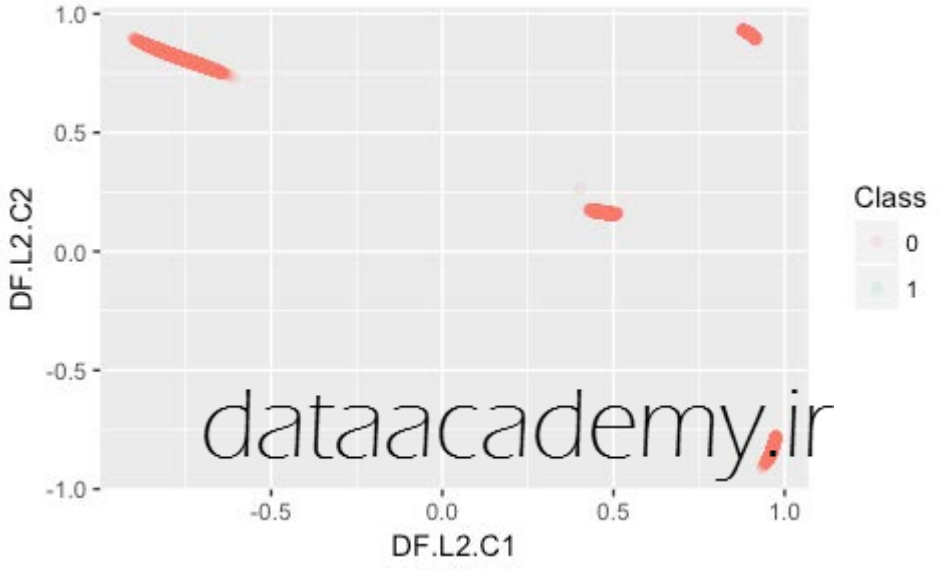
که در آن $\sigma(x)$ به صورت زیر تعریف می شود:

$$\partial(x) = ex/1 + ex \quad (2)$$

با بررسی داده‌ها توسط فرد خبره، الگوریتمی طراحی شد که داده‌های متقلبانه را شناسایی و برچسب گذاری کرده و ستونی به داده ها اضافه شد که در آن مقدار ۱ به ما می گوید که این تراکنش تقلب بوده است.

مدل خودرمزگذار، الگوهای داده های ورودی را بدون درنظرگرفتن برچسب‌های داده، یاد می‌گیرد. در این مورد باید یاد بگیرد که کدام تراکنش‌های کارت اعتباری شبیه هستند و کدام تراکنش‌ها بی‌نظیر هستند یا ناهنجاری‌ها هستند. باید در نظر داشت که مدل‌های خودرمزگذار در داده‌های نامتقارن بسیار پیچیده و حساس هستند، که ممکن است الگوهای غیرمعمول را شناسایی کنند و ما را گمراه کنند.

در مرحله بعد به کاهش اندازه داده با لایه‌های پنهان پرداخته شد، از آنجایی که از مدل گلوگاه با دو گره در لایه مخفی و در میانه مدل شبکه عصبی استفاده شده است، می‌توانیم از این کاهش اندازه داده، برای کشف فضای ویژگی‌ها استفاده شود (مشابه آنچه که می توان با تجزیه و تحلیل مولفه اصلی انجام داد). می توانیم این ویژگی لایه‌های پنهان را از عملکرد الگوریتم استخراج کرد و آن را برای نمایش داده‌های ورودی استفاده نمود.



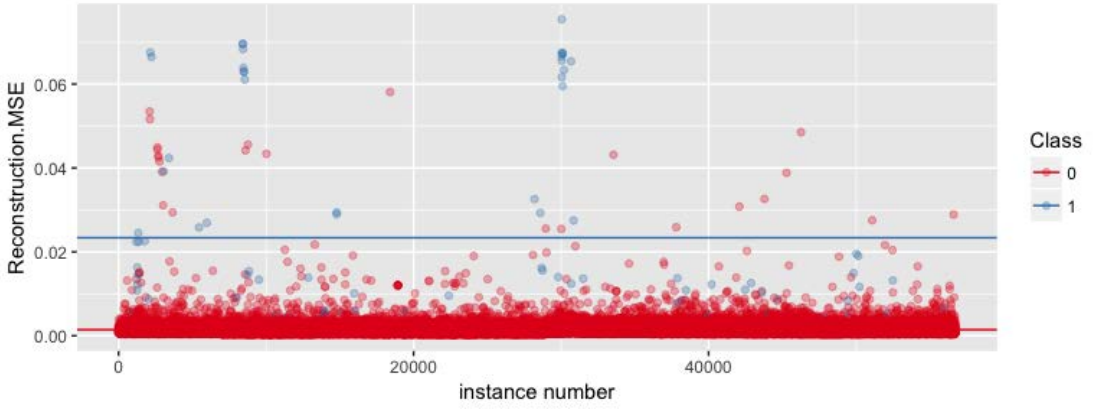
شکل ۳– طبقه‌بندی داده ها بر اساس مجاز و متقلبانه

در نمودار شکل ۳، همان‌طور که مشاهده می‌نمایید، یک دسته‌بندی از تراکنش‌های تقلبی که از نمونه‌های مجاز متمایز نشده است دیده می‌شود، بنابراین کاهش اندازه داده با مدل خودرمزگذار به تنهایی نمی‌تواند برای شناسایی تقلب در این مجموعه داده کافی باشد. اما راه حلی که به نظر می‌رسید این است که می‌توان داده‌های انتخاب شده، که از کاهش اندازه‌ی داده‌های لایه‌های پنهان به‌دست آمده است، را به عنوان ویژگی‌هایی برای آموزش مدل مورد استفاده قرار داد. به عنوان مثال می‌تواند از ۱۰ ویژگی موجود در لایه اول یا سوم لایه مخفی استفاده شود. برای این منظور برای اندازه گیری عملکرد مدل در داده‌های آزمون، باید داده‌های آزمون را به همان اندازه‌ی کاهش یافته‌ی داده‌های آموزش تبدیل کرد.

در این مرحله، به نظر می‌رسد شناسایی موارد تقلب با درصدی بالای ۹۲٪ بسیار خوب است. با این حال، بسیاری از موارد مجاز نیز به عنوان تقلب محسوب شده است و این موضوع برای دنیای واقعی، یک مدل خوب به شمار نمی‌آید. بنابراین بر آن می‌شویم که برخی از تکنیک‌های دیگر را امتحان کنیم[۱].

در ادامه به تشخیص ناهنجاری پرداخته شده است، سوالی که اینجا مطرح می‌شود اینست که از نمونه‌هایی که در مجموعه داده‌های آزمون وجود دارد کدام داده‌ها ناهنجار هستند؟ که برای این منظور می‌توان از الگوریتم خودرمزگذاری استفاده کرد. بر اساس مدل خودرمزگذار که قبلا آموزش دیده بود، داده‌های ورودی بازسازی شدند و برای هر نمونه میانگین

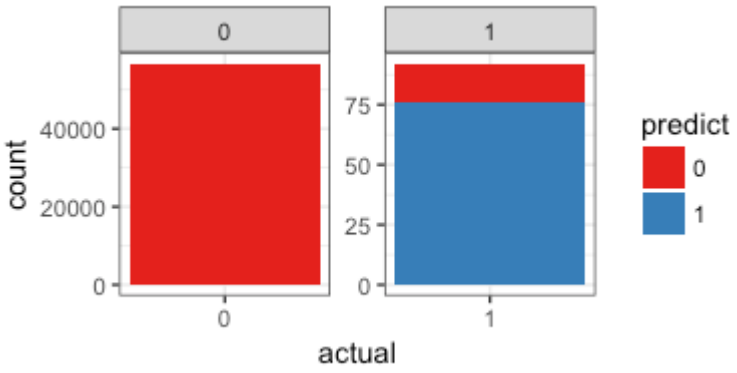
خطای مربع (MSE) بین مقدار واقعی و بازسازی شده محاسبه شد. در نتیجه‌ی محاسبه میانگین مربعات، برای هر دو برچسب کلاس، نمودار زیر بدست آمد.



شکل ۴ – میزان میانگین خطای مربعات برای طبقه‌بندی مدل

همانطور که در نمودار شکل ۴ مشاهده می‌نمایید، یک طبقه‌بندی خوب در موارد داده‌های تقلب و مجاز وجود ندارد، اما میانگین خطای مربعات برای تفکیک کردن تراکنش‌های تقلبی از مجاز قابل قبول است. در این مرحله می‌توان نمونه‌های ناهنجار را با استفاده از آستانه MSE برای آنچه که در نظر گرفته می‌شود، شناسایی کرد. به عنوان مثال هر نمونه که دارای $MSE > 0.02$ (مطابق با نمودار بالا) است را به عنوان یک ناهنجاری در نظر گرفت. در این قسمت به این نتیجه می‌توان رسید که، تشخیص درست ناهنجاری با طبقه‌بندی تراکنش‌های جعلی کارت اعتباری (یا حداقل با این مجموعه داده‌ها) مهیا نیست[]!

در ادامه مدل تحت نظارت پیش آموزش دیده شده را بررسی کرده و سپس از مدل خودرمزگذار به عنوان ورودی از قبل آموزش دیده برای یک مدل تحت نظارت استفاده خواهد شد. در اینجا، دوباره از یک شبکه‌ی عصبی استفاده شده است. این مدل از وزن مدل خودرمزگذار برای تنظیم گره‌های مدل استفاده کرده است.

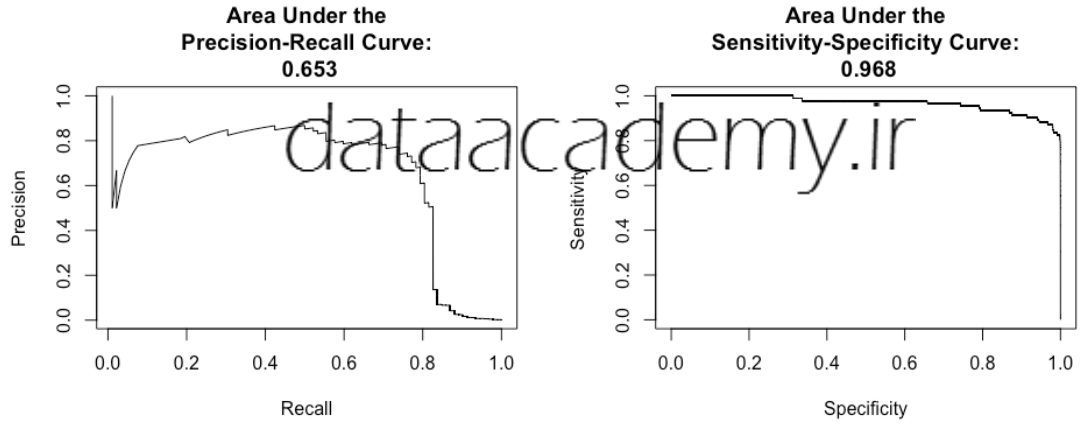


شکل ۵ – نسبت میزان پیش بینی های مدل به کل داده

با این روش نتیجه بهتری بدست آمد. آنچه از نمودار شکل ۵ نمایان است، این است که ۱۷ درصد از موارد تقلب از دست داده شده، اما برای تعداد زیادی از موارد مجاز طبقه‌بندی به درستی انجام شده است. در حقیقت، اکنون اعتماد بیشتری می‌توان به مدل داشت زیرا پارامترهای مدل دقیق‌تر طراحی شدند، به عنوان مثال، زمان هایی که برای جستجو در شبکه برای بهینه‌سازی پارامترها، بازگشت به ویژگی‌های اصلی و تلاش‌هایی که برای محاسبه ویژگی‌ها و الگوریتم‌های مختلف صرف شد موثر واقع شدند.

اندازه‌گیری عملکرد مدل در داده‌های بسیار نامتعادل صورت گرفته است و با توجه به اینکه شناسایی موارد مجاز از حساسیت بالایی برخودار است، نمی‌توان از معیارهای عملکرد مانند دقت و یا سطح زیر منحنی (AUC[1]) استفاده کرد، زیرا نتایج بسیار خوش‌بینانه را براساس درصد بالایی از طبقه بندی‌های صحیح طبقه اکثریت ارائه می‌دهند.

یک جایگزین خوب برای AUC استفاده از منحنی یادآوری دقیق[2] یا یادآوری حساسیت[3] است. روش‌های مختلفی برای محاسبه مساحت زیر یک منحنی وجود دارد، اما در این مقاله از یک تابع ساده استفاده شده است که محدوده بین هر جفت نقطه متوالی x را محاسبه می کند (یعنی x1 - x0، x2 - x1، و غیره) و نسبت به فضای تحت مقادیر مربوطه y بیان می‌شود[1].



شکل ۶– نمودار ارزیابی نهایی مدل

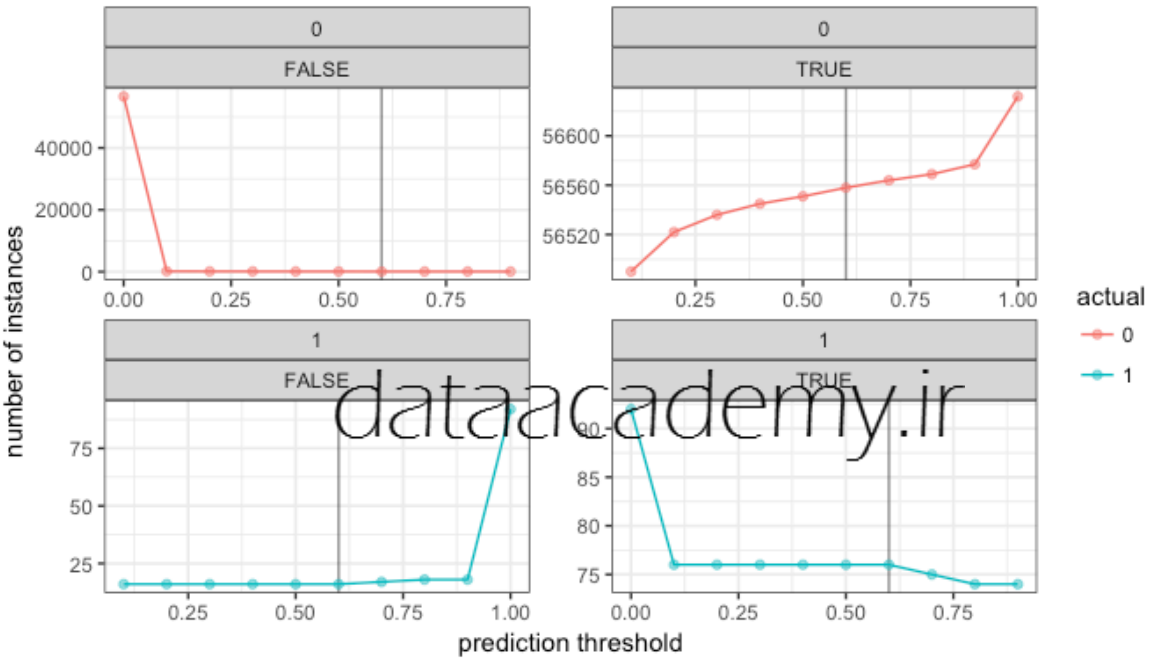
در نمودار شکل ۶ دو شاخص حساسیت و صحت برای ارزیابی مدل نمایش داده شده است. از آن‌جایی که اطلاعات مدل به دو قسمت متقلبانه و مجاز تقسیم می شود می توان برای ارزیابی مدل از نمودارهای حساسیت و صحت استفاده نمود. زیرا این نمودارها برای مدل‌های دودویی کاربرد دارند. صحت[4]، در این مدل نسبت موارد مورد آزمایش پیش‌بینی شده‌ی متقلبانه که در واقع جعلی هستند بیان می‌شود (یعنی همان پیش‌بینی‌های مثبت واقعی[5])، در حالی که حساسیت[6]،

[1] . area under the curve
[2] . precision-recall curve
[3] . Sensitivity recall-specificity curve
[4] . Precision
[5] . True Negative Rate
[6] . Sensitivity

نسبت موارد سالم است که به عنوان غیرمتقلبانه شناخته شده‌اند.[1] و مشخصه یا ویژگی[2] نسبت موارد غیر تقلب است که به عنوان عدم تقلب شناخته شده است.[3]

منحنی یادآوری صحت نسبت تقلب واقعی به موارد تقلب که شناسایی شده است را نشان می دهد. (به عنوان مثال مواردی از تقلب، و همچنین مواردی از موارد مجاز که پیش‌بینی کرده‌ایم که تقلب است و بالعکس). منحنی حساسیت به این ترتیب ارتباط بین دسته‌بندی‌هایی که به درستی شناسایی شده برای هر دو برچسب را بیان می‌کند (یعنی اینکه ما موارد تقلب را به درستی تقلب پیش‌بینی کرده باشیم و موارد مجاز را هم به درستی مجاز تشخیص داده باشیم).[12]

همچنین می توان با نگاهی متفاوت به این مسئله و دقت به آستانه‌های پیش‌بینی‌های مختلف و محاسبه تعداد موارد درست در دو کلاس، داده‌ها را طبقه بندی کرد.



شکل ۷ – نمودارهای حساسیت و دقت نتیجه مدل

این نمودار نشان می دهد که می توان تعداد موارد به‌درستی طبقه بندی شده‌ی موارد غیرتقلب را بدون از بین بردن موارد طبقه تقلب، درست طبقه بندی کرد، هنگامی که آستانه پیش‌بینی را از پیش فرض ۰,۵ تا ۰,۶ افزایش داد. و در آخر مدل نهایی به درستی ۸۳٪ موارد تقلب و تقریبا ۱۰۰٪ موارد غیر تقلب را شناسایی کرده است.

۴. نتیجه‌گیری

[1] . True Positive Rate
[2] . Specificity
[3] . True Negative Rate

از آنجایی که تقلب مانع پیشرفت فناوری‌های نوین در سیتم‌های بانکی شده است و با توجه به رشد روزافزون تقلب که باعث از دست دادن سرمایه‌های زیادی در حوزه‌ی بانکداری الکترونیک شده و روش‌های تقلب در تراکنش‌های بانکی روز به روز افزایش یافته و تغییر می‌کنند، در این مقاله بر آن شد که روشی برای کشف تقلب در حوزه‌ی پرداخت با کارت‌های اعتباری ارائه شود و در این حوزه تمرکز بر روی تقلب‌هایی که از سوی پذیرنده صورت می گیرد قرار داده شد. در این پژوهش برای شناسایی تقلب از روش ترکیبی یادگیری عمیق با شبکه های عصبی (ANN) به همراه متد خودرمزگذار به شناسایی ناهنجاری‌ها در مجموعه داده پرداخته شد و داده های آموزش شامل دو دسته با ناظر و بدون ناظر بودند که با دقت بالایی تراکنش‌ها به دو دسته متقلبانه و مجاز طبقه بندی شدند. و با دقت بالای ۸۳ درصد موارد متقلبانه به درستی تشخیص داده شد و نیز با دقت تقریبا ۱۰۰ درصد موارد مجاز طبقه بندی و تشخیص داده شد.

۵. مراجع

۱ . حاتمی راد، علی ؛ شهریاری، حمید رضا (۱۳۹۰)؛ «روش ها و راهکارهای شناسایی تقلب دربانکداری الکترونیک»؛ فصل نامه تازه های اقتصاد، شماره ۱۳۴، سال نهم، ص ۲۲۸-۲۱۹.

۲. بنائی، هادی؛ خوش نیت، حسام (۱۳۹۰)؛ «نقش و کاربرد هوش عملیاتی و داده کاوی در کشف تقلب بر خط»؛ ششمین همایش ملی تجارت و اقتصاد الکترونیکی.

۳ . وثوق، م و تقوی فرد، م. ت والبرزی، م. شناسایی تقلب در کارت‌های بانکی با استفاده از شبکه‌های عصبی مصنوعی. نشریه مدیریت فناوری اطلاعات، ۶ (۴)، ص ۲۲۱-۲۴۶.

۴ . سلطانی حلوایی، ندا؛ اکبری، محمد کاظم و سرگلزایی جوان، مرتضی؛(۱۳۹۱) ارائه مدل پیاده سازی سیستم کشف تقلب کارت های اعتباری در محیط ابری با استفاده از نگاشت-کاهش، اولین کارگاه ملی رایانش ابری، تهران، دانشگاه صنعتی امیرکبیر.

۵ Olszewski, D. (2014). Fraud detection using self-organizing map visualizing the user profiles. Knowledge-Based Systems, 70: 324-334.

۶. Celik, E. (2017) & Kondiloglu, A. Detection of fake banknotes with Artificial Neural Networks and Support Vector Machines, 2165-0608.

۷ Modeling word perception using the Elman network, Liou, C. -Y. , Huang, J. -C. and Yang, W. -C. Neurocomputing, Volume 71, 3150–3157 (2008), doi:10.1016 /j.neucom.2008.04.030.

۸ Auto-association by multilayer perceptrons and singular value decomposition, H. Bourlard and Y. Kamp Biological, Cybernetics Volume 59, Numbers 4-5, 291-294, doi: 10.1007/BF00332918.

۹ 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.

۱۰Ogwueleka, F. N. (2011). Datamining application in credit card fraud detection system. Journal of Engineering Science and Technology, 6(3): 311-322.

۱۱Patidar, R. & Sharma L. (2011). Credit card fraud detection using neural network. International Journal of Soft Computing and Engineering, 1 (NCAI2011): 2231-2307.

۱۲Sakharova, I. (2012). Payment card fraud: Challenges and solutions .Proceedings of IEEE International Conference on Intelligence and Security Informatics (ISI), 227-234.