

مقدمه

❖ راهکارهای مبارزه با تقلب

- ❖ شناسایی تقلب در سریعترین زمان ممکن و جلوگیری از گسترش آن
- ❖ پیشگیری از تقلب و جلوگیری از عدم وقوع آن

❖ ضررهای تقلب

- ❖ تحمیل ضررهای مستقیم مالی به سازمان
- ❖ تأثیر منفی بر خدمت‌رسانی به مشتریان
- ❖ تأثیر منفی بر اعتبار و کارایی سازمان
- ❖ سلب اعتماد عموم افراد جامعه نسبت به خدمات ارائه شده

ضررهای غیر مستقیم به مراتب با اهمیت‌تر از ضررهای مستقیم مالی هستند.

راهکار: سرعت عمل در شناسایی فعالیتهای متقلبانه

اصول پیشگیرانه برای مدیریت خطر وقوع تقلب به نحو موثر

- ❖ برنامه مدیریت خطر تقلب بخشی از ساختار راهبری (خطامشی‌های مکتوب برای برآوردن انتظارات هیات مدیره و مدیریت ارشد)
- ❖ ارزیابی زمینه‌های مستعد خطر تقلب به طور دوره‌ای
- ❖ تدوین فنون جلوگیری در بخش‌ها و در موارد ممکن برای اجتناب از وقوع رویدادهای دارای خطر تقلب بالقوه با اهمیت، جهت کاهش آثار احتمالی این مخاطرات
- ❖ به کارگیری فنون لازم برای کشف در مواقعی که معیارهای اندازه‌گیری، نارسا شده یا احتمال وقوع خطر تقلب موجود کاهش نمی‌یابد
- ❖ برقراری فرآیند گزارش‌گیری جهت برملا شدن عوامل شکل‌گیری موارد خطر تقلب بالقوه
- ❖ رویکردی هماهنگ برای بررسی و انجام اقدامات اصلاحی جهت شناسایی مناسب و به موقع احتمال وقوع تقلب



جمهوری اسلامی ایران



پژوهشکده پولی و بانکی
بانک ملی ایران، بانک تجارت، بانک صادرات



دفترکارت ملی صورتمحاسب



جمهوری اسلامی ایران



پژوهشکده پولی و بانکی
بانک ملی ایران، بانک تجارت، بانک صادرات



دفترکارت ملی صورتمحاسب



کشف تقلب

❖ کشف تقلب یعنی:

- ❖ ماکزیمم کردن نرخ دقت و پیش‌بینی‌های درست
- ❖ مینیمم کردن تقلب‌های تشخیص داده نشده و اشتباه تشخیص داده شده (حفظ اشتباهات در سطح قابل قبول)

❖ روش‌های آماری کشف تقلب:

- ❖ با ناظر: نمونه‌هایی از موارد تقلبی و غیر تقلبی موجود است (مانند آنتی وپروس)
- ❖ بدون ناظر: اطلاعات و دانش قبلی در خصوص تراکنش‌های تقلبی وجود ندارد. یعنی کشف تقلب‌های جدید

کم هزینه‌ترین روش تشخیص تقلب:
خارج کردن تراکنش‌های مشکوک به تقلب از پایگاه داده
توسط الگوریتم‌های ریاضی (داده کاوی، هوش مصنوعی، الگوریتم‌های ژنتیک، شبکه‌های عصبی و ...)



پایگاه ملی آماری



پژوهشکده ملی و دانشی
داده کاوی، هوش مصنوعی، ژنتیک



مركز ملی داده کاوی



داده کاوی

- ❖ جمع‌آوری، پردازش و استفاده از داده‌ها
- ❖ کشف الگوهای معتبر و ناشناخته و وابستگی‌های موجود در مجموعه‌ای حجیم از داده‌ها با استفاده از ابزارهای تحلیلی پیچیده

❖ راهکارهای داده کاوی:

- ❖ طبقه‌بندی: ارزشیابی تراکنش و تخصیص به گروه‌های از پیش تعریف (شبکه‌های عصبی و درختان تصمیم)
- ❖ خوشه‌بندی: تراکنش‌های یک خوشه با یکدیگر مشابه و متفاوت از سایر خوشه‌ها
- ❖ پیش‌بینی: برآورد مقدارهای عددی و پیوسته آینده بر مبنای الگوهای از یک مجموعه داده (شبکه‌های عصبی)
- ❖ کشف نقاط پرت: داده‌هایی با ویژگی‌هایی متفاوت از بقیه جمعیت
- ❖ رگرسیون: روشی آماری برای کشف رابطه بین یک یا چند متغیر مستقل و یک متغیر وابسته
- ❖ تصویرسازی: تبدیل الگوهای پیچیده کشف شده به الگوهای واضح و قابل درک برای کاربران



پایگاه ملی آماری



پژوهشکده ملی و دانشی
داده کاوی، هوش مصنوعی، ژنتیک



مركز ملی داده کاوی



شبکه های عصبی

- ❖ روشی محاسباتی بر پایه اتصال چندین واحد پردازشی
- ❖ تشکیل شده از تعداد دلخواهی سلول (گره یا نرون)
- ❖ حداقل شامل یک لایه ورودی، یک لایه خروجی با امکان وجود لایه های پنهان
- ❖ مجموعه ای پیچیده و یادگیرنده از نرون های به هم متصل با ارزش وزنی مشخص
- ❖ ارتباط دهنده مجموعه ورودی به مجموعه خروجی
- ❖ **شبکه عصبی توانایی آموختن دارد:**
- ❖ ارسال پالس به یک لایه و آغاز فعالیت آن
- ❖ بررسی و اصلاح پالس توسط نرون های آن لایه
- ❖ افزایش قدرت پالس توسط نرون ها
- ❖ انتقال به لایه بعدی

شبکه‌های عصبی

❖ مزیت:

❖ امکان تشخیص رفتارهای کاربران در هر دو رویکرد با ناظر و بدون ناظر

❖ معایب:

❖ دشوار بودن تفسیر روشی که این شبکه‌ها به تصمیمات خود می‌رسند

❖ تعریف عواملی نظیر توپولوژی شبکه به طور تجربی

❖ عدم وجود مفروضاتی در خصوص ویژگی توزیع داده‌ها و متغیرهای مستقل ورودی بر خلاف روش‌های آماری

کلاسیک



انستیتوت ملی فناوری‌های نوین



پژوهشگاه ملی و دانش
تکنولوژی‌های نوین



دفترت ملی فناوری‌های نوین

نمونه کاربردی شبکه‌های عصبی

❖ سیستم مدیریت تقلب فالكون

❖ ابزار بسیار قدرتمندی جهت جلوگیری از فعالیت متقلبان در سوءاستفاده از کارت‌های اعتباری

❖ آموزش الگوی خرج کردن صاحب کارت

❖ تشخیص هرگونه مغایرت در روش و چگونگی پرداخت وجه

❖ تماس تلفنی با دارنده کارت بلافاصله پس از تشخیص تراکنش مشکوک روی کارت

❖ بلوکه کردن کارت با تایید تقلب از سوی دارنده کارت

❖ بلوکه شدن موقت کارت در شرایط عدم امکان برقراری تماس تلفنی با دارنده کارت

پایاده سازی سیستم فالكون توسط:

(۲) تشخیص الگوی تطبیقی

(۱) تکنیک‌ها و فناوری‌های یادگیری ماشینی

(۴) مدل‌های آماری

(۳) شبکه‌های عصبی



الگوریتم ژنتیک

- ❖ فرزندان به والدین خود شباهت دارند اما با آنها یکسان نیستند (ارث بردن ویژگی‌ها از هر دو والد و جهش ژنتیکی)
- ❖ فرزندان ممکن است نسبت به والدین خود مناسب‌تر باشند یا نباشند
- ❖ فرزندان همان راه والدین خود را ادامه می‌دهند
- ❖ بعد از چندین نسل موجوداتی ایجاد می‌شوند که نسبت به اجداد اولیه خود سازگاری و تناسب بیشتری دارند
- ❖ **عدم کاربرد در کشف الگوها، کاربرد در یافتن راه‌حل بهینه:**
- ❖ ارائه هر یک از پاسخ‌ها در قالب یک رشته (کروموزم) از اعداد (ژن)
- ❖ جمعیت نسل اول شامل تعدادی از پاسخ‌های اولیه
- ❖ ثابت بودن تعداد پاسخ‌ها و بهبود کیفیت آن‌ها نسل به نسل
- ❖ سنجش پاسخ‌ها با تابع برازش در هر نسل
- ❖ ایجاد نسل بعد با ثابت ماندن برخی پاسخ‌ها و جهش در کروموزم برخی دیگر از پاسخ‌ها



مرکز ملی مهندسی ژنتیک



پژوهشگاه ملی و دانش

تکنولوژی و نوآوری، تهران، ایران



دفترت ملی مهندسی ژنتیک

11



سیستم‌های خبره

- ❖ نوعی سیستم محاسباتی با بهره‌گیری از قانون «اگر-آنگاه»
- ❖ توانایی حل مشکلات و ارائه راهکار در حوزه‌های مختلف با پیش‌بینی «در چه حالتی، چه اتفاقی باید بیفتد»
- ❖ موفق‌ترین کاربرد هوش مصنوعی در مسائل واقعی
- ❖ پیچیدگی در طراحی و گسترش به دلیل استفاده از دانش متخصصین در حوزه‌های خاص (افراد مختلف مسائل را به شیوه خاص خود حل می‌کنند. یک فرد خاص ممکن است یک مسئله خاص را هر بار به شیوه‌ای متفاوت حل کند)

بخش‌های اصلی:

- ❖ پایگاه دانش: محل ذخیره سازی مجموعه‌ای از قوانین «اگر-آنگاه» (کدگذاری شده و قابل فهم برای سیستم)
- ❖ موتوراستنتاج: تصمیم می‌گیرد چه قانونی و در چه مورد و رده‌ای باید برای ارزیابی انتخاب شود.
- ❖ امکانات توضیح: برای نشان دادن مراحل نتیجه‌گیری یک مسئله خاص به کاربر به زبان قابل فهم وی
- ❖ رابط کاربر برای ارتباط سیستم و کاربر



مرکز ملی مهندسی ژنتیک



پژوهشگاه ملی و دانش

تکنولوژی و نوآوری، تهران، ایران



دفترت ملی مهندسی ژنتیک

12

درخت تصمیم‌گیری

- ❖ از ابزارهای داده‌کاوی و روشی کارآمد برای ایجاد دسته‌بندی از داده‌ها
- ❖ مورد استفاده در رده‌بندی داده‌های کیفی
- ❖ دسته‌بندی داده‌های جدید با ایجاد درخت تصمیم براساس داده‌های موجود با رده‌بندی مشخص
- ❖ هر برگ درخت تصمیم، نماینده یک طبقه
- ❖ مهم‌ترین خصوصیت: قابلیت شکستن فرآیند پیچیده تصمیم‌گیری به مجموعه‌ای از تصمیمات ساده و قابل تفسیر
- ❖ روشی راهگشا برای کشف تقلب با قابلیت فهم بالا و سرعت مناسب در یادگیری الگو

روش تک مرحله‌ای دسته‌بندی	درخت تصمیم
امتحان هر نمونه روی تمام دسته‌ها	امتحان نمونه روی زیر مجموعه‌های خاصی از دسته‌ها و حذف محاسبات غیرضروری
انتخاب زیر مجموعه‌ای از صفات (با یک معیار بهینه سراسری) و استفاده برای روش بین دسته‌ها	انتخاب زیر مجموعه‌های متفاوتی از صفات در گروه‌های داخلی مختلف که به نحو بهینه دسته‌های این گروه را تفکیک می‌کند یعنی بهبود کارایی



جمهوری اسلامی ایران



سازمان ملی استاندارد و تحقیقات صنعتی ایران



سازمان ملی استاندارد و تحقیقات صنعتی ایران

13

استدلال بر پایه مدل و مبتنی بر مورد

- ❖ **استدلال بر پایه مدل**
 - ❖ تکنیک تشخیص سوءاستفاده (روش با ناظر)
 - ❖ تشخیص تقلب با مقایسه فعالیت‌های در حال انجام با بانک اطلاعاتی شامل مجموعه‌ای از سناریوی حملات
 - ❖ دقیقاً مشابه روال کار نرم‌افزارهای ویروس‌یاب
 - ❖ جمع‌آوری شواهدی دال بر حمله و تکرار این کار به طور پیوسته و مکرر تا رسیدن به حد آستانه و اعلام آن

❖ استدلال مبتنی بر مورد

- ❖ روشی استنتاجی (استفاده از تجربیات کسب شده در حل مسائل گذشته به عنوان راهنمایی برای مسئله جدید)
- ❖ بازیابی مورد مشابه بازیابی شده با مسئله جدید
- ❖ استفاده از پاسخ مسئله مشابه بازیابی برای تهیه پاسخ پیشنهادی برای مسئله جدید
- ❖ بازیابی در پاسخ پیشنهادی در صورت وجود مغایرت در شرایط مسئله جدید و مسائل بازیابی شده
- ❖ نگهداری مورد جدید (مسئله جدید و پاسخ آن) برای استفاده در آینده



جمهوری اسلامی ایران



سازمان ملی استاندارد و تحقیقات صنعتی ایران



سازمان ملی استاندارد و تحقیقات صنعتی ایران

14

سایر روش‌های بدون ناظر

❖ خوشه‌بندی

- ❖ شناسایی گروه‌های عادی تراکنش‌ها و نقاط دور افتاده یک پایگاه داده
- ❖ اهمیت بسیار زیاد نحوه خوشه‌بندی داده‌ها
- ❖ تراکنشی با حجم بسیار بالا در مقایسه با سایر تراکنش‌هایی که حجم کمتری دارد
- ❖ تراکنشی با مبلغ بالا برای یک حساب کاربری که تاریخچه حجم تراکنش‌های آن بسیار کمتر بوده

❖ نزدیکترین همسایگی

- ❖ ترکیب اطلاعات تراکنش حساب‌های کاربری که رفتارهای مشابهی دارند
- ❖ مقایسه تراکنش‌های متوالی هر حساب کاربری به منظور کشف تغییر در رفتار



پایگاه ملی آماری



پژوهشکده ملی آماری و رایانش

دانشگاه تهران، تهران، ایران



دفترکارت ملی آماری

سایر روش‌های بدون ناظر

❖ تحلیل گروه همتا:

- ❖ ابزاری جدید برای نظارت بر رفتار مشترکین جهت شناسایی تراکنش‌های متفاوت با گذشته
- ❖ انتخاب هر تراکنش به عنوان تراکنش هدف و مقایسه با سایر تراکنش‌های پایگاه داده با استفاده از معیارهای داخلی و خارجی (خلاصه‌ای از رفتارهای پیشین مشتری)
- ❖ شناسایی گروهی از تراکنش‌های مشابه به تراکنش هدف
- ❖ بررسی رفتارهای آتی این گروه و مقایسه با رفتارهای آتی تراکنش هدف
- ❖ شناسایی تراکنش هدفی که رفتاری بسیار متفاوت نسبت به گروه خود انجام داده

یعنی:

دنباله‌ای از تراکنش‌ها در مقایسه با کل تراکنش‌ها ممکن است کاملاً عادی باشد اما در مقایسه با گروه هم‌تای خود رفتاری غیرعادی تلقی شود.



پایگاه ملی آماری



پژوهشکده ملی آماری و رایانش

دانشگاه تهران، تهران، ایران



دفترکارت ملی آماری

سایر روش های بدون ناظر

❖ تجزیه و تحلیل نقطه انفصال

- ❖ استفاده در سطح هر حساب کاربری به طور جداگانه برای مقایسه تعداد و حجم تراکنش های متوالی جهت شناسایی تغییر در رفتار کاربران
- ❖ بررسی گروهی شامل تراکنش های متوالی (تعیین طول گروه)
- ❖ انجام تراکنش جدید، ورود این تراکنش به گروه مورد بررسی، خروج قدیمی ترین تراکنش از گروه
- ❖ کشف آنکه تراکنش های جدید، الگویی متفاوت نسب به تراکنش های قدیمی دارند



جمهوری اسلامی ایران



پژوهشکده پولی و بانکی

بانک ملی ایران، تهران، ۱۳۹۷



دفترکسب و کار ملی

سخن آخر

- ❖ بسیاری از انواع تقلب ها به دلیل محدودیت در انتشار اطلاعات، همچنان ناشناخته باقی مانده
 - ❖ بسیاری از روش های کشف تقلب به دلایل امنیتی در دسترس عموم قرار نمی گیرد
 - ❖ به کارگیری هر یک از روش های کشف تقلب
 - ❖ ضمانتی برای کشف تمامی تقلب ها، نیست.
 - ❖ ضمانتی برای حتمی بودن تقلب موارد مشکوک شناسایی شده، نیست.
- یعنی نمی توان انتظار عملکردی بی نقص**
- (کامل بودن نرخ مثبت درست و صفر بودن نرخ منفی اشتباه) داشت.**



جمهوری اسلامی ایران



پژوهشکده پولی و بانکی

بانک ملی ایران، تهران، ۱۳۹۷



دفترکسب و کار ملی



با تشکر

سومین همایش سالانه بانکداری الکترونیک و نظام های پرداخت

۱۶ و ۱۷ دی ماه ۱۳۹۲ - مرکز همایش های برج میلاد

conf.mbri.ac.ir/ebps3

