به نام خدا

بررسی معماری کلان سامانه تشخیص تقلب پایا

دکتر جلال الدین نصیری

گروه هوش تجاری، معاونت عملیات

چکیده

با افزایش سرویس‌های مالی بانک‌ها، جرایم مالی نیز به موازات در حال رشد است. بانک‌ها به صورت میانگین سالانه 5٪ از درآمد خود را به دلیل تقلب‌های مالی از دست می‌دهند.کاهش اعتماد مشتریان از دیگر اثرات مخرب تقلب‌های مالی است که قابل اندازه-گیری نمی‌باشد. بانک مرکزی به عنوان متولی نظام‌های پرداخت ملی مانند پایا (ACH)، ساتنا، چکاوک و... به دنبال کشف متقلبان و کسب اطمینان بیشتر مردم به نظام‌های پرداخت می‌باشد. سامانه پایا با توجه به فراگیر بودن آن در ارتباط با سامانه شاپرک و اهمیت کلیدی آن در پرداخت‌های روزمره و نسبتا کلان، مورد توجه ویژه‌ای قرار گرفته است. بنابراین وجود سیستمی با قابلیت تشخیص و جلوگیری از جرایم مالی در آن ضروری به نظر می رسد.

یکی از چالش‌های اساسی در سامانه‌های تشخیص تقلب، استفاده از روش‌های بدیع در فرایند تقلب می‌باشد. به عبارت دیگر، فرایند انجام تقلب معمولا به صورت پویایی در حال تغییر می‌باشد. در این نوشتار نحوه مقابله با تقلب‌های جدید تبیین می‌گردد . همچنین سامانه تشخیص تقلب پایا معرفی و معماری کلان آن توضیح داده خواهد شد.

1. سیستم های خبره مقابله با تقلب

کشف تقلب به معنای طراحی سیستمی جامع و کامل است که قادر به تحلیل و بررسی رفتارهای کاربران بوده و علاوه بر آن با یادگیری و نظارت مداوم بر عملکرد مشتریان، رفتارهای مشکوک آنها را شناسایی نموده و از بروز آن جلوگیری می‌نماید. معمولا روش‌های مقابله با تقلب به چهار دسته تقسیم می‌شوند، که در ادامه به اختصار توضیح داده شده اند.

الف) استفاده از قوانین ساده[2]: این دسته از روش‌ها از پیچیدگی کمی برخوردار می‌باشند ولی نسبت به تقلب‌های جدید ناکارآمد است. به طور مثال عدم امکان تراکنش بالاتر از 500 میلیون ریال در پایا (بجز موارد خاص) از این دست می‌باشد. از نقاط قوت این دسته از قوانین، سرعت آن می‌باشد.

ب) استفاده از قوانین مبتنی بر پروفایل[3]: هر فردی بر اساس خصوصیات شخصی و اقلیمی رفتاری را در تعاملات مالی از خود بروز می‌دهد. این رفتار می‌تواند شامل مبلغ، تعداد و محدوده جغرافیایی تا نوع سیستم عامل و مرورگر در تراکنش‌های اینترنتی باشد. متقلبان از رفتار نرمال دارندگان حساب‌ها آگاهی ندارند. معمولا در هنگام تقلب رفتار فرد دستخوش تغییرات زیادی می‌شود. این گونه قوانین در مقابل تقلب‌های جدید کارآمد می‌باشند. ولی معمولا مشکل این دسته از قوانین خبره، کمبود اقلام اطلاعاتی مفید می‌باشد.

ج) استفاده از یادگیری ماشین: در این روش‌ها تراکنش‌های نرمال و متقلبانه به سیستم هوشمندی داده شده و سیستم از طریق آموزش با الگوی تراکنش‌های متقلبانه آشنا می‌شوند. این دسته از روش‌ها نسبت به تقلب‌های پیچیده کارآمد بوده ولی یادگیری درست که موارد نرمال را به اشتباه تشخیص ندهد نیاز به دانش فنی ویژه‌ای دارد.

د) استفاده از شبکه‌های مالی: بعضی از تقلب‌ها بوسیله هیچ‌کدام از روش‌های پیشین قابل تشخیص نبوده و فقط بر اساس الگوهای شبکه‌ای که در تعاملات مالی وجود دارد قابل تشخیص می‌باشد. به طور مثال تعاملات حلقه در پولشویی و شبکه‌های هرمی از این موارد می‌باشند.

بنابراین برای اینکه سیستمی بتواند تقلب‌های جدید را نیز شناسایی کند، باید رفتار نرمال برای هر مشتری مدل شده و در صورت بروز هر گونه انحراف از این رفتار به عنوان مشکوک ثبت گردد. رفتارشناسی هر مشتری می تواند با کمک اقلام داده‌ای جغرافیایی، زمانی، مقدار تراکنش مالی و .... با استفاده از الگوریتم‌های آماری،یادگیری ماشین، شبکه‌های اجتماعی و ... انجام پذیرد. سامانه

---

[2] Simple Rules
[3] Profile Based Rules

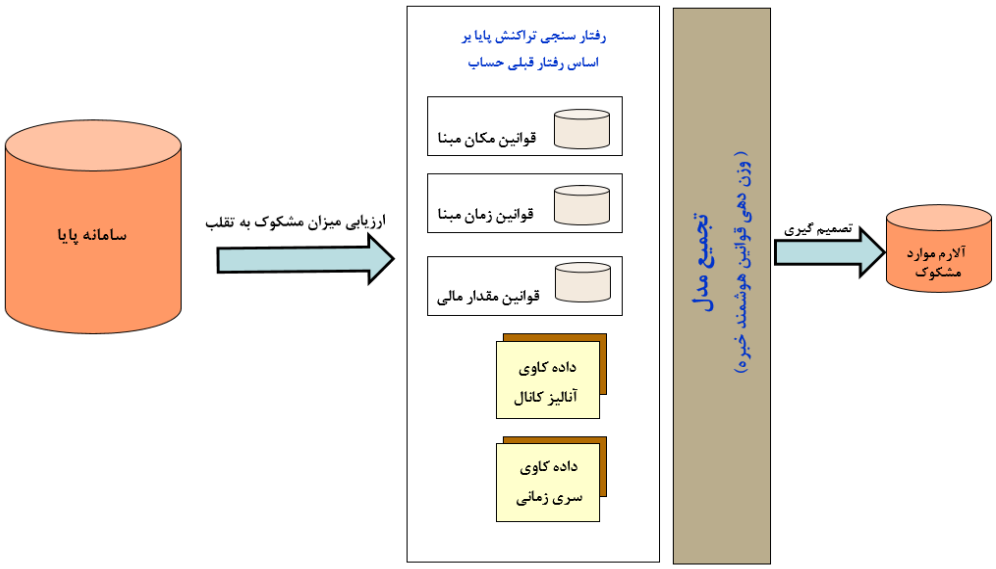
سامانه تشخیص تقلب پایا از روش‌های چهارگانه تشخیص تقلب، سه دسته قوانین ساده، قوانین خبره مبتنی بر پروفایل و استفاده از یادگیری ماشین برای بهبود دقت به کاربرده است.

2. استخراج رفتار چگونه انجام می پذیرد؟

یکی از موثرترین مدل‌های مقابله با تقلب رفتارشناسی هر مشتری می باشد. به عبارت دیگر، رفتار نرمال برای هر مشتری مدل شده و در صورت بروز هر گونه انحراف از این رفتار به عنوان مشکوک ثبت گردد. رفتارشناسی هر مشتری می تواند با کمک اقلام داده‌ای جغرافیایی، زمانی، مقدار تراکنش مالی و .... با استفاده از الگوریتم‌های یادگیری ماشین، داده‌کاوی، شبکه‌های اجتماعی و ... انجام پذیرد. در معماری کنونی سامانه تشخیص تقلب دو نوع رفتار برای هر شبا وجود دارد: الف) رفتار کلی ب) رفتار روزانه.

در رفتار کلی تراکنش‌های 6 ماه هر فرد مورد تجزیه و تحلیل قرار می‌گیرد و به عنوان رفتار نرمال ثبت می‌گردد. همچنین تراکنش‌های چرخه‌ای که در حال بررسی موارد مشکوک آن هستیم، سیستم به صورت خودکار برای هر فرد رفتار آن روز / چرخه را استخراج می‌نماید.

قوانین خبره به دسته‌های قوانین مکان مبنا، قوانین زمان مبنا و قوانین مقدار مالی برای هر مشتری تقسیم می‌شود. در قوانین مکان مبنا از نظر جغرافیایی رفتار قبلی مشتری سنجیده شده و در صورتی که درخواست جدید تغییر شدیدی از جهت جغرافیایی داشته باشد پارامتر مشکوک بودن افزایش پیدا می‌کند. همچنین قوانین زمان مبنا و مقدار مالی نیز در کاهش و افزایش پارامتر مشکوک بودن تاثیرگذارهستند. معماری مفهومی قوانین خبره در سه حوزه مکان مبنا، زمان مبنا و مقدار مالی در شکل 1 آورده



شده است.

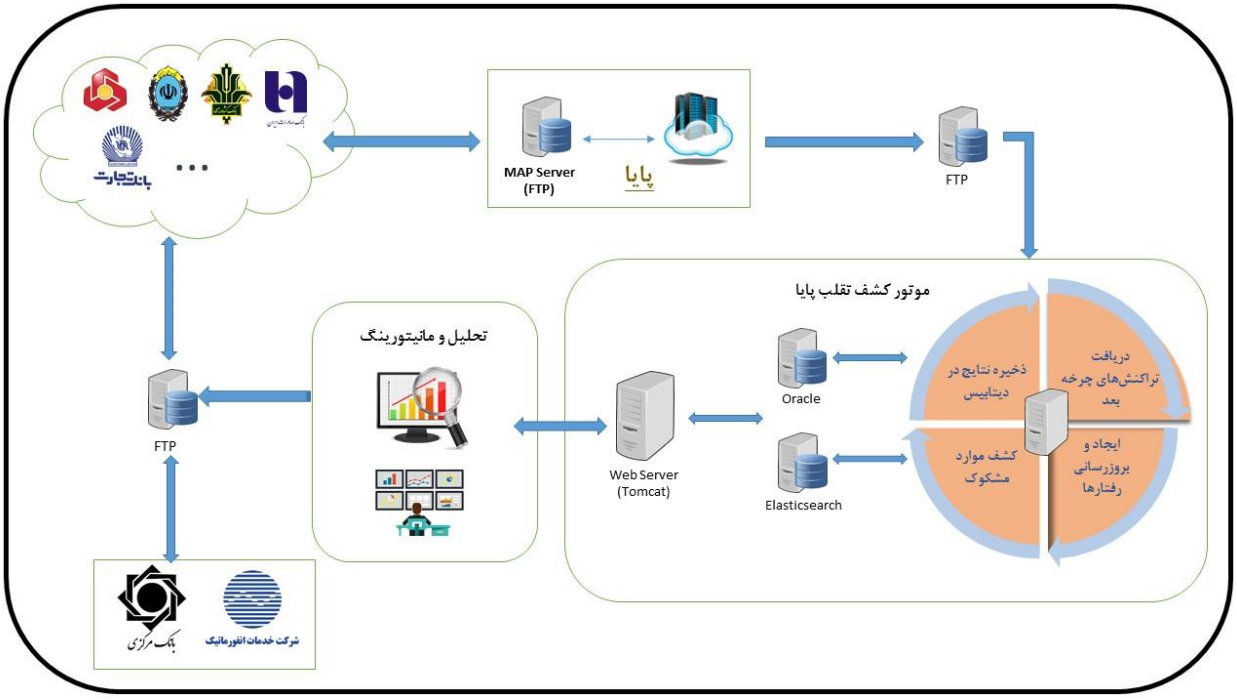
شکل ۱ رفتارسنجی تراکنش پایا

3. معماری سامانه تشخیص تقلب

در این قسمت معماری کلان سامانه تشخیص تقلب به همراه مولفه‌های اصلی تشریح می‌شود. همانطور که گفته شد سامانه آریا پایا یکی از سامانه‌های ملی پرداخت می‌باشد که در پرداخت‌های خرد و متوسط استفاده می‌شود. در شکل 2 نحوه تعامل سامانه تشخیص تقلب با سامانه آریا پایا نشان داده شده است. بعد از درخواست انجام انتقال توسط افراد حقیقی یا حقوقی از طریق کانال‌های متفاوت مانند مراجعه حضوری به شعبه یا با استفاده از اینترنت، سرپرستی شعب درخواست تجمیع شده برای انتقال به مرکز عملیات پایا ارسال می کند. مرکز عملیات درخواست‌ها را از جهت صحت ساختاری و تا حدودی محتوایی بررسی کرده و درصورت گذراندن این مرحله به سامانه تشخیص تقلب ارسال می گردد. کلیه استخراج رفتارها و همچنین قوانین بر بستر کلان داده[۴] انجام شده تا با سرعت مناسبی بدون اختلال در انجام چرخه موارد مشکوک را تشخیص دهد.

4. مولفه‌های سامانه تشخیص تقلب

در این بخش مولفه های مختلف سامانه تشخیص تقلب پایا به همراه کارکردهای هر یک از بخش‌ها توضیح داده می‌شود.



[4] Big Data

شکل ۲ معماری مفهومی سامانه تشخیص تقلب

سرویس اتوماتیک تشخیص تقلب:

تراکنش‌های انجام شده در سامانه پایا پس از اتمام هر سیکل از طریق یک سرور FTP در اختیار سامانه کشف تقلب قرار می‌گیرد. به محض دریافت تراکنش‌های هر سیکل، عملیات ایجاد و بروزرسانی داده‌ها و الگوها آغاز می‌گردد، بلافاصله پس از آن قواعد مربوط به کشف تقلب که شامل موارد گوناگون در حوزه شبا و بانک می‌باشند بر روی تراکنش‌ها اجرا می‌گردد و در صورتی که شماره شبا و یا بانکی یافت شود که طبق قوانین موجود و در مقایسه با رفتارها و الگوهای ایجاد شده از قبل دارای اختلاف معناداری باشد مشکوک تلقی شده و به همراه جزئیات بیشتر درون پایگاه داده ثبت می‌کند. بعضی از کارکردهای سرویس تشخیص تقلب عبارتند از :

- بارگذاری و استخراج اتوماتیک رفتار تراکنش های پایا
- به روز رسانی اتوماتیک رفتار کلی شبا (رفتار شش ماهه)
- اجرای قوانین سرویس تشخیص تقلب با استفاده از پروفایل ساخته شده
- درج موارد مشکوک در پایگاه داده

موتور قوانین خبره تشخیص تقلب:

قوانین پیاده سازی شده در سامانه کشف تقلب به سه بخش کلی زیر تقسیم می شوند:

1- رفتار سنجی تراکنش‌های شبا: این نوع قوانین تراکنش جدید را با رفتار گذشته آنان مقایسه کرده و در صورت وجود اختلاف معنادار آن‌را مشکوک شناسایی می‌کنند.
2- رفتار سنجی کلی تراکنش‌های شبا: در این قسمت مجموعه قوانین پیاده‌سازی شده به بررسی تراکنش‌های غیرنرمال در کل تراکنش‌ها می پردازند.
3- رفتار سنجی تراکنش‌های بانک: بررسی تجمیعی و رفتارسنجی تراکنش‌های بانک با گذشته خود بانک در این بخش مورد نظر می باشد.

سامانه مانیتورینگ تشخیص تقلب:

این سامانه به پایگاه داده موارد مشکوک حال و گذشته دسترسی داشته و برای دسترسی سریع و آسان به موارد ذیل طراحی گردیده است:

- ✓ مشاهده آنلاین موارد مشکوک به تقلب در صورت رخداد.
- ✓ تاریخچه تراکنش‌ها و بانک‌های مشکوک به تقلب به تفکیک تاریخ، شماره سیکل و حتی بانک.
- ✓ توزیع تعدادی و مبلغی تراکنش‌های مشکوک به تفکیک بانک.
- ✓ توزیع درصدی شباها و بانک‌های مشکوک در هر سیکل.
- ✓ جزئیات و نمودارهای مربوط به شباها و بانک‌های مشکوک به تقلب.
- ✓ تحلیل رفتار هر شبا بر مبنای مبلغ تراکنش برداشتی و واریزی، تعداد تراکنش برداشتی و واریزی و تعداد شباهای یکتا برداشتی و واریزی در روزهای متفاوت

ماژول جستجوی ریزتراکنش سریع :

این ماژول با استفاده از بستر پردازش سریع الاستیک سرچ[5]، انواع جستجو در اختیار کاربران سامانه قرار می‌دهد شامل :

- انواع جستجو روی اقلام اطلاعاتی (نام و نام خانوادگی فرستنده و گیرنده، کد ملی فرستنده و گیرنده ، شماره شبا فرستنده و گیرنده و مقدار تراکنش)
- انواع دسته بندی نتایج بر مبنای (نام و نام خانوادگی فرستنده و گیرنده ، کد ملی فرستنده و گیرنده ، شماره شبا فرستنده و گیرنده و مقدار تراکنش، بانک مبدا و بانک مقصد)
- انواع جستجوی هوشمند تقریبی و دقیق
- امکان استفاده از عملگرهای منطقی
- سرعت بالای جستجو با استفاده از تکنیک های کلان داده

ماژول مدیریت کاربران و سطوح دسترسی :

این ماژول امکانات ذیل را در اختیار کاربران و مدیر سیستم قرار می دهد :

- افزودن کاربر
- افزودن نقش
- تغییر رمز ورود
- تخصیص و تغییر سطوح دسترسی

[5] Elastic search