فصل ششم ــ مدیریت ریسک تقلب و احراز هویت مستمر

۶–۱– مقدمه

در بانکداری سنتی، احراز هویت معمولاً در یک نقطه مشخص از رابطه مشتری با بانک انجام می‌شد؛ برای مثال هنگام افتتاح حساب، مراجعه حضوری یا انجام یک عملیات حساس. در این مدل، فرض غالب این بود که اگر هویت فرد در زمان ورود یا انجام عملیات تأیید شود، می‌توان فعالیت بعدی او را نیز به همان هویت منتسب کرد.

اما بانکداری دیجیتال این فرض را با چالش جدی مواجه کرده است. ممکن است هویت مشتری در زمان افتتاح حساب کاملاً صحیح باشد، اما در ادامه، اعتبارنامه او سرقت شود، تلفن همراهش در اختیار شخص دیگری قرار گیرد، اطلاعات ورود او افشا شود یا مهاجم از طریق مهندسی اجتماعی کنترل حساب را به دست آورد.

از این منظر، مسئله اصلی دیگر فقط «چه کسی در ابتدا وارد حساب شد؟ » نیست؛ بلکه باید پرسید «آیا فردی که در هر لحظه از رابطه بانکی در حال استفاده از حساب است، همچنان همان دارنده مجاز هویت و اعتبارنامه است؟ » همین تغییر زاویه دید، مبنای شکل‌گیری مفهوم احراز هویت مستمر است.

بنابراین، احراز هویت باید از یک کنترل نقطه‌ای به فرآیندی تبدیل شود که بتواند سطح اعتماد را در طول چرخه استفاده از خدمت بررسی و در صورت لزوم تعدیل کند.

۶–۲– احراز هویت مستمر چیست؟

احراز هویت مستمر[1] به رویکردی اشاره دارد که در آن اعتماد سامانه به هویت کاربر فقط در لحظه ورود ایجاد نمی‌شود، بلکه در طول استفاده از خدمت نیز به‌صورت پویا ارزیابی می‌شود.

---

[1] . Continuous Authentication

در این مدل، سامانه می‌تواند عواملی مانند:

- دستگاه مورد استفاده؛
- الگوی ورود؛
- زمان فعالیت؛
- رفتار کاربر؛
- نوع تراکنش؛
- مقصد تراکنش؛
- سرعت انجام عملیات؛
- الگوی حرکتی یا تعاملی

را بررسی کند.

نکته مهم این است که احراز هویت مستمر الزاماً به معنای درخواست مکرر رمز عبور یا احراز هویت آشکار از مشتری نیست. بخش مهمی از این فرآیند می‌تواند در پس‌زمینه و بدون ایجاد اصطکاک برای مشتری انجام شود. سامانه با جمع‌آوری و تحلیل سیگنال‌های مختلف، سطح اطمینان خود را نسبت به ادامه مالکیت یا کنترل حساب به‌روز می‌کند. در نتیجه، می‌توان احراز هویت را یک «سطح اعتماد پویا» در نظر گرفت؛ سطحی که با تغییر شواهد می‌تواند افزایش یا کاهش یابد.

۶-۳- تحلیل رفتاری

یکی از مهم‌ترین ابزارهای احراز هویت مستمر، تحلیل رفتار است. رفتار مشتری معمولاً دارای الگوهایی نسبتاً پایدار است و می‌توان بر اساس سابقه، یک خط مبنا یا Baseline ایجاد کرد.

این الگو ممکن است شامل موارد زیر باشد:

- ساعات معمول ورود؛
- نوع تراکنش‌های رایج؛

- مبالغ معمول؛
- دستگاه‌های مورد استفاده؛
- الگوی انتقال وجه؛
- مخاطبان معمول؛
- سرعت انجام عملیات

مزیت خط مبنا این است که سامانه به‌جای تعریف یک رفتار ثابت برای همه مشتریان، رفتار هر مشتری را با سابقه خودش مقایسه می‌کند. این موضوع اهمیت زیادی دارد؛ زیرا رفتاری که برای یک مشتری طبیعی است ممکن است برای مشتری دیگری کاملاً غیرمعمول باشد.

با این حال، خط مبنا نباید به یک قالب خشک تبدیل شود. رفتار مشتریان در طول زمان تغییر می‌کند؛ برای مثال تغییر شغل، سفر، تغییر الگوی درآمد یا استفاده از یک خدمت جدید می‌تواند رفتار طبیعی گذشته را تغییر دهد. بنابراین مدل باید امکان به‌روزرسانی و بازتنظیم داشته باشد.

در ادامه با ذکر یک مثال ساده این موضوع را بررسی می‌کنیم:

فرض کنیم مشتری معمولاً در ساعات روز وارد سامانه می‌شود، از تلفن همراه مشخصی استفاده می‌کند، تراکنش‌های نسبتاً محدود دارد و مبالغ مشخصی را انتقال می‌دهد.

حال ناگهان:

- ورود از دستگاه جدید رخ می‌دهد؛
- رمز عبور تغییر می‌کند؛
- چند دقیقه بعد انتقال مبلغ قابل توجه انجام می‌شود؛
- مقصد انتقال نیز برای مشتری جدید است.

هیچ‌یک از این موارد به‌تنهایی اثبات تقلب نیست.

اهمیت در این مثال از «ترکیب زمانی رخدادها» ناشی می‌شود. وقتی چند رویداد متفاوت در یک بازه کوتاه و به‌صورت متوالی رخ می‌دهند، اطلاعات حاصل از ترکیب آن‌ها می‌تواند از مجموع اهمیت هر رویداد به‌تنهایی بیشتر باشد.

بنابراین، یک نشانه لزوما به معنای خطر بالا نیست.

اما چند نشانه مستقل و هم‌زمان نشانه افزایش قابل توجه سطح ریسک می‌باشد.
این همان جایی است که موتورهای ریسک و تحلیل رفتاری می‌توانند نسبت به کنترل‌های ساده و مستقل، ارزش بیشتری ایجاد کنند.

۶-۴- تصاحب حساب

تصاحب حساب (ATO) [1]، یکی از تهدیدهای مهم بانکداری دیجیتال است. در این وضعیت، هویت اصلی مشتری ممکن است واقعی باشد، اما شخص دیگری تلاش می‌کند کنترل حساب او را در اختیار بگیرد.
روش‌های مختلفی ممکن است برای این کار مورد سوءاستفاده قرار گیرند، مانند:

- سرقت اطلاعات ورود؛
- فیشینگ؛
- مهندسی اجتماعی؛
- سوءاستفاده از نشست کاربر؛
- سرقت یا سوءاستفاده از دستگاه؛
- فریب مشتری.

اهمیت ATO در این است که ممکن است بسیاری از کنترل‌های اولیه را پشت سر بگذارد. برای مثال، اطلاعات ورود ممکن است کاملاً صحیح باشند، زیرا مهاجم آن‌ها را از خود مشتری به دست آورده است. در این شرایط، تفاوت اصلی در رفتار پس از ورود ظاهر می‌شود.
به همین دلیل، سیستم ضدتقلب نباید فقط موفقیت ورود را بررسی کند، بلکه باید بتواند پس از ورود نیز به دنبال نشانه‌هایی مانند تغییر ناگهانی دستگاه، تغییر اطلاعات امنیتی، الگوی جدید تراکنش، انتقال به مقصد جدید یا رفتار غیرمعمول باشد.

[1]. Account Takeover

۶–۵– احراز هویت مبتنی بر ریسک

در احراز هویت مبتنی بر ریسک[1]، سیستم بر اساس میزان ریسک تصمیم می‌گیرد چه سطحی از کنترل لازم است. مفهوم احراز هویت مبتنی بر ریسک بر این اساس توضیح داده شده است که سامانه بتواند متناسب با سطح ریسک، سطح کنترل را تغییر دهد.

یک مدل ساده می‌تواند سه وضعیت داشته باشد:

ریسک پایین: رفتار با سابقه سازگار است و نشانه معناداری وجود ندارد.

ریسک متوسط: یک یا چند نشانه غیرعادی مشاهده شده و کنترل تکمیلی می‌تواند لازم باشد.

ریسک بالا: چند عامل خطرناک هم‌زمان مشاهده شده و امکان توقف یا ارجاع عملیات وجود دارد.

مزیت این رویکرد آن است که همه مشتریان را با یک سطح اصطکاک مواجه نمی‌کند. مشتری کم‌ریسک می‌تواند فرآیند ساده‌تری داشته باشد و منابع کنترلی سازمان به عملیات پرریسک‌تر اختصاص یابد.

البته احراز هویت مبتنی بر ریسک به معنی حذف کنترل برای مشتری کم‌ریسک نیست؛ بلکه به معنای متناسب کردن شدت کنترل با شرایط و سطح ریسک است.

۶–۶– موتور ریسک

موتور ریسک مجموعه‌ای از قواعد و مدل‌های تحلیلی است که اطلاعات مختلف را ترکیب و یک سطح یا امتیاز ریسک تولید می‌کند. بعنوان مثال، ترکیب ریسک هویت، دستگاه، رفتار، تراکنش و سابقه مشتری نمونه‌ای از موتور ریسک است.

می‌توان این رابطه را به‌صورت مفهومی چنین نمایش داد:

ترکیب چند سیگنال مرتبط = ریسک نهایی

اما این یک فرمول ثابت و جهانی نیست؛ نحوه وزن‌دهی و ترکیب متغیرها باید بر اساس محیط عملیاتی، داده‌های موجود و سیاست‌های بانک طراحی شود.

---

[1] . Risk-Based Authentication

امتیاز ریسک در واقع بیانگر سطحی از احتمال یا نگرانی کنترلی است. ارزش آن زمانی افزایش پیدا می‌کند که بانک بداند این امتیاز چگونه ایجاد شده، چه عواملی روی آن اثر گذاشته‌اند و برای هر سطح چه اقدام مشخصی باید انجام شود.

۶-۷- ارتباط انسان و سامانه

در نظام بانکی، سامانه‌های احراز هویت و تشخیص جعل به‌طور فزاینده‌ای بر الگوریتم‌های یادگیری ماشین، تحلیل رفتاری و امتیازدهی ریسک متکی شده‌اند. با این حال، تصمیم نهایی در مورد تأیید یا رد یک تراکنش، مشتری یا سند، در بسیاری از موارد همچنان نیازمند قضاوت انسانی است. تقسیم کار میان سامانه و کارشناس نه یک فرایند خطیِ ساده، بلکه یک حلقه تعاملی پویا است که در آن هر یک از طرفین نقشی مکمل ایفا می‌کنند.

در یک سوی این تعامل، سامانه قرار دارد. سامانه وظیفه دارد الگوهای مشکوک را کشف کند، داده‌های مربوط به هویت، تراکنش یا سند را تحلیل نماید، به هر مورد یک امتیاز ریسک اختصاص دهد و در نهایت موارد را بر اساس سطح خطر اولویت‌بندی کند. خروجی سامانه معمولاً شامل نمره ریسک، دلایل فنیِ پرچم‌گذاری، و مستندات الگوریتمی است که به کارشناس امکان می‌دهد زمینه تصمیم را درک کند. این مرحله را می‌توان به‌صورت زیر خلاصه کرد:

سامانه: کشف ← تحلیل ← امتیازدهی ← اولویت‌بندی

در سوی دیگر، کارشناس انسانی قرار دارد. کارشناس باید خروجی سامانه را بررسی کند، آن را با اطلاعات زمینه‌ای و شرایط واقعی تطبیق دهد، در چارچوب اختیارات تعیین‌شده قضاوت کند و در نهایت تصمیم خود را مستندسازی نماید. این مرحله نیز به شکل زیر قابل نمایش است:

کارشناس: بررسی ← قضاوت ← تصمیم در حدود اختیار ← مستندسازی

این مدل، معنای واقعی Human-in-the-Loop را نشان می‌دهد. حضور انسان زمانی ارزشمند است که بتواند نتیجه سامانه را به‌صورت انتقادی بررسی کند؛ نه اینکه صرفاً خروجی مدل را بدون بررسی تأیید کند. تأییدِ منفعلانه و بدون پرسشِ هشدارهای سامانه، نه‌تنها ارزش افزوده‌ای ایجاد نمی‌کند، بلکه می‌تواند خطاهای سیستمی را بازتولید و تقویت نماید.

انسان می‌تواند عواملی را ببیند که در داده‌های مدل وجود ندارند؛ برای مثال یک توضیح منطقی از طرف مشتری، شرایط خاص عملیات، یک وضعیت استثنایی یا اطلاعات کیفی‌ای که در متغیرهای کمی منعکس نشده است. مدل‌های آماری عمدتاً بر الگوهای تاریخی و داده‌های ساخت‌یافته متکی هستند و ممکن است زمینه‌های انسانی، حقوقی یا عملیاتی خاص را نادیده بگیرند. در چنین مواردی، قضاوت انسانی می‌تواند از بروز خطاهای مثبت کاذب یا منفی کاذب جلوگیری کند.

در مقابل، مدل نیز می‌تواند حجم عظیمی از داده را در زمانی بسیار کوتاه بررسی کند که انجام آن برای انسان دشوار یا غیرعملی است. توانمندی سامانه در پردازش سریع، پوشش گسترده، یکنواختی در اعمال قواعد، و کشف همبستگی‌های پیچیده میان متغیرهاست؛ قابلیت‌هایی که خارج از ظرفیت شناختی و زمانی انسان قرار دارند.

بنابراین، نقطه قوت واقعی در همکاری انسان و سامانه ایجاد می‌شود. این همکاری را می‌توان در قالب مفهوم «هوش افزوده[1]» توصیف کرد: سامانه به‌عنوان یک ابزار تحلیلی قدرتمند عمل می‌کند و انسان به‌عنوان ناظرِ انتقادی و تصمیم‌گیرنده نهایی، آن را هدایت و تکمیل می‌کند. در این حالت، تصمیم نهایی نه صرفاً بر پایه خروجی الگوریتم، بلکه بر اساس تلفیق شواهد الگوریتمی و قضاوت زمینه‌ای انسانی اتخاذ می‌شود.

برای تحقق این همکاری مؤثر، چند شرط ضروری است:

شفافیت خروجی سامانه: کارشناس باید بتواند دلایل پرچم‌گذاری یا امتیاز ریسک را بفهمد. بدون شفافیت، بررسی انتقادی ممکن نیست و کارشناس به سمت تأیید کورکورانه سوق داده می‌شود.

آموزش تفکر انتقادی: کارشناسان باید آموزش ببینند که خروجی مدل را به‌عنوان یک «فرضیه» در نظر بگیرند، نه یک «حکم». آن‌ها باید بتوانند خطاهای بالقوه مدل را تشخیص دهند و در صورت نیاز، آن را به چالش بکشند.

[1] . Augmented Intelligence

مستندسازی تصمیم: ثبت دلایل تصمیم انسانی، به‌ویژه زمانی که با خروجی سامانه مغایرت دارد، برای ممیزی، پاسخگویی و بهبود مستمر مدل ضروری است.
بازخورد دوطرفه: تصمیمات کارشناسان می‌تواند به‌عنوان داده آموزشی برای اصلاح آستانه‌ها، کاهش خطاها و بهبود عملکرد سامانه مورد استفاده قرار گیرد. این بازخورد، حلقه یادگیری را کامل می‌کند و سامانه را با شرایط واقعی

۶-۸- کاهش هشدارهای کاذب

یکی از چالش‌های اساسی در سامانه‌های ضدتقلب بانکی، فراوانیِ هشدارهای اشتباه یا همان هشدارهای کاذب[1] است. در بسیاری از پیاده‌سازی‌های عملیاتی، سامانه حجم بالایی از هشدارها را تولید می‌کند که بخش قابل‌توجهی از آن‌ها پس از بررسی انسانی، بی‌اهمیت یا نادرست تشخیص داده می‌شوند. این پدیده پیامدهای چندلایه‌ای دارد که در متون تخصصی و گزارش‌های میدانی به‌طور مکرر به آن‌ها اشاره شده است:
خستگی کارکنان: کارشناسان مجبورند زمان قابل‌توجهی را صرف بررسی مواردی کنند که در نهایت به تأیید تقلب منجر نمی‌شود. این کارِ تکراری و کم‌بازده، فرسودگی شغلی ایجاد می‌کند و کیفیت تمرکز کارشناس را کاهش می‌دهد.
افزایش زمان رسیدگی: انباشت هشدارهای کاذب، صف بررسی را طولانی می‌کند و زمان پاسخگویی به موارد واقعیِ پرخطر را افزایش می‌دهد. در نتیجه، حتی هشدارهای درست نیز ممکن است با تأخیر بررسی شوند.
نارضایتی مشتریان: هشدارهای کاذب اغلب به مسدودسازی موقت تراکنش، تماس با مشتری یا درخواست مستندات اضافی منجر می‌شوند. اگر این موارد به‌طور مکرر برای مشتریانِ بی‌خطر رخ دهد، تجربه کاربری آسیب می‌بیند و اعتماد به بانک کاهش می‌یابد.

[1] . False Positives

گم شدن هشدارهای واقعی: وقتی حجم هشدارها زیاد باشد، احتمال نادیده گرفتن یا کم‌اهمیت‌شمردن هشدارهای واقعی در میان انبوه موارد کم‌ارزش افزایش می‌یابد. این پدیده به‌عنوان «اثر سوزن در انبار کاه» شناخته می‌شود.

این پدیده را می‌توان «خستگی هشدار[1]» دانست. اگر کارمند هر روز با تعداد زیادی هشدار کم‌ارزش روبه‌رو شود، احتمال دارد به‌مرور حساسیت خود را نسبت به هشدارها از دست بدهد. خستگی هشدار یک خطر عملیاتی جدی است؛ زیرا می‌تواند منجر به تأیید خودکار هشدارها بدون بررسی دقیق، یا برعکس، نادیده گرفتن هشدارهای مهم شود. در هر دو حالت، اثربخشی کل سامانه کاهش می‌یابد.

بنابراین، کیفیت یک سامانه ضدتقلب را نمی‌توان صرفاً با این معیار سنجید که: «چند مورد تقلب کشف شد؟ »

این معیار به‌تنهایی گمراه‌کننده است، زیرا ممکن است سامانه‌ای با تولید انبوه هشدار، تعداد تقلب‌های کشف‌شده را بالا ببرد، اما در عین حال هزینه عملیاتی سنگینی بر سازمان تحمیل کند و تجربه مشتری را تخریب نماید. در ارزیابی عملکرد چنین سامانه‌هایی، باید مجموعه‌ای از شاخص‌های مکمل را در نظر گرفت که تصویری جامع از کیفیت، کارایی و قابلیت استفاده ارائه دهند. از جمله مهم‌ترین این شاخص‌ها می‌توان به موارد زیر اشاره کرد:

نرخ هشدار کاذب) : نسبت هشدارهایی که پس از بررسی، غیرتقلبی تشخیص داده می‌شوند. این شاخص نشان می‌دهد سامانه تا چه حد در تشخیص موارد مشکوکِ واقعی دقیق عمل می‌کند.

زمان متوسط رسیدگی[2]: مدت‌زمانی که از تولید هشدار تا بسته‌شدن پرونده توسط کارشناس صرف می‌شود. افزایش این زمان معمولاً نشانه‌ای از فشار کاری ناشی از هشدارهای زیاد یا کیفیت پایین خروجی سامانه است.

---

[1] . Alert Fatigue
[2] . Mean Time to Resolution

درصد هشدارهای تأییدشده[1]: نسبت هشدارهایی که در نهایت به تأیید تقلب یا اقدام اصلاحی منجر منجر می‌شوند. این شاخص نشان می‌دهد سامانه چقدر توانسته است موارد واقعاً مهم را شناسایی کند.

حجم پرونده‌های ارجاع‌شده[2]: تعداد کل مواردی که برای بررسی انسانی ارجاع می‌شوند. این شاخص باید در تناسب با ظرفیت واقعی تیم بررسی باشد؛ حجم بیش از حد، به‌معنای اتکای بیش از حد به نیروی انسانی و کاهش کارایی سامانه است.

هدف از طراحی سامانه ضدتقلب، تولید بیشترین هشدار نیست؛ هدف، تولید هشدارهایی است که ارزش تصمیم‌گیری داشته باشند. به بیان دیگر، یک سامانه مطلوب باید بتواند میان «حساسیت» (توانایی شناسایی موارد تقلب) و «دقت» (توانایی اجتناب از هشدارهای کاذب) تعادل برقرار کند. این تعادل، همان نقطه بهینه در منحنی مشخصه عملکرد سیستم (ROC) است که با توجه به هزینه‌های نسبی خطاهای نوع اول و دوم برای هر بانک تعیین می‌شود.

۶-۹- احراز هویت نامرئی

در مدل‌های سنتی احراز هویت، مشتری معمولاً در لحظه ورود یا انجام تراکنش، یک اقدام صریح مانند وارد کردن رمز عبور، کد یکبارمصرف یا اثر انگشت انجام می‌دهد. اما یکی از جهت‌گیری‌های آینده در نظام بانکی، حرکت به سمت «احراز هویت نامرئی[3]» یا «احراز هویت پیوسته[4]» است. در این رویکرد، مشتری بدون انجام اقدامات اضافی، به‌صورت مستمر و در پس‌زمینه ارزیابی می‌شود و سطح اطمینان از هویت او به‌طور پویا به‌روزرسانی می‌گردد.

در این مدل، سامانه در پس‌زمینه می‌تواند مجموعه‌ای از عوامل زمینه‌ای و رفتاری را به‌صورت هم‌زمان بررسی کند. از جمله مهم‌ترین این عوامل می‌توان به موارد زیر اشاره کرد:

---

1. True Positive Rate / Confirmed Alert Rate
2. Referral Volume
3. Invisible Authentication
4. Continuous Authentication