



هفتمین همایش سالانه
بانکداری الکترونیک
و نظام‌های پرداخت

تهران، مرکز همایش‌های بین‌المللی برج میلاد - ۲ و ۳ بهمن ۱۳۹۶

7th Annual Conference
on Electronic Banking
and Payment Systems

نوآوری، بازیگران جدید و کارایی در کسب و کار مالی



شناسایی هویت مشتری در پارادایم همه‌کاناله Omnichannel

علی حاجی زاده مقدم، مدیرعامل شرکت آدانیک، Alix@adanic.ir

چکیده

شناسایی هویت مشتریان^۱ همواره یکی از چالش‌های پایه‌ای در ارائه خدمات در صنعت بانکداری بوده است. روش‌های کلاسیک مورد استفاده در شعب فیزیکی هنوز براساس رویت و تطابق کارت شناسایی (چیزی که دارید + کسی که هستید) و تطابق امضای کاغذی (چیزی که می‌دانید + کسی که هستید) و در مواردی نیز با تطابق اثر انگشت (کسی که هستید) کار می‌کند. در کانال‌های دیجیتالی و مدرن، مهم‌ترین روش‌های متداول همچنان استفاده از گذرواژه (چیزی که می‌دانید)، و کارت و توکن فیزیکی (چیزی که دارید) است. در کانال‌های غیرحضور مبتنی بر صدا، بیشتر از روش‌های ورود پین و پرسیدن سوال در خصوص اطلاعات شخصی یا بانکی مشتری (چیزی که می‌دانید) استفاده می‌شود و روشی مانند کنترل کالر آیدی (جایی که هستید) آن را تقویت می‌کند.

در رویکرد همه‌کاناله^۲، تمرکز اصلی و ویژه بر موجودیت مشتری و تجربه‌ی کاربری او از تمامیت کسب و کار است و تلاش می‌شود این تجربه‌ی کاربری، یکنوا و یکپارچه باشد. به کار گرفتن این رویکرد، پیش از هر چیزی نیازمند بازطراحی همه‌ی فرآیندها و خدمات و محصولات سازمان با در مرکز قراردادن مشتری و یکپارچگی تجربه‌ی کاربری او در کانال‌های مختلف است. به عبارت دیگر، در این رویکرد مرز بین کانال‌های مختلف از نگاه مشتری هر چه کم‌رنگ‌تر می‌شود.

برای آغاز به‌کارگیری رویکرد همه‌کاناله، یکی از نخستین و پایه‌ای‌ترین گام‌های فناورانه‌ای که باید برداشته شود، یکپارچه سازی رویکرد سازمان به مفهوم شناسایی مشتری است. این رویکرد باید به گونه‌ای طراحی شود که سطح یکسان و یکنوایی از آسانی، دسترس‌پذیری، امنیت، و اطمینان را برای مشتری و سازمان فراهم نماید. همچنان که نتیجه‌ی شناسایی اشخاص (به عنوان فرد انسان و نه لزوماً مشتری) باید مستقل از وضعیت ارتباط فرد با سازمان (مشتری بالقوه، مشتری حقیقی، مشتری حقوقی، همکار، شریک تجاری و ...) باشد.

در این مقاله ابتدا مفهوم همه‌کاناله به اختصار مورد بررسی قرار می‌گیرد، نقاط اصلی تمایز آن با رویکرد چند کاناله^۳ بررسی می‌شود، و یک معماری مفهومی مستقل از پیاده سازی برای این رویکرد عرضه می‌شود. در ادامه روش‌های متداول مورد استفاده برای شناسایی مشتری در رویکرد چندکاناله و نیز روش‌های جدیدتر مانند روش‌های بیومتریک، روش‌های مبتنی بر رمزنگاری (امضای نامتقارن زنجیره بلوک^۴ و ...)، روش‌های مبتنی بر هوش مصنوعی، و روش‌های مبتنی بر شبکه‌ی اجتماعی

^۱ Know Your Customer = KYC

^۲ Omnichannel

^۳ Multi-channel

^۴ Blockchain



هفتمین همایش سالانه
بانکداری الکترونیک
و نظام های پرداخت

تهران، مرکز همایش های بین المللی برج میلاد - ۲۰ و ۲۱ بهمن ۱۳۹۶

7th Annual Conference
on Electronic Banking
and Payment Systems

نوآوری، بازیگران جدید و کارایی در کسب و کار مالی



معرفی و ارزیابی و مقایسه می شوند. سرانجام در بخش پایانی، روش های معرفی شده در یک نقشه ی راه فناورانه برای تحقق بخشیدن به آرمان همه کاناله ° تجربه ی کاربری یکنوا و یکپارچه ی مشتری- طبقه بندی خواهند شد.

معرفی رویکرد همه کاناله

با پیشرفت فناوری و پیدایش کانال های ارتباطی جدید با مشتری، فرآیند ارایه سرویس در کسب و کارهای گوناگون دچار پیچیدگی و چالش های تازه ای شده است. بانک ها و موسسات مالی نیز با توجه به گستردگی و تنوع مشتریان و سرویس ها، به شکل روز افزونی با این چالش ها رو برو می شوند.

روزگاری شعب فیزیکی و ارتباط پستی و تلفنی، راه های اصلی ارتباط بانک ها با مشتریان بود. دستگاه های خودپرداز برای نخستین بار، کانالی دیجیتالی و سلف سرویس در مسیر ارتباطی بین مشتری و بانک گشودند. پس از آن با گسترش شبکه اینترنت، کانال دیجیتالی سلف سرویس قدم به دوره شکوفایی و گسترش گذاشت و با همه گیر شدن شبکه موبایل (و بخصوص گوشی های هوشمند)، بدل به کانال اصلی مورد انتظار مشتریان برای دریافت خدمات گشت.

افزایش کانال های ارتباطی بین بانک و مشتریان و بخصوص گسترش کانال های دیجیتالی سلف سرویس، از یک سو هزینه های گسترش شبکه ی ارتباطی بین بانک و مشتری (مانند اجاره و تجهیز شعب و استخدام کارکنان شعبه) را کاهش داد و از سوی دیگر، ظرفیت عرضه ی خدمات و نوآوری های روزافزون به مشتریان را فراهم نمود. ولی در عین حال، گسترش این کانال ها باعث افزایش پیچیدگی فرآیندها و خدمات بانکی نیز شده است. این پیچیدگی و تنوع هم انتخاب کانال مناسب برای دریافت خدمت توسط مشتری را دشوار می کند و هم کارکنانی که در معرض تماس مستقیم با مشتریان هستند (مانند کارکنان شعبه و مرکز تماس) دشواری بیشتری در معرفی و پیشنهاد کانال مناسب برای دریافت هر خدمت به مشتری دارند.

برخلاف رویکرد چندکاناله که در آن تمرکز طراحی بر محصول است، در رویکرد همه کاناله تمرکز اصلی بر موجودیت مشتری و تجربه ی کاربری او از تمامیت کسب و کار است و تلاش می شود این تجربه ی کاربری، یکنوا و یکپارچه باشد. به این منظور نیاز است همه ی فرآیندها و خدمات و محصولات سازمان با در مرکز قراردادن مشتری و یکپارچگی تجربه ی کاربری او در کانال- های مختلف بازبینی و بازطراحی شوند. هدف این است که نخست مرز بین کانال های مختلف از نگاه مشتری هرچه کم رنگ تر می شود و دوم، کسب و کار بتواند به مشتری نگاهی فراتر از کانال های مورد استفاده ی وی بیاندازد و شناختی همه جانبه از او بیابد. این موضوع از برخی جهات شبیه انتقال از مدل خدمات توزیع شده در شعب در بانکداری سنتی به مدل بانکداری مبتنی بر هسته ی متمرکز بانکی است. همانطور که در تحول قبلی، مشتریان یک شعبه تبدیل به مشتریان همه ی شعب شدند که اطلاعاتشان همه جا قابل دستیابی بود، در این تحول مشتریان یک کانال تبدیل به مشتریان همه ی کانال ها خواهند شد.

برای حرکت از مدل فعلی به مدل تغییر یافته، دشواری ها و چالش های زیربنایی وجود خواهد داشت، از جمله:

- حرکت دادن سیستم های سنتی و سیلو بندی شده ی فعلی به سمت یکنوایی
- باز طراحی همه ی فرآیندها در همه ی کانال ها برای تطابق با دو اصل یکنوایی و تمرکز بر مشتری
- ایجاد زیرساخت فناورانه مورد نیاز برای تعامل و کاربرد هر دو سوی فرآیند خدمت رسانی (مشتریان ° کارکنان)



هفتمین همایش سالانه
بانکداری الکترونیک
و نظام‌های پرداخت

تهران، مرکز همایش‌های بین‌المللی برج میلاد - ۲۰ و ۲۱ بهمن ۱۳۹۶

7th Annual Conference
on Electronic Banking
and Payment Systems

نوآوری، بازیگران جدید و کارایی در کسب و کار مالی



معماری مفهومی زیرساخت فناوری همه‌کاناله

برای حرکت در مسیر رسیدن به رویکرد همه‌کاناله، علاوه بر لزوم بازبینی و بازطراحی فرآیندهای کاری بانک با قرار گرفتن مشتری در مرکز آنها، نیاز به فراهم کردن زیرساختی فنی و فناورانه است که بتواند فرآیندهای جدید را به درستی پشتیبانی کند. مهمترین اجزای این معماری چنین است:

- **انباره‌ی داده‌ای یکپارچه با مرکزیت مشتری:** اساسی‌ترین زیرساخت مورد نیاز برای تامین تجربه‌ی کاربری یکنوا بین کانال‌ها از دید مشتری این است که در همه‌ی کانال‌ها (از جمله کانال‌های فیزیکی و سنتی چون شعبه و مرکز تماس) دسترسی برابر و یکسانی به داده‌های مشتری در همه‌ی تعاملات او با بانک در دسترس باشد. وقتی از تعاملات مشتری با بانک صحبت می‌کنیم، اشاره‌ی ما به چیزی بیش از تراکنش‌های مستقیم مالی مشتری (تراکنش‌های سپرده‌ها، تسهیلات، تضامین، خرید و ...) است. بخش بزرگتر و عموماً مغفول داده‌های تعاملی مشتری مربوط به مواردی است که در حالت سنتی یا ثبت نمی‌شوند و یا به طور شایسته مورد توجه قرار نمی‌گیرند. ورود مشتری به شعبه، مدت انتظار مشتری در شعبه، بازدید از یکی از صفحات وب سایت، تماس تلفنی یا ارسال ایمیل برای یکی از واحدهای بانک، بروز خطا در یکی از نرم‌افزارهای بانکی مشتری، مشاهده‌ی مانده‌ی کارت روی خودپرداز نمونه‌هایی از این گونه داده‌ها هستند. با در نظر گرفتن حجم بسیار بیشتر این داده‌ها، نیاز به زیرساختی برای تحلیل و داده‌کاوی میان داده‌های بزرگ و بهره‌مند از هوش مصنوعی بسیار کلیدی است.

یکی دیگر از تفاوت‌های اساسی رویکرد همه‌کاناله در برابر رویکرد چندکاناله، تعریف حوزه‌ی بررسی و کسب اطلاعات است. از یک سو نگاه به مشتری با رویکرد سنتی متفاوت است و هر مشتری بالقوه (از جمله مشتریان دیگر بانک‌ها) موضوع شناخت و تحلیل سازمان است و از سوی دیگر، کانال‌ها نیز محدود به کانال‌های خود بانک نیستند و رفتار مشتری در تعامل با سایر بانک‌ها و موسسات مالی نیز با اهمیت تلقی می‌شود.

- **رویکرد یکپارچه و یکنوا در شناسایی و احراز هویت مشتریان:** از جمله مهمترین چالش‌ها در رویکرد همه-کاناله، انتخاب روش‌هایی برای شناسایی و احراز هویت مشتریان^۵ است، به شکلی که سطح یکسان و یکنوایی از آسانی، دسترس‌پذیری، امنیت، و اطمینان در همه‌ی کانال‌ها را برای مشتری و سازمان فراهم نماید. همچنان که باید روش شناسایی اشخاص بتواند مستقل از وضعیت ارتباط فرد با سازمان (مشتری بالقوه، مشتری حقیقی، مشتری حقوقی، همکار، شریک تجاری و ...) عمل کند. در طراحی مکانیزم شناسایی و احراز هویت باید این نکته را هم در نظر داشت که ارتباط مشتری با بانک محدود به نشست‌های^۶ کوتاه در نظر گرفته نشود. بلکه این نشست باید تا حد امکان در همه‌ی کانال‌ها طولانی و ادامه‌دار باشد و تا زمان تغییر ابزار و استفاده از یک ابزار جدید، نشست باز شده قبلی باز بماند.

- **لایه‌ی تجربه‌ی کاربری یکپارچه و یکنوا:** یکی دیگر از جنبه‌های مهم در رویکرد همه‌کاناله، فراهم کردن تجربه‌ی کاربری یکنوا و یکپارچه در همه‌ی کانال‌های فیزیکی و الکترونیکی است. لایه‌ی تجربه‌ی کاربری باید در کانال‌های

^۵ Identification and Authentication

^۶ Session



هفتمین همایش سالانه
بانکداری الکترونیک
و نظام‌های پرداخت

تهران، مرکز همایش‌های بین‌المللی برج میلاد - ۲۰ و ۲۱ بهمن ۱۳۹۶

7th Annual Conference
on Electronic Banking
and Payment Systems

نوآوری، بازیگران جدید و کارایی در کسب و کار مالی



گوناگون چنان باشد که کاربر با آموختن شیوه‌ی کار یکی، بتواند با دیگری کار کند و درک و شناخت او از برند در همه‌ی این کانال‌ها یکسان باشد. همچنان که باید فرآیندها به گونه‌ای مدیریت شوند که کاربر بتواند کاری را که در یک کانال آغاز کرده، در کانال دیگر ادامه دهد. تحقیقات نشان می‌دهد جابجایی بین ابزارها برای تکمیل یک کار بین کاربران به یک عادت روزانه تبدیل شده است. الگوی غالب چنین است که مشتریان فعلیتی را در ابزارهای موبایل همراه خود آغاز می‌کنند و پس از طی کردن مراحل مقدماتی، به کانال‌های دیگر (وب سایت، شعب فیزیکی، خودپرداز و ...) با امکانات بیشتر منتقل می‌شوند.

بخش مهم دیگر که شکل دهنده‌ی تجربه‌ی کاربر است، لایه دسترسی کارکنان داخلی بانک است. ابزار مورد استفاده در این لایه نیز باید همخوانی و ارتباط ارگانیک با لایه دسترسی بیرونی مشتری داشته باشد، به شکلی که بتوان در شعب و مراکز تماس، فرآیند آغاز شده توسط مشتری را به شکل مناسب تکمیل و راهنمایی کرد.

- **لایه تجمیع سرویس:** معماری سرویس‌گرا که از سال‌ها پیش به استاندارد در راهبرد بلوغ و تکامل فناوری در سازمان‌های بزرگ تبدیل شده بود، در رویکرد همه‌کاناله اهمیت و نقشی دوچندان می‌یابد. داشتن یک رویکرد باز در طراحی و ارائه API بانکی، چابکی و سرعت در ساخت و بهبود لایه‌ی تجربه‌ی کاربری را به شکل چشم‌گیری افزایش می‌دهد. لایه‌ی تجمیع سرویس همچنین کمک می‌کند فرآیندهای خدمت رسانی به مشتری در کانال‌های مختلف بتوانند یکپارچگی و تداوم تجربه‌ی کاربری را از طریق دسترسی به داده‌ها و سرویس‌های مشترک فراهم کنند. مشخصات و ویژگی‌های کلیدی که در طراحی این لایه برای رسیدن به هماهنگی فراکانالی^۷ مورد نیاز است عبارتند از:

- بهره بردن از معماری میکرو سرویس برای کاهش چسبندگی بین سرویس‌ها، افزایش چابکی در توسعه‌ی این لایه، از بین بردن سیلوهای نرم‌افزاری و ایجاد امکان تشکیل تیم‌های توسعه‌ی فرا-وظیفه‌ای^۸
- بهره بردن از موتور کنترل قواعد تجاری^۹ فرا-کاناله برای اعمال قواعد و قوانین یکپارچه.
- بهره بردن از موتور کنترل فرآیند فرا-کاناله برای حفظ یکپارچگی و تداوم فرآیندهای آغاز شده در یک کانال در کانال‌های دیگر

شکل زیر اجزای اصلی معماری سامانه‌های پشتیبانی کننده‌ی رویکرد همه‌کاناله را در ارتباط با یکدیگر نشان می‌دهد.

Cross-channel orchestration^۷

Cross-functional^۸

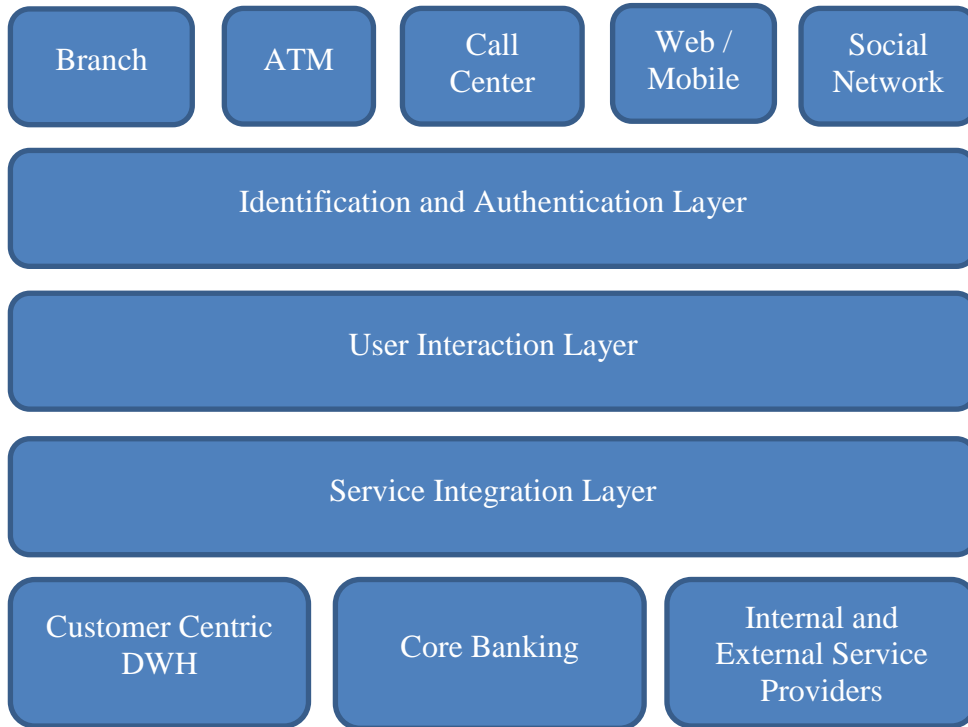
Business Rule Engine^۹



هفتمین همایش سالانه
بانکداری الکترونیک
و نظام های پرداخت

تهران، مرکز همایش های بین المللی برج میلاد - ۲۰ و ۳۰ بهمن ۱۳۹۶
7th Annual Conference
on Electronic Banking
and Payment Systems

نوآوری، بازیگران جدید و کارایی در کسب و کار مالی



شناسایی و احراز هویت مشتریان

همانطور که اشاره شد، یکی از اجزای پایه ای در استقرار موفق رویکرد همه کاناله، شناسایی و احراز هویت مشتری به شکلی یکنوا، آسان و قابل اتکاست. فرآیند احراز هویت به طور کلاسیک با شناسایی مشتری (ابراز و ادعای داشتن هویتی خاص توسط کاربر، همچون اعلام یک نام یا نام کاربری یا کد ملی) شروع می شود و پس از آن با ارایه مدارک و شواهدی^۱، این ادعا تایید می شود. این شواهد می تواند مواردی از قبیل کلمه عبور، کارت شناسایی، بلیط، گواهیمامه و ... باشد. شواهد احراز هویت عموماً در یکی از دسته های زیر قرار می گیرند:

- چیزی که می دانید: روش کلاسیک احراز هویت مبتنی بر پرسیدن رمزی از پیش توافق شده از کاربر است. این رمز می تواند عبارتی صرفاً بی معنی و قراردادی (مثل امضای فیزیکی، یا کلمه عبور)، یا بخشی از اطلاعات و دانسته های کاربر (همچون اطلاعات شخصی وی) باشد.
- چیزی که دارید: روش های مبتنی بر دانستن همواره در معرض خطر افشا هستند. برای محافظت در برابر این خط، توصیه می شود عامل دیگری (در کنار یا به جای عامل نخست) برای احراز هویت استفاده شود. استفاده از چیزی که در اختیار کاربر است و به راحتی قابل جعل یا کپی شدن یا سرقت نیست (و یا حداقل در صورت سرقت، کاربر به

^۱ Credentials



هفتمین همایش سالانه
بانکداری الکترونیک
و نظام‌های پرداخت

تهران، مرکز همایش‌های بین‌المللی برج میلاد - ۲۰ و ۲۱ بهمن ۱۳۹۶

7th Annual Conference
on Electronic Banking
and Payment Systems

نوآوری، بازیگران جدید و کارایی در کسب و کار مالی



سرعت و راحتی مطلع می‌شود) یکی از پر کاربردترین این عوامل است. نمونه‌هایی از این ابزارها عبارتند از: توکن‌های تولید رمز، کلیدهای فیزیکی، کارت بانکی، کارت شناسایی، بلیط و ...

- کسی که هستید: قوی‌ترین روش شناسایی و احراز هویت کاربر، استفاده از ویژگیهای بیومتریک انسانی است. مواردی چون اثرانگشت، اسکن عنبیه، تشخیص صدا، تشخیص چهره، تشخیص دستخط و ... در این دسته قرار می‌گیرند. مزیت مهم این روش‌ها، دشواری جعل و تکرار و قابلیت اطمینان و انکارناپذیری بالاتر آن است. از سوی دیگر با این دسته از روش‌ها می‌توان شناسایی و احراز هویت را همزمان و با سادگی بیشتر (و حتی بدون نیاز به شروع فعالیت توسط کاربر) انجام داد. به عنوان مثال، ممکن است بانک بخواهد کاربر را در لحظه ورود به شعبه شناسایی کند و بلافاصله براساس سوابق وی، رویکرد متفاوتی در خوش‌آمد و خدمت به وی اتخاذ نماید.

علاوه بر سه دسته‌ی اصلی و کلاسیک بالا، شواهد تکمیلی بیشتری نیز می‌توانند برای احراز هویت بکار روند، یا به عنوان عامل دوم به عوامل اصلی افزوده شوند. مواردی همچون:

- جایی که هستید: استفاده از آدرس فیزیکی، آدرس آی‌پی، کالرایدی تلفن و ... در کنار عوامل دیگر به مدیریت ریسک تراکنش‌ها کمک می‌کند و می‌تواند به عنوان ابزار شناسایی استفاده شود.
- کسانی که شما را می‌شناسند: با گسترش شبکه‌های اجتماعی، نقش کاربر در شبکه به عنوان شاهدی بر هویت وی روز به روز اهمیتی پر رنگ‌تر پیدا می‌کند.

در بیشتر موارد، نیاز است شناسایی و احراز هویت بین بانک و کاربر جنبه‌ی دوطرفه‌ای نیز داشته باشد. به این معنی که کاربر هم نیاز دارد اطمینان یابد با طرف قابل اطمینانی در بانک تعامل می‌کند. در شعب فیزیکی و سنتی، از آنجا که کاربر به محل فیزیکی مورد تایید بانک مراجعه می‌کند، فرض او بر این است که کاربر پشت باجه دارای صلاحیت لازم برای تعامل است (عامل جایی که هستید). در فرآیندهای برخط، امروزه نقش اصلی و پر رنگ بر عهده گواهینامه‌های امنیتی همچون **SSL Certificate** است (چیزی که دارید). با گسترش شبکه‌های اجتماعی و افزوده شدن جنبه‌ی تعاملی بین بانک و مشتری، نیاز به بازبینی و نوآوری در این مسیر هم بیش از پیش خواهد بود.

روش‌های اصلی شناسایی و احراز هویت

برای شناسایی و احراز هویت مشتری در کانال‌های فیزیکی و دیجیتالی موجود، عموماً در بانک‌ها از روش‌های زیر استفاده می‌شود:

- **تطابق کارت شناسایی:** اصلی‌ترین روش شناسایی (و احراز هویت) در کانال‌های فیزیکی هنوز رویت کارت شناسایی (و بررسی اصالت آن با کنترل پارامترهای فیزیکی و/یا کنترل برخط با سامانه ثبت احوال) و تطابق تصویر روی آن با چهره شخص است. این روش با استفاده از دو عامل کسی که هستید و چیزی که دارید، علاوه بر شناسایی، سطح امنیت قابل قبولی برای احراز هویت کاربر در بسیاری از خدمات بانکی فراهم می‌کند. به عنوان مثال ارایه برخی اطلاعات می‌تواند تنها با تایید در همین سطح انجام شود. هرچند این روش از جنبه انکارناپذیری ضعیف است.



هفتمین همایش سالانه
بانکداری الکترونیک
و نظام‌های پرداخت

تهران، مرکز همایش‌های بین‌المللی برج میلاد - ۲۰ و ۲۱ بهمن ۱۳۹۶

7th Annual Conference
on Electronic Banking
and Payment Systems

نواوری، بازیگران جدید و کارایی در کسب و کار مالی



- **امضا:** برای تامین انکارناپذیری بیشتر در کانال‌های فیزیکی، از امضا برای احراز هویت (در کنار شناسایی برپایه‌ی روش نخست) استفاده می‌شود. امضا به عنوان الگویی منحصر به فرد که توسط مشتری در ابتدا به بانک اعلام شده، در تعاملات بعدی نقش عامل چیزی که می‌دانید را ایفا می‌کند. در عین حال (بخصوص زمانی که به شکل حضوری عمل امضا انجام شود)، می‌تواند مانند عامل کسی که هستید هم کار کند. هرچند امضای فیزیکی به عنوان عاملی قوی همچنان می‌تواند انکارناپذیری را به شکل مناسبی تامین کند، در تامین و اثبات یکپارچگی سند امضا شده ضعیف است.
- **کلید یا کارت فیزیکی:** در برخی از خدمات بانکی (مانند صندوق امانات) از کلید فیزیکی (چیزی که دارید) برای احراز هویت مشتری استفاده می‌شود. در کلید در واقع رمزی به شکل ساختاری فیزیکی بین کلید و قفل مشترک است. در بسیاری از خدمات بانکی، داشتن کارت بانکی فیزیکی (که برخی اطلاعات روی آن به شکل مغناطیسی ذخیره شده) به عنوان ابزاری برای شناسایی مشتری (و نه احراز هویت) مورد قبول است. پس از شناسایی با کارت، برای احراز هویت عموماً از روش بعدی که استفاده از پین است استفاده می‌شود.
- **کلمه عبور یا پین:** به طور کلاسیک و سنتی، سامانه‌های دیجیتالی از ترکیب شناسایی کاربری و کلمه‌ی عبور برای شناسایی و احراز هویت استفاده می‌شود. مزیت این روش در سادگی و در دسترس بودن آن است. ولی با افزایش روزافزون تعداد کلمات عبوری که یک فرد در زندگی روزمره نیاز به استفاده از آنها دارد، دشواری به خاطر سپردن یا مدیریت کلمات عبور متعدد و حفظ قوت و تازگی همه‌ی آنها در حد مطلوب برای بسیاری از کاربران قابل توجه است. از سوی دیگر با گسترش روش‌های شنود روی خط یا ابزارهای ضبط کلیدهای فشرده شده توسط کاربر و ابزارهای استخراج خودکار کلمه عبور براساس کلمات دیکشنری و ترکیبات پرکاربرد و ...، امنیت این روش روز به روز در معرض خطرهای بیشتری است و انکارناپذیری تراکنش‌هایی که بر این مبنا تایید شده‌اند بسیار ضعیف و در بسیاری دعاوی حقوقی بانک‌ها غیر کارآمد است.
- **رمز یکبار مصرف و توکن:** برای کاهش مشکلات امنیتی رمز عبور و افزایش امنیت، در کاربردهای حساس استفاده از رمزیکبار مصرف توصیه می‌شود. در این روش هر رمز عبور تنها یکبار قابل پذیرش و استفاده است. در نتیجه ریسک‌های ناشی از کلمات عبور (انتخاب کلمات عبور ساده، شنود کلمه‌ی عبور روی ابزار کاربر یا در مسیر) کاهش می‌یابد. ساده‌ترین روش استفاده از رمز یکبار مصرف، تولید و اشتراک لیستی فیزیکی از کلمات عبور با کاربر است که براساس الگوریتم مورد توافق، هر بار یکی از این کلمات عبور استفاده و از لیست حذف می‌شود. روش‌های جدیدتر بر استفاده از توکن‌هایی استوار هستند که با روش‌های مختلف ریاضی، دنباله یکسانی از کلمات عبور را تولید می‌کنند. این روش در زمره‌ی عوامل چیزی که دارید قرار می‌گیرد.
- در کنار روش‌های کلاسیک فوق، ابزارهای نوین و مبتنی بر فناوری به عنوان روش‌های جایگزین یا مکمل بیش از پیش مورد توجه و استفاده قرار می‌گیرند.
- **روش‌های بیومتریک:** در این روش‌ها از عواملی چون حسگرهای اثرانگشت و اسکنرهای عنبیه و ... استفاده می‌شود. شواهد بیومتریک ممکن است تنها برای احراز هویت استفاده شوند^{۱۱}، یا همزمان برای شناسایی و احراز هویت به کار روند^{۱۲}. در حالت دوم، هنگامی که اسکن عامل بیومتریک انجام شد، باید نتایج با دیتابیس قبلی مقایسه شود

Verification ^{۱۱}

Recognition ^{۱۲}



و بهترین نتیجه نزدیک به آن شناسایی گردد. در این حالت علاوه بر صرف زمان بیشتر، نرخ خطا در نتیجه به هر دو شکل نرخ پذیرش اشتباه^{۱۳} و نرخ رد اشتباه^{۱۴} افزایش می‌یابد. به طور کلی دو دسته‌ی اصلی از روش‌های بیومتریک در شناسایی و احراز هویت مورد استفاده قرار می‌گیرند:

○ **روش‌های ایستا (برمبنای الگو):** در این روش شواهد مورد استناد بر الگوهایی ایستا از ویژگی‌های بیومتریک همچون اثر انگشت بنا شده‌اند. شواهد عموماً به صورت تصاویری برداری در دیتابیس ذخیره می‌شوند و در هنگام تطابق، براساس تعداد نقاط هم‌پوشانی بین تصویر ذخیره شده و تصویر دریافت شده، دقت نتیجه تعیین می‌گردد.

○ **روش‌های پویا (برمبنای رفتار):** در این روش الگوهای رفتاری مشتری تحلیل می‌شوند و براساس آن هویت وی تایید می‌شود. مواردی چون تشخیص گفتار، تشخیص دست‌خط یا شیوه‌ی امضا، تشخیص سرعت و شیوه‌ی تایپ یک عبارت همچون کلمه عبور یا نام شخص، شیوه‌ی راه رفتن و ... از این خانواده هستند. روش‌های پویا بیش از پیش بر استفاده از الگوریتم‌های هوش مصنوعی و یادگیری ماشین تکیه می‌کنند و با پیشرفت فناوری و افزایش دقت و کاهش هزینه در این عرصه، استفاده از آنها رو به افزایش است. در عین حال به دلیل کمترین میزان دخالت و مشارکت کاربر، بیشترین سادگی و پذیرش را نیز در بین کاربران ایجاد می‌کنند.

- **روش‌های مبتنی بر رمزنگاری:** در این دسته از روش‌ها، از الگوریتم‌های رمزنگاری برای اطمینان از هویت کاربر استفاده می‌شود. مزیت مهم این دسته از روش‌ها در توانایی تایید اصالت و یکپارچگی کل پیام (همزمان با شناسایی و احراز هویت کاربر) و ویژگی عدم انکار قوی‌تر آنهاست. از سوی دیگر این دسته از روش‌های احراز هویت، قابلیت استفاده در ابزارهای خودکار متصل به اینترنت اشیا را نیز به خوبی فراهم می‌کنند. مهمترین روش‌های مورد استفاده در این خانواده عبارتند از:

○ **امضای دیجیتال:** در این روش با استفاده از مکانیزم رمزنگاری نامتقارن، یک زوج کلید مرتبط تولید می‌شود. بخش‌های حساس پیام یا فشرده‌ای از آن با این کلید (که از ابتدا توسط کاربر تولید شده و صرفاً و به شکل فیزیکی در اختیار کاربر است) رمزنگاری می‌شوند. در سوی دیگر بانک با استفاده از کلید عمومی مرتبط که قبلاً به شکل امن از کاربر دریافت کرده (یا با از طریق زیرساخت کلید عمومی^{۱۵} از صحت آن اطمینان یافته) هویت کاربر و صحت و یکپارچگی و اصالت پیام وی را بررسی می‌کند.

○ **زنجیره‌ی بلوک:** زیرساخت توزیع شده و عمومی مورد استفاده در ارزهای دیجیتالی مانند بیت‌کوین و اتریوم، این امکان را فراهم می‌کنند که بتوان یک کاربر را شناسایی و احراز هویت کرد. پایه امنیت این روش بر روش رمزنگاری نامتقارن مورد استفاده در انجام یک تراکنش (موسوم به الگوریتم امضای دیجیتال منحنی بیضوی^{۱۶}) استوار است. در این روش‌های احراز هویت، کاربر برای احراز هویت تراکنشی را با کلید خصوصی خود امضا می‌کند. این تراکنش در زنجیره بلوک‌ها تایید و ذخیره می‌شود و سامانه‌ی احراز هویت کننده با بررسی زنجیره بلوک و مشاهده‌ی تراکنش امضا شده، هویت وی را تایید می‌کند. محصولات

FAR^{۱۳}

FRR^{۱۴}

PKI^{۱۵}

ECDSA^{۱۶}



هفتمین همایش سالانه
بانکداری الکترونیک
و نظام‌های پرداخت

تهران، مرکز همایش‌های بین‌المللی برج میلاد - ۲۰۲۰ بهمن ۱۳۹۶

7th Annual Conference
on Electronic Banking
and Payment Systems

نوآوری، بازیگران جدید و کارایی در کسب و کار مالی



متنوعی برپایه این روش توسعه یافته‌اند که از جمله آنها می‌توان به **Shoadge, remme, Civic** اشاره کرد.

- **روش‌های مبتنی بر شبکه‌ی اجتماعی:** با توجه به گسترش و همه‌گیری شبکه‌های اجتماعی، می‌توان از ظرفیت و اعتماد متقابل میان افراد در این شبکه برای مقاصدی چون اعتبار سنجی یا احراز هویت کاربران استفاده کرد. در این روش، ادعای یک کاربر ناشناخته برای تعدادی از کاربران شناخته شده در شبکه‌ی اجتماعی وب ارسال می‌شود و با تایید اکثریت این درخواست‌ها، درخواست اصلی نیز معتبر تلقی خواهد شد. این روش بخصوص زمانی کارآمد و مفید است که موضوع احراز هویت یک کاربر برای بار نخست در میان باشد. استفاده از اعتماد و تایید متقابل کاربران شناخته شده‌ی دیگر برای تایید هویت کاربر جدید، می‌تواند نقش عامل مکمل را ایفا کند و اعتماد کافی برای برخی از انواع تعاملات با کاربر را ایجاد کند. این مکانیزم روندی مشابه استشهاد محلی در برخی دعاوی، یا امضای تضامنی اسناد توسط ضامنین داشته باشد.

شناسایی و احراز هویت کاربر در رویکرد همه‌کاناله

همانطور که در بخش نخست اشاره شد، یکی از اجزای محوری مورد استفاده در رویکرد همه‌کاناله، شناسایی و احراز هویت مشتری به شکل یکنوا و همسان در همه‌ی کانال‌های ارتباطی است. روش‌های مورد استفاده باید دارای این ویژگی‌ها باشند:

- کاربری آسان و تجربه‌ی کاربری مناسب
- تامین نیازهای پایه امنیتی چون انکار ناپذیری، یکپارچگی، محرمانگی، و دسترس پذیری
- تامین درجات مختلف اطمینان برای کاربردهای گوناگون دارای ریسک‌های مختلف
- قابلیت استفاده در کانال‌های دیجیتالی و فیزیکی
- شناسایی و احراز هویت افراد مستقل از نقش
- قابلیت استفاده در ابزارها و تجهیزات متصل به اینترنت اشیا^{۱۷}

روش‌های کلاسیک و سنتی مورد استفاده در برقراری تعادل بین امنیت و راحتی استفاده دچار مشکل‌اند. از یک سو کلمات عبور با حملات و ریسک‌های روزافزون، قابلیت اطمینان خود را از دست داده‌اند و از سوی دیگر، با افزایش تعداد کلمات عبور مورد نیاز یک فرد حتی در تعامل با یک بانک، حفظ و نگهداری و استفاده از آنها به چالشی برای کاربران تبدیل شده است. مکانیزم‌های تولید رمزیکبار مصرف کلاسیک مانند توکن‌های فیزیکی، به رغم اینکه در زمینه‌ی تامین یکپارچگی موفق عمل کرده‌اند، در زمینه‌ی انکار ناپذیری دچار ضعف هستند و از تجربه‌ی کاربری ضعیفی رنج می‌برند.

جدول زیر روش‌های مختلف احراز هویت در کانال‌های مختلف را به شکل خلاصه مقایسه می‌کند.



هفتمین همایش سالانه
بانکداری الکترونیک
و نظام های پرداخت

تهران، مرکز همایش های بین المللی برج میلاد - ۲۰ و ۲۱ بهمن ۱۳۹۶

7th Annual Conference
on Electronic Banking
and Payment Systems

نوآوری، بازیگران جدید و کارایی در کسب و کار مالی



مکانیزم	نقاط قوت	نقاط ضعف	نوع کانال قابل استفاده	قابلیت توسعه
کارت شناسایی و امضای کاغذی	سادگی استفاده پذیرش گسترده امکان تعامل با غیرمشتریان	گسترده‌گی جعل	شعبه	امکان ترکیب با روش بیومتریک پویا برای بالا بردن ضریب دقت
کارت بانکی و پین	سادگی استفاده پذیرش گسترده زیرساخت چند بانکی برای تعامل با مشتریان دیگر بانکها	امنیت پایین دشواری تعدد کارت محدودیت های امنیتی و رگولاتوری در توسعه	همه کانال های فیزیکی و الکترونیکی	افزایش امنیت در ترکیب با رمزیکبار مصرف
نام کاربری و کلمه عبور	سادگی استفاده پذیرش گسترده	دشواری مدیریت رمزهای متعدد ضعف در برابر افشا قابلیت انکار	همه کانال های فیزیکی و الکترونیکی	استفاده به عنوان روش ابتدایی در کاربردهای کم ریسک و در ترکیب با رمز یکبار مصرف و امضای دیجیتال و بیومتریک پویا
رمز یکبار مصرف	امنیت مناسب	دشواری همراه داشتن توکن قابلیت انکار	همه کانال های فیزیکی و الکترونیکی	با همه گیر شدن گوشی های هوشمند، دشواری همراه داشتن توکن برطرف می شود.
روش های بیومتریک	سادگی استفاده و کمترین دشواری برای کاربر	هزینه تجهیز پذیرش فعلی کم	همه کانال های فیزیکی و الکترونیکی	با بلوغ و بهبود عملکرد الگوریتم ها و ارزان شدن تجهیزات پذیرش افزایش می یابد.
بر پایه رمزنگاری	امنیت بسیار بالا	دشواری تبادل و نگهداری کلید	کانال های الکترونیکی	با همه گیر شدن گوشی های هوشمند، دشواری تبادل و نگهداری کلید برطرف می شود و قابلیت استفاده در کانال های فیزیکی نیز فراهم می گردد.
بر پایه شبکه اجتماعی	امکان تعامل با غیر مشتریان قابلیت پذیرش گسترده	قابلیت اتکای پایین	کانال های الکترونیکی	برای کاربردهای با ریسک پایین و غیر مشتریان دارای مزیت است

روش های احراز هویت بیومتریک با افزایش دقت الگوریتم های مورد استفاده از یک سو ارزان شدن تجهیزات مورد نیاز برای اسکن و پردازش مشخصات بیومتریک از سوی دیگر، نقشی پر رنگ در چشم انداز پیش رو ایفا می کنند.



با توجه به نیازهای پایه‌ای مورد نیاز در رویکرد همه‌کاناله و وضعیت جاری روش‌های شناسایی و احراز هویت مشتری، به نظر می‌رسد ترکیب عوامل بیومتریک، روش‌های مبتنی بر رمزنگاری، و روش‌های مبتنی بر شبکه‌ی اجتماعی با ابزار موبایل می‌تواند پوششی کافی برای شناسایی و احراز هویت کاربران را فراهم کند. در عین حال در انتخاب مکانیزم شناسایی و احراز هویت در کانال‌های مختلف، همواره باید پارامتر پذیرش و آشنایی عمومی و راحتی استفاده را در نظر داشت.

با سطح بندی ریسک تعامل در کانال به ازای هر کانال و به ازای هر خدمت عرضه شده در کانال، می‌توان روش‌های مختلف احراز هویت را بر مبنای سادگی استفاده و میزان امنیت به کار گرفت. همچنین استفاده از الگوریتم‌های تشخیص ناهنجاری می‌تواند نقش مهمی در انتخاب روش مناسب برای احراز هویت داشته باشند و روش‌های پیچیده‌تر و پرهزینه‌تر زمانی به کاربر پیشنهاد شود که ریسک متناظر با ارایه سرویس در کانال از سطح مشخصی عبور کند. به عنوان مثال، استفاده از کارت بانکی و پین همچنان می‌تواند در شعب و در کانال‌های دیجیتالی و سلف سرویس به عنوان روشی فرابانکی و در کاربردهای بسیاری مورد توجه و استفاده باشد.

با همه‌گیر شدن استفاده از گوشی‌های تلفن همراه به عنوان ابزار در اختیار مشتری، نقش این ابزار برای جایگزینی با انواع توکن و کلید و کارت فیزیکی مورد استفاده در روش‌های کلاسیک روزه روز افزایش می‌یابد. این امر در کنار ویژگی‌های امنیتی و توانایی‌های پردازشی این گوشی‌ها، امکان ترکیب عوامل گوناگون در کنار هم برای رسیدن به بالاترین میزان امنیت و راحتی کاربر را ممکن می‌سازد: کاربرد همزمان پین یا الگو، عوامل بیومتریک چون اثر انگشت یا اسکن عنبیه یا چهره یا صدا، رمزنگاری، و سنسورها و روش‌های تعامل.

منابع

- Banking Technology. (2013). Omnichannel: the new normal for retail banks.
- CloudTags. (2017). What is Omnichannel?
- Cresitello-Dittmar, B. (2016). Application of the Blockchain For Authentication and Verification of Identity.
- Efma. (2015). *Omni-channel banking, The digital transformation roadmap*.
- Google. (2012). The New Multi-Screen World Study.
- SITA. (2016). Travel Identity of The Future.
- Taylor & Francis Group, L. (2007). *User Identification and Authentication Concepts*. infosectoday.com.