هویت در دنیای دیجیتال

فصلی جدید در قراردادهای اجتماعی

هویت ما ارزشمند است، هر برنامه مبتنی بر هویت دیجیتالی باید از لحاظ اعتماد، کنترل و حسابرسی معنی‌دار باشد. علیرغم این‌که توافق در این اصول مهم دشوار است، اما پیاده‌سازی آن‌ها به دلیل تلاقی فاکتورهای سیاسی، اقتصادی، تکنولوژیکی، فرهنگی، حقوقی و اجتماعی بس دشوارتر نیز خواهد بود.

آماندا لانگ، مدیر کل، اینترنشنال کنسیومرز (Consumers International)

هر انسانی منحصربه‌فرد است. فاکتورهای بسیاری وجود دارد که ما و سلامت ما را تعریف می‌کند، از ژن ما و نحوه مدیریت بهداشت و سلامت خودمان گرفته تا محیط و بستر اجتماعی که هر یک از ما در آن زاده شده و پرورش یافته‌ایم. بر همین اساس، ایجاد یک زیرساخت اطلاعاتی امن که در بستر آن هویت دیجیتال هر یک از ما شکل بگیرد حیاتی است. زیرساختی که زمینه تحقیق برای دسترسی به روش‌های درمانی و دارویی نوین را فراهم ساخته، مسیرهای مراقبتی را بهبود بخشیده و دسترسی به خدمات درمانی با کیفیت را ممکن سازد.

جرون تاس، مدیر ارشد نوآوری و استراتژی، رویال فیلیپس (Royal Philips)

هویت‌های دیجیتال، در صورتی که به خوبی طراحی شده باشند، می‌توانند منجر به تحول‌پذیری در تمام جوانب زندگی شوند. برای کشاورزان خرد که سرمایه‌های ناچیز خود را برای غلبه بر انزوای جغرافیایی، اقتصادی و اجتماعی و هم‌چنین تقسیم‌بندی‌های ناعادلانه که ریشه اصلی فقر در جهان هستند نگه داشته‌اند، این می‌تواند یک راهکار فوق‌العاده باشد. این راهکار می‌تواند در مقیاسی عظیم انجام شود.

اسماعیل سانگا، مدیر ارشد اجرایی، کنفدراسیون اتحادیه‌های کشاورزی آفریقای جنوبی (South African Confederation of Agricultural Unions)

در نهایت باید به این نتیجه برسیم که هیچ راه‌حل فناورانه‌ای برای مشکلات پیچیده اجتماعی - اقتصادی وجود ندارد. باید متوقف شویم و دلایل این‌که هویت به مانعی جدی و بزرگ تبدیل شده است را درک کنیم. باید به جای توسل به سیستم‌های هویتی پیچیده، موانع غیرضروری را از سر راه برداریم. ما باید در قبال اراده‌های سیاسی و مالی قدرتمندی که در صدد استفاده از سیستم‌های هویتی برای کارایی و اهداف خود به جای تامین رفاه حال افراد هستند ایستادگی کنیم.

گاس حسین، مدیر ارشد اجرایی، پرایویسی اینترنشنال (Privacy International)

همه ما می‌خواهیم در دنیای دیجیتال پیشرفت کنیم و هیچ‌کس نباید از این قافله عقب بماند. این، بدان معنی است که همه باید آموزش داده شوند تا بدانند که چگونه باید از خود محافظت کنند و داده‌های آنلاین خود را ایمن نگه دارند و این، دقیقا همان چیزی است که ما در بارکلیز به شدت در مورد آن مشتاقیم. اما این امر، از طرفی نیز به معنای کسب اطمینان از دسترسی جهانی به هویت دیجیتال ایمن، امن و آسان برای استفاده است، به طوری که در سایه آن، هرکسی قادر باشد در کمال اطمینان قفل‌های مزایای اقتصاد دیجیتال را بگشاید.

جس استیلی، مدیر ارشد اجرایی گروه بارکلیز، بارکلیز (Barclays)

هویت دیجیتال، نیرویی قدرتمند برای هر دو تجربه مثبت و منفی انسانی است. برای پیاده‌سازی یک سیستم مبتنی بر هویت دیجیتال، که بتواند در دراز مدت مثبت و پایدار عمل کند، ما باید راهکارهای مشتری مداری را توسعه دهیم که ایمنی، کنترل و مزایای کاربران را ارتقا دهد.

میشل بیکر، رئیس هیات مدیره، بنیاد موزیلا و شرکت موزیلا (Mozilla Foundation and Mozilla Corporation)

ما در آستانه مدل جدیدی از هویت دیجیتال قرار داریم که افراد را به فراتر از سازمان‌ها، اشیا، دستگاه‌ها و اماکن بسط می‌دهد. این مدل، شالوده‌ای است که به هویت‌های ما این امکان را می‌دهد تا با سیستم‌های آنلاین در تعامل باشند، دستگاه‌های متصل ما را کنترل کنند، یادگیری هوش‌های اکتسابی ما را ارتقا دهند و از منابع زمینی حفاظت کنند. دستیابی به این حق برای رشد آینده ما حیاتی است، مهار مسئولیت‌پذیرانه نوآوری‌های فناورانه را در بر می‌گیرد و زندگی دیجیتال بهتر و مسئولیت‌پذیرتری را فراهم می‌سازد.

پاول داتری، مدیر کل فناوری و نوآوری، اکسنچر (Accenture)

فهرست

پیشگفتار ٤
خلاصه اجرایی ٥
چطور از این گزارش استفاده کنیم ٧
فصل اول: موردی در خصوص هویت دیجیتال خوب ٨
هویت، شکل‌دهی قراردادهای اجتماعی ٩
هویت‌های دیجیتال در زندگی روزمره ما ٩
رشد پیچیدگی و مسئولیت‌پذیری ١١
آینده‌ای واگرا ١٢
پنج پارامتریک هویت خوب ١٢
سیستم‌های هویتی امروز: سه طرح

فصل دوم: منظور از خوب چیست؟ ١٧
بهبود هویت دیجیتال ١٨
١) متناسب با هدف ١٩
٢) همه‌جانبه ٢٠
٣) سودمندی ٢١
۴) ارائه حق انتخاب ٢٢
۵) ایمن ٢٣

فصل سوم: پیش به سوی آینده: روندها، فرصت‌ها و چالش‌ها ٢٥
چه اتفاقی می‌افتد؟ ٢٦
روندها ٢٦
چالش‌ها ٢٦
فرصت‌ها ٢٧

فصل چهارم: اولویت‌هایی برای مشارکت بخش خصوصی و دولت ٢٨
پیوست ١: ملاحظات طراحی برای دست‌اندرکاران ٣٠

پیشگفتار

درک او هالوران
رئیس، جامعه و اقتصاد دیجیتال آینده (Future of Digital Economy and Society)، عضو کمیته اجرایی، مجمع جهانی اقتصاد (World Economic Forum)

همان‌طور که اغلب افراد، دستگاه‌ها و اطلاعات شخصی به سمت آنلاین بودن می‌روند، تمرکز روی عنصر اصلی این محیط دیجیتال جدید یعنی هویت‌های ما نیز بیشتر می‌شود. توانایی درک، تعریف و اثبات این‌که ما چه هستیم، که هستیم و چه می‌خواهیم، این امکان را در اختیار ما قرار خواهد داد تا از فرصت‌های پیش آمده نهایت استفاده را برده و با ایجاد اعتماد میان یکدیگر، تعاملات‌مان در اقتصاد و در حالت کلی دنیای دیجیتال مدرن را مدیریت کنیم.

در سراسر جهان، تعداد روزافزون سازمان‌ها اعم از بخش‌های دولتی و خصوصی، در حال طراحی و توسعه سیستم‌هایی هستند که هویت دیجیتال منحصر به‌فرد و مدرنی را در اختیار کاربران، دستگاه‌ها و سایر نهادها قرار دهند. این جامعه، در طیف گسترده‌ای در حال توسعه است و بسیار فراتر از معنا و مفهوم سنتی هویت در حال پیش‌روی است. جامعه‌ای که متشکل از بازیگران قدرقدرتی است که روی ریسک‌ها و مزایای هویت دیجیتال کاوش می‌کنند تا بتوانند این نوآوری خارق‌العاده را وارد عرصه‌های مختلفی همچون بهداشت و درمان، خدمات مالی، فعالیت‌های بشردوستانه و امثال آن کنند.

با این حال، ما هنوز هم در مفهوم «هویت در دنیای دیجیتال» گیر کرده‌ایم. ما هنوز هم در گیرودار نحوه گردآوری، پردازش و استفاده از داده‌های مرتبط با هویت هستیم که می‌توانند افراد را بدون پایمال کردن حقوق آن‌ها، سلب آزادی‌شان یا آسیب رساندن به آن‌ها، تقویت کنند. زمینه بسیار مساعدی برای بهره‌مندی و ارتقای داده‌های هویتی آنلاین وجود دارد و این‌که افراد، در این بستر ایمن، به معنای واقعی کلمه در کمال کنترل امکان رشد پیدا کنند.

در نشست سالانه مجمع جهانی اقتصاد سال ۲۰۱۸ میلادی، که در داووس برگذار شد، تیم‌های مختلفی از سهام‌داران خصوصی و دولتی گرد هم آمدند تا روی مشارکت با یکدیگر و کار روی محصولات و خدمات کاربر محور مبتنی بر هویت دیجیتال همفکری و همکاری کنند. از آن تاریخ به بعد، حجم دست‌اندرکارانی که به این مبحث مهم روی آورده‌اند کم نبوده است. تیم‌هایی متشکل از متخصصین صنعت، سیاست‌گذاران، مدیران کسب‌وکارها، مشاغل و اصناف، مدافعان حقوق بشر و جامعه مدنی، که همگی به دنبال دنیایی مدرن با محوریت هویت دیجیتال هستند.

در این گزارش سعی شده نکته نظرات و بینش جمعی این دست‌اندرکاران در مجموعه‌ای جامع، کامل و مختصر گرد هم آمده و به صورت مرجعی قابل استفاده در اختیار تصمیم گیرندگان و علاقه‌مندان به مبحث هویت دیجیتال قرار گیرد. این گزارش و مفاهیمی که در آن مطرح شده است، می‌تواند در همین نقطه‌ای که اکنون در آن قرار گرفته‌ایم جاری شده و بسیاری از شکاف‌هایی که در هماهنگی بین ذینفعان و بخش‌های مختلف وجود دارد را پر کند. این مقاله، تمام آن‌چه که تاکنون آموخته‌اید را مورد پرسش قرار می‌دهد و دانسته‌های شما در مورد کاربر محوری را خطاب قرار می‌دهد. این‌که مشتری‌مداری و کاربر محوری به چه معنا است و چطور می‌توان آن را در مقیاس عملی تحقق بخشید؟ در حقیقت، این تلاش را می‌توان دستورالعملی برای همگان دانست که فهرستی جامع از اولویت‌ها و اقدامات فوری موردنیاز برای مشارکت و تعامل را ارائه می‌دهد. در یک کلام، این مقاله، بازتاب دهنده اولین مرحله از یادگیری جمعی و تعریف راه‌ها و اهداف مشترک است. در همین نقطه‌ای که در آن قرار گرفته‌ایم، نیاز مبرم به همفکری، همکاری و تلاش برای تعریف و پیاده‌سازی هویت دیجیتال وجود دارد. در غیر این صورت، با خطرات جبران‌ناپذیری از تقسیم‌بندی‌های دیجیتال مواجه خواهیم شد. همان طور که نیازهای کاربران و شهروندان، آن‌گونه که از انقلاب چهارم دیجیتال انتظار می‌رود برآورده نخواهد شد.

امید است که این گزارش بتواند به‌عنوان دستورالعملی کاربردی، مرجع این مشارکت و همکاری جهانی قرار گیرد.

خلاصه اجرایی

هویت دیجیتال ما، به معنای واقعی کلمه، خود ما است؛ یعنی همان چیزی که هستیم. از طرفی، همان‌طور که فناوری‌ها روزبه‌روز در حال پیشرفت و توسعه هستند و نسل چهارم انقلاب دیجیتال در حال اتفاق افتادن است، هویت ما نیز به سوی دیجیتال شدن می‌رود. این هویت دیجیتال، تعیین می‌کند که چه محصولات، خدمات و اطلاعاتی را می‌توانیم در اختیار داشته باشیم یا برعکس، چه مسیرها و تسهیلاتی به رویمان بسته است.

با روند فزاینده تحولات دیجیتال عصر جدید و انفجار خدمات دیجیتال، میلیاردها عنصر تاثیرگذار در روند زندگی ما نیز رو به دیجیتالی شدن و اتصال به دنیای دیجیتال و مدرن گذاشته‌اند و در این میان، این هویت ما است که خود را در بحبوحه مدرنیته گم کرده و نمی‌داند چطور باید شرایط را کنترل و تعاملات خود با دنیای بیرون را مدیریت کند. به عبارت دیگر، فقدان هویت دیجیتال در این دنیای مدرن و دیجیتال، مساوی است با ممنوعیت بسیاری از مزایا، نوآوری‌ها، تسهیلات و خدمات. در یک کلام، ممنوعیت از زندگی دیجیتال. نتیجه این ممنوعیت، چالشی است که قراردادهای اجتماعی در نحوه مدیریت تعاملات بین افراد و سازمان‌ها در دنیای دیجیتال با آن مواجه شده‌اند.

در صورتی که امروز در عمل شکست بخوریم، در آینده‌ای نه چندان دور با سیستم هویتی روبه‌رو خواهیم شد که به تقسیم‌بندی‌های عمیقی در جامعه خواهد انجامید. تقسیم‌بندی جامعه به دو دسته افراد دارای هویت دیجیتال و افراد فاقد آن، که به تعبیری روشن‌تر، مساوی است با آینده‌ای که در آن، بخش عمده‌ای از افراد فاقد حق انتخاب، اعتماد و حقوق بشری خود در دنیای آنلاین بی‌کران هستند که کسی نظیر آن را تاکنون ندیده است.

اما اگر در همین زمان و در همین نقطه، عاقلانه عمل کنیم، هویت دیجیتال قادر خواهد بود تا آینده را برای میلیاردها انسانی که روی این کره خاکی زندگی می‌کنند به شکلی دیگر رقم بزند. تحولی شگرف، که میلیاردها انسان از سراسر جهان را قادر به دسترسی به اقتصاد نوین، فرصت‌های سیاسی و اجتماعی و مزایای دیگر می‌کند و این امکان را به آن‌ها می‌دهد تا از ایمنی دیجیتال، حریم خصوصی و حقوق بشری بهره‌مند شوند.

در این گزارش، برخی از ایده‌های تحقق این آینده آرمانی به تصویر کشیده شده و سرآغاز آن نیز تحولاتی است که افراد را در مرکزیت ارزش قرار می‌دهد.

نیاز به درک مشترک و اقدام هماهنگ

هویت‌های دیجیتال تکامل یافته‌اند. آن‌ها دیگر شامل قطعات منزوی و ساده‌ای از اطلاعات مربوط به افراد نیستند بلکه شبکه‌های پیچیده، مبتنی بر اینترنت و تلفیقی از داده‌های شخصی، تاریخ دیجیتال و الگوریتم‌ها و رابط‌هایی هستند که می‌توانند سبک زندگی افراد را متحول کنند. هویت‌های دیجیتال ما، به شکل معجزه‌آسایی در تمام فرایندهای زندگی‌مان و تمام فعالیت‌های روزمره‌ای که به سادگی تمام از کنارشان رد می‌شویم، تعبیه شده‌اند.

هویت‌های دیجیتال قابل بازبینی برای کسب‌وکارها، دولت‌ها و افراد ارزش آفرینی می‌کنند. با این حال، فقدان اصول، استانداردها، هماهنگی‌ها و نقاط اشتراک بین ذینفعان مختلف هنوز هم در این تلاش‌ها و جریان‌های به راه افتاده مشاهده می‌شود که اندکی توسعه هویت دیجیتال را کند کرده است.

پنج پارامتر ارزش کاربری

در نشست سالانه مجمع جهانی اقتصاد سال ۲۰۱۸ در داووس، گروهی از ذینفعان اعم از دولت‌ها، کسب‌وکارها و جوامع مدنی، گرد هم آمده و متعهد شدند تا در کنار هم و با مشارکت یکدیگر، یک آینده آرمانی برای هویت‌های دیجیتال رقم بزنند. از آن زمان تاکنون جمع کثیری به این جریان پیوسته‌اند و مجموعه‌ای پنج‌گانه از عناصر تاثیرگذار و لازم برای آینده مبتنی بر هویت دیجیتال را شناسایی کرده و ارائه داده‌اند. تمام این پنج عنصر به یک اندازه حائز اهمیت هستند و برخی از آن‌ها، دارای تنش‌هایی با عناصر دیگر نیز هستند که نمی‌توان آن را نادیده گرفت. به‌عنوان مثال، ویژگی‌هایی که برای بهبود سطح امنیتی هویت‌های دیجیتال طراحی و ارائه می‌شوند ممکن است سطح راحتی آن‌ها را دچار چالش کرده و بر پیچیدگی‌های آن‌ها بیافزایند. هویت‌های دیجیتال کاربر محور، که به ایجاد ارزش واقعی برای افراد می‌انجامند و در نهایت منجر به پذیرش می‌شوند، بایستی در کلیه جوانب موفق ظاهر شوند.

۱. تناسب با هدف. هویت‌های دیجیتال خوب، راه‌حل قابل اطمینانی در دسترس اشخاص قرار می‌دهند تا بتوانند اعتماد لازم را ایجاد کنند، تا حقوق و آزادی‌های خود را اعمال کنند یا شایستگی خود برای استفاده از خدمات و محصولات دیجیتال را ثابت کنند.

۲. مشمولیت. هویت همه‌جانبه و مشمول، کلیه کسانی که دارای هویت دیجیتال هستند یا دست کم بدان احساس نیاز می‌کنند را از تبعیض‌ها و تقسیم‌بندی‌های مبتنی بر داده‌های هویتی می‌رهاند. در سایه این عنصر، کاربران بدون دست و پنجه نرم کردن با فرایندهای احراز هویت پیچیده‌ای که امکان دارد آن‌ها را از برخی خدمات و تسهیلات محروم کنند، وارد تعامل با سازمان‌ها و همدیگر می‌شوند.

۳. سودمندی. هویت‌های دیجیتال سودمند، دسترسی کاربران به طیف گسترده‌ای از خدمات، محصولات و تعاملات سودمند را تضمین می‌کنند و در توسعه و استفاده دارای سهولت هستند.

۴. ارائه حق انتخاب. افراد زمانی که بدانند چه سیستم‌هایی، توانایی استفاده و بهره‌برداری از داده‌های شخصی و عمومی آن‌ها را دارند، حق انتخاب خواهند داشت. ضمن این‌که در سایه این حق انتخاب، کاربران این امکان را خواهند داشت تا خودشان انتخاب کنند که چه داده‌هایی را با چه شرکت‌ها و سازمان‌هایی و تا چه مدت زمانی به اشتراک بگذارند.

۵. ایمن. امنیت می‌تواند شامل حفاظت از افراد، سازمان‌ها، دستگاه‌ها و زیرساخت‌ها از سرقت‌های هویتی، به اشتراک‌گذاری غیرمجاز داده‌ها و نقض حقوق بشر باشد.

در حال حاضر، سه نمونه اولیه از سیستم‌های هویتی در جهان وجود دارند. در سنتی‌ترین و معمول‌ترین حالت شاهد نمونه‌ها و سیستم‌های «متمرکز» هستیم که در آن، سازمان‌ها، عموما دولت‌ها یا شرکت‌ها، هویت کاربران را مدیریت کرده و اطلاعات مبتنی بر هویت کاربران را به شیوه خود در سطح سیستم ایجاد و کنترل می‌کنند. این در حالی است که در مدل‌های دوم که تحت عنوان سیستم‌های «فدرالی» فعالیت می‌کنند، این نقش میان سازمان‌های مختلف توزیع شده است. سیستم‌هایی که جدیدترین مدل یعنی مدل «غیرمتمرکز» را دنبال می‌کنند، عمدتا در فاز آزمایشی قرار دارند و بر این اساس طراحی شده‌اند تا به افراد، قدرت عمل و کنترل بیشتری برای مدیریت داده‌های هویتی‌شان بدهند.

اولویت‌های همکاری

دولت‌ها، بخش خصوصی و جوامع مدنی شرکت کننده در نشست مجمع جهانی اقتصاد، در حالت کلی شش اولویت برای مشارکت و همکاری در راستای تحقق چشم‌انداز هویت دیجیتال معرفی کرده‌اند که عبارتند از:

- انتقال اهمیت و تمرکز از صرف هویت به هویت‌هایی که به ارزش آفرینی برای کاربر می‌انجامند.
- تعریف معیارها و مسئولیت‌پذیری برای ارائه هویتی خوب
- ایجاد مدل‌های جدید حکومتی برای اکوسیستم‌های مبتنی بر هویت دیجیتال
- ارتقای نظارت بر هویت خوب
- تشویق به مشارکت و تعامل‌پذیری در صورت لزوم
- نوآوری مبتنی بر فناوری و مدل‌های مدرن و ساخت کتابخانه‌ای از برنامه‌های آزمایشی موفق

مجمع جهانی اقتصاد، به عنوان یک سازمان بین‌المللی فعال در حیطه مشارکت‌های خصوصی و دولتی، پلتفرمی در اختیار علاقه‌مندان به این قبیل راه‌اندازی‌ها و تلاش‌ها قرار می‌دهد که می‌تواند در عمل، هویت‌هایی به معنای واقعی کلمه «خوب» را به ارمغان بیاورد و برای افراد، ارزش آفرینی کند.

چطور از این گزارش استفاده کنیم

فصل اول اهمیت هویت‌های دیجیتال را شـــرح می‌دهد. این‌که چرا ممکن اســـت فناوری‌های دیجیتال، نابرابری‌های اجتماعی و اقتصادی را افزایش دهند و یا در صورت مدیریت درست سبب برابری شوند و رفاه پایدار و مشترک را گسترش دهند. هم‌چنین، مروری کلی بر سیستم‌های هویت مبتنی بر هویت دیجیتال کنونی و در حال ظهور ارائه می‌دهد.

فصل دوم به بررسی چیستی یک سیستم مبتنی بر هویت دیجیتال خوب می‌پردازد که می‌تواند پنج عنصر کلیدی ایجاد ارزش برای اشخاص را تامین کند. ضمن این‌که در این فصل، نحوه دستیابی به این پنج عنصر نیز مورد بررسی قرار گرفته و کاربرد هریک در قالب مثالی واقعی تشریح شده است.

فصل سوم روندها، فرصت‌ها و چالش‌های پیش روی طراحان، سیاست‌گذاران و سایر دست‌اندکاران و ذینفعان را مورد ارزیابی قرار می‌دهد تا در نهایت، یک سیستم مبتنی بر هویت دیجیتال خوب طراحی و پیاده‌سازی شود.

فصل چهارم شـــش پیش‌زمینه و اولویت موردنیاز برای همکاری و مشـــارکت کوتاه مدت و متوسط مدت میان اعضا و ذینفعان مجمع جهانی اقتصاد را مورد بررسی قرار می‌دهد.

پیوست به ارائه برخی ملاحظات طراحی برای توسعه دهندگان و متخصصان برای طراحی یک سیستم هویت دیجیتال خوب می‌پردازد.

یادداشت: بدیهی است که این مقاله، مجموعه‌ای جامع از گفت‌وگوها و نشست‌های اعضای مجمع جهانی اقتصاد در خصوص هویت دیجیتال نیست و نمی‌تواند باشد و بررســـی کلیه جوانب عنوان شده در این نشست‌ها از حوصله چنین مقاله‌ای خارج است. این مبحث، بیشتر روی نیازهای دیجیتال عوامل انسانی متمرکز شده است. بسیاری از عناوین از قبیل سیستم‌های دسترسی مستعار و ناشناس به صورت عمیق در این مقاله مورد پوشش قرار نمی‌گیرند. به سایر مباحث مرتبط اعم از نمایندگی دستگاه‌ها، هویت‌های قانونی و هوش مصنوعی نیز به صورت سطحی پرداخته می‌شود اما بررسی دقیق و عمیق‌تر آن‌ها مستلزم زمان و فرصت بیشتری است چراکه چنین مفاهیم مهم و گسترده‌ای، مستقیما با افراد، فناوری‌ها و نیازهای هویتی و دیجیتال آن‌ها در ارتباط هستند.

فصل اول:

موردی برای یک هویت دیجیتال خوب

هویت - شکل‌دهی قراردادهای اجتماعی

هیچ چیز به اندازه هویت انسان‌ها دارای اهمیت نیست. هویت ما، به معنای واقعی کلمه، چیزی است که هستیم. تلفیقی از تاریخچه شخصی ما، باورها و رفتارهای ذاتی یا اکتسابی‌مان و مجموعه‌ای از فرهنگ، خانواده، ملیت، احزاب، جنسیت یا هویت‌ها و مشخصات دیگرمان. با وجود این که همه ما این را درک کرده‌ایم، اما هویت هنوز هم به اهمیت خود باپرجا است.

هویت ما از اهمیت بالایی برخوردار است به این دلیل که در ارتباطات و تعاملات ما با یکدیگر تاثیرگذار است. به علاوه، هویت ما در تعاملات و زیرساخت‌های اجتماعی و اقتصادی جامعه‌ای که در آن زندگی می‌کنیم نیز جاری است. این که هر یک از ما در سیستم‌های اقتصادی، اجتماعی و سیاسی چگونه ظاهر می‌شویم و این که هر یک از ما چه درجه‌ای از انتخاب و کنترل را در نحوه برقراری ارتباط و رفتار در جامعه برخوردار هستیم، فرصت‌ها و حقوقی را تعیین می‌کند که می‌تواند زندگی روزمره ما را دستخوش تغییر و تحول کند.

در طول تاریخ، شاهد نبردها و انقلاب‌های سرسختانه‌ای بوده‌ایم که بخش عمده‌ای از آن‌ها، برای دفاع از حقوق افراد به راه افتاده‌اند. از زمزمه‌های نفی مالیات بدون نمایندگی (no taxation without representation) تا پایان آپارتاید، همه نشان دهنده نحوه ظهور بشر در جامعه و تمام تلاش‌هایی که برای به دست آوردن حقوق و آزادی‌اش انجام داده است. تعریف‌های اولیه پلیس و شهروندی در یونان باستان، منشور کبیر و قانون اساسی ایالات متحده آمریکا، همگی چارچوب‌ها و تعاریفی هستند که برای شکل‌دهی روابط و قراردادهای اجتماعی بین مردم و سازمان‌ها به وجود آمده‌اند.

چه ما بخواهیم و چه نه، هویت ما به سمت دیجیتالی شدن گام برداشته است و با ساختارشکنی‌های صورت گرفته، همین هویت خواهد بود که تصمیم خواهد گرفت به کدام خدمات، محصولات و اطلاعاتی می‌توانیم دسترسی داشته باشیم. از چه تسهیلاتی محروم خواهیم بود. این مفهوم جدید از هویت، دیگر محدود به احراز هویت‌های ساده اینترنتی در سایت‌ها یا آواتارهای آنلاین نیست، بلکه مجموعه‌ای سترگ و روزافزون از کلیه اطلاعاتی است که در خصوص ما وجود دارند، یا پروفایل‌ها و تاریخچه‌ای که از فعالیت‌های‌مان، رفتارها و تعاملاتمان بر جای گذاشته‌ایم. در حقیقت، این هویت دیجیتال مدرن، نتیجه‌گیری کلیه اطلاعات و تاریخچه‌ای است که از ما به ثبت رسیده است و خود این هویت نیز یک نقطه آغاز جدید برای داده‌های آتی است.

در حال حاضر، کاربران اینترنت به طور متوسط هر کدام بالغ بر ۹۲ حساب کاربری آنلاین دارند که این رقم، انتظار می‌رود تا سال ۲۰۲۰ مرز ۲۰۰ حساب را نیز رد کند. بدیهی است که این حجم از لاگین‌های آنلاین و داده‌های مرتبط جزو اهداف کوتاه مدت سازمان‌ها جهت بهبود کارایی یا افزتیش درآمد یک سری خدمات خاص است. ضمن این که می‌توان با تکیه بر همین اطلاعات، خدمات و محصولات بسیار ویژه و درخوری نیز ارائه کرد. البته ممکن است تمام سازمان‌های استفاده کننده از این داده‌ها، با حسن نیت وارد عمل شده باشند. در هر صورت، هنگامی که این حجم از خدمات و محصولات و این حجم از هویت‌های آنلاین در هم می‌آمیزد، در صورتی که هنجارهای مشترک و استانداردی در اکوسیستم وجود نداشته باشد، پیامدهای بسیار گسترده‌تری در انتظار جوامع، سازمان‌ها و اشخاص خواهد بود. در مورد افراد، نتیجه مساوی خواهد بود با عدم کنترل روی هویت و تصویری که از آن‌ها در فضای آنلاین ترسیم می‌شود.

هرگونه بحث در خصوص هویت دیجیتال و شکل‌گیری آن باید با افرادی صورت گیرد که در دنیایی کاملا دیجیتال زاده شده‌اند و این هویت‌های دیجیتال، آینده آن‌ها را شکل خواهند داد. ما باید بتوانیم اعتماد به سیستم را از بیرون در آن نهادینه کنیم. باید بتوانیم معنای واقعی و ارزش حقیقی هویت دیجیتال را با معیار آزادی و ارزش واقعی انسان‌ها بیان کنیم. با تشدید ارتباطات، اتصالات و تعاملات، آن هم در دنیایی که سالانه میلیون‌ها یا حتی میلیاردها دستگاه متصل به هم بدان افزوده می‌شوند، ما به شدت نیازمند این هستیم تا اهمیت و ارزش واقعی این هویت‌های دیجیتال را بر همگان روشن کنیم.

سیستم‌های مدرن مبتنی بر هویت دیجیتال، باید در کشورهای در حال توسعه نیز طراحی و پیاده‌سازی شوند تا بتوانند خدمات اساسی و انعطاف‌پذیری شمول مالی و اجتماعی را حتی به فقیرترین و محروم‌ترین افراد جهان سوم نیز توسعه دهند. با وجود تمام پیشرفت‌های تکنولوژیکی صورت گرفته طی سال‌های اخیر، بالغ بر ۱/۱ میلیارد نفر از افراد جهان فاقد هویت رسمی هستند و این مشکل عدیده‌ای است که جهان نیز سعی دارد با پیشبرد برنامه‌های اهداف توسعه پایدار تا سال ۲۰۳۰ میلادی، در خلال برخی پیشرفت‌های آموزشی و بهداشتی و درمانی و همچنین توسعه شمول مالی و اقتصادی به خانواده‌ها و نسل‌های جدید در اقصی نقاط جهان، بخش قابل توجهی از آن را حل کند. هیچ جایی برای از دست دادن زمان وجود ندارد ضمن این که باید به خاطر داشته باشیم که طراحی و پیاده‌سازی یک سیستم مبتنی بر هویت دیجیتال بد و مریض، حتی آسیب‌رسان‌تر از فقدان کامل آن است. ما باید از آسیب‌پذیرتر کردن زندگی میلیارد فرد آسیب‌پذیر در این سیاره مصون داریم.

برای دوری از این فاجعه و دستیابی به سیستمی هویت محور و در عین حال موفق، نیاز به برخی هنجارها داریم و درکی مشترک از این که یک سیستم مبتنی بر هویت خوب چیست. این گزارش، گامی بلند در راستای درک همین مهم است.

هویت‌های دیجیتال در زندگی روزمره ما

هر چه ارتباطات دیجیتال و فعالیت های آنلاین پیشرفت می‌کند، هویت‌های دیجیتال نیز بیشتر در زندگی روزمره ما رخ می‌دهد. همه‌روزه از فرایندهای احراز هویت مختلفی عبور می‌کنیم که باعث می‌شوند تا دیگران، نسبت به ادعاهای ما، یا حقوقی که در مورد محصولات یا خدمات مختلف داریم احساس اطمینان کنند. همه ما تاکنون بارها از لاگین‌ها برای ورود به حساب‌های کاربری آنلاینمان یا از فرایندهای احراز هویت بیومتریک نظیر اسکن چهره یا اثر انگشت استفاده کرده‌ایم تا بتوانیم به محصولات، خدمات، اطلاعات یا برخی تعاملات و تراکنش‌های دیجیتال دسترسی داشته باشیم. بسیاری از ما، دارای پروفایل‌های مشخصی هستیم که سال‌ها است داده‌های ثابت و غیرقابل تغییرمان اعم از تاریخ و محل تولد، یا شماره‌های ملی و امثال ما را در خود جای داده‌اند و همین پروفایل‌ها، بخشی از هویت دیجیتالی هستند که برای آینده ضروری است.

هویت دیجیتال: حوزه‌ای در حال تکامل

- احراز هویت: فرایندهایی نظیر اثر انگشت، کلمه‌های عبور و غیره که صحت ادعای افراد مدعی در مورد یک هویت را ارزیابی و تعیین می‌کنند.

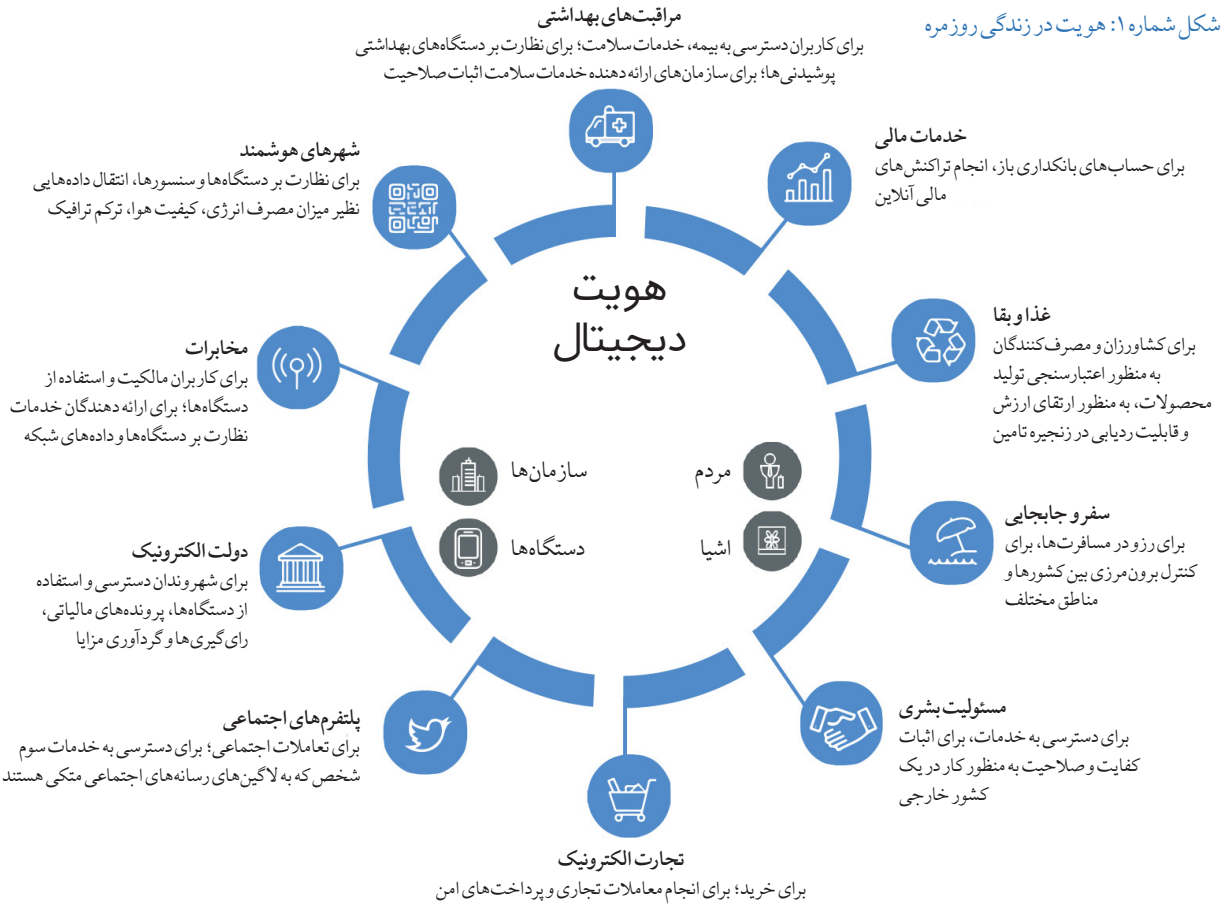
- پروفایل: می‌تواند شامل برخی مشخصات ذاتی نظیر اطلاعات بیومتریک یا مشخصات معین نظیر نام یا شماره‌های ملی افراد باشد.

- تاریخچه: تاریخچه‌های اعتباری یا بهداشت و درمان، رفتارهای خرید آنلاین و غیره

- نتایج: قضاوت یا تصمیم‌گیری بر اساس فرایندهای احراز هویت، پروفایل کاربران و تاریخچه‌های آن‌ها به عنوان مثال هنگام ارزیابی بانک برای تخصیص وام به کاربران.

با گذشت زمان، رفتارها، تراکنش‌ها و تعاملات ما، دنباله‌ای از تاریخچه شخصی مبتنی بر داده‌ها و رفتارهای آنلاینمان را رقم می‌زنند که اطلاعات مالی، مالیات‌ها، خریدها، پرونده‌های حقوقی، تاریخچه‌های بهداشت و درمان و اعتباری و بسیاری از داده‌های مهم دیگر از آن جمله‌اند. افراد و سازمان‌ها، به طور فزاینده‌ای در حال استفاده از این داده‌ها هستند و روزبه‌روز نیز نیاز به آن‌ها افزایش پیدا می‌کند. چه داده‌هایی که خود روی آن‌ها کنترل و حق تصمیم‌گیری داریم و چه داده‌ها و پروفایل‌هایی که از کنترل ما خارج شده و در اختیار منابع خارجی قرار گرفته‌اند. برای درک بهتر این موضوع می‌توانید دستگاه‌های ارائه‌دهنده بیمه را متصور شوید که برای اعتبارسنجی و اعطای تسهیلات بیمه به کاربران، کلیه رفتارهای رانندگی، داده‌ها و تاریخچه‌های حقوقی، تاریخچه‌های اعتباری و سن و سال افراد را مورد ارزیابی قرار می‌دهند تا بدانند چه سطح از ریسک متوجه آن‌ها است.

شکل شماره ۱: هویت در زندگی روزمره



برای کسب‌وکارها، هویت‌های قابل تایید ایجاد کننده بازارها و خطوط تجاری جدید، تجربه‌های کاربری بهتر، داده‌های بهبود یافته و ابزارهایی ضد تقلب هستند. برای دولت‌ها، این هویت‌ها ارائه دهنده راه‌های جدیدی برای حکمرانی هستند که ارائه خدمات بهتر، تعامل شهروندی بیشتر و ابزارهای ضد فساد و جنایت از دستاوردهای آن است. برای افراد نیز هویت هرکسی باز کننده (یا موجب بستن) درهای دنیای دیجیتال با استفاده از اشتغال وی، فعالیت‌های سیاسی و اجتماعی‌اش، آموزشش، خدمات مالی‌اش، بهداشت و درمان و... به سمت او است.

رشد پیچیدگی و مسئولیت‌پذیری

هرچه هویت‌های دیجیتال ما شکل گرفته و رشد یابند، هرچه ارائه دهندگان خدمات فرایندهای احراز هویت خود را توسعه می‌دهند و هرچه سطح بی‌نظیری از داده‌های شخصی در سطح دنیای آنلاین پراکنده می‌شوند، چالش‌های جدیدی پیش روی دولت‌ها، صاحبان کسب‌وکارها و جامعه مدنی پدیدار می‌شوند.

ارزش دادن به کاربر و حفظ اعتماد: در پی تلاش برای دادن راحتی و رفاه بیشتر به کاربران، خدمات شخصی‌سازی شده، و مدیریت ریسک‌های در حال رشدی نظیر سرقت‌های هویتی، ارائه دهندگان خدمات نیاز به حجم بسیار گسترده‌تری از داده‌ها آن هم از منابع مختلفی دارند تا بتوانند فرایندهای احراز هویت، طراحی محصولات و ارائه خدمات را به بهترین شکل ممکن انجام دهند. بدیهی است که این حجم از دسترسی، مستلزم مسئولیت‌پذیری بیشتری نیز خواهد بود تا حقوق کاربران، امنیت آن‌ها و حریم خصوصی‌شان رعایت شده و در عین حال، اعتماد آن‌ها به سیستم نیز حفظ شود. طبعیتا مدیریت چنین پیچیدگی و در پی آن مسئولیت سنگینی آسان نخواهد بود. درک مختلف سازمان‌ها، جوامع و کاربران از مفاهیم حریم خصوصی و امنیت نیز این پیچیدگی و دشواری را دوچندان می‌کند. دولت‌ها، در حالت کلی توسعه سیستم‌های مبتنی بر هویت دیجیتال را برای اهداف مشخصی در دستور کار خود قرار داده‌اند: ارائه خدمات عمومی کارآمد، حاکمیت قانون پایدار و فرایندهای دموکراتیک قوی. همزمان با این اهداف، باید اطمینان حاصل کنند که فرایندها و زیرساخت‌های سیستم مبتنی بر هویت دیجیتال به حریم خصوصی کاربران یا شهروندان لطمه‌ای وارد نمی‌کند، یا به ابزاری برای نظارت‌ها و دخالت‌های غیرقانونی تبدیل نمی‌شود و موجب تبعیض یا سوء استفاده نمی‌شود. اولویت‌بندی نیازها و حقوق افراد، علاوه بر تامین خواسته‌ها و اعتماد کاربران، برای سازمان‌ها نیز منافع خودش را دارد: ارائه محصولات و خدمات باارزش‌تر و قابل اعتمادتر که به پذیرش و توسعه گسترده‌تر می‌انجامد.

اجتناب از تکه تکه شدن، و هارمونی استانداردها: دنیای مدرن امروز میزبان سیستم‌های هویتی مختلف است، توسط دولت‌های مختلفی اداره می‌شود و تنوع بانک‌ها، خرده‌فروشی‌ها و سازمان‌ها در آن سر به فلک گذاشته است. هر یک از این دولت‌ها و سازمان‌ها، داده‌های کاربران را با هدف خاصی گردآوری کرده و مورد بهره‌برداری قرار می‌دهند که برگزاری انتخابات الکترونیک برای دولت‌ها و یا ارائه تسهیلات بانکی، خدمات بیمه یا خدمات بهداشت و درمان از آن جمله‌اند. بسیاری از افراد، در طول زندگی خود مجموعه اطلاعات ارزشمندی از خود و اطرافیانشان در اختیار این سازمان‌ها و دولت‌ها قرار می‌دهند. آن‌ها ورژن های مختلفی از خود یا به عبارت بهتر هویت خود در فضای آنلاین دارند. اما اغلب این سیستم‌ها، فارغ از تعاملات و ارتباطات فعالیت می‌کنند. اغلب آن‌ها در سیستمی ایزوله و مستقل زا سایر سیستم‌های در حال گردآوری و استفاده از داده‌های کاربرانشان هستند که هزینه‌ها را افزایش داده و ناکارآمدی و اصطکاک را به دنبال دارد. افزایش تعامل‌پذیری بین سیستم‌ها و سازمان‌ها می تواند این چالش را پاسخ داده و تجربه کاربران را نیز به نحو مطلوبی ارتقا دهد. البته، در نظر داشتن پارامترهای مهمی همچون امنیت و حریم خصوصی نیز باید توامان با این تعامل‌پذیری رعایت شود. سیستم‌هایی که

با اهداف مختلف و چندگانه‌ای راه‌اندازی شده‌اند، نیاز به داده‌ها و سطوح اعتماد مبتنی بر هویت مختلفی نیز دارند، ضمن این‌که طراحی و پیاده‌سازی آن‌ها نیز تحت تاثیر فناوری‌ها، نوآوری‌ها و ملاحظات، سیاست‌ها، ویژگی‌های اجتماعی و مقتضیات جغرافیایی متنوعی است. به همین دلیل نیز می‌توان درک کرد که چرا یک مدل و راهکار هویت دیجیتال جامع و جهانی که مصداق حقیقی یک سایز برای همه (one-size-fits-all) باشد وجود ندارد. با این حال، در این‌که یک سری استانداردها و اصول مشترک برای طراحی و پیاده‌سازی سیستم‌های مبتنی بر هویت دیجیتال در سراسر جهان وجود دارند شکی نیست. چالشی که این جا مطرح است، ارتقای تجربه و ارزش برای همه افراد و سازمان‌های درگیر، در کنار حفظ امنیت و احترام به حریم خصوصی است.

آینده‌ای واگرا

ما همه‌روزه در حال ایجاد و توسعه هویت‌های دیجیتال خود هستیم و همه‌روزه نیز تعداد بیشتری از افراد وارد حوزه دیجیتال می‌شوند. با توجه به نقش پررنگی که هویت در جامعه دیجیتال ایفا می‌کند، به راحتی می‌توان راه‌ها و مسیرهای متفاوت و واگرایی که در آینده نه چندان دور و در میان مدت شکل خواهند گرفت را تصور کرد. انتخاب‌ها و تصمیمات ما در مورد نحوه طراحی و اجرای سیستم‌های مبتنی بر هویت دیجیتال امروز، تعیین کننده آینده‌ای هستند که فردا رقم خواهد خورد.

آینده شماره ۱: دیجیتالی‌ها و غیردیجیتالی‌ها، جدایی بین نسل‌ها

در محیطی با انقلاب، پذیرش و نوآوری تکنولوژیکی سریع، مزایای اقتصاد دیجیتال کاملا مشهود است. کسانی که بتوانند از این انقلاب و نوآوری‌ها به نفع خود استفاده کنند، گوی سبقت را از سایر رقبا خواهند ربود و مزایای دگرگون‌شده‌ای را از آن خود خواهند ساخت. کسانی که نتوانند، از قافله عقب خواهند ماند. در غیاب تلاش های متفرکانه و متمرکز برای افزودن افراد محروم به این اکوسیستم دیجیتال جدید، شکاف بین افراد دارای هویت دیجیتال و غیردیجیتال‌ها بیش از پیش نیز افزایش خواهد یافت و این شکاف، نسل به نسل نیز ادامه خواهد داشت. در حال حاضر، نیمی از جمعیت جهان - بالغ بر ۴ میلیارد نفر - دسترسی قابل قبول و قابل اعتمادی به اینترنت و فرصت‌های خارق‌العاده آن ندارند. بیش از ۱/۱ میلیارد نفر در سراسر جهان هنوز هم نامرئی هستند. به این مفهوم که این افراد، فاقد هرگونه هویت قابل شناسایی و قانونی، چه به صورت آنلاین و چه به صورت آفلاین هستند. این نابرابری عظیم، در سطح درآمد افراد، موقعیت جغرافیایی و سبک زندگی آن‌ها تاثیر مستقیم دارد. ما باید در اسرع وقت به مساله شمول در سراسر جهان پاسخ دهیم تا از ادامه تشکیل زیرساخت‌های نابرابر و دو کلاس دیجیتال از انسان‌ها جلوگیری شود.

آینده شماره ۲: بدون انتخاب، بدون اعتماد، بدون حقوق

آینده قابل پیش‌بینی دیگری که می‌توان متصور شد، آینده‌ای است که همه افراد دارای شمولیت هستند، اما در دنیایی مملو از آسیب‌پذیری و بی‌اعتمادی. در صورتی افراد هیچ‌گونه کنترلی روی داده‌ها و هویت‌های دیجیتال خود نداشته باشند، و نتوانند در نحوه استفاده یا حتی سواستفاده از داده‌های‌شان دخالت داشته باشند، در استفاده از مزایا و فرصت‌های دنیای دیجیتال محدود خواهند بود. بدتر از همه این‌که افرادی که با سازمان‌ها و سیستم‌های فاقد حاشیه اطمینان و امنیت مناسب کار می‌کنند، حقوق و حریم خصوصی‌شان در معرض خطر قرار گرفته و ریسک امنیتی و نوع جدیدی از محرومیت‌ها را نیز متحمل خواهند شد. در چنین آینده‌ای، دولت‌ها و سازمان‌هایی که سیستم‌های مبتنی بر هویت دیجیتال را اجرا کرده و داده‌های کاربران را مدیریت می‌کنند، اعتماد افراد یا شهروندان را از دست می‌دهند.

آینده شماره ۳: شمول تحول یافته

هویت‌های دیجیتال اگر برای آینده‌ای فراگیر و کاربر محور طراحی شده باشند، تبدیل به فرصت، ارزش، امنیت و احترام به آزادی‌های افراد می‌شوند. چنین هویت‌هایی این قدرت را دارند تا تحول را در همه ابعاد زندگی ما، از آموزش تا سلامت و بهداشت و درمان گرفته فعال کنند و شمول اقتصادی و شمول مالی را وارد حیات بشریت در جای جای جهان کنند. برای درک بهتر چنین آینده‌ای کافی است شرایطی را متصور شوید که نوآوری و انرژی در حال رشد و توسعه است: هویت‌های دیجیتال، در صورتی که به درستی طراحی و اجرا شده باشند، این قدرت را خواهند داشت تا در چنین فضای در حال رشدی سیستم‌های بهداشت و درمان را دستخوش تحول کنند. در طول زندگی بشر، بیماری‌ها و خطرات بسیاری سلامت جسم و روان وی را تهدید می‌کند و به همین دلیل نیز بازبینی راهکارهای بهداشت و درمان و مدل‌های سلامت، و در عین حال بازنگری، تصحیح و بهبود سیستم‌های مبتنی بر داده‌های سلامت سنتی یکی از الزامات مهم ما در این عرصه است و می‌تواند سیستم‌های مبتنی بر هویت بسیار کارآمدتر و بیمار محورتری را ارائه دهد. ما نیاز داریم تا زیرساخت‌های قدرتمند و قابل اطمینانی از داده‌های سلامت را ایجاد کنیم. زیرساخت‌هایی که در تحقیق و تفحص، ارزیابی روندها و راهکارهای موجود، کشف راهکارهای درمانی و دارویی جدید، و همچنین بهبود و ارتقای مسیرهای مراقبتی و درمانی کنونی تاثیر بسزایی خواهند داشت. با ارتباط‌دهی کاربران یا افراد، داده‌ها و سیستم‌ها، شبکه‌ای قدرتمند حاصل خواهد شد که امکان جاری شدن آسان داده‌ها در سطح سیستم‌های ارائه دهنده خدمات بهداشت و درمان، اماکن و سازمان‌ها را میسر خواهد ساخت.

در حال حاضر، اکثریت قریب به اتفاق بیماران هیچ‌گونه حق مالکیت و کنترلی روی پرونده‌ها و داده‌های سلامت خود ندارند یا دست کم، این دسترسی بسیار محدود است. هنوز هم موانع مبتنی بر فناوری بسیاری وجود دارند که استانداردسازی، دسترسی به داده‌ها، تعامل‌پذیری و مدیریت هویت از آن جمله‌اند. بدیهی است که به محض پاسخگویی به این نیازها و مرتفع شدن این موانع، هویت دیجیتال ما در راس تحولات سلامت قرار خواهد گرفت. در صورتی که بیماران و دستگاه‌های سلامت و دارویی آن‌ها در هر کجای دنیا قابل اعتبارسنجی، احراز هویت و تایید باشند، و در عین حال اطلاعات پزشکی افراد با مدیریت و رضایتمندی قدرتمند خودشان در دسترس قرار گیرند، موج جدیدی از نوآوری‌های پزشکی آغاز خواهد شد.

یا سیستم‌های غذایی را در نظر بگیرید. هویت دیجیتال می‌تواند کشاورزان پایین دستی را پشتیبانی کرده و معیشت پایدار اقتصاد محور آن‌ها و افراد وابسته به محصولات آن‌ها را بهبود ببخشد. بسیاری از کشاورزان پایین دستی که در مقیاس‌های کوچک فعالیت می‌کنند، در حال حاضر در سراسر جهان برای امرار معاش در تقلا هستند. درآمدهای این قشر اغلب غیرقابل پیش‌بینی است و این در حالی است که از مبالغ پرداختی در ازای محصولات توسط استفاده کنندگان، تنها سهم بسیار ناچیزی به کشاورزان می‌رسد که گاهی حتی کفاف مواد اولیه موردنیاز را نیز نمی‌دهد. ضمن این‌که، استفاده کنندگان از محصولات کشاورزی نیز به شدت تمایل دارند منشا تولید محصولات مصرفی و روش‌های به عمل آوری این محصولات را نیز بررسی کنند.

فناوری‌های نوینی همچون اینترنت اشیا (Internet of Things)، که امکان اعتبارسنجی و احراز هویت محصولات را فراهم کرده‌اند، این قابلیت را دارند تا مدل‌های قابل ردیابی و اند-تو-اندی (end-to-end) از زنجیره‌های تامین را معرفی کنند. چنین زنجیره‌هایی، شفافیتی خارق‌العاده در مورد چرخه حیات محصولات در اختیار کاربران قرار می‌دهند. شفافیت در مورد منشا محصولات، نقل و انتقالات و سفر آن‌ها و تحولاتی که در چرخه حیات و در زنجیره تامین داشته‌اند. با افزایش شفافیت و اعتماد، کاربران این امکان را خواهند داشت تا با پرداخت مبالغ بالاتر در ازای محصولات باکیفیت، کشاورزان را تشویق کنند. پرواضح است که چنین مدلی، انگیزه‌های موردنیاز برای پیشرفت را در سرسر اکوسیستم جهانی تامین خواهد کرد و همه دست‌اندرکاران، در نهایت انگیزه، دقت و در عین حال سودآوری به کار خود ادامه خواهند داد.

تفاوت شناسایی هویت و احراز هویت

شناسایی هویت (Identification) به فرایندهایی اطلاق می‌شود که درصدد اثبات هویت یک فرد در یک جامعه یا محتوا هستند. این فرایندها اغلب زمانی اتفاق می‌افتند که قصد داریم هویت افراد را با استفاده از برخی صفات قابل تایید و معتبر نظیر نام، تاریخ تولد، اثر انگشت یا اسکن عنبیه، شناسایی و تایید کنیم.

احراز هویت (Authentication) فرایندهایی هستند که فرد اقدام کننده قصد دارد با استفاده از آن‌ها ادعای خود مبنی بر یک هویت دیجیتال مشخص را ثابت کند. این فرایندها، بر اساس اثر انگشت، پسـوردها و غیر صورت می‌گیرند و هویتی را احراز می‌کنند که قبلا تثبیت شده است.

پنج پارامتر یک هویت خوب

در نشست سالانه مجمع جهانی اقتصاد سال ۲۰۱۸ در داووس، مجموعه‌ای متشکل از ذینفعان، دست‌اندرکاران، دولت‌ها، کسب‌وکارها و جامعه مدنی گرد هم آمدند تا در مورد هویت دیجیتال و فاکتورهای و پارامترهای آن به توافق برسند.

طی ماه‌های گذشته، این مجمع و گروه کاری آن توانسته است پنج عنصر کلیدی برای یک هویت دیجیتال خوب معرفی کند. هویت دیجیتال کاربر محور، که می تواند ارزش را به معنای واقعی کلمه برای کاربران به ارمغان بیاورد، مفهوم مهمی است که باید در کلیه جوانب با موفقیت پیاده‌سازی شود.

این پارامترها می‌توانند در کنار هم یا روی هم ساخته شوند. اما ممکن است برخی تنش‌ها نیز میان آن‌ها وجود داشته باشد. به عنوان مثال، معیارهای امنیتی ممکن است طراحان را با برخی چالش‌ها مواجه کنند. بخشی از رسالت دست‌اندرکاران مجمع اقتصاد جهانی، درک روشن این تداخلات و تعاملات و مدیریت صحیح آن‌ها است.

۱. متناسـب با هدف. یک هویت دیجیتال خوب راهکاری قابل اعتماد برای افراد اسـت تا بتوانند نسـبت به هویتی که ادعا می کنند جلب اعتماد کنند، و در سایه این هویت به آزادی‌ها و حقوق خود دسـت یافته یا توانایی شـرکت در تعاملات و تراکنش‌های دیجیتال را داشته باشند. با افزایش تعاملات و تراکنش‌های دیجیتال بین افراد، بدون وجود روابط از پیش تعریف شده و دخالت ربات‌های هوش مصنوعی، این فرایند با چالش جدی مواجه خواهد شد.

۲. همه‌جانبه. یک هویت دیجیتال جامع و همه‌جانبه، به همه این امکان را می‌دهد تا فارغ از ریسک تبعیض مبتنی بر داده‌های هویتی، هویت دیجیتال خود را فعال کرده، تثبیت کنند و از آن بهره بجویند؛ بدون این‌که با فرایندهایی که ممکن است آن‌ها را حذف کنند روبه‌رو شوند.

۳. سودمندی. یک هویت دیجیتال مفید، عبارت است از هویتی که دسترسی افراد به تراکنش‌ها و خدمات مفید را میسر می‌سازد و در عین حال تثبیت و استفاده از آن نیز ساده و آسان است. در حال حاضر، بسیاری از هویت‌های دیجیتال دارای الزامات و ملاحظات پیچیده‌ای هستند که استفاده از آن ها را دشوار و محدود ساخته است.

۴. ارائه حق انتخاب. افراد، در صورتی که بتوانند سیسـتم‌های اسـتفاده کننده از داده‌های هویتی خود را شناسـایی کرده و از اهداف آن‌ها سر در بیاورند دارای حق انتخاب خواهند بود. این‌که قادر باشند خود تصمیم بگیرند که کدام داده‌ها، در اختیار کدام سیستم‌ها قرار گیرد و از این داده‌ها با چه هدفی و برای چه مدت زمانی داده‌ها استفاده شود. در غیاب این حق انتخاب، افراد به شکل غیرقابل توصیفی در معرض ریسک شکاف اطلاعاتی، پایمال شدن حریم خصوصی، سرقت هویتی، تقلب و یا سایر سوء استفاده‌ها قرار خواهند گرفت.

۵. ایمن. امنیت شـامل حفاظت از افراد، سازمان‌ها، دسـتگاه‌ها و زیرساخت‌ها از سرقت‌های هویتی، به اشـتراک‌گذاری‌های غیر مجاز و نامعتبر داده‌ها و نقض حقوق بشر اسـت. چنین امنیتی در حال حاضر به شکا حقیقی و جامع پیاده‌سازی نشده است، چرا که داده‌های دیجیتال هویتی، هنوز به شکل قابل استفاده و استناد گردآوری نشـده‌اند و اطلاعات، در سراسـر حـوزه دیجیتال به شـکل ناهمگون پراکنده‌اند.

سیستم‌های هویتی امروز: سه طرح

سیستم‌های هویتی امروز و سیسـتم‌های هویتی در حال ظهور فردا، عموما به سه دسته کلی تقسیم می‌شـوند: متمرکز، فدرالی و غیر متمرکز. همان‌طور که از عنوان آن‌ها نیز بر می‌آید، زیرساخت هریک از این مدل‌ها، پیاده‌سازی برای پذیرش و جلب اعتماد، چالش‌ها و مزایای هر یک از آن‌ها برای افراد و کاربران اسـت که آن‌ها را از سایرین متمایز می‌سازد.

همان‌طور که انتظار می‌رود، سنتی‌ترین و معمول‌ترین طرح برای مدل هویتی مدل متمرکز است، که در آن‌ها سازمان‌ها، همان دولت‌ها یا شرکت‌ها، هویت‌های افراد و داده‌های مربوط به آن‌ها را تثبیت کرده و مدیریت می‌کنند. این در حالی است که در مدل دوم، یعنی مدل فدرالی، این نقش میان سـازمان‌ها یا شرکت‌های مختلفی تقسیم شده است. سیستم‌هایی که جدیدترین مدل یا همان مدل غیر متمرکز را دنبال می‌کنند، به دنبال دنیایی آرمانی برای کاربران هسـتند کـه در آن، افراد خود روی هویت‌های دیجیتال و داده‌های مربوط به آن کنترل دارند و اطلاعات هویتی خود را شخصا مدیریت می‌کنند.

شکل شماره ۲: پنج عنصر اصلی یک هویت خوب

شکل شماره ۳: سه مدل سیستم هویتی

انواع سیستم‌ها	متمرکز	فدرالی	غیر متمرکز
تعریف	یک سازمان واحد هویت‌ها را تثبیت و مدیریت می‌کند.	سیستم‌های مستقل مختلف که هرکدام با مدل اعتمادی خود کار می‌کنند و بین یکدیگر اعتمادسازی کرده‌اند.	مشارکت نهادهای مختلف چندگانه در سیستم غیر متمرکز هویت دیجیتال؛ کنترل کاربران روی به اشتراک‌گذاری داده‌های هویتی
مثال‌ها	نقش انتخاباتی دولت‌ها؛ بانک‌ها؛ پلتفرم‌های رسانه‌های اجتماعی	بانک آی‌دی سوئد؛ سیستم احراز هویت بریتانیایی گاو. یوکی و ریفای	نمونه آزمایشی آمزوش و پرورش دولت مالتا؛ شهر آزمایشی آنتورپ
سطح پذیرش و اعتماد	پذیرش به ارزش ارائه شده وابسته است؛ اعتماد، به مالکیت سیستم و نحوه اثبات هویت بستگی دارد.	پذیرش به توسعه و تثبیت رابطه مبتنی بر اعتماد وابسته است؛ اعتماد، به مالکیت سیستم و نحوه اثبات هویت بستگی دارد.	پذیرش هنوز در مراحل اولیه قرار دارد. مکانیسم اجماع گواه اثبات کار؛ اعتماد، به مدل‌ها و الگوریتم‌های اعتماد و گواهینامه‌ها بستگی دارد.
نقاط قوت	می‌توان برای اهداف خاصی پیاده‌سازی کرد؛ برای بررسی سازماندهی شده داده‌های هویتی مناسب است.	کاربران می‌توانند به طیف وسیعی از خدمات دسترسی داشته باشند؛ کارایی برای سازمان‌ها بالاتر است.	افزایش کنترل کاربران و کاهش حجم داده‌های هویتی گردآوری شده و ذخیره‌سازی شده توسط سامان‌ها
چالش‌ها	عموما دارای کنترل کاربری پایینی است؛ مسئولیت‌پذیری و ریسک‌پذیری متمرکز آن بالا است؛ و امکان سوء استفاده در آن بالا است.	عموما دارای کنترل کاربری پایینی است؛ پیچیدگی‌های فنی و حقوقی بیشتر است.	مدل حکومتی، پذیرش و مشارکت پیچیده‌تر است؛ دورنمای مدل هنوز مشخص نیست؛ مسئولیت‌پذیری پیچیده‌تر شده است.

مدل متمرکز

تعریف

در این سیستم‌های هویتی سنتی، هر یک از افراد به عنوان کاربران از خدمات سازمان‌هایی که مالک سیستم هستند و آن را مدیریت می‌کنند استفاده می‌کنند. مدیر یا مالک سیستم، اعم از ارائه دهندگان سوم شخص فناوری، که از جانب مالک فعالیت می‌کنند، داده‌های هویتی افراد را گردآوری کرده، استفاده می‌کند یا در پایگاه‌های اطلاعاتی خود ذخیره‌سازی می‌کند. ضمن این‌که این مدیران و مالکین، با همکاری اشخاص ثالث ارائه دهنده و سایر دست‌اندرکاران صنعت، خدمات و محصولات مورد انتظار کاربران را آماده کرده و به آن‌ها عرضه می‌کنند و تراکنش‌های آن‌ها را پشتیبانی می‌کنند. این مدیر یا مالک می‌تواند دولت باشد، همانند سیستم ای-آی‌دی استونی یا سیستم احراز هویت بیومتریک ادهار هندوستان، یا یک سازمان بخش خصوصی نظیر یک سیستم بانکداری و یا یک شرکت ارائه دهنده پلتفرم رسانه‌های دیجیتال باشد.

سطح اعتماد و پذیرش

پذیرش برخی از سیستم‌های هویتی سنتی در سطح گسترده‌ای صورت گرفته است. دولت‌ها در اقصی نقاط جهان چنین سیستم‌هایی را به رسمیت شناخته‌اند و در برخی موارد، این پذیرش به دلیل قوانینی بوده که از آن‌ها استفاده می‌کنند. بسیاری از افراد، از رسانه‌های اجتماعی قدرتمندی استفاده می‌کنند که مجهز به سیستم‌های تایید هویت دیجیتال هستند، درست مثل سیستم تایید هویت فیسبوک، تا کاربران خود را برای استفاده از خدماتشان اعتبارسنجی کنند. بسیاری از سیستم‌های بانکداری سنتی نیز برای ارائه محصولات و خدمات خود به کاربران، آن‌ها را از فرایندهای اعتبارسنجی و تایید هویت ویژه خود عبور می‌دهند.

سیستم‌های هویتی دولت‌ها یا سیستم‌هایی که توسط ارائه دهندگان خدمات مالی قانونی ارائه می‌شوند، اغلب از فرایندهای تایید و احراز هویت قدرتمندی بهره‌مند هستند که باعث شده است کاربران و سازمان‌ها، با اعتماد بیشتری نسبت به به اشتراک‌گذاری داده‌های هویتی خود، به‌ویژه در مورد تراکنش‌های با ریسک بالا، با چنین سیستم‌هایی اقدام کنند. در سیستم‌هایی که فرایندهای اثبات هویت ناکارمد، محدود و یا ضعیف است، درست مثل برخی از رسانه‌های اجتماعی، که ساخت پروفایل‌های مشابه یا جعلی کار چندان دشواری نیست، اعتماد نیز محدود است و همین امر نیز باعث می‌شود تا پای بسیاری از تراکنش‌ها که نیاز به سطح اعتماد بالاتری دارند، در چنین سیستم‌هایی لنگ بزند. هنوز هم بسیاری از پلتفرم‌های دیجیتال در حال توسعه سیستم‌های تایید هویت و اعتبارسنجی دیجیتال خود هستند تا بتوانند طیف گسترده‌تری از کاربران و ارائه دهندگان خدمات را به سمت خود جذب کنند. وی‌چت و دولت چین، مثال بارزی از چنین تلاش‌ها است که به‌ویژه طی سال‌های اخیر شدت نیز گرفته است.

نقاط قوت

افراد، به محض این‌که در سیستم تثبیت شده و از فرایندهای احراز هویت سربلند بیرون بیایند، این امکان را خواهند داشت تا به خدمات و محصولات ارائه شده توسط ارائه دهندگان دسترسی داشته باشند؛ خواه این خدمات خدمات بانکی باشند، خواه خدمات عمومی باشند و خواه شبکه‌های اجتماعی. مالک سیستم هویتی، الزامات و سطح امنیتی سیستم را بر اساس مقررات و ضوابط حقوقی، الزامات انطباقی، ریسک‌پذیری و سیاست‌های موجود تعیین می‌کند و به‌طور بالقوه سعی می‌کند تا بالاترین سطح امنیتی ممکن را برای سیستم پیاده کند تا بتواند کاربران را اقناع نماید. ضمن این‌که این مالکین می‌توانند همچون یک دروازه‌بان، از ورود داده‌های هویتی نامعتبر و نامناسب به سیستم نیز جلوگیری کنند. بسیاری از ارائه دهندگان و مالکین سیستم‌های هویتی، با نهادها دولتی و بخش خصوصی نیز دست دوستی می‌دهند تا بتوانند با کمک به تایید برخی اسناد هویتی نظیر گذرنامه‌ها، آی‌دی کارت‌ها یا اعلامیه‌های بانکی، دسترسی کاربران به خدمات و محصولات مختلف را ممکن سازند.

چالش‌ها

سیستم‌های هویتی سنتی، کمترین میزان کنترل را به افراد می‌دهند تا در مورد به اشتراک‌گذاری و استفاده از داده‌های شخصی خود تصمیم‌گیری کنند. برخی از این

سیستم‌ها نیز تنها بخش ناچیزی از خدمات را پشتیبانی می‌کنند و فاقد تعامل‌پذیری با سایر سیستم‌ها و سازمان‌ها هستند. سیستم‌های هویتی مبتنی بر معماری سنتی و متمرکز را می‌توان به نوعی هانی‌پات‌هایی برای داده‌های هویتی کاربران قلمداد کرد که اهدافی جذاب برای هکرها هستند و می‌توانند ریسک‌ها و سطح بالاتری از مسئولیت‌پذیری را به سمت مالکین این دست سیستم‌ها معطوف کنند. ضمن این‌که، متمرکزسازی، در صورت غلفت می‌تواند در را به روی برخی سوء استفاده‌ها نظیر نظارت‌های غیرمجاز، ردیابی و نمایه‌سازی‌ها باز کند. محرومیت، تبعیض یا سرکوب‌های سیاسی نیز از چالش‌های دیگری است که در این قبیل سیستم‌ها می‌توان با آن مواجه بود.

عناصر یک اکوسیستم مبتنی بر هویت دیجیتال

به لحاظ تاریخی، یک اکوسیستم هویتی عموما دارای دو عضو یا دو شرکت کننده است. دو عضو که کاملا نیز یکدیگر را می‌شناسند. اما در اکوسیستم‌های هویتی مدرن امروز، تعداد زیادی عنصر نقش‌آفرین وجود دارند:

- افرادی که به هویت‌های دیجیتال نیاز دارند تا در امنیت به سیستم‌های دیجیتال و تراکنش‌ها دسترسی داشته باشند.
- دستگاه‌ها، مجموعه‌ای از دستگاه‌ها، نهادهای حقوقی و دارایی‌های فیزیکی و مجازی که ممکن است افراد مالک آن‌ها باشند یا از آن‌ها استفاده کنند و مستلزم هویت دیجیتال هستند.
- مدل‌های اعتماد، منابع معتبر اثبات هویت
- کنترل کننده یا نماینده داده‌های هویتی، که در اغلب موارد از یک مدل اعتماد خاص بهره‌مند است، نظیر دولت‌ها و می‌تواند کنترل‌های لازم روی داده‌های هویتی را اعمال کند.
- اپراتور سیستم هویتی، که ممکن است نهاد ارائه دهنده یا مالک سیستم باشد، یا یک سازمان مجزا و مستقل نظیر شرکت‌های سوم شخص ارائه دهنده خدمات مبتنی فناوری باشد که از جانب مالک فعالیت می‌کند.
- طرفین متکی، که سازمان‌هایی هستند که برای اجازه یا رد دسترسی به محصولات، خدمات و یا داده‌ها به هویت‌های دیجیتال وابسته‌اند.
- متولیان یا پشتیبانان، که هویت‌های دیجیتال را قادر می‌سازند تا وارد عمل شوند.
- و رگولاتورها، که بر نحوه مدیریت هویت‌های دیجیتال حکم‌رانی یا راهنمایی می‌کنند.

مدل فدرالی

تعریف

هنگامی که دو یا چند سازمان و سیستم متمرکز به یک اعتماد متقابل می‌رسند، خواه با توزیع مولفه‌های اثبات اعتماد بین طرفین و خواه با به شناسایی قابلیت‌ها و شناسه‌های اعتمادی یکدیگر و به رسمیت شناختن استانداردهای مبتنی بر اعتماد هم، یک سیستم هویتی مبتنی بر مدل فدرالی شکل می‌گیرد. به عنوان مثال، دولت‌ها یا سازمان‌های بین‌المللی هم می‌توانند با تثبیت استانداردهای موجود تشکیل یک اکوسیستم هویتی را بدهند و هم می‌توانند با پذیرش، موافقت و به رسمیت شناختن استانداردها و مولفه‌های هویتی یکدیگر به اجماع در این زمینه دست یابند، نظیر سیستم eIDAS اتحادیه اروپا، یا استانداردهای ICAO که برای مسافرت‌های برون مرزی طراحی و ارائه شده‌اند. در حالت کلی، سازمان‌ها غ می‌توانند مدارک و مولفه‌های قانونی و هویتی یکدیگر را به رسمیت شناخته و بر اساس این مدارک، سیستم‌های هویتی فدرالی خود را راه‌اندازی کنند. درست مانند کاری که بسیاری از بانک‌ها و همچنین سایر سازمان‌های مالی و غیرمالی در اقصی نقاط جهان از جمله سوئد، بانک آی‌دی سوئد، انجام می‌دهند. یا همان رویه‌ای که شماری از سازمان‌های بخش خصوصی و دولتی در بریتانیا در پیش گرفته‌اند و از گاو. یوکی وریفای استفاده می‌کنند. در چنین مدل‌هایی، اغلب سازمان‌ها از توافق‌نامه‌ای فرد به فردی که در سیستم تعریف می‌شود و یا از استانداردهای تکنیکی موجود تبعیت می‌کنند. بدیهی است که هرچه تعداد این قبیل استانداردها و توافق‌نامه‌ها بیشتر باشد، سیستم نیز رشد بیشتری خواهد یافت.

سطح اعتماد و پذیرش

برخی از سیستم‌های هویتی فدرالی در سطح گسترده‌ای مورد پذیرش عموم قرار گرفته‌اند. افراد معمولا دسترسی آسان‌تری به خدمات و محصولات ارائه شده توسط چندین سازمان دارند. همان‌چیزی که در این مدل هویتی ارائه شده است. با این حال، پیچیدگی‌های برقراری اعتماد بین سازمان‌هایی که متولی و تشکیل دهنده چنین سیستمی هستند می‌تواند راه‌اندازی و اجرای آن را با محدودیت مواجه کند. همان‌طور که در سیستم‌های متمرکز نیز عنوان شد، در این سرویس‌ها نیز سطح اعتماد به سازمان‌های متولی و ارائه دهنده و همچنین درجه‌ای از حفاظت اطلاعاتی و اثبات هویتی که آن‌ها عرضه می‌کنند وابسته است.

نقاط قوت

شبکه‌های فدرالی این قابلیت را دارند تا در مقایسه با سیستم‌های متمرکز متکی به یک سازمان واحد، دسترسی افراد به طیف گسترده‌ای از خدمات و محصولات را فراهم کنند. این تعامل‌پذیری، رفاه و راحتی بیشتری برای کاربران رقم می‌زند. ضمن این‌که این قبیل سیستم‌ها، به سازمان‌ها کمک می‌کند تا داده‌ها و هویت‌های دیجیتال کاربران را بهتر ارزیابی کرده، مدیریت کنند و به کارایی لازم دست یابند.

چالش‌ها

درست مانند سیستم‌های متمرکز، سیستم‌های هویتی فدرالی نیز اختیار و قدرت تصمیم‌گیری و کنترل کمتری به کاربران در مورد نحوه و میزان استفاده از داده‌هایشان می‌دهند. برای مالکین سیستم، پیچیدگی‌های ناشی از نیاز بالقوه با توافق‌های قانونی، تفاوت در ریسک‌ها و مسئولیت‌پذیری‌ها، به اشتراک‌گذاری داده‌ها و همچنین استانداردهای فنی در این مدل به مراتب بیشتر است. چنین پیچیدگی‌هایی ممکن است راه‌اندازی و اجرا را پرهزینه‌تر کرده و سیستم را از ارائه برخی محصولات و خدماتی که کاربران انتظار دارند باز دارد.

مدل غیرمتمرکز

تعریف

سیستم‌های غیرمتمرکز هویتی، همان‌طور که از نام آن‌ها نیز برمی‌آید، برای مدیریت و اجرا به یک سازمان واحد یا مجموعه‌ای از سازمان‌ها وابسته نیستند. در عوض، چنین سیستم‌های غالبا مجهز به یک دستگاه دیجیتال هستند که در مالکیت یک فرد است و یک فروشگاه داده‌های هویتی، که اغلب توسط یک نفر مدیریت می‌شود. این فروشگاه داده، که می‌تواند دستگاه‌های مموری کاربران یا فضاهای ابری باشد، توافق‌نامه‌ها و مجوزهایی از سیستم‌های مبتنی بر اعتماد سنتی، نظیر بانک‌ها یا دولت‌ها را در خود نگه داشته‌اند و در عین حال، از سایر مدل‌های اعتمادی ارائه شده توسط عناصر تاثیرگذار، نظیر کارفرمایان، خرده‌فروشان، رسانه‌ها و امثال آن نیز بهره می‌جویند. این افراد هستند که تصمیم می‌گیرند کدام داده‌ها یا مدارک، برای چه سازمان‌هایی قابل دسترسی باشند و این دسترسی، تا چه زمانی ادامه پیدا کند.

سطح اعتماد و پذیرش

این مدل از سیستم‌های هویتی، هنوز در نخستین مراحل خود یعنی در مراحل آزمایشی و گواه اثبات مفهوم به سر می‌برد.

در بخش دولتی، دولت مالتا در حال راه‌اندازی سیستم هویتی خود مبتنی بر فناوری دفتر کل توزیع شده بلاکچین است که در صورت موفقیت این راه‌اندازی آزمایشی، سیستم آموزشی این دولت قادر خواهد بود کلیه گواهینامه‌های تحصیلی نظیر

دیپلم‌ها و صدور سایر گواهینامه‌های حرفه‌ای و تخصصی را با اعتبارسنجی و تایید هویت افراد از طریق گوشی‌های تلفن همراه‌شان صادر کند. شهر آنتورپ نیز از اقداماتی است که به صورت آزمایشی در دستور کار قرار گرفته است و در این نوآوری، سعی می‌شود تا با بهره‌مندی از فناوری بلاکچین، کلیه داده‌های هویتی افراد، از بدون تولد، اعم از دکترها، بیمارستان‌ها، سازمان‌های دولتی و غیره به صورت دیجیتال و توزیع شده ثبت و نگه‌داری شوند.

در بخش خصوصی نیز کنسرسیوم‌های بانکداری در تلاش هستند تا با استفاده از اکوسیستم‌های توزیع شده خود، طرح‌های شناخت مشتری مشترک یا سایر چارچوب‌های توزیع شده هویتی را به صورا آزمایشی در دستور کار خود قرار دهند. برخی از برنامه‌های وفاداری راه‌اندازی شده توسط شرکت‌های هواپیمایی و نوآوری‌های مشابهی که برخی از شرکت‌های بیمه ارائه کرده‌اند نیز باعث شده‌اند تا چنین مدل‌هایی بیش از پیش جا افتاده، و در عین افزایش راندمان سازمان‌ها، کنترل افراد روی داده‌های هویتی نیز بهبود یابد.

سطح اعتماد و پذیرش در مورد این قبیل سیستم‌ها، مستقیما به نحوه اثبات هویت و فرایندهای مدیریت داده بر می‌گردد که این نیز به نو به خود به مدل اعتماد جاری در سیستم وابسته است. در چنین سیستم‌هایی، این کاربران هستند که تصمیم می‌گیرند چه سازمان‌هایی از کدام داده‌ها استفاده کنند. بدیهی است که افرادی که دولت‌ها را برای دسترسی به داده‌های هویتی خود بر می‌گزینند، اعتماد بیشتری به سیستم خواهند داشت تا افرادی که با سازمان‌ها یا کاربران شخصی طرف هستند.

نقاط قوت

مهم‌ترین نقطه قوت یک سیستم هویتی غیر متمرکز کنترل کاربران روی داده‌ها و شفافیتی است که به آن‌ها ارزانی می‌کند. کنترل روی این‌که کدام داده‌های هویتی می‌تواند به اشتراک گذاشته شوند، با چه سازمان‌ها و افرادی به اشتراک گذاشته شوند و این به اشتراک گذاری تا چه زمانی می‌تواند ادامه پیدا کند. ضمن این‌که سیستم‌های مبتنی بر هویت دیجیتال غیر متمرکز یا به اصطلاح دیگر توزیع شده، تجربه کاربری خارق‌العاده و متفاوتی نیز برای افراد رقم می‌زنند، چرا که انتظارات افراد از شفافیت و مدیریت به نحو قابل توجهی برآورده می‌شود و سطح قابل قبولی از شخصی‌سازی را تجربه می‌کنند که به ایجادارزش برای آن‌ها می‌انجامد. به علاوه، تعامل‌پذیری یکی از ماهیت‌های عمده و منحصر به‌فرد این قبیل سیستم‌ها است که بسیاری از خدمات، محصولات و شبکه‌ها را قابل دسترسی می‌کند.

چالش‌ها

بزرگ‌ترین چالشی که سیستم‌های هویتی مبتنی بر دفتر کل توزیع شده با آن مواجه هستند، سطح بالای ریسک تراکنش برای افراد است که فارغ از قراردادها و چارچوب‌های قانونی بانک‌ها و دولت‌ها وارد تراکنش می‌شوند. بسیاری از مدل‌های اعتمادی دولت‌ها و بانک‌ها برای سیستم‌های مترمکز و روابط تعریف شده در آن‌ها قابل استفاده هستند و جایی در سیستم‌های توزیع شده ندارند. در حقیقت تغییر در زیرساخت‌ها و روابط باعث شده است تا مالکیت داده‌ها، مدیریت آن‌ها و حفظ امنیت آن‌ها با چالش جدی مواجه شود، هرچند که برخی از الزامات امنیتی و ملاحظات قانونی سنتی، بخشی از این نیاز مهم را پاسخگو هستند و این تغییر بزرگ را پوشش می‌دهند. بدیهی است که ارائه دهندگان خدمات غیر متمرکز و اشخاص ثالث وابسته به آن‌ها، برای استفاده از این راهکارهای سنتی باید به آن‌ها اعتماد داشته باشند و آن‌ها را به رسمیت بشناسند.

در حالت کلی، نوآوری‌ها، فناوری‌ها و استانداردهایی که برای توسعه و تکامل سیستم‌های هویتی توزیع شده یا غیر مترمکز نیاز هستند به سرعت در حال رشد و اوج گرفتن است. اما این در حالی است که چارچوب‌های رگولاتوری و دستورالعمل‌ها و مدل‌های عملیاتی، اغلب برای سیستم‌های سنتی و متمرکز طراحی شده‌اند و پاسخگوی سیستم‌های توزیع شده مدرن نیستند. این دستورالعمل‌ها و چارچوب‌ها نیز باید در اسرع وقت دستخوش تحول شده، تغییر یابند و برای آدرس‌دهی به الزامات غیر متمرکزسازی آماده شوند. تخصیص مسئولیت برای جبران و مدیریت ریسک‌ها و نشت‌های اطلاعاتی احتمالی در این قبیل سیستم‌ها نیز از پیچیدگی بالایی برخوردار است. احتمالا، برای این‌که بتوانند به روشی صحیح از این سیستم‌های هویتی استفاده کرده و در قبال داده‌های خود مسئولیت‌پذیر باشند، نیاز به آموزش خواهد بود.

شکل شماره ۴: مثال‌های برگزیده از انواع مدل‌های سیستم‌های هویتی در اقصی نقاط جهان

آی‌دی درخت‌های کوه تای، چین
بیش از ۲۰،۰۰۰ درخت باستانی در کوی تای (Mount Tai)، در شاندونگ چین دارای کارت آی‌دی هستند که به جنگل‌بانان اجازه می‌دهد تا سلامت درختان و محیط اطراف آن‌ها را بررسی کنند.

تی-اوث کره جنوبی
اپراتورهای تلفن همراه در کره جنوبی راهکار هویتی مشترکی مبنی بر شماره‌های تلفن همراه کاربران راه‌اندازی کرده‌اند که طی آن، امکان دسترسی به داده‌های کاربران در صورت صدور اجازه از سمت آن‌ها وجود دارد.

وی‌چت آی‌دی-چین
این اپلیکیشن موبایلی که با پایگاه کاربری یک میلیارد نفری خود با دولت چین نیز همکاری می‌کند، در حال پیاده‌سازی یک سیستم آزمایشی هویتی با عنوان وی‌چت آی‌دی است. یک شناسه دیجیتال، که امکان برقراری ارتباط و رزرو هتل یا پذیرش و تحویل را برای کاربران میسر می‌سازد.

ادهار-هندوستان
دولت هند، در این پروژه بالغ بر ۹۹ درصد از جمعیت خود را بر اساس مشخصات بیومتریک‌شان و با استفاده از یک آی‌دی مشخص احراز هویت کرده که برای همگان رایگان است. بسیاری از افرادی که تاکنون فاقد هویت دیجیتال بوده‌اند، در سایه این ابتکار اکنون دارای آی‌دی هستند.

بانک آی‌دی-سوئد
دولت سوئد با همکاری و پشتیبانی برخی از سازمان‌های مالی، سیستم بانک آی‌دی را به عنوان یک سیستم قانونی تایید هویت به رسمیت شناخته که قادر است هویت افراد مرتبط با سیستم‌های بانکداری را شناسایی و تایید کند.

شهر آنتورپ-بلژیک
راه‌اندازی آزمایشی مبتنی بر فناوری دفتر کل توزیع شده به منظور قادر ساختن کاربران برای مدیریت هویت‌های دیجیتال خود.

کارت هوشمند بریتیش کلمبیا
بریتیش کلمبیا استانی است که کارت هوشمند بی‌سی سرویسز کلمبیا (BC Services Card) را به شهروندان خود ارائه می‌دهد. کارتی سه منظوره که همزمان گواهینامه رانندگی، کارت سلامت و آی‌دی کارت الکترونیک کاربران را پوشش می‌دهد.

سازمان غذا و دارو آمریکا
سازمان غذا و داروی ایالات متحده آمریکا شرکت‌های ارائه دهنده دستگاه‌های درمانی و دارویی در این کشور را وادار ساخته است تا از استانداردهای خاصی برای اعتبارسنجی و تایید دستگاه‌ها پیروی کنند. این امر، ضمن کنترل ارائه دهندگان از کاربران یا بیماران در قبال ریسک‌های احتمالی محافظت می‌کند.

ام-کوپا کنیا
این سیستم پرداخت مدرن، فرایندهای پرداخت دیجیتال و فناوری اینترنت اشیا را در هم آمیخته است تا امکان ردیابی دارایی‌ها از راه دور و شناسایی افراد استفاده کننده از این دارایی‌ها را در اختیار کاربران و سازمان‌ها قرار دهد.

وزارت آموزش و پرورش و استخدام-مالتا
مالتا اقدام به استفاده از فناوری بلاکچین برای ثبت، نگهداری و تایید پرونده‌ها و گواهینامه‌های آموزشی کرده است که طی آن، سازمان‌ها، کارفرمایان و کارکنان می‌توانند داده‌های خود را به اشتراک گذاشته و صحت و سقم گواهینامه‌ها یا هویت‌های افراد را بررسی و اعتبارسنجی کنند.

فصل دوم:

منظور از خوب چیست؟

بهبود هویت دیجیتال

در سراسر دنیا، هنوز هم بخش عمده‌ای از افراد از هویت‌های دیجیتال محروم هستند و یا به دلیل عدم شمول از اکثر محصولات و خدماتی که حق آن‌ها است محروم مانده‌اند. بسیاری از سیستم‌ها، علیرغم این‌که هویتی دیجیتال به افراد بخشیده‌اند، اما نمی‌توانند دسترسی کاربران به برخی خدمات و محصولات مورد نیازشان را تامین کنند و این امر، به‌ویژه در کشورهای محروم و دور افتاده فراگیرتر نیز هست. بسیاری از این سیستم‌ها، هیچ کنترلی به کاربران روی داده‌ها و هویت‌های دیجیتالشان نمی‌دهند. بسیاری از افراد نیز با تبعیض ناشی از هویت‌های دیجیتالشان مواجه هستند که در اغلب موارد، به سرقت‌های هویتی یا سایر تهدیدهای سایبری می‌انجامد.

ما می‌توانیم با تعریف و پیروی از یک پارادایم جدید، شرایط را تغییر دهیم. هویت‌های دیجیتال، در آینده‌ای نه چندان دور نیازمند تلاش برای ایجاد ارزش فزون‌تر در کاربران و در عین حال تناسب با انتظارات مالکین شبکه خواهند بود که به دست‌اندرکاران اکوسیستم و اشخاص ثالث مرتبط با آن وابسته است. با تمرکز روی افراد، مالکین قادر خواهند بود تا سرویس‌دهی و ایجاد ارزش بهتری از خود ارائه دهند و پذیرش گسترده‌تری را برای سیستم‌های مبتنی بر هویت دیجیتال خود رقم بزنند.

پرواضح است که مالکین سیستم‌های هویتی، با مشارکت حوزه دولتی، بخش خصوصی و جامعه مدنی، به دنبال پیاده‌سازی پنج عنصر کلیدی موردنیاز برای موفقیت سیستم‌های خود هستند. پنج عنصری که در فصل نخست به اختصار مورد بحث و بررسی قرار گرفتند. در این فصل، توصیفی روشن و مفصل از هر یک از این عناصر ارائه خواهیم داد و این‌که منظور از خوب، به معنی واقعی کلمه چیست. ضمن این‌که مثال‌هایی از دنیای واقعی نیز ارائه خواهیم کرد که می‌توانند به درک بهتر موضوع کمک کنند.

همان طور که هر یک از پنج عنصر را مرور می‌کنیم و به تفصیل در مورد آن‌ها صحبت می‌کنیم، ضروری است که برخی ملاحظات و خط مشی‌ها را نیز مدنظر قرار دهیم:

هر یک از این پنج عنصر به یک اندازه دارای اهمیت و کاربر محور هستند.

کسی که به دنبال ایجاد ارزش برای کاربران و در ادامه موفقیت است باید بتواند هر پنج عنصر را توامان تامین کند.

این پنج عنصر به یکدیگر وابسته هستند و ممکن است یکی روی دیگری ساخته شود. به عنوان مثال، معیارهای حریم خصوصی قدرتمند امنیت را می‌سازند.

میان برخی از عناصر تنش وجود دارد.

ممکن است برخی از عناصر، نظیر امنیت، طراحان را با چالش‌های جدی مواجه کنند.

ممکن است ناچار باشید تراکنش‌ها و تعاملات را مدیریت کنید.

تنها راه دستیابی به موفقیت در ایجاد ارزش برای کاربران این است که چالش‌های هر پنج عنصر با توجه به زمینه‌های فرهنگی و حقوقی پاسخ داده شوند. در این فصل، قصد داریم بهترین راهکار برای پاسخگویی به این چالش‌ها را عنوان کرده و مثال‌هایی واقعی از دنیای واقعی برای هر عنصر ارائه کنیم. این مثال‌ها، لزوما بهترین راهکارها را نشان نمی‌دهند، اما می‌توانند در شکل‌گیری بینش در شما کمک کننده باشند.

شکل شماره ۵: پنج عنصر موردنیاز برای طراحی هویت دیجیتال کاربر محور

۱. متناسب با هدف

یک سیستم هویتی متناسب با هدف سیستمی است که موارد زیر را ارائه دهد:
دقت: جای هیچ‌گونه خطایی در داده‌های هویتی وجـود ندارد. این دقت در تمام جزئیات مهم است و باید به‌روزرسانی شود.
منحصربه‌فرد بودن: شکی نیست که در میان طیف گسترده‌ای از کاربران یک سیستم هویتی، هر یک از افراد منحصربه‌فرد هستند. نیاز به منحصربه‌فرد بودن به ویژه در تراکنش‌هایی که سطح بالایی از ریسک را تجربه می‌کنند غیرقابل انکار است و این مهم نیز مستلزم تضمین هویت قوی‌تر است.
پایداری: بقای سیستم‌های هویتی دیجیتال مستلزم بهره‌مندی از مدل‌های مالی قوی و رویکرد مبتنی بر فناوری و سیاست‌هایی است که بتواند در آینده نیز به حیات خود ادامه دهد.
مقیاس‌پذیری: سیستم‌ها باید بتوانند همسو با ارتقای انتظارات و تقاضا رشد کنند.

این عنصر چرا اهمیت دارد؟

دقت و منحصربه‌فرد بودن پیش‌نیازهای تایید هویت و احراز هویت یک فرد هستند. در صورتی که داده‌های هویتی موجود در سیستم دقیق نباشند، افراد و سازمان‌های وابسته قادر به اعتماد و پذیرش سیستم نخواهند بود.
مقیاس‌پذیری و پایداری نیز سیستم‌های هویتی را برای افراد جذاب‌تر می‌کنند و انگیزه لازم برای شرکت سازمان‌ها و طرفین ثالث در سیستم را فراهم می‌کنند. برای کسب اطمینان از اثربخشی در آینده، سیستم‌ها باید بتوانند در فناوری، چشم‌انداز ریسک‌ها و تهدیدات، سیاست‌ها و چشم‌انداز فرهنگی و سیاسی سرمایه‌گذاری کنند و همسو با رشد انتظارات کاربران خود را ارتقا دهند.

منظور از خوب چیست؟

تثبیت منحصربه‌فرد بودن

منحصربه فرد بـودن، در عین حـال که به کاهـش تقلبات و تخلفـات هویتی می‌انجامد، هویت‌های دیجیتال را قابل اطمینان‌تر نیز می‌کند.
راه‌های زیادی برای تثبیت و توسـعه منحصربه‌فرد بودن هویت‌های دیجیتال بین توده کاربران وجود دارد. یک راهـکار جامع که امروزه نیز که مورد اسـتفاده قرار می‌گیرد، اعطـای نام‌های کاربری منحصربه‌فرد به کاربران، درسـت مانند آن‌چه که در حساب‌های کاربری یا در کارت‌های اعتباری و... مشاهده می‌کنید و تلفیق این نام‌های کاربری با رمزهای به اشـتراک گذاشته اسـت و در ادامه، گردآوری و ثبت مجموعه‌ای از داده‌های چندگانه اعم از لوکیشن، آی‌پی آدرس و یا تاریخچه فعالیت کاربران و ترکیب آن‌ها با این گذرواژه‌ها و نام‌های کاربری است. روش رایج دیگری که وجود دارد، اسـتفاده از داده‌ها یا مشخصات بیومتریک کاربران است. برخی از ویژگی‌های منحصربه‌فرد و ذاتی افراد مانند ویژگی‌های چهره، اثر انگشت یا اسکن‌های عنبیه جزو همین مشخصات بیومتریک هستند.
با این حال، علیرغم این‌که مشـخصات بیومتریک کاربران دارای تضمین هویتی بالایی هستند، اما مستلزم احتیاط، آموزش و ورزیدگی عملیاتی هستند. در صورتی که طراحی ضعیف باشد، ممکن اسـت به محرومیت یا حذف کابران از سیستم بیانجامد. کیفیت اثرانگشـت‌های دریافتی از کاربران ممکن است در طول زمان افت پیدا کند. ضمن این‌که در مورد کارگرانی که با دست کار می‌کنند، افرادی دارای زخم در انگشتان خود هسـتند یا از نقص عضو رنج می‌برند، چالش‌های جدی مواجه سیسـتم احراز هویت و تایید هویت بیومتریک خواهد بود تا زمانی که این قبیل مشکلات به نحو درست پاسخ داده شوند. با توجه به این‌که داده‌های بیومتریک کاربران از جمله اطلاعات منحصربه‌فرد، قابل شناسـایی، حساسـا و شخصی کاربران هستند، الزامات و ملاحظات امنیتی و حریم خصوصی پیرامون آن‌ها باید به شکل کاملا بی‌عیب‌ونقصی پیاده‌سازی شوند.
توصیه می‌شود که تلفیقی از این راهکارها را به کار ببندید یا بسته به نوع تعاملات، سطح ریسـک‌پذیری سـازمان، الزامان انطباقی و رگولاتوری و سطح اطمینان از داده‌ها و تراکنش‌هـا مدل‌های مختلفی را برگزینید. به عنـوان مثال، برای دریافت ویزای مسافرتی داده‌های مورد نیاز، در میان سایر داده‌های هویتی ممکن، عبارت خواهند بود از نام، تاریخ تولد، تاریخچه سـفری، و برخی مشخصات بیومتریک نظیر اثر انگشـت و تصویر چهره کاربران. در حالت کلی، برای کسب اطمینان از صحت و سقم و اعتبار داده‌ها، بهترین رویکرد این است که داده‌های منحصربه‌فرد را در اولویت قرار دهید.

مشارکت‌های دولتی - خصوصی

سیسـتم‌های هویتی نیازمنـد نوآوری‌های مبتنـی بر فنـاوری، چارچوب‌های رگولاتوری، پذیرش و اعتماد عمومی گسـترده و طراحی هسـتند که به سیسـتم انطباق با نیازهای کاربران و پایداری مالی در دراز مدت بدهد. چنین سیستم‌هایی، کاندیداهایی ایده‌آل برای مشـارکت‌های دولتی - خصوصی خواهند بود که نقش همه افراد در آن‌ها از پیش تعیین شده است و انگیزه‌های مشارکت نیز کاملا واضح و مبرهن است. این مشارکت می‌تواند شامل مواردی اعم از تسهیم مسئولیت‌های مالی، همکاری با هم برای طراحی کاربر محور، مالکیت مشـترک سیسـتم‌های مبتنی بر هویت دیجیتال و داده‌ها و دسـتاوردهای آن‌ها، شناخت متقابل از هم و تعامل‌پذیری بین سیستم‌ها و در نهایت ساختن اکوسیستمی باشد که ارزش بیشتری را برای طرفین ایجاد می‌کند.

مدل کسب‌وکار پایدار

سیسـتم‌های مبتنی بر هویت دیجیتال مسـتلزم قابلیت‌های مالـی بلندمدت و طول عمر عملیاتی مفید هستند و در همین راسـتا، مدل‌های کسب‌وکاری پایدار فراوانی نیز در دست ظهور و توسـعه‌اند. مثال‌های بارزی که می‌توان عنوان کرد، کنسرسیوم‌های مبتنی بر اعتماد و ارائه دهندگانی هسـتند که هزینه‌ها و داده‌های هویتی خود را با یکدیگر به اشتراک گذاشـته‌اند تا بتوانند برای کاربرانشان ایجاد ارزش کنند. این به اشـتراک گذارندگان هم می‌توانند شامل سازمان‌ها و دولت‌ها شـوند و کاربران را مورد خطاب قرار دهند و تعداد آن‌ها نیز هـر روز رو به فزونی می‌گذارد. با این حال، این نکته نیز مهم اسـت که انگیزه‌های مالی این مدل‌های کسب‌وکار حقوق افراد را پایمال نکنند و حق انتخاب و کنترل آن‌ها روی داده‌هایشان را در معرض ریسـک قرار ندهند. برای این‌که سیسـتم‌های هویتی در طول زمان پایدار باقی بمانند، نیازمند تغییر زیرسـاخت‌ها و مدل‌های کسـب‌وکاری خود مطابق با تحولات تقاضای کاربران خواهنـد بود تا بتوانند با عملکرد و تجربه‌های نوین کاربران سازگار باشند. در ضمن، مدل‌های کسب‌وکار انتخاب شده باشد با تحولات و انقلاب‌های تکنولوژیکی نیز سازگار باشند و از فناوری‌های مدرن آینده برای تجربه‌ای بدون درز و امنیت سایبری پشتیبانی کنند. نقص‌های امنیتی می‌تواند سیستم را از هر دو بعد اعتماد و کارایی با مشکلات جدی و ناکارآمدی مواجه کرده و پایداری آن در طول زمان را خدشه‌دار کند.

مثال‌هایی از دنیای واقعی

مشارکت‌های دولتی - خصوصی: بانک آی‌دی سوئد
در کشور سوئد، موسسات مالی اقدام به راه‌اندازی یک سیستم هویتی مدرن تحت عنوان بانک آی‌دی کرده‌اند، که دولت نیز آن را به عنوان مرجعی قانونی برای اسناد، تراکنش‌ها و غیره مالی به رسمیت شناخته است. هم مقامات دولتی و هم کاربران از این سیستم هویتی برای خدمات عمومی و خصوصی مورد نظر خود استفاده می‌کنند. این مشارکت بخش خصوصی با دولت، توانسته است ۷/۵ میلیون کاربر فعال جذب کند.

ثبات مالی: نادرا (NADRA) در پاکستان
اداره ملی ثبت احوال پاکستان، آی‌دی کارت‌های رایگانی برای شهروندان کم بضاعت خود طراحی و ارائه کرده است که به کاربران اجازه می‌دهد تا بدون پرداخت هیچ هزینه‌ای از هویت دیجیتال بهره‌مند شوند. درآمد این کارت‌ها، از کارمزدهای اندک اما گسترده‌ای است که از برخی فرایندها نظیر افتتاح حساب بانکی به دست می‌آید. ارائه دهندگان خدمات، نظیر بانک‌های کشور که برای تایید هویت کاربران خود به این کارت‌ها و داده‌های کاربران آن‌ها نیاز دارند این کارمزدها را پرداخت می‌کنند. این ساختار به اداره ملی ثبت احوال پاکستان کمک می‌کند تا بدون نیاز به بودجه دائمی دولت، روی فناوری سرمایه‌گذاری کند.

فعال‌سازی هویت‌های مهاجران: سازمان ملل متحد
کمیساریای عالی سازمان ملل متحد برای پناهندگان یک سیستم مدیریت هویت بیومتریک جدید راه‌اندازی کرده است. بر اساس سیاست ثبت‌نام تایید هویت بیومتریک پناهندگان در سال ۲۰۱۰ میلادی، مشخصات بیومتریک این قابلیت را دارند تا به صورت روتین بخشی از احراز هویت و تایید هویت پناهندگان باشند تا اطمینان حاصل شود که هویت‌های این افراد گم یا حذف نمی‌شود، چندین بار ثبت نمی‌شود و در معرض تقلب یا سرقت هویتی قرار نمی‌گیرد. از ماه می سال ۲۰۱۸، سیستم مدیریت هویت بیومتریک کمیساریای عالی سازمان ملل متحد برای پناهندگان در قالب سیستم ایریش گارد در منا جامه عمل پوشیده است و تاکنون بیش از ۵ میلیون کاربر را ثبت‌نام کرده است.

۲. همه‌جانبه

برای مشمولیت همه کاربران و اعطای اختیار به آن‌ها برای دسترسی به هر محصول یا خدماتی که نیاز دارند، سیستم‌های هویتی باید بتوانند الزامات زیر را فراهم کنند:

فرصت‌های مساوی: هر فردی که در اکوسیستم وجود دارد باید بتواند از هویت دیجیتال ثبت شده و قابل تایید بهره‌مند شود.

حفاظت از تبعیض: هیچ کس نباید با مانعی برای تثبیت و یا استفاده از هویت دیجیتال خود روبه‌رو باشد و جای هیچ‌گونه تبعیض یا محرومیت وجود ندارد.

سازوکارهایی برای پیامدهای غیرمنتظره و سهوی: نظیر استانداردهای امنیتی و داده‌هایی که مانع ورود، حضور یا محرومیت برخی از افراد به اکوسیستم مبتنی بر هویت دیجیتال می‌شوند.

این عنصر چرا اهمیت دارد؟

دستیابی به دسترسی جهانی و شمول به پذیرش جهانی و گسترده می‌انجامد و از تکه تکه شدن‌های دیجیتالی می‌کاهد. چنین دستاوردی در عین سرعت بخشیدن به توسعه درونی سیستم، به توسعه اقتصادی محیط بیرون نیز کمک می‌کند. ضمن این‌که استفاده گسترده ثبات و پایداری می‌آورد و به سیستم‌های هویتی این امکان را می‌دهد تا از پایگاه کاربری خود مزایای هنگفتی از آن خود ساخته و در سایه این مزایا مدل‌های عملیاتی موفق‌تری را طراحی و عرضه کنند.

منظور از خوب چیست؟

قابلیت دسترسی و چندگانگی

این‌که افراد بتوانند فارغ از موقعیت دموگرافیکی یا اجتماعی و اقتصادی که در آن قرار دارند، در هر سیستم هویتی که انتخاب کرده‌اند به راحتی شرکت کنند یک الزام است. برای افزایش و توسعه شمول، نقاط ورودی مختلف و چندگانه‌ای می‌توانند تعریف شوند تا به همه افراد این امکان را بدهند که به آن‌چه که نیاز دارند دسترسی داشته باشند. گزینه‌های نام‌نویسی و ثبت‌نام دیجیتال می‌توانند در شمول کاربرانی که از راه دور تمایل به ورود به سیستم دارند را تسریع و تسهیل کنند. در حالت کلی، ثبت‌نام اجباری افراد در سیستم‌های هویتی و اعطای یک هویت دیجیتال منفرد به هر فرد، نمی‌تواند به مفهوم شمول گسترده بیانجامد و هر فردی باید قادر باشد، بسته به نیازها و تمایلاتی که دارد، نگرانی‌هایی که دارد و حقوقی که به وی تعلق می‌گیرد، سیستم موردنیاز خود را از میان سیستم‌های هویتی متنوع و چندگانه انتخاب نماید. فقدان چنین چندگانگی می‌تواند به منزله فقدان انتخاب و اشکال جدیدی از محرومیت باشد.

طراحی برای همه

برای جلوگیری از محرومیت یا به حاشیه رانده شدن افراد، سیستم‌های مبتنی بر هویت دیجیتال باید به گونه‌ای طراحی شده باشند که کلیه طیف‌های فرهنگی، مهارتی، سنی، سواد دیجیتالی، دسترسی به فناوری و استفاده‌های موردی را پوشش دهند. برای بسط دادن شمول، این قبیل سیستم‌ها می‌توانند نقاط ورود چندگانه‌ای را تعریف کرده و راه‌های متعددی برای استفاده از هویت‌های دیجیتال ارائه دهند. به عنوان مثال، گزینه‌های استفاده و ثبت‌نام آفلاین برای کاربرانی که فاقد اینترنت مناسب در موقعیت جغرافیایی خود هستند می‌تواند به شمول بیشتر در سطح جهانی بیانجامد. یا پذیرش طیف گسترده‌ای از مدارک و شواهد برای تثبیت هویت دیجیتال می‌کند بخشی از محدودیت‌های این قبیل سیستم‌ها برای افراد را کاهش دهد و شمول بیشتر بیانجامد.

ضمن این‌که طراحان نیز باید این موضوع را مدنظر قرار دهند که چگونه می‌توانند از فناوری‌های مدرن در راستای ارتقای شمول بهره بجویند، در عین این‌که این فناوری‌ها منجر به تکه تکه شدن دیجیتالی یا پیامدهایی نظیر افزایش هزینه‌ها مثل هزینه‌های گزاف خرید گوشی‌های تلفن همراه هوشمند و غیره، افزایش تقاضا برای زیرساخت‌های واهی، نظیر دسترسی به اینترنت داده ۴G در نقاطی که هنوز فعال نشده است، یا موانع سازگاری، همچون معرفی هر فرد برای استفاده از یک سیستم و خدمات آن، نشوند. درگیری با کاربران در حین طراحی می‌تواند این اطمینان را ایجاد کند که سیستم طراحی شده، پاسخگوی نیازهای هویتی همه افراد است و شمول و قابلیت دسترسی در آن رعایت شده است.

حداقل داده‌ها

طراحی درست می‌تواند تبعیض‌ها یا عواقب ناخواسته ناشی از گردآوری، استفاده یا افشای داده‌هایی که برای یک تراکنش خاص داده شده‌اند را کاهش دهد. به عنوان مثال، در سیستم‌هایی که فرد برای ورود و استفاده از خدمات به لحاظ دارا بودن سن قانونی اعتبارسنجی می‌شود، دیگر نیازی نیست طرف در تعامل با کاربر سن او را ببیند یا نام و نشان او را مشاهده کند. این اصل، به‌ویژه در مورد اطلاعاتی که ممکن است سبب آسیب‌رسیدن به کاربران شوند از اهمیت بالایی برخوردار است. به عنوان مثال، شاید بهتر باشد برخی از سیستم‌های هویتی، نسبت به گردآوری، ثبت، استفاده و افشای داده‌های موقعیت مکانی و مذهبی کاربران اقدام نکنند چرا که چنین داده‌هایی می‌توانند منجر به تبعیض، آزار یا حتی شکنجه کاربران شوند. داده‌های سیاسی نیز از این قضیه مستثنی نیستند.

استانداردهایی برای شمول

یک سیستم مبتنی بر هویت دیجیتال می‌تواند در صورت پیروی از برخی استانداردهای داده‌های هویتی و پایبندی به برخی الگوهای اعتمادی متداول که عموم کاربران نیز به آن اشراف دارند و از آن تبعیت می‌کنند به شمول دست

پیدا کند. در غیر این صورت، امکان این‌که داده‌های هویتی کاربران رد شـــوند یا اعتماد اشخاص ثالث وابســـته به ارائه دهندگان به برخی از داده‌ها و هویت‌های دیجیتال باعث بروز تبعیض میان کاربران شود بالا خواهد بود. این استانداردها می‌توانند به شکل فعالانه‌ای حفره‌ها و شکاف‌های احتمالی موجود در سیستم‌های هویتی را که به محرومیت یا تبعیض می‌انجامند شناسایی کرده و برطرف کنند. اســـتانداردهایی که به منظور حفاظت از کاربـــران و رضایتمندی آن‌ها طراحی و ارائه شـــده‌اند و آن‌ها را قادر می‌ســـازند تا روی داده‌ها، حقوق، امنیت و حریم شخصی‌شان کنترل داشته باشند.

تاثیر بسزای کانال‌های توزیع

در صورت استفاده از کانال‌های توزیع قدرتمند و بهره‌مندی از فناوری‌های روز دنیا، دسترسی به طیف وسیعی از افراد در اقصی نقاط جهان چندان هم دور از ذهن نیست. به ویژه در حضور کانال‌های تاثیرگذاری همچون گوشی‌های تلفن همراه، که اکنون به بخشی لاینفک از زندگی کاربران تبدیل شده‌اند. ورود و بهره‌برداری از کانال‌های توزیع مدرن کنونی می‌تواند راهکاری خارق‌العاده برای شمول در سطح جهانی باشد.

مثال‌هایی از دنیای واقعی

قابلیت دسترسی: اینترنت اشیا در کنیا

در کشور کنیا، سنسورهای اینترنت اشـــیا به ارائه دهندگان خدمات پرداخت کمک می‌کنند تا در پمپ بنزین‌ها کاربران و پرداخت‌هـــای آن‌ها را مدیریت کنند. ضمن این‌که این سنســـورها به کاربران این امکان را می‌دهند تا صورت‌حساب‌های خود را با اســـتفاده از کیف پول‌های موبایلی‌شـــان پرداخت کنند. به علاوه، این قابلیت نیز وجود دارد تا با ایجاد پروفایل‌های هویتی، بـــه خدمات و محصولات مالی نیز دسترسی داشته باشند.

ثبت‌نام آسان: ادهار در هندوستان

به نظر شما چطور می‌توان بیش از ۱٫۳ میلیارد کاربر را در یک سیستم هویتی ثبت‌نام کرد؟ سیستم هویتی بیومتریک ادهار که توســـط دولت هندوستان راه‌اندازی شده است، در حال ثبت‌نام طیف گسترده‌ای از کاربران و شهروندان این کشور است و برای ثبت‌نام، مدارک و مشخصات گیسترده‌ای را نیز می‌پذیرد. در ضمن، این سیستم برای افرادی که سابق بر این فاقد هویت دیجیتال بوده‌اند نیز برخی گزینه‌های پیشنهادی ارائه می‌دهد. گوشـــی‌های تلفن همراه، وظیفه ثبت‌نام بخـــش عمده‌ای از کاربران مناطق دورافتاده و روستایی کشور را بر عهده دارند و با وجود فقدان اینترنت در برخی نواحی، کاربران را تحت پوشش قرار می‌دهند و این در حالی است که این ثبت‌نام، فاقد هرگونه هزینه برای کاربران است. بین سال‌های ۲۰۰۹ تا ۲۰۱۸ میلادی، بالغ بر ۱٫۲۱ میلیارد کاربر یعنی ۹۹ درصد جمعیت هندوستان در سیستم ادهار ثبت‌نام کرده‌اند. با این وجود، هنوز هم مشـــاجرات و مباحث قانونی و سیاست‌گذاری‌ها پیرامون این پروژه در هند برقرار است تا تعادل لازم بین آزادی‌های کاربران و حقوق آن‌ها با سیستم هویتی کشور برقرار شود.

۳. سودمندی

برای افرادی که به دنبال استفاده از هویت‌های دیجیتال هستند، یک سیستم هویتی باید بتواند الزامات زیر را ارائه دهد:

کاربردپذیری: یک سیســـتم هویتی خوب باید بتواند دسترســـی افراد به طیف گســـترده‌ای از محصولات، خدمـــات و تراکنش‌های دیجیتـــال را فراهم کند و کاربردپذیر باشد.

تسهیلات: تسهیلات یک سیستم هویتی شامل استفاده، ثبت‌نام و مدیریت آن می‌شود.

سهولت در استفاده: سهولت در استفاده بیشـــتر بـــه فرایندهای احراز هویت و تایید هویت در سیستم‌های هویتی برمی‌گردد و رعایت کم‌ترین میزان اصطکاک ممکن در این فرایندها.

تعامل‌پذیری و پرتابل بودن: سیســـتم‌های مبتنی بر هویت دیجیتال باید بتوانند در سطح همه صنایع، خدمات، حوزه‌ها و موقعیت‌های جغرافیایی کار کنند و در عین حال، تعامل‌پذیری، الزامات امنیتی و حریم خصوصی را نیز رعایت کنند.

این عنصر چرا اهمیت دارد؟

کاربردپذیری، تسهیلات، سهولت در استفاده، تعامل‌پذیری و پرتابل بودن نه تنها زندگی را برای کاربران ساده‌تر می‌کنند، بلکه شانس پذیرش سیستم توسط افراد و سازمان‌ها را نیز افزایش می‌دهد. بدیهی اســـت که در این صورت، انگیزه برای استفاده از چنین سیســـتم‌های هویتی بالاتر رفته و در نهایت، به توسعه و شمول گسترده سیستم می‌انجامد.

پذیرش گسترده نیز به نوبه خود، نه تنها می‌تواند به ثبات مالی بیانجامد، بلکه سبب ارتقای کارایی نیز می‌شـــود. با هویت‌های دیجیتالی که در طول تمامی حوزه‌ها پذیرفته شده‌اند و مرزهای جغرافیایی را پشت سر گذاشته‌اند، افراد به هویت‌های کمتری برای انجام تعامـــلات و تراکنش‌های خود نیاز خواهند داشـــت. همین هویت‌های کمتر، به نوبه خود، به معنی ســـیلوهای مبتنی بر داده کمتر، تکه تکه شدن‌های دیجیتال کمتر و در حالت کلی ریسک‌ها و ناکارآمدی‌های کمتر است.

منظور از خوب چیست؟

خدمات دیجیتال غالبا پا فراتر از محدودیت‌های سیاسی و جغرافیایی گذاشته‌اند و افراد سراسر جهان، دولت‌ها، کشورها، صنایع، کسب‌وکارها و بخش‌های عمومی و خصوصی را در هم تنیده‌اند. اما هویت‌های دیجیتال از چنین قابلیتی برخوردار نیستند. به عنوان مثال، زمانی که در صدد اجازه یا خرید یک آپارتمانی برای خود در یک شکور خارجی هستید، ممکن اســـت صاحبخانه قبض برق یا تاریخچه اعتباری شما را قبول نداشته باشد.

به رســـمیت شـــناختن مشـــترک یکدیگر، که طی آن مـــدارک و گواهینامه‌ها یا اســـتانداردهای ارائه شده از ســـوی یک طرف توسط ســـایر طرفین ارائه دهنده خدمات یا هویت‌ها مورد اعتماد قرار می‌گیرد و به رســـمیت شـــناخته می‌شود، می‌تواند همکاری‌ها و تعاملات را بهبود بخشیده، ســـرعت بیشتری بدهد و در عین حال هزینه‌ها و اصطکاک‌های تعاملات برون‌مرزی و برون‌حوزه‌ای را نیز به شدت کاهش دهد. سیستم‌های تعامل‌پذیر، که قابلیت تعامل و تبادل اطلاعات با یکدیگر را دارند و به هم اعتماد دارنـــد، راحتی را افزایش می‌دهند. با این حال، طراحان هنوز هم باید ریســـک‌هایی را که از این تعامل‌پذیری ناشـــی می‌شوند مدنظر قرار دهند. بدیهی است که یک سیستم متصل، دارای ریسک‌ها و تهدیدات سایبری و امنیتی بیشتری نسبت به سیستم‌های بسته و منفرد است.

ارزشی در مقیاس گسترده

هویت‌های دیجیتال، در صورتی که نتوانیم آن‌ها را در سطح طیف گسترده‌ای از خدمات و تراکنش‌هایی که کاربران به آن‌ها نیاز دارند پیاده‌سازی کنیم، بی‌معنی خواهند بود. با وجود این‌که هر تراکنشی نیاز به هویت دیجیتال ندارد، اما زمانی که هویت‌های دیجیتال بسیاری از فرایندها و تراکنش‌ها را تسهیل می‌کنند، افراد تمایل بیشتری برای اســـتقبال از آن‌ها خواهند داشت. این سهولت و راحتی برای کاربران، مستلزم بازنگری در ســـبک زندگی آن‌ها، رفتارهای آن‌ها و هنجارهای فرهنگی‌شـــان دارد تا انگیزه‌های احتمالی کاربران برای اســـتفاده از هویت‌های دیجیتال بیش از پیش ارزیابی شده و مورد بهره‌برداری قرار گیرند. عاقلانه است که از اشتباهات معمول نظیر سیستم‌های هویتی خاص، یا فرایندهای اثبات هویت پیچیده و زمان‌بری که هیچ الزامی نیز برای آن‌ها وجود نداشته است نیز پیش‌گیری شود، تا انتخاب کاربران، انگیزه آن‌ها و ارزشی که قرار است برای آن‌ها رقم بخورد دستخوش آسیب نشود.

ارزش در طول زمان

ممکن است آن‌چه که امروز برای کاربران ارزشمند است، فردا دیگر نباشد. برای سیستم‌های مبتنی بر هویت دیجیتال، ادامه ارائه ارزش به کاربران، مستلزم نظارت و ارزیابی مداوم نیازها و انتظارات آن‌ها در طول زمان است.

اصطکاک مناسب

تراکنش‌های پیچیده‌ای که از ریسک بالایی برخوردار هستند، ممکن است به ارزیابی‌ها و طیف گسترده‌ای از اسناد و داده‌ها نیاز داشته باشند، اما در این میان، برخی از تراکنش‌ها نیز وجود دارند که به ارزیابی‌ها و داده‌های به مراتب کمتری نیاز دارند و فرایندهای احراز هویت و تایید هویت در مورد آن‌ها ساده‌تر است. زمینه و موارد کاربردی می‌تواند سطح سخت‌گیری و اصطکاک را برای تایید هویت و احراز هویت مشخص کند. در برخی موارد، مشارکت‌های بخش خصوصی و دولتی می‌توانند با کاهش فرایندهای احراز هویت و تایید هویت کاربران، اصطکاک موجود در زیرساخت‌های خدماتی را کاهش دهند.

مثال‌هایی از دنیای واقعی

عبور از مرزها و شناخت متقابل: eIDAS، اتحادیه اروپا

سیستم رگولاتوری eIDAS اتحادیه اروپا، استانداردهایی را برای امضاهای دیجیتال، گواهینامه‌های واجد شرایط بودن دیجیتال، مهر و موم‌های دیجیتالی، تایم‌استمپ‌ها و سایر فرایندها و مکانیسم‌های تایید و احراز هویتی تبیین کرده است که به سازمان‌های مستقر در اتحادیه اروپا کمک می‌کند تا از سیستم‌های هویتی و فرایندهای اعتبارسنجی در کمال امنیت و اطمینان استفاده کنند. بدیهی است که چنین رویکردی اعتماد به تراکنش‌ها و تعاملات برون‌مرزی را نیز ارتقا خواهد بخشید، تعامل‌پذیری را افزایش خواهد داد، هویت‌های تکراری را از اکوسیستم حذف کرده و کاهش خواهد داد و سیستم‌های مبتنی بر هویت دیجیتال را در اقصی نقاط جهان و در اغلب حوزه‌ها قابل استفاده خواهد ساخت.

ادغام با زندگی روزمره: تی-اوث، کره جنوبی

اپراتورهای قدرتمند تلفن همراه در کره جنوبی، یک راهکارهای مبتنی بر هویت دیجیتال مشترک راه‌اندازی کرده‌اند. این شبکه، پس از این‌که مشتریان مجوز ورود به آن را پیدا می‌کنند، شماره تلفن کاربران و سایر داده‌های هویتی مربوط به آن‌ها را ثبت کرده و به اشتراک می‌گذارند. کاربران با وارد کردن یک پین کد در گوشی‌های تلفن همراه‌شان، ازفرایند تایید هویت این سیستم عبور کرده و به راحتی می‌توانند تراکنش‌های خود را انجام دهند. این سهولت و راحتی، به پذیرش سیستم به شکل معجزه‌آسایی کمک کرده است، به طوری که بالغ بر ۹۹ درصد از سایت‌های کره جنوبی، و بیش از ۳۰،۰۰۰ ارائه دهنده خدمات نظیر بانک‌ها، ارائه‌دهندگان محتوا و رسانه‌های اجتماعی آن را پذیرفته و مورد استفاده قرار داده‌اند. بیش از ۱۵ میلیون کاربر فعال ماهانه تراکنش‌های خود را از طریق این سیستم هویتی جذاب انجام می‌دهند و حجم تراکنش‌های سالانه آن را به رقم ۶۵۰ میلیون دلار رسانده‌اند.

۴. ارائه حق انتخاب

اصول انتخابی برای یک سیستم هویتی عبارتند از:

شفافیت: در سایه این شفافیت، کاربران قادر واهند بود تا افراد و سازمان‌هایی که در پی گردآوری و افشای اطلاعات هویتی‌شان هستند را شناسایی کرده و در مورد این‌که چگونه این داده‌ها پردازش می‌شوند و مورد بهره‌برداری قرار می‌گیرند، یا برای چه اهدافی از آن‌ها استفاده می‌شود آگاهی می‌یابند.

حریم خصوصی: سیستم‌های هویتی باید بتوانند حریم خصوصی افراد را در فناوری‌ها و فرایندها تامین کنند. ضمن این که افراد نیز باید بتوانند در مورد این‌که که کسانی قابلیت استفاده از داده‌های هویتی آن‌ها را دارند، برای چه اهدافی می‌توانند از این داده‌ها استفاده کنند و تا چه زمانی این دسترسی می‌تواند ادامه داشته باشند حق انتخاب داشته باشند و هر زمان که نیاز داشته باشد، داده‌ها را به‌روزرسانی کرده یا امحا نمایند.

حفاظت از داده‌ها: طراحی مبتنی بر فناوری، کنترل‌های عملیاتی و مدیریت‌های رگولاتوری، همه و همه باید به نحوی باشند که داده‌های هویتی کاربران را از افشا، نقص، نشت و یا نابودی مصون دارند.

کنترل کاربری: این‌که کاربران بتوانند در مورد نحوه بهره‌برداری از داده‌های هویتی خود، میزان دسترسی و هدف دسترسی حق انتخاب داشته باشند و فرایندهای گردآوری، پردازش و استفاده از داده‌ها را رصد کنند بسیار مهم است. هرچند که این کنترل، هرچه بالاتر می‌رود چالش‌ها، ریسک‌ها و فرصت‌های بیشتری را نیز پیش روی کاربران قرار می‌دهد.

این عنصر چرا اهمیت دارد؟

طراحی یک سیستم مبتنی بر هویت دیجیتال مدرن می‌تواند حقوق افراد را که در اعلامیه جهانی حقوق بشر در سال ۱۹۴۸ میلادی نیز توصیف شده، پایمال کرده یا ضمانت کند. در حال حاضر، شاهد تقاضای فزاینده کاربران برای افزایش کنترل روی داده‌های شخصی‌شان هستیم. در سیستم هویتی که بتواند به این تقاضا پاسخ دهد، با اعتمادی پرشتاب روبه‌رو خواهد شد، خطر ابتلا به سوء استفاده یا دستکاری را به حداقل خواهد رساند، و از پذیرشی فوق‌العاده لذت خواهد برد. در این میان، رگولاتورها نیز توامان روی حریم خصوصی و امنیت متمرکز شده‌اند.

منظور از خوب چیست؟

خود مدیریتی (Self-management)

توانمندسازی افراد برای مدیریت حرفه‌ای داده‌ها و هویت‌های دیجیتال خود، یک ابزار حریم خصوصی قدرتمند است که به آن‌ها اجازه می‌دهد تصمیم‌گیری کنند چه کسانی می‌توانند به داده‌های آن‌ها دسترسی داشته باشند یا آن‌ها را به اشتراک بگذارند، هرگونه تغییر در داده‌ها یا سیستم را شناسایی کنند، و به دیگران حق پردازش داده‌ها و نتیجه‌گیری بدهند یا آن‌ها را رد و منع کنند. کاربران باید در تمام تراکنش‌ها حق انتخاب باشند تا بتوانند تراکنش‌ها و گزینه‌هایی را برگزینند که حقیقتا به آن نیاز دارند. با این حال، گاهی ممکن است نیاز به حق انتخاب، با نیازهای امنیتی و حمایتی دیگری نیز عجین شده باشد. نیازهایی از قبیل نیاز به بررسی‌های جرایم سایبری، امنیت ملی یا امثال آن. هنگامی که کاربران از به اشتراک‌گذاری داده‌های هویتی خود مزایای مستقیمی را دریافت می‌کنند؛ مانند دریافت تخفیف از فروشگاه‌ها و غیره، لازم است که هر دو هم به اشتراک‌گذاری را مدنظر داشته باشند، هم مزایا و دستاوردهای آن را، و هم ملاحظات امنیتی و حریم خصوصی آن را. رابط‌های دیجیتال و فرایندهایی که به کاربران کمک می‌کنند تا اطلاعات خود را با رضایت کامل به اشتراک بگذارند، باید متناسب با سطح ارزش خدماتی باشند که قرار است به کاربران ارائه شوند و ریسک‌های بالقوه این افشای اطلاعاتی را مدنظر قرار دهند. در غیر این‌صورت، ممکن است منجر به آسیب رسیدن به کاربران، عدم تمایل آن‌ها و افت پذیرش سیستم شود.

حمایت‌های قانونی

مقررات، به‌ویژه آن دسته از مقررات که حفاظت از داده‌ها و چارچوب‌های حریم خصوصی را دنبال می‌کنند، یک پیش‌شرط لازم و ضروری برای پیاده‌سازی سیستم‌های هویتی هستند. ممکن است رگولاتورها، به دنبال پیاده‌سازی سیستم‌های مبتنی بر هویت شفاف و شکل‌دهی هویت‌های دیجیتال به شکلی باشند که در بالا نیز عنوان شد. این در حالی است که عموم دولت‌ها و بخش‌های خصوصی نیز به دنبال سطح بالایی از حریم خصوصی، به‌ویژه در مورد داده‌هایی هستند که امکان نشت آن‌ها به ملل خارجی وجود دارد. بر همین اساس، طراحان باید چارچوب‌های رگولاتوری ویژه هویتی، داده‌های مبتنی بر حریم خصوصی

و مرتبط با داده‌های عمومی، و همچنین زمینه‌های فرهنگی، سیاسی، اقتصادی و اجتماعی را هنگام طراحی سیستم‌های هویتی مدنظر قرار دهند. در این بین، نوع خدمات یا تراکنش‌های مورنظر نیز از اهمیت بالایی برخوردار است. البته، بهتر نیز خواهد بود اگر طراحان، سیستمی را طراحی کنند که در عین رعایت چارچوب‌های رگولاتوری عمومی، عاری از محدودیت‌های جغرافیایی و ملی نیز باشد.

نظارت مستقل

کمیسیون‌های حریم خصوصی و مقامات حفاظت از داده‌ها، در صورتی که بتوانند مقررات و چارچوب‌های درستی را تبیین کرده و پیاده‌سازی کنند، می‌توانند به حفظ حریم خصوصی کاربران، حفاظت از داده‌های حساس، و همچنین ارتقای حس مسئولیت‌پذیری و وفاداری نسبت به منابع اطلاعاتی کمک کنند. البته، پرواضح است که این مقامات نظارتی، باید از دولت‌ها و بخش‌های خصوصی مستقل باشند تا از صحت و سقم و بدون قصد و غرض بودن نظارت‌ها و چارچوب‌ها اطمینان حاصل شود. به‌ویژه زمانی که پای منافع متضاد؛ نظیر منافع ملی، حفاظت از اطلاعات و امثال آن‌ها، به میان می‌آید، این عدم وابستگی و استقلال اهمیت بیشتری می‌یابد.

آگاهی و توانمندسازی

بسیاری از حقوق نیز وجود دارند که کاربران از وجود آن‌ها بی‌خبر هستند تا توانایی استفاده از آن‌ها را ندارند. بسیاری از افراد، برای این‌که بتوانند به حقوق خود آگاه بوده، توانایی استفاده از آن را داشته باشند و کنترل داده‌های خود را شخصا بر عهده بگیرند، نیاز به آموزش دارند. هدف این است که افراد را به قدری توانمند کنیم که بتوانند در مورد داده‌های هویتی و حریم خصوصی خود به درستی تصمیم‌گیری کرده، و بهترین رویکرد را در پیش بگیرند. قطعا انتخاب دو مسیر حریم خصوصی یا امنیت و در مقابل آن راحتی و رفاه بیشتر، موضوع ساده‌ای نیست و نیاز به آگاهی و توانمندسازی دارد. تجربه کاربری می‌تواند یک راهنمای عالی برای این آموزش و آگاهی قلمداد شود.

حریم خصوصی در طراحی

حریم خصوصی، فاکتور بسیاری مهمی است که باید در طراحی، ساخت‌وساز و اجرای فرایندهای یک سیستم مبتی بر هویتی دیجیتال نهادینه شده باشد. این نهادینه شدن، به مفهوم رویکردی کاربر محور به سمت حریم خصوصی است که شامل گردآوری کم‌ترین حجم داده‌های هویتی ممکن برای هر استفاده موردی، کاهش حدالامکان فرایندهای مربوط به پردازش این داده‌ها و تایید و احراز هویت‌ها، کنترل نحوه ثبت و ذخیره‌سازی داده‌های هویتی و همچنین تعریف و پیاده‌سازی سازوکارهای رضایتمندی قابل فهم برای کاربران است که نه تنها به راحتی و رضایت بیشتر کاربران می‌انجامد، بلکه کنترل داده‌ها و تصمیم‌گیری در مورد نحوه دسترسی سایرین به آن‌ها را نیز برای کاربران آسان‌تر می‌کند. ضمن این‌که به کاربران، این امکان را می‌دهد تا افراد دارای دسترسی به داده‌های هویتی موجود، هدف آن‌ها ازاین دسترسی و میزان و مدت زمان این دسترسی را رصد کرده و آن‌ها را رد یا تایید نمایند.

مثال‌هایی از دنیای واقعی

حمایت‌های قانونی: مقررات عمومی حفاظت از داده، اتحادیه اروپا

مقررات عمومی حفاظت از داده اتحادیه اروپا که به اختصار GDPR خوانده می‌شود، تعریف ویژه‌ای از داده‌های شخصی قابل شناسایی افراد ارائه کرده است. به‌عنوان مثال، در حال حاضر آدرس‌های ایمیل کاربران و آی‌پی آدرس‌های آن‌ها در این مجموعه جای داده می‌شوند. ضمن این‌که مقررات عمومی حفاظت از داده اتحادیه اروپا مشخص می‌کند این داده‌های شخصی قابل شناسایی، به چه صورتی می‌توانند ارزیابی و اعتبارسنجی شده و به دسترسی اعضای اتحادیه اروپا به حقوقشان بیانجامند. داده‌هایی که داده‌های هویتی نیز زیر مجموعه آن هستند. این حقوق می‌تواند شامل کنترل دسترسی سازمان‌ها به داده‌های شخصی افراد، آگاهی از دلیل گردآوری این داده‌ها و کنترل و یا رد دسترسی باشد. ضمن این‌که در سایه این مقررات، کاربران قادر شده‌اند تا داده‌های خود را پاک کرده و یا استفاده از آن‌ها را برای برخی از بازارها یا سازمان‌ها محدود کنند.

حقوق شفاف: شناسه الکترونیکی (eID)، بلژیک و استونی

کارت تایید هویت دولت بلژیک، eID، مجهز به یک چیپ الکترونیکی برای کاربران است تا دسترسی آن‌ها به اسناد، خدمات عمومی آنلاین و معرفی و احراز هویتشان را تسهیل کند. ضمن این‌که این کارت‌ها، به کاربران این امکان را می‌دهند تا نسبت به مقامات دولتی که روی داده‌های شخصی و هویتی آن‌ها کار می‌کنند و به آن‌ها دسترسی دارند، آگاهی یابند و در صورت نیاز، نام دپارتمان رسمی مربوطه را نیز شناسایی کنند. به علاوه، کاربران این امکان را در اختیار دارند تا در صورت تمایل، نسبت به بررسی دلیل دسترسی دپارتمان‌های دولتی به داده‌های شخصی و هویتی‌شان به صورت رسمی اقدام کنند و درخواست توضیح نمایند. در استونی نیز کاربران سیستم هویتی ملی این کشور، این قابلیت را در اختیار دارند تا اطلاعات هویتی خود را رصد کرده و نسبت به بررسی این‌که چه مقاماتی از دولت در حال بازبینی یا بازرسی پرونده‌های هویتی آن‌ها است کسب اطلاع کنند.

غیرمتمرکزسازی زیر سایه بلاکچین: شهر آنتوپ

شهر آنتوپ یکی از شهرهای مدرنی است که قصد دارد با پیاده‌سازی آزمایشی فناوری دفتر کل توزیع شده بلاکچین در زیرساخت‌های اطلاعاتی خود، این امکان را به کاربران بدهد تا داده‌ها و هویت‌های دیجیتال خود را شخصا کنترل و مدیریت کنند. این کاربران، این قدرت را در اختیار دارند تا تصمیم بگیرند کدام داده‌های شخصی و هویتی‌شان ثبت شود و کدام داده‌ها با چه کسانی به اشتراک گذاشته شود. با توجه به این‌که بسیاری از سازمان‌ها نیز در این پروژه آزمکایشی شرکت کرده‌اند، این طرح می‌تواند بسیاری از بارهای اداری و اجرایی را بکاهد، و به کاربران، کنترلی بسیار بیشتر از پیش روی داده‌های‌شان ارزانی کند. با دادن حق انتخاب به کاربران مبنی بر این‌که کدام داده‌ها می‌توانند ثبت شده و افشا شوند، این سیستم هویتی غیرمتمرکزسازی شده می‌تواند حامی یک مدل افشای حداقلی باشد. در مورد ماهیت این مدل، در ادامه توضیح خواهیم داد.

۵. ایمن

یک سیستم هویتی ایمن باید بتواند فاکتورهای زیر را ارائه دهد:

حفاظت: اقدامات سخت‌گیرانه مبتنی بر امنیت سایبری به شکلی مداوم صورت می‌پذیرند تا تهدیدهای سایبری احتمالی به حداقل رسیده و از دسترسی غیرمجاز یا غیرقانونی به داده‌ها، افشای آن‌ها یا دستکاری‌شان جلوگیری به عمل آید.

تمامیت داده‌ها: سیستم‌های ایمن تمامیت یا یکپارچگی داده‌های شخصی و هویتی کاربران را حفظ می‌کنند، هرچند که افراد باید بتوانند در مورد دلیل حذف داده‌های خود پرسش کنند.

مسئولیت‌پذیری: چارچوب‌های یک سیستم هویتی ایمن باید به گونه‌ای طراحی شده باشد که بتواند دنباله حسابرسی را پشتیبانی کرده، مسئولیت‌پذیری را در طول شبکه برقرار کند و در صورت نشت اطلاعاتی یا نقص، اقدامات لازم را انجام دهد.

این عنصر چرا اهمیت دارد؟

امنیت، برای برقراری اعتماد بین طرفین یک سیســـتم هویتی، از افراد و کاربران آن گرفته تا اشخاص ثالث وابسته، عنصری حیاتی اســـت چرا که در سایه این امنیت می‌توان تهدیدها و جرایم سایبری نظیر ســـرقت‌های هویتی را کاهش داد و جلوی پیامدهای ناخواسته‌ای همچون نقض حقوق بشر را گرفت. یک سیستم ایمن که از داده‌ها محافظت می‌کند، به افراد این امکان را می‌دهد تا در همه سطوح اجتماعی و اقتصادی بالاترین میزان سود را دریافت کنند.

با توجه به دنیای درهم امروز که دســـتگاه‌های متصل در همه ابعاد زندگی روزمره افراد و ســـازمان‌ها نفوذ کرده‌اند، اهـــداف فزاینده جدیدی پیـــش روی هکرها و مهاجمین سایبری قرار گرفته اســـت. هویت‌های دیجیتال قابل تایید می‌توانند در کنار دســـتگاه‌های اجرایی، امنیتی و نظارتی، در به حداقل رساندن آسیب‌هایی که ممکن است متوجه افراد و سازمان‌ها شوند نقش داشته باشند.

منظور از خوب چیست؟

افشای حداقلی

سیســـتم‌های هویتی باید به گونه‌ای طراحی شده باشـــند که کاربران را به افشای حداقل اطلاعـــات موردنیاز برای تایید و احراز هویـــت وادار کنند. در صورتی که دست کاربران از کنترل داده‌های شخصی و هویتی‌شان کوتاه باشد، این سیستم‌های هویتی خواهند بود که ملزم به کنترل داده‌ها و افشای حداقل داده‌های موردنیاز برای فرایندهای تایید هویت و انجام تراکنش‌ها هستند. به عنوان مثال، یک آی‌دی کارت رسمی، ممکن است هنگام تایید سن شما آدرس‌تان را نیز نمایش دهد که نیازی به آن نیست و باید اصلاح شود.

آموزش

آموزش داده کاربران برای این‌که بتوانند داده‌های خود را به بهترین شـــکل ممکن مدیریت و کنترل کنند، ریســـک‌های احتمالی متوجه هویت‌های دیجیتالشان را شناسایی کرده و کاهش دهند و در عین حال در مقابل جرایم سایبری ناگواری نظیر تقلب، سرقت‌های هویتی یا سوء استفاده از داده‌ها نیز بایستند.

ترمیم

حتی بهترین سیستم‌های هویتی نیز ممکن است در برخی مواقع دچار ایراد و اختلال شده و داده‌های حساس کاربران را در معرض افشا قرار دهند. این‌که سیستم بتواند بلافاصله پس از بروز اختلال یا حادثه خود را بازیابی کرده، با پشتیبانی سازمانی و مالی ترمیم‌های لازمه برای پسخگویی به پیامدهای حاصل از حادثه را انجام دهد، موضوع مهمی است که باید در بطن یک سیستم هویتی نهادینه شود. بدیهی است که فقدان چنین فرایندهای بازیابی و ترمیمی سریع و کارآمدی سبب از دست رفتن اعتماد کابران و سازمان‌ها خواهد شد.

مثال‌هایی از دنیای واقعی

امنیت و حفاظت: ایتس می (Itsme)، بلژیک

پلتفرم هویت دیجیتال ایتس می از فرایند تایید هویت چند منظوره‌ای استفاده می‌کند که شامل داده‌های بیومتریک اســـت و امنیت را ارتقا می‌بخشد. فرایند تایید هویت این پلتفرم به عنصر نیاز دارد: یک گوشی تلفن همراه که به کاربرا متصل باشد، یک سیم کارت که امنیت آن توسط اپراتورهای تلفن‌های همراه ضمانت شده باشد، و کد مخصوص هر کاربر که توسط ایتس می برای وی صادر شده و منحصر به‌فرد است. گفتنی است، این پلتفرم توسط مقررات عمومی حفاظت از داده اتحادیه اروپا نیز به رسمیت شناخته شده و دارای مجوز eIDAS است.

فصل سوم:

پیش به سوی آینده:
روندها، فرصت‌ها و چالش‌ها

چه اتفاقی می‌افتد؟

هویت‌های دیجیتال، در حال حاضر به بسیاری از جوانب زندگی روزمره ما نفوذ کرده‌اند. هرچه فناوری‌های نسل چهارم انقلاب دیجیتال، از جمله اینترنت اشیا، هوش مصنوعی و خودروهای خودران و امثال آن پیشرفت بیشتری می‌کنند، سیستم‌های دیجیتال نیز بیش از پیش نیاز به تحول پیدا می‌کنند و هویت‌های دیجیتال نیز از این نیاز مستثنی نیستند. هرچه این تحولات دیجیتال سرعت بیشتری می‌گیرد، سیستم‌های هویتی نیز بیشتر برای تحول و اوج گرفتن آماده می‌شوند، تا بتوانند با معطوف کردن تمام تمرکز خود روی ارزش آفرینی برای کاربرانشان، از قافله مدیرنته عقب نمانند. در این فصل، قصد داریم برخی از روندهای مهم هویت های دیجیتال، چالش‌ها و فرصت‌هایی را که احتمال دارد سازمان‌ها، ارائه دهندگان، سیاست‌گذاران و طراحان سیستم‌ها در آینده‌ای نه چندان دور با آن‌ها مواجه شوند در بوته بحث و بررسی قرار دهیم.

روندها

غیرمتمرکزسازی سیستم‌های هویتی، مدل‌های اعتمادی نوین و یا تایید هویت‌های غیرانسانی، مباحثی هستند که جای بحث بسیار دارند و در این مقاله، به اختصار به برخی از آن‌ها پرداخته شده است.

سیستم‌های هویتی غیرمتمرکز. فناوری‌ها و معماری‌های جدید، از قبیل فناوری دفتر کل توزیع شده، می‌توانند نقش تعیین کننده‌ای در تغییر روند رسیدگی و کنترل داده‌های هویتی و شخصی توسط کاربران داشته باشند. پذیرش این قبیل فناوری‌ها و نوآوری‌ها و تغییر کامل زیرساخت‌های جوامع اقتصادی بر مبنای آن‌ها، می‌تواند بسته به زیرساخت‌های فرهنگی، سواد فناوری، میزان دسترسی به فناوری‌های روز دنیا، میزان مشارکت‌ها سازمان‌ها و ارائه دهندگان و همچنین مدل‌ها و الگوهای اعتمادی مورد استفاده متفاوت باشد.

تحکیم الگوهای اعتماد. اکثریت قریب به اتفاق دست‌اندرکاران و افرادی که در فضای مشارکتی با یکدیگر در تعامل هستند، بر اساس الگوها و مدل‌های اعتمادی فعالیت می‌کنند که می‌توانند هویت افراد و سازمان‌ها را تایید کرده و سلامت و امنیت داده‌ها را ضمانت کنند. الگوهایی که به لحاظ تاریخی توسط دولت‌ها، سیستم‌های بانکداری سنتی و امثال آن تبیین شده و در اختیار خرده‌فروشان، پلتفرم‌های مبتنی بر فناوری، بیمارستان‌ها، اپراتورهای تلفن‌های همراه، پلتفرم‌های تجارت الکترونیک، رسانه‌های اجتماعی، روابط و تراکنش‌های شخصی و امثال آن‌ها قرار گرفته‌اند.

اکوسیستم‌های هویتی. هرچه تحولات دیجیتال پا فراتر از محدوده‌های جغرافیایی می‌گذارند و مرزها را درمی‌نوردند، هویت‌های دیجیتال نیز به دنبال آن توسعه می‌یابند. هویت‌های دیجیتال، اکنون به عناصر بسیار تعامل‌پذیری میان مرزها؛ نظیر پلتفرم تبادل داده ایکس رود (X-Road) که در کشورهای استونی و فنلاند مورد استفاده قرار می‌گیرد و در بین حوزه‌ها؛ به عنوان مثال، بین حوزه بانکداری و مخابرات، یا بین حوزه ثبت املاک و شرکت‌های زنجیره تامین، تبدیل شده‌اند که می‌توانند تراکنش‌ها و تعاملات سازمان‌ها و کاربران را نیز در سطح دهکده جهانی توسعه دهند.

پذیرش محلی. حتی اگر هویت‌های دیجیتال و سیستم‌های مبتنی بر آن نیز در سطح جهانی به رشد و بالندگی دست یافته باشند، هنوز هم پذیرش آن‌ها در گرو برخی فاکتورهای محلی نظیر فرهنگ، عادات و رفتارهای محلی کاربران است و مشارکت برای توسعه چنین سیستم‌های مستلزم تمرکز روی کاربران و نحوه ارزش آفرینی برای آ»ها است.

هویت برای عوامل غیرانسانی. نیاز به دستگاه‌ها، هویت‌های حقوقی، دارایی‌ها و منابع طبیعی از جمله غذا، به شدت در حال توسعه است و زمانی که این روند رو به توسعه با رشد و پیشرفت فناوری‌های مدرنی نظیر اینترنت اشیا، یادگیری ماشین یا هوش مصنوعی یا مفاهیمی همچون دوقلوهای دیجیتال عجین همسو می‌شود، هویت برای عناصر غیرانسانی نیز مفهوم و اهمیت می‌یابد. دوقلوی دیجیتال، به مفهوم یک قلوی یا کپی دیجیتال از دارایی‌های فیزیکی یا مجازی است که با افراد یا سازمان‌ها در تعامل و ارتباط هستند. طراحان سیستم‌های هویتی و سیاست‌گذاران، برای ارائه سیستم‌های توانمند و پاسخگو در عصر جدید، ملزم به تمرکز روی روابط و تعاملات بشر با این عناصر غیرانسانی هستند و این‌که هدف و مقصود حقیقی از کاربر محور بودن و پاسخگویی، آن‌هم در این دنیای پیچیده و در هم تنیده چه می‌تواند باشد.

چالش‌ها

چه چالش‌های جدیدی می‌توانند در سایه تحولات دیجیتال، پیشرفت‌های فناورانه، روندهای نوظهور و تاکید روی تجربه کاربری و ارزش آفرینی برای افراد ظهور کنند؟

بهبود تجربه کاربری. هرچه سازمان‌ها، شرکت‌ها و ارائه دهندگان خدمات و محصولات برای اکتساب کاربران تلاش می‌کنند، به‌ویژه زمانی که پای استانداردها و اصول مشترک نیز لنگ می‌زند و هرکس به شیوه خود به دنبال موفقیت است، طراحان نیز با چالش‌های عدیده‌ای در ارتباط با تجربه مشتریان مواجه می‌شوند. بدیهی است که در این رقابت تنگاتنگ، طراحان ملزم هستند برای عقب نماندن از قافله، بیشتر روی اعتماد کاربران، تجربیات آن‌ها از سیستم‌های طراحی شده و ارزش آفرینی برای آن‌ها تمرکز کنند. ممکن است در این میان، برای جلب توجه و اعتماد کاربران، گزینه‌های دسترسی و کنترلی بیشتری به آن‌ها عرضه کنند و مدیریت هویت‌های دیجیتال و داده‌ها را به خود کاربران موکول کنند.

به اشتراک‌گذاری مالکیت. مالکین سیستم‌های هویتی حال حاضر، که کلیه مسئولیت‌های مدیریتی و کنترلی هویت کاربران را بر عهده دارند، ممکن است به سازگاری با اکوسیستم‌هایی که در آن‌ها مالکیت به اشتراک گذاشته شده است نیاز پیدا کنند. اکوسیستم‌هایی که در آن‌ها کاربران از حقوق بیشتری برخوردار هستند و مشارکت کمک می‌کند تا هویت‌ها، فراتر از مرزهای فرهنگی و جغرافیایی مدیریت شوند.

به‌روز نگه داشتن مقررات. قانون‌گذاران و سیاست‌گذاران باید بتوانند سرعت خود را با تحولات دیجیتال و شتاب سرسام‌آور رشد سیستم‌های هویتی هماهنگ کنند تا بتوانند قوانین و چارچوب‌های رگولاتوری را به نحوی تنظیم و تبیین کنند که زمینه را برای نوآوری‌ها فراهم ساخته و موانع پذیرش آن‌ها را بکاهند. ضمن این‌که این چارچوب‌ها باید بتوانند در هر زمان و مکانی امنیت داده‌ها را ضمانت کرده، از حریم خصوصی و سایر حقوق قانونی کاربران حفاظت کنند. سیستم‌های هویتی برای تعامل‌پذیری نیازمند چارچوب‌های رگولاتوری و حقوقی جدید، فناوری‌های جدید و غیره هستند.

کارکرد موثرتر. با ظهور و توسعه سیستم‌های جدید، طراحان و سیاست‌گذاران باید مراقب همپوشانی‌هایی که می‌توانند منجر به افزایش هزینه‌ها و کاهش کارایی سیستم شوند نیز توجه داشته باشند.

توسعه سواد دیجیتال و دسترسی. برای این‌که افراد بتوانند هویت‌های دیجیتال را به رسمیت شناخته و به نحوی کارآمد از آن‌ها استفاده کنند؛ به‌ویژه با توجه به روندی که به سمت خود مدیریتی در پیش گرفته شده، لازم است که برای این پذیرش و استفاده، آموزش دیده و به سطح قابل قبولی از فناوری و سواد دیجیتال دسترسی داشته باشند.

تکه تکه شدن هویت دیجیتال. بیایید یک سناریوی ساده را متصور شویم: از یک سو تعدادی از کاربران داده‌ها و هویت‌های دیجیتال خود را با حاشیه قابل قبولی از امنیت و یا حریم خصوصی مدیریت و کنترل می‌کنند. از سوی دیگر، افراد بیشماری نیز وجود دارند که داده‌ها و هویت‌هایشان در دست دیگران است و یا حتی برخی فاقد هرگونه هویت دیجیتال ثبت شده و قانونی هستند. احتمال و ریسک قرار گرفتن در طرف دوم، به‌ویژه در کشورهایی که فاقد چارچوب‌های رگولاتوری و حقوقی محکم برای حقوق بشر و حریم خصوصی کاربران هستند بالا است این، یعنی تکه تکه شدن دیجیتال.

بی‌تفاوتی کاربران. یکی از نتایج بارز توسعه بیش از حد سیستم‌های مبتنی بر هویت دیجیتال، ظهور بیش از اندازه چنین سیستم‌هایی و گزینه‌های بیشماری از کنترل‌های اطلاعاتی و مدیریتی برای کاربران، سرریز شدن داده‌ها است. در چنین حالتی است که افراد از مدیریت و کنترل بیش از حد داده‌های خود خسته شده و نسبت به رفتارها یا فرایندهایی که ممکن است امنیت، حریم خصوصی، داده‌ها یا حتی هویت‌های آن‌ها را تهدید کند بی‌تفاوت عمل کنند.

ریسک‌ها و مسئولیت‌ها. هرچه یک حوزه توسعه بیشتری می‌یابد، بازیگران جدیدی نیز به آن ملحق می‌شوند، و این جا است که مالکیت و مسئولیت‌پذیری ریسک‌ها شفافیت بیشتری می‌طلبد و نیاز به مدیریت بیشتر احساس می‌شود.

پیامدهای ناخواسته طراحی ضعیف. طراحی ضعیف یک سیستم هویتی، نه تنها می‌تواند به کارایی و راندمان ضعیف بیانجامد، بلکه به افراد نیز آسیب می‌رساند. به عنوان مثال، یک هویت دیجیتال ناکارآمد که به صورت غیرحرفه‌ای و ضعیف طراحی شده است، می‌تواند در را به روی نظارت‌های غیرقانونی و جاسوسی باز کند. کلیه تصمیمات طراحی باید با در نظر گرفتن پیامدهای منفی ممکنه صورت بگیرند و جای هیچ‌گونه اهمال کاری وجود ندارد.

فرصت‌ها

هویت‌های دیجتال و سیستم‌های مبتی بر این هویت‌های دیجیتال، نه تنها می‌توانند برای کاربران مفید واقع شوند بلکه برای جامعه نیز فرصت‌هایی را در پی دارند.

دنیای دیجیتالی پرتابل، امن‌تر و قابل اعتمادتر. یک هویت دیجیتال راحت و قابل اعتماد، نه تنها شما، داده‌های هویتی و شخصی و دارایی‌هایتان را ایمن نگه می‌دارد، بلکه دری به سمت امنیت و اعتماد نیز می‌گشاید. امنیت و اعتمادی که شبکه‌ای بسیار گسترده‌تر از تعاملات رودرروی سابق رقم می‌زند و مرزهای جغرافیایی و اجتماعی را درمی‌نوردد.

سادگی، کارایی و اعتماد در به اشتراک‌گذاری داده‌ها. در سایه هویت‌های دیجیتالی که ساده و راحت هستند، قابل اعتمادند و به افراد حق انتخاب و کنترل روی داده‌های‌شان را می‌دهند، شرکت‌ها و سازمان‌ها نیز از منابع اطلاعاتی هنگفتی بهره‌مند خواهند شد که می‌تواند به بسیاری از آمال و اهداف آن‌ها جامه عمل بپوشاند. شرکت‌هایی که تاکنون به سیلوهای اطلاعاتی محدود و تکه تکه سنتی وابسته بوده‌اند و اکنون، به سهولت هرچه تمام، دریایی از داده‌های به اشتراک‌گذاشته شده و ایمن را پیش روی خود دارند. دادن حق انتخاب و کنترل داده‌ها به افراد، آن هم در شرایطی که همه‌روزه به فناوری‌ها و نوآوری‌های جدیدی دست می‌یابیم و مشارکت‌ها و تعاملات بین سازمانی نیز رو به فزونی گذاشته است، منجر به برداشته شدن بار انطباق خواهد شد و با حذف تکرار از فرایندهای تایید هویت در سطح سازمان‌ها، کارایی را ارتقا بخشیده و هزینه‌ها و اصطکاک‌ها را خواهد کاست.

مشارکت‌های بیشتر برای سیستم‌هایی بهتر. نیاز به تعامل‌پذیری و تجربه کاربری یکپارچه، فرصت‌هایی را پیش روی بخش‌های خصوصی، دولت‌ها و جامعه مدنی قرار می‌دهد تا بتوانند با یکدیگر کار کنند. با کاهش سیستم‌های هویتی و عاری از تعامل‌پذیری، افراد و سازمان‌ها قادر خواهند بود هزینه‌ها را کاهش داده و فرصت‌های جدیدی برای تجربه دیجیتال بهتر بیابند.

ارزشی گسترده برای کاربران. مدل‌ها و الگوهای اعتمادی مدرن این قدرت را دارند تا تعاملات و تراکنش‌هایی همه‌روزه و با حداقل ریسک برای کاربران رقم بزنند. تراکنش‌هایی که دارای کمترین هزینه و در عین حالا بالاترین کارایی و راحتی هستند. ضمن این‌که دسترسی افراد به طیف گسترده و روزافزونی از خدمات، تراکنش‌ها و شبکه‌ها نیز به منزله ارزش آفرینی برای آن‌ها در سطحی وسیع است.

انگیزه‌ها و رفتارهای بهتر. هویت‌های دیجیتال، به‌ویژه در مورد کودکان می‌تواند انگیزه‌ای برای رفتار بهتر و پایدار باشد. به عنوان مثال، سازمان‌ها و دولت‌ها می‌توانند از هویت‌های دیجیتال برای بررسی کارگران معدن استفاده کنند تا اطمینان حاصل شود که از هیچ کودک کاری در این معادن استفاده نمی‌شود.

ردیابی در زنجیره‌های تامین. زمانی که هویت‌های دیجیتال با تولیدات کشاورزی یا سایر محصولات پیوند می‌خورد، اعتماد در تمام سطح زنجیره تامین به‌ویژه در نقاط اند-تو-اند آن افزایش پیدا می‌کند. دلیل این افزایش اعتماد نیز این است که افراد می‌توانند در مورد صحت و سقم منبع محصولات، نحوه و محل تولید آن‌ها، به بار آوری و نقل و انتقال و غیره آن تحقیق کنند.

انقلاب صنعتی چهارم. رسالت انقلاب دیجیتال چهارم، ادغام بی‌کم‌وکاست و یکپارچه فناوری‌های دیجیتال برای بهبود زندگی ما است. هویت‌های دیجیتال ایمن، موثر، راحت، پایبند به حریم خصوصی و همه‌جانبه به این ادغام کمک خواهد کرد.

فصل چهارم:

اولویت‌هایی برای مشارکت بخش خصوصی و دولت

مجمع جهانی اقتصاد، به عنوان سازمانی بین‌المللی برای مشارکت‌های بخش خصوصی و دولتی پلتفرمی برای دست‌اندرکاران و ذینفعان معرفی کرده است تا در خلال آن به بحث در مورد ایده‌های خود بپردازند، اولویت‌ها را مشخص کنند و به شکل‌گیری بهتر هویت‌های دیجیتال در آینده‌ای نه چندان دور کمک کنند.

در حالت کلی، ذینفعان هویت‌های دیجیتال از بخش‌های خصوصی، دولت‌ها، کسب‌وکارها و جامعه مدنی، شش اولویت برای پیشبرد مشارکت در حیطه هویت‌های دیجیتال تعیین و تبیین کرده‌اند:

تمرکز روی ارزش آفرینی برای کاربران. تخصیص یک هویت دیجیتال به تمام افراد جامعه به تنهایی نمی‌تواند خوب یا کافی باشد. ماجرا همان انتخاب میان بد و بدتر است و به عبارت ساده‌تر، نداشتن هویت، از داشتن یک هویت بد به مراتب بهتر است. طراحان سیستم‌های هویتی و سیاست‌گذاران ملزم هستند تا روی دستاورد حقیقی این سیستم‌ها تمرکز کنند: پذیرش مبتنی بر تقاضای هویت‌هایی که پنج عنصر موردنیاز برای ارزش آفرینی در خود دارند و دسترسی بهتر به خدمات، امنیت مضاعف و تراکنش‌های آنلاین کارآمد را برای افراد به دنبال می‌آورند.

قابل حسابرسی. چگونه می‌توان میزان ارزش ایجاد شده برای کاربران توسط یک سیستم هویتی را اندازه‌گیری کرد و معیار سنجش این قبیل سیستم‌ها چیست؟ چطور می‌توان آن‌ها را قابل حسابرسی و سنجش نگه داشت؟ بدیهی است که پاسخ به این سوالات بسته به حوزه‌ها و عملکردها متفاوت خواهد بود و در طول زمان نیز تحول و تکامل خواهد یافت. اما آن‌چه که از اهمیت بالایی برخوردار است، توسعه معیارهای مشترک برای سیستم‌ها، کشورها و جنبش‌های فرامرزی ارزش آفرین برای کاربران است.

حکومت یا مدیریت. اکوسیستم‌های جدید هویتی نیاز به مدل‌های حکومتی جدید نیز دارند تا بتوانند نظارت مستقل و قابل حسابرسی بودن به لحاظ فرامرزی را حفظ کرده و سازوکارهایی را برای تحقق انطباق، مدیریت مسئولیت‌ها و ارائه منابع در صورت لزوم تعریف کند. هدف از مشارکت‌ها باید تعریف و تعیین چارچوب‌هایی به اندازه کافی انعطاف‌پذیر به منظور تکامل در طول زمان باشد.

نظارت. هویت‌های دیجیتال خوب به اراده سیاسی قوی، توجه دولت‌ها، صاحبان کسب وکارها و رهبران جامعه مدنی نیاز دارند. درک مشترک از اصول می‌تواند به سیاست‌گذاران، رهبران سازمان‌ها و طراحان کمک کند تا شیوه‌های استاندارد و هماهنگی در پیش بگیرند. روایت متقابل بخش‌های مختلف از هویت‌های دیجیتال می‌تواند تا حد زیادی کمک کننده باشد.

مشارکت‌ها. هویت‌های دیجیتال ریسک تکه تکه شدن و انزوا را همواره به یدک می‌کشند، مگر این‌که سازمان و دست‌اندرکاران صنعت به دنبال مشارکت و استفاده از راهکارها و شیوه‌هایی برای ایجاد انگیزه، توصیف اولویت‌های مشترک و تعامل‌پذیری باشند.

نوآوری. این‌که کدام‌یک از شیوه‌ها، اعم از پروژه‌های فانوس دریایی (lighthouse projects) که روی استفاده‌های موردی خاص تکیه می‌کنند یا سندباکس‌های چابک (agile sandboxes) که بر فرضیات آزمایشی تاکید دارند و یا سایر راهکارها و متدها این قابلیت را دارند تا هماهنگی لازم و تعادل موردنیاز بین سرعت رشد فناوری‌های مدرن و نیازهای کاربران را حفظ کنند از اهمیت بالایی برخوردار است. چرا که در این صورت سازمان‌ها قادر خواهند بود در کنار هم بهتر مشارکت کرده و در سایه اولویت‌های مشترک، به نتایج مطلوبی دست یابند. ضمن این‌که یکی از مهم‌ترین دستاوردهای این نوآوری‌ها و مشارکت‌ها، کتابخانه‌ای موفق از آزمایش‌هایی است که هریک دانشگاهی برای آیندگان هستند.

زمینه‌های فعالیت مشترک

به‌عنوان نتیجه‌گیری، لیستی از اولویت‌ها را تدارک دیده‌ایم که می‌توانند به هویت‌های دیجیتال خوب و به معنای واقعی کلمه کاربر محور منجر شوند.

سیاست و حکومت

- سازوکارهای احراز هویت و سیاست‌های متناسب با سطح اطمینان موردنیاز
- چارچوب‌های حقوقی مناسب برای حریم خصوصی، امنیت سایبری و حفاظت از داده‌ها
- سیاست‌های ملی هویت دیجیتال که با استراتژی‌های گسترده‌تری برای امنیت سایبری، ایمنی بیماران، توسعه اقتصادی و امثال آن در هم می‌آمیزند.
- سیاست‌های کاربر محور و فرایندهایی برای ارائه دهندگان بخش خصوصی
- گردآوری، پردازش و استفاده شفاف از داده‌ها به منظور حمایت از اعتماد کاربران
- نظارت مستقل بر هویت‌های ملی و چارچوب‌های حفاظت از داده‌ها
- یک چارچوب جهانی مشترک برای حکومت فرامرزی
- مدیریت سیاست‌ها و عملکردها در میان دولت‌ها، کسب‌وکارها و سایر سازمان‌ها

جامعه خوب و عمومی

- تعریف و درک مشترک از یک هویت دیجیتال خوب و ارزش آفرینی برای کاربران
- سرمایه‌گذاری روی تحقیقات به منظور دستیابی به سناریوهای مبتنی بر هوش مصنوعی یا اینترنت اشیای مرتبط با هویت دیجیتال
- معیارها، ابزارها و استفاده موردی مناسبی را ارزش یک هویت دیجیتال خوب را نشان می‌دهند.
- تعریف یک هویت دیجیتال خوب برای یک جامعه آماری خاص از کاربران، دامنه‌ها و استفاده‌های موردی

قابلیت‌ها

- مشارکت بین دولت‌ها، بخش‌های خصوصی و جامعه مدنی به منظور آگاه‌سازی افراد از حقوق، ریسک‌ها و وظایفشان و همچنین سازوکارهای مسئولیت‌پذیری موجود پیرامون هویت‌های آن‌ها
- چارچوب‌های پاسخگویی و حسابرسی مشترک
- به اشتراک‌گذاری متدولوژی و توانمندسازی سیاست‌گذاران و دست‌اندرکاران
- توسعه بازارهای بیمه همسو با تکامل هویت‌های دیجیتال و رشد ریسک‌ها
- حمایت‌های حقوقی و غیرحقوقی به منظور کمک به کاربران در مواقع نیاز

نوآوری و طراحی راهکارها

- نهادینه کردن سیاست‌های امنیتی و حریم خصوصی در خطوط مشی کسب‌وکارها و راهکارهای مبتنی بر فناوری
- تست‌بدها (testbeds) و سندباکس‌های چابک برای اولویت‌بندی چالش‌های متوجه ارزش کاربران، نظیر امنیت و تعامل‌پذیری
- نوآوری در تحولات فرایندهای آنالوگ و دیجیتال و همچنین ادغام، نظیر دوقلوهای دیجیتال
- پاسخگویی به رشد فزاینده داده‌های شخصی قابل شناسایی کاربران، به‌ویژه زمانی که پای اینترنت اشیا به میان می‌آید.

توسعه برنامه

- اولویت‌بندی استفاده‌های موردی بر اساس بالاترین پتانسیل آن‌ها در کاهش اصطکاک و ارزش آفرینی برای کاربران
- طراحی و پیاده‌سازی مشترک و توامان راهکارها توسط ذینفعان چندگانه زیر سایه مشارکت‌های بخش خصوصی و دولتی
- شناسایی نمونه‌های آزمایشی و فرصت‌های پیاده‌سازی نمونه‌های موفق در مقیاس گسترده عملی زیر چتر مشارکت
- مشارکت با جامعه مدنی به منظور شناسایی ارزش‌های مختلف کاربران در جوامع مختلف

پیوست ۱: ملاحظات طراحی برای دست‌اندرکاران

در حال حاضر، راهکارهای بسیار زیادی برای پیاده‌سازی هویت دیجیتال در سطح جهانی در دسترس هستند، اما برخی از آن‌ها ممکن است دارای مشکلاتی بوده، مستلزم سبک و سنگین کردن باشند و هنوز جای کار دارند. برخی دیگر نیز هستند که کاملا امتحان شده و می‌توان روی آن‌ها حساب باز کرد، با این حال این قبیل راهکارها نیاز به سرمایه‌گذاری و مشارکت و گاهی تغییر در سبک زندگی و حتی نگرش‌ها دارند.

در این پیوست، سعی کرده‌ایم ایده‌هایی عملی ارائه کنیم که می‌توانند برای پیاده‌سازی یک سیستم مبتنی بر هویتی دیجیتال خوب مورد استفاده قرار گیرند. یک نقشه راه برای طراحان و سیاست‌گذاران، تا بتوانند به آن‌چه که «خوب» نامیده می‌شود دست پیدا کنند. اگرچه ممکن است این نقشه راه برخی مسیرهای پرپیچ‌وخم، برخی پستی و بلندی‌ها و حتی نقاط خالی داشته باشد. بدیهی است که این لیست از ایده‌ها با کمال فاصله زیادی دارد و تنها مفاهیم آن هستند که حیاتی‌اند؛ اما امیدواریم بتواند جوامع را در دستیابی به هدف غایی یاری کند: طراحی و پیاده‌سازی یک سیستم هویتی خوب که بتواند برای کاربران ارزش آفرینی کند.

لازم به ذکر است که پیاده‌سازی چهارچوب‌های رگولاتوری و حقوقی و در عین حال پایبندی به سیاست‌ها نیز باید با این نقشه راه همراه شود. این مهم، یکی از الزامات دستیابی به یک سیستم هویتی خوب یا همان موفقیت است.

آن‌چه در ادامه آمده است، مجموعه‌ای از رهنمودها و ملاحظات برای پشتیبانی از طراحان و در ادامه ساخت و راه‌اندازی یک سیستم مبتنی بر هویت دیجیتال است که با تحقق بخشیدن به نیازها و انتظارات کاربران، برای آن‌ها ایجاد ارزش می‌کند.

شکل شماره ۶: چک لیستی گویا برای شروع سفر به مقصد هویت دیجیتال خوب

۱ شروع

۱-۱ مشخص کردن کاربران
۱-۲ در نظر گرفتن زمینه‌ها
۱-۳ تصویر برداری از چشم‌انداز
۱-۴ تعیین شرکای بالقوه اکوسیستم
۱-۵ مشورت با کاربران بالقوه
۱-۶ ایجاد یک روایت
۱-۷ آموزش
۱-۸ برنامه‌ریزی برای به اشتراک‌گذاری ریسک‌ها
۱-۹ یافتن فرصت‌های جدید برای ثبات

۲ طراحی و ساخت سیستم‌های کاربر محور

۲-۱ حداکثر ارزش کاربری و عملکرد
۲-۲ وارد کردن فضای فناوری، صنعت، فرهنگی و حوزه بازار
۲-۳ شناسایی و انتخاب بهترین الگو
۲-۳ شناسایی و انتخاب بهترین رویکردها برای انطباق و امنیت
۲-۵ کاهش خطرات و حل و فصل مشکلات

۳ بازگویی ارزش در آینده

۳-۱ در نظر داشتن نیازهای در حال توسعه برای جلوگیری از تبعیض
۳-۲ آمادگی برای مقابله با چالش‌های ناشی از نهادهای حقوقی، دستگاه‌ها، منابع طبیعی و غیره
۳-۳ آمادگی برای رودررویی با نهادهای مجازی، هوش مصنوعی و غیره
۳-۴ در نظر گرفتن پیامدهای ناشی از فناوری‌های نوین

۱. شروع

۱-۱ مشـــخص کردن کاربران. ارزش یعنی خدمات و محصولات مختلفی برای کاربران مختلف ارائه کنیم و همواره نیز به دلیل اختلافات و تفاوت‌های فاحش میان کاربران و ترکیب محصولات با مشکلات عدیده‌ای روبه‌رو می‌شود. درک این‌که سیستم به چه کسی در حال ارائه خدمات است، ارزش برای وی به چه مفهوم است، و چه موانعی ممکن است در مسیر پذیرش وی در حال و آینده وجود داشته باشد، حائز اهمیت است.

۱-۲ در نظر گرفتن زمینه‌ها. هویت‌های دیجیتال مختلف با زمینه‌ها و محیط‌های میکرواقتصادی، اجتماعی، فرهنگی، سیاسی و حقوقی مختلفی روبه‌رو هستند. درک این زمینه‌ها برای ساختن یک سیستم مبتنی بر هویت دیجیتال خوب حیاتی است. سیستمی که نیازها و انتظارات دست‌اندرکاران و ذینفعان را به خوبی درک می‌کند و آن‌ها را به مشارکت وا می‌دارد.

۱-۳ تصویربرداری از چشم‌انداز. قبل از ایجاد یک سیستم هویتی، نقشه‌برداری از زیرساخت‌ها و معماری‌های حقوقی موجود و دست‌اندرکاران حائز اهمیت است. این نقشه‌برداری می‌تواند به طراحی سفر در آینده کمک کند و فاکتورهایی اعم از انگیزه‌های آتی بازیگران فعلی را نمایان سازد. همچنین ممکن است برخی از ویژگی‌ها و قابلیت‌های سیستم‌های میرا و منسوخ کنونی را برای ادغام و استفاده در سیستم‌های مدرن آتی معرفی کند.

۱-۴ تعیین شرکای بالقوه اکوسیستم. بر اساس شناخت به دست آمده از ارزش هر یک از کاربران و فضای موجود از جمله الگوهای اعتمادی در دسترس و اپراتورهای سیستم، می‌توان شرکای بالقوه برای اکوسیستم را شناسایی کرد. هر مشارکتی نیاز به انگیزه و به احتمال زیاد برآورد هزینه‌ها و منافع متقابل دارد. این به معنای بازنگری در مدل‌های سرمایه‌گذاری، مالکیت، مالکیت معنوی، فرایندها و عملکردهای سیستم، مسئولیت‌پذیری و غیره است.

۱-۵ مشورت با کاربران بالقوه. تجربیاتی که در بلژیک، بریتیش کلمبیا و کانادا به دست آمده تایید می‌کند که تحقیقات روی گروه‌های کاربری و درگیر ساختن کاربران در طراحی سیستم‌های هویتی می‌تواند منجر به تسریع پذیرش در بلند مدت و درگیر ساختن کاربران، همان لحظه آغاز سفر شود.

۱-۶ ایجاد یک روایت. تفصیل کامل ارزش مورد هدف یک سیستم مبتنی بر هویت دیجیتال و اهداف آن برای کاربران، آن‌هم با تکیه بر طرفین، دست‌اندرکاران سیستم و سایر شرکا، یعنی ایجاد یک روایت. بسیاری از سیستم‌های هویتی از دستیابی به پذیرش باز می‌مانند به این دلیل که در برقراری ارتباط میان مزایای سیستم و انگیزه‌های آن ناتوان هستند.

۱-۷ آموزش. حامیان هویت‌های دیجیتال، معمولا ناچار هستند تا سفر ایجاد سیستم‌های هویتی را با آموزش سیاســت‌گذاران آغاز کنند. سیاست‌گذاران و طراحان سیستم‌های هویتی، پس از آن این قابلیت را خواهند داشت تا کاربران و سایر شرکا و متکیان به سیستم‌ها را پیرامون هویت‌های دیجیتال آموزش دهند. همکاری‌های اولیه با جامعه مدنی، به ویژه با سازمان‌های اجتماعی، می‌تواند کمک کننده باشد.

۱-۸ برنامه‌ریزی برای به اشــتراک‌گذاری ریسک‌ها. سیاســت‌گذاران و رهبران سازمان‌ها شــاید به دنبال دسترســی به راه‌های جلوگیری از ریسک‌هایی باشند که اکوسیســتم‌های مبتنی بر هویت‌های دیجیتال را تهدید می‌کنند. یکی از مثال‌های بارز این قبیل راهکارها، استفاده از محصولات و خدمات شرکت‌های ارائه دهنده بیمه است که بخش عمده‌ای از ریسک‌ها را پوشش می‌دهند. به عنوان مثال، بیمه‌گران معمولا ریسک‌های ناشی از تقلبات کارت‌های اعتباری را پوشش می‌دهند که بانک‌ها را قادر می‌سازد تا در صورت بروز تقلب روی کارت‌های اعتباری کاربران، خسارات وارده را به سرعت جبران کرده و اعتماد آن‌ها را جلب کنند.

۱-۹ یافتن فرصت‌های جدید برای ثبات. مدل‌های مالی مناسب و درخور می‌توانند ســودآوری و موفقیت برای سیستم‌های هویتی در پی داشته باشند. این مدل‌ها، معمولا با به اشتراک‌گذاری هزینه‌ها و ریسک‌ها میان ذینفعان و سازمان‌های مختلف و ارائه طیف گسترده‌ای از خدمات نوین و متنوع، برای سیستم‌های هویتی درآمدزایی می‌کنند. در کره جنوبی، شــرکت‌های بخش خصوصی منافع و سودآوری زیادی از راه‌اندازی و مشــارکت در راهکار هویتی تی‌اوث (T-Auth) از آن خود ساخته‌اند. سیستمی که بخش قابل توجهی از بازار را پوشش داده است و با ادغام فنی و تجاری کسب‌وکارها، درآمدهای هنگفتی را به سمت آن‌ها روانه می‌کند. تبادل اطلاعات نیز تا زمانی که به حقوق کاربران احترام بگذارد و حریم خصوصی آن‌ها را رعایت کند، می‌تواند به درآمدزایی بیانجامد. ضمن این‌که این احترام به حریم خصوصی و حقوق کاربران، به نوعی ارزش آفرینی برای آن‌ها نیز قلمداد می‌شود و در نهایت منجر به پذیرش، توسعه، سودآوری و ثبات سیستم می‌گردد.

با تکیه بر گام‌های آغازین عنوان شده، گام بعدی برای سیاست‌گذاران، رهبران سازمان‌ها و طراحان دستیابی به یک طراحی موفق است که بتواند برای کاربران ارزش آفرینی کند. هر سیستم و اکوسیستمی نیاز به یک طراحی منحصربه‌فرد و متفاوت دارد که به نیازهای کاربران، دست‌اندرکاران و بازیگران اصلی آن‌ها بستگی دارد. اما اصولی که کلیه این سیستم‌ها و اکوسیستم‌ها رعایت می‌کنند، در حالت کلی مشترک و واحد است.

۲. طراحی و ساخت سیستم‌های کاربر محور

۲-۱ حداکثر ارزش کاربری و عملکرد

- طراحی برای پذیرش گسترده‌تر و شناخت متقابل. در صورتی که چنین طراحی صورت پذیرد، طرفین متکی بسیاری سیستم را به رسمیت خواهند شناخت و کاربران بسیاری به سمت اعتماد و استفاده از آن سرازیر خواهند شد. این می‌تواند به به‌روز نگه داشتن داده‌های هویتی کمک شایانی کرده و منجر به ایجاد مدل‌های کسب‌وکاری باثبات و پایدار شود. به عبارت ساده‌تر، شناخت متقابل به پذیرش و استفاده می‌انجامد.

- طراحی برای دسترسی در دنیای واقعی. در کنار طراحی و پیاده‌سازی یک سیستم مبتنی بر هویت دیجیتال که راحتی، سهولت در ثبت‌نام و عدم تبعیض را به دنبال دارد، طراحان باید این موضوع را نیز مد نظر داشته باشند که کاربران، در کنار تمام این راحتی‌ها به دنبال دسترسی نیز هستند. به عنوان مثال، برای افتتاح حساب بانکی با استفاده از یک شناسه دولتی، ممکن است برخی اطلاعات فراتر از داده‌های هویتی عادی کاربران موردنیاز باشد.

- تعریف و برقراری ارتباط. برای توسعه و عمق بخشیدن به پذیرش، سیستم‌های هویتی نه تنها باید راحت و قابل دسترسی و استفاده باشند، بلکه باید به نحوی طراحی شده باشند که کاربران نیز این راحتی و سودمندی را احساس کنند. تعریف، تبیین و توصیف روشن استفاده‌های موردی یک سیستم هویتی به کاربران، طرفین متکی و سایر شرکت‌کنندگان در اکوسیستم، و برقراری ارتباط موثر با آن‌ها، می‌تواند به پذیرش و توسعه بیش از پیش سیستم کمک کند.

- پیوند هویت‌های انسانی به غیرانسانی. بسیاری از دستگاه‌ها، عناصر حقوقی و عناصر فیزیکی و مجازی نیاز به هویت‌های دیجیتال دارند. طراحان و سیاست‌گذاران باید به خوبی نحوه برقراری ارتباط عناصر انسانی با این عوامل را مد نظر قرار داده و در مورد نحوه پاسخگویی به این تعاملات تحقیق کنند. به عنوان مثال، دستگاه‌های زیر مجموعه فناوری مدرن اینترنت اشیا، امروزه فرایندهای خرید را به شدت تسهیل و تسریع کرده‌اند چرا که فرایندهای احراز هویت و اعلام آسیب‌پذیری به شدت ساده‌سازی شده است و می‌توان با یک عبارت صوتی یا یک کلمه به هدف مورد نظر دست یافت. البته، این قبیل اتصالات و پیوندها باید به صورت دقیق در بوته ارزیابی قرار گیرند تا

اطمینان حاصل شود که داده‌های مربوط به هویت‌های دیجیتال غیرانسانی در امنیت هستند.

- احترام به حریم خصوصی در طراحی. برای کاهش هر چه بیشتر مداخلات انسانی در سیستم‌های هویتی، حفظ اصول حریم خصوصی و احترام به خصوصی کاربران باید در طراحی مدنظر قرار گیرد و در عین حال، رگولاتورها نیز نحوه پایبندی به این اصول و نتایج حاصله را به صورت مداوم رصد کنند.

- حفظ تعادل بین راحتی و امنیت. برای بهینه‌سازی مشکل راحتی / امنیت و حفظ تعادل بین دو فاکتور مهم، و در عین حال گردآوری کم‌ترین حجم داده‌های موردنیاز، یک سیستم هویتی ممکن است راه‌ها و مسیرهای زیادی برای پیاده‌سازی پیش روی خود داشته باشد. مسیرهایی که بسته به تراکنش‌های ارائه شده و سطح ریسک‌ها دارای تنوع بالایی هستند. به عنوان مثال، باز کردن یک حساب کاربری در رسانه‌های اجتماعی یا دسترسی به آن، ممکن است به اندازه افتتاح حساب بانکی در یک بانک سنتی، نیاز به حجم بالایی از داده‌های شخصی و هویتی و عبور از فرایندهای احراز هویت پیچیده نداشته باشد.

۲-۲ شمول در فضای فناوری، صنعت، فرهنگی و حوزه بازار

- در نظر گرفتن زمینه. این‌که حریم خصوصی برای افراد با توجه به فرهنگ آن‌ها، ارزش‌های شخصی‌شان و نوع تراکنش‌های مورد نیاز به چه مفهوم است، دارای اهمیت است. ضمن این‌که این باید در نظر داشت این حریم خصوصی، به مروز زمان تا چه میزان تحول و تکامل خواهد یافت. به عنوان مثال، مقررات عمومی حفاظت از داده اتحادیه اروپا اکنون برخی از فاکتورها و اصول کلیدی عمومی را برای حفاظت از داده‌های شخصی قابل شناسایی افراد تبیین کرده است.

- صرفا ایمن بودن کافی نیست. یک سیستم هویتی موفق یا به اصطلاح خوب، باید بتواند در کنار ایمن بودن در قبال ریسک‌ها و تهدیدهای سایبری، از کاربرانش نیز محافظت کند. چنین سیستمی باید بتواند سیاست‌هایی را برای مسسولیت‌پذیری در استفاده، به اشتراک گذاری و مدیریت داده‌ها تبیین کند.

- تحقق انعطاف‌پذیری و چابکی. سیستم‌های هویتی حال حاضر دنیا، با برخی چالش های نوظهور مواجه هستند که ناشی از تحولات شدید مبتنی بر فناوری است. برای پاسخگویی به این تحولات، سرعت بسیار مهم است. یک معماری چابک و در عین حال انعطاف‌پذیر می‌تواند برای بقای سیستم‌های هویتی در بحبوحه تحولات حیاتی باشد.

- برقراری اصول حفاظت از داده در مورد عناصر غیرانسانی. دستگاه‌ها و گزاره‌های حقوقی به شدت رو به سوی دیجیتالی شدن و مشمولیت هویت‌های دیجیتال گذاشته‌اند و در این میان، قرار گرفتن داده‌های این عناصر غیرانسانی در معرض اسیب، نشت یا سوء استفاده می‌تواند پیامدهای جبران‌ناپذیری برای افراد و سازمان‌ها در پی داشته باشد. حیوانات و منابع طبیعی حساس ، به‌ویژه آن‌ها که در معرض انقراض یا شکارهای غیر مجاز هستند، جزو عناصر غیرانسانی به شمار می‌آیند که نیاز به حریم خصوصی و اصول حفاظت از داده دارند.

- شفافیت و آموزش. کاربران باید در سایه شفافیت و آموزش، هر آن‌چه که هنگام به اشتراک‌گذاری داده‌های هویتی‌شان اتفاق می‌افتد را درک کنند. این‌که چه کسانی از این داده‌ها استفاده می‌کنند، دلیل این دسترسی و استفاده چیست و چگونه داده‌ها را پردازش کرده و مورد استفاده قرار می‌دهند. آموزش، برای توسل به این درک باید فراتر از کاغذبازی‌های متداول و کتبی باشد و کاربران به صورت عملی به درکی جامع از داده‌ها و سیستم‌های هویتی برسند. ضمن این‌که این آموزش‌ها باید روشن و به اندازه کافی جذاب باشند تا کاربران را ورطه بی‌تفاوتی بیرون بکشند.

- کار با اینترنت اشیا. در حال حاضر، میلیون‌ها دستگاه متصل در خانه‌ها و اداره‌ها وجود دارند و میلیارد دستگاه دیگر نیز در حال پیوستن به آن‌ها هستند. تمامی این دستگاه‌های دارای هویت‌های دیجیتالی هستند که به کاربران و سازمان‌ها متصل‌اند و سبب توسعه تعامل‌پذیری و در ازای آن بروز برخی چالش‌های مدیریتی و امنیتی می‌شوند. یک سیستم هویتی خوب باید بتواند کلیه این دستگاه‌ها را در چرخه حیات‌شان به روشنی، سادگی و دقت مدیریت کند. فناوری‌های نوین همچون هوش مصنوعی و تجزیه و تحلیل‌های پیشرفته می‌توانند به حفاظت از این قبیل دستگاه‌ها، کاربران آن‌ها، زیرساخت‌های صنعتی که این دستگاه‌ها بخشی از آن هستند و سایر عناصر مسئول کمک کنند.

- اکوسیستم‌های جدید. شرکت‌کنندگان در اکوسیستم‌های هویتی که قبلا به آن‌ها اشاره کردیم، این قابلیت و قدرت را دارند تا پا فراتر از حوزه‌ها و مرزهای جغرافیایی گذاشته، و اکوسیستم‌های بسیار وسیع‌تر و متنوع‌تری از سیستم‌های هویتی سابق ایجاد کنند. برای این‌که این قبیل اکوسیستم‌های نوپا بتوانند به ارزش آفرینی و موفقیت برسند، نمونه‌های آزمایشی و آزمون و خطاهای بسیاری نیاز خواهد بود تا تعامل‌پذیری مورد انتظار حاصل شود.

۲-۳ شناسایی و انتخاب بهترین الگو

- نگاهی به زمینه، ارزش و اکوسیستم. زمانی که به دنبال ارزیابی الگوهای ارائه شده برای سیستم‌های هویتی هستید، از شناسایی و اعتبارسنجی افراد و دست‌اندرکاران اکوسیستم شروع کنید و این‌که آن‌ها چه نیازها و انتظاراتی دارند و مهم‌تر این‌که ارزش برای آن‌ها به چه مفهومی است. سپس لازم است به شرایط اجتماعی و اقتصادی، زمینه‌های سیاسی و فناوری از جمله دسترسی و اتصال، نگاه کنید.

- آمادگی برای تکامل الگوهای موجود کنونی. نسخه‌های هیبریدی سه الگویی که در فصل دوم به تفصیل مورد بحث و بررسی قرار گرفتند، در حال ظهور هستند. سیستم‌هایی که در مالکیت دولت‌ها هستند و توسط آن‌ها مدیریت می‌شوند، به احتمال زیاد در بازار هویت‌های دیجیتال سیطره خواهند داشت، اما این موضوع توسعه زمینه‌های مشارکتی برای پیاده‌سازی سایر الگوها را نفی نمی‌کند. شناخت متقابل سیستم‌ها از یکدیگر می‌تواند در روند فزاینده رشد این مشارکت‌ها تاثیر بسزایی داشته باشد.

- تدارک مدل‌های عملیاتی و حکومتی نوین. هرچه الگوهای سیستم‌های هویتی به سمت اکوسیستم‌های بزرگ‌تر پیش می‌رود، طراحان و عملیات ایزوله و محدود سابق نیز نیاز به تحول و مدل‌های حکومتی و عملیاتی نوینی می‌یابند که بتواند مالکیت، سرمایه‌گذاری، حقوق معنوی، مسئولیت‌پذیری‌ها و فرایندها را به شکل کارآمدتری تعریف کند. تجربه تشکیل کنسرسیوم در سایر مناطق می‌تواند به بسط این قبیل مدل‌ها کمک کند.

۲-۴ شناسایی و انتخاب بهترین رویکردها برای انطباق و امنیت

- طراحی برای انعطاف‌پذیری. سیستم‌های مبتنی بر هویت دیجیتال ممکن است میلیون‌ها کاربر داشته باشند، بخشی از یک اکوسیستم بسیار پیچیده باشند، و در معرض حملات سایبری بزرگ قرار بگیرند. هر سیستم، دارای مدل حکومتی و عملیاتی منحصربه‌فردی است که باید قادر باشد به تمام چالش‌ها و تهدیدهای احتمالی پاسخ گوید. منظور از انعطاف‌پذیری توانایی انطباق با تهدیدها و چالش‌های در حال رشد است. چالش‌هایی نظیر تحولات پیوسته تعریف خوب از منظر کاربران و مفهوم

ارزش برای آن‌ها، یا تهدیدهایی نظیر تهدیدهای سایبری که همسو با پیشرفت فناوری تغییر می‌یابند.

- ایمن‌سازی پیوندها. این‌که معماری و زیرساخت‌های یک سیستم هویتی و داده‌های آن را ایمن کنید به تنهایی کافی نیست. طراحان سیستم‌های هویتی باید روی ایمن‌سازی رابط‌های سیستم، تاریخچه‌ای که به ثبت می‌رساند، ارتباطات و اتصالات افراد به دستگاه‌ها، نهادهای حقوقی و سایرین نیز کار کنند.

- تنظیم و برقراری سازوکارهایی برای جبران. چارچوب‌های تعریف شده برای یک سیستم هویتی نه تنها باید بتوانند داده‌ها را به دقت گردآوری کرده و به ثبت برسانند، بلکه باید بتوانند هرگونه اختلال یا خطا در شبکه را نیز شناسایی کرده و برطرف نمایند. چه این خطاها به صورت طبیعی و ناشی از تکامل طبیعی سیستم بشاند و چه منشا خارجی نظیر تقلب یا سوء مدیریت داشته باشند. با در چنته داشتن سازوکارهایی برای رفع اشتباهات و اشکالات و ارائه منابع در صورت لزوم، سیستم‌های دیجیتال می‌توانند اعتبار و اعتماد لازم برای بقا را حفظ کنند.

- نظارت مستقل در چارچوب‌های حقوقی. مقامات دولتی و نظارت‌ها و چارچوب‌های آن‌ها نقشی اساسی در حصول اطمینان از رعایت حریم خصوصی در سیستم‌های هویتی ایفا می‌کنند، اما این امکان نیز وجود دارد که برخی از سازمان‌های دولتی، به نحوی که برای کاربران قابل قبول نیست یا به تبعیض میان آن‌ها می‌انجامد به این داده‌ها دسترسی داشته باشند. نظارت مستقل، نظیر کمیته‌های حفظ حریم خصوصی، می‌تواند برای پاسخگویی به این مشکل کمک کننده باشد.

۵-۲ کاهش خطرات و حل و فصل مشکلات

- بده بستان پایدار / جامع را در نظر بگیرید. همان طور که در فصل دوم نیز به تفصیل عنوان شد، سیستم‌های هویتی برای این‌که بتوانند در دراز مدت تاثیرگذار باشند، ملزم به پایداری مالی و عملیاتی هستند. با این حال تمرکز بیش از اندازه روی افزایش درآمدزایی می‌تواند کاربران را از سیستم محروم کرده و از چرخه خارج کند. با توجه به فناوری‌ها، فرصت‌ها و چالش‌هایی که در دنیای امروز روزبه‌روز نیز به تعداد آن‌ها افزوده می‌شود، انعطاف‌پذیری ممکن است مستلزم صرف هزینه‌های هنگفت و تن دادن به کاهش درآمد باشد. از طرفی، در قبال پایداری مالی باید پذیرش و شمول را نیز مدنظر قرار داد. برای درک بهتر این تنش، سیستمی را در نظر بگیرید که برای توسعه شمول دست به دامان ارائه خدمات بدون کارمزد برای کاربران شده است و پایداری مالی خود را در معرض تهدید قرار داده است.

- ساخت یک بده بستان رضایت‌بخش با حفظ حریم خصوصی. برای دستیابی به یک تجربه دیجیتال آسان، شخصی‌سازی شده و همه‌جانبه، اغلب افراد راضی به افشای داده‌های شخصی خود می‌شوند. یک ابزار قدرتمند برای طراحان، اعطای حق انتخاب به کاربران برای برقراری تعادل بین حریم خصوصی و راحتی از جمله این‌که افراد بتوانند در عین سهولت استفاده از خدمات و محصولات ناشناس باقی بمانند، در سایه آموزش و شفافیت است.

- ساخت دستورالعمل‌هایی برای مسئولیت‌پذیری. حتی امن‌ترین سیستم‌های هویتی نیز خالی از آسیب نیستند. برای پاسخگویی به این مشکل لازم است در مورد نحوه تخصیص و مدیریت مسئولیت‌ها برنامه‌ریزی شود و بیمه‌های هویت دیجیتال نیز مدنظر قرار گیرند. آموزش افراد، طرفین وابسته و سایر ذینفعان، نسبت به این‌که در صورت بروز حادثه باید چکار کنند می‌تواند بسیار کمک کننده باشد.

۳. بازگو کردن ارزش در آینده

۳-۱ در نظر داشتن نیازهای در حال توسعه برای جلوگیری از تبعیض. جنسیت، سن یا قومیت شما، ممکن است امروز و در محلی که در آن زندگی می‌کنید شما را در معرض تبعیض قرار ندهد، اما این‌که همین داده‌ها فردا روز و در یک کشور بیگانه چه سرونوشتی را برایتان رقم خواهد زد، در هاله‌ای از ابهام قرار دارد. هویت‌های دیجیتال ما باید همسو با تغییرات زندگی در طول زمان، ما را از هرگونه آسیب و تبعیض مصون بدارند. تلاش برای گردآوری و ثبت حداقل داده‌هایی که ممکن است روزی به تبعیض یا پایمال شدن حقوق افراد بیانجامند، و همچنین دادن حق انتخاب به افراد برای برگزیدن داده‌های قابل افشا، می‌تواند کمک کننده باشد.

۳-۲ آمادگی برای مقابله با چالش‌های ناشی از نهادهای حقوقی، دستگاه‌ها، منابع طبیعی و غیره. نه تنها هر نهاد حقوقی، دستگاه یا منبع طبیعی نیاز به هویت دیجیتال دارد، بلکه ماجرا از این نیز مهم‌تر و فراتر است. به عنوان مثال، در دنیای مدرن امروز بسیاری از عناصر غیرانسانی دارای دوقلوی دیجیتال هستند، به ویژه در دنیای تجارت و در مدیریت زنجیره‌های تامین. برای افرادی که به دنبال استفاده، دادوستد، ردیابی، تاثیرگذاری، فعالیت، تراکنش یا مدیریت از جانب این نهادها هستند، سیستم‌های هویتی نیاز به طراحی دقیق و مناسب، مسئولیت‌های مدون و مشخص، و اکوسیستم‌هایی با بازنگری‌های منظم دارند.

۳-۳ آمادگی برای رودررویی با نهادهای مجازی، هوش مصنوعی و غیره. هرچه اهمیت و کارایی فناوری‌های مجازی و مبتنی بر هوش مصنوعی رشد و توسعه بیشتری می‌یابند، سیستم‌های هویتی نیز بیش از پیش برای توسعه، پذیرش و ماندگاری به این قبیل فناوری‌ها وابسته می‌شوند. سیستم‌های هویتی باید کلیه جوانب استفاده از این قبیل فناوری‌ها از جمله چت‌بات‌های مبتنی بر هوش مصنوعی، را ارزیابی کنند و اطمینان حاصل کنند که این ابزارها می‌توانند رضایت کاربران را برآورده کنند. ضمن این‌که باید مسئولیت و عواقب استفاده از این قبیل ابزارها و فناوریها را نیز در نظر بگیرند.

۳-۴ در نظر گرفتن پیامدهای ناشی از فناوری‌های نوین. فناوری‌ها و نوآوری‌های نوین بسیاری هستند که می‌توانند مدیریت داده‌ها و حریم خصوصی کاربران را برای آن‌ها با کاهش اصطکاک‌های موجود تسهیل کنند. اما این فناوری‌ها و نوآوری‌ها برخی چالش‌ها و پیامدهای مضاعف نیز با خود به همراه خواهند داشت. هوش مصنوعی و بلاکچین جزو فناوری‌هایی هستند که در کنار مزایای خارق‌العاده خود نیاز به ارزیابی زیربنایی، طراحی و تنظیم مقررات برای کسب اطمینان از رعایت حریم خصوصی دارند.

این گزارش با حمایت شرکت ققنوس توسط تیم راه پرداخت، ترجمه و بازتولید شده است