

هویت در دنیای دیجیتال

فصلی جدید در قراردادهای اجتماعی



“

هویت ما ارزشمند است، هر برنامه مبتنی بر هویت دیجیتال باید از لحاظ اعتماد، کنترل و حسابرسی معنی دار باشد. علیرغم این که توافق در این اصول مهم دشوار است، اما پیاده سازی آن ها به دلیل تلافی فاکتورهای سیاسی، اقتصادی، تکنولوژیکی، فرهنگی، حقوقی و اجتماعی بس دشوارتر نیز خواهد بود.

”

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

“

هر انسانی منحصر به فرد است. فاکتورهای بسیاری وجود دارد که ما و سلامت ما را تعریف می کند، 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 یافته ایم. 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 روش های 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)

“

هویت های دیجیتال، در صورتی که به خوبی طراحی شده باشند، می توانند منجر به تحول پذیری در تمام جوانب زندگی شوند. برای کشاورزان خرد که سرمایه های ناچیز خود را برای غلبه بر انزوای جغرافیایی، اقتصادی و اجتماعی و هم چنین تقسیم بندی های ناعادلانه که ریشه اصلی فقر در جهان هستند نگه داشته اند، این می تواند یک راهکار فوق العاده باشد. این راهکار می تواند در مقیاسی عظیم انجام شود.

”

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

“

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

”

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

“

همه ما می خواهیم در دنیای دیجیتال پیشرفت کنیم و هیچ کس نباید از این قافله عقب بماند. این، بدان معنی است که همه باید آموزش داده شوند تا بدانند چگونه باید از خود محافظت کنند و داده های آنلاین خود را ایمن نگه دارند و این، دقیقاً 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 قفل های 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 پیاده سازی 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 بیگرو، 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 سازمان ها، اشیا، دستگاه ها و اماکن بسط می دهد. این مدل، شالوده ای است که به هویت های ما این امکان را می دهد تا با سیستم های آنلاین در تعامل باشند، دستگاه های متصل ما را کنترل کنند، یادگیری هوش های اکتسابی ما را ارتقا دهند و از منابع زمینی حفاظت کنند. دستیابی به این حق برای رشد آینده ما حیاتی است، مهار مسئولیت پذیرانه نوآوری های فناورانه را در بر می گیرد و زندگی دیجیتال بهتر و مسئولیت پذیری را فراهم می سازد.

”

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

فهرست

۴	پیشگفتار
۵	خلاصه اجرایی
۷	چطور از این گزارش استفاده کنیم
۸	فصل اول: موردی در خصوص هویت دیجیتال خوب
۹	هویت، شکل دهی قراردادهای اجتماعی
۹	هویت های دیجیتال در زندگی روزمره ما
۱۱	رشد پیچیدگی و مسئولیت پذیری
۱۲	آینده ای واگرا
۱۲	پنج پارامتریک هویت خوب
	سیستم های هویتی امروز: سه طرح
۱۷	فصل دوم: منظور از خوب چیست؟
۱۸	بهبود هویت دیجیتال
۱۹	۱) متناسب با هدف
۲۰	۲) همه جانبه
۲۱	۳) سودمندی
۲۲	۴) ارائه حق انتخاب
۲۳	۵) ایمن
۲۵	فصل سوم: پیش به سوی آینده: روندها، فرصت ها و چالش ها
۲۶	چه اتفاقی می افتد؟
۲۶	روندها
۲۶	چالش ها
۲۷	فرصت ها
۲۸	فصل چهارم: اولویت هایی برای مشارکت بخش خصوصی و دولت
۳۰	پیوست ۱: ملاحظات طراحی برای دست اندرکاران

پیشگفتار

همان طور 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 این که 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، تعاملات مان 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 به فرد 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 پیش روی است. جامعه‌ای که متشکل از بازیگران قدر قدرتی 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 گیر و دار 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 این که 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 برگزار 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 کسب و کارها، 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 مر جعی 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 آن چه که تاکنون آموخته‌اید را مورد پرسش قرار می‌دهد و دانسته‌های شما در مورد کاربر محوری را خطاب قرار می‌دهد. این که مشتری مداری 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 مورد نیاز 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، آن گونه که از انقلاب چهارم دیجیتال انتظار می‌رود بر آورده نخواهد شد.

امید است که این گزارش بتواند به عنوان 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، همان طور که فناوری ها روز به روز در حال پیشرفت و توسعه هستند و نسل چهارم انقلاب دیجیتال در حال اتفاق افتادن است، هویت ما نیز به سوی دیجیتال شدن می رود. این هویت دیجیتال، تعیین می کند که چه محصولات، خدمات و اطلاعاتی را می توانیم 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 روبه

دیجیتالی شدن و اتصال به دنیای دیجیتال و مدرن گذاشته اند و در این میان، این هویت ما است که خود را در بحبوحه مدرنیته گم کرده و نمی داند 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، نوآوری ها، 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 سازمان ها در دنیای دیجیتال با آن مواجه شده اند.

در صورتی که امروز در عمل شکست بخوریم، در آینده ای نه چندان دور با سیستم هویتی روبه رو خواهیم شد که به تقسیم بندی های عمیقی در جامعه خواهد انجامید. تقسیم بندی جامعه به دو دسته افراد دارای هویت دیجیتال و افراد فاقد آن، که به تعبیری روشن تر، مساوی است با آینده ای که در آن، بخش عمده ای از افراد فاقد حق انتخاب، اعتماد و حقوق بشری خود در دنیای آنلاین بی کران 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 می کنند به شکلی دیگر رقم بزند. تحولی شگرف، که میلیاردها انسان از سراسر جهان را قادر به دسترسی به اقتصاد نوین، فرصت های سیاسی و اجتماعی و مزایای دیگر می کند و این امکان را به آن ها می دهد تا از ایمنی دیجیتال، حریم خصوصی و حقوق بشری بهره مند شوند.

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

نیاز به درک مشترک و اقدام هماهنگ

هویت های دیجیتال تکامل یافته اند. آن ها دیگر شامل قطعات منزوی و ساده ای از اطلاعات مربوط به افراد نیستند بلکه شبکه های پیچیده، مبتنی بر اینترنت و تلفیقی از داده های شخصی، تاریخ دیجیتال و الگوریتم ها و رابط هایی هستند که می توانند سبک زندگی افراد را متحول کنند. هویت های دیجیتال ما، به شکل معجزه آسایی در تمام فرایندهای زندگی مان و تمام فعالیت های روزمره ای که به سادگی تمام از کنارشان رد می شویم، تعبیه شده اند.

هویت های دیجیتال قابل بازبینی برای کسب و کارها، دولت ها و افراد ارزش آفرینی می کنند. با این حال، فقدان اصول، استانداردها، هماهنگی ها و نقاط اشتراک بین ذینفعان مختلف هنوز هم در این تلاش ها و جریان های به راه افتاده مشاهده می شود 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 دولت ها، کسب و کارها و جوامع مدنی، گرد هم آمده و متعهد شدند تا در کنار هم و با مشارکت یکدیگر، یک آینده آرمانی برای هویت های دیجیتال رقم بزنند. از آن زمان تاکنون جمع کثیری به این جریان پیوسته اند و مجموعه ای پنج گانه از عناصر تاثیرگذار و لازم برای آینده مبتنی بر هویت دیجیتال را شناسایی کرده و ارائه

داده اند. تمام این پنج عنصر به یک اندازه حائز اهمیت هستند و برخی از آن ها، دارای تنش هایی با عناصر دیگر نیز هستند که نمی توان آن را نادیده گرفت. به عنوان مثال، ویژگی هایی که برای بهبود سطح امنیتی هویت های دیجیتال طراحی و ارائه می شوند ممکن است سطح راحتی آن ها را دچار چالش کرده و بر پیچیدگی های آن ها بیافزایند. هویت های دیجیتال کاربر محور، که به ایجاد ارزش واقعی برای افراد می انجامند و در نهایت منجر به پذیرش می شوند، بایستی در کلیه جوانب موفق ظاهر شوند.

۱. تناسب با هدف. هویت های دیجیتال خوب، راه حل قابل اطمینانی در دسترس اشخاص قرار می دهند تا بتوانند اعتماد لازم را ایجاد کنند، تا حقوق و آزادی های خود را اعمال کنند یا شایستگی خود برای استفاده از خدمات و محصولات دیجیتال را ثابت کنند.

۲. مشمولیت. هویت همه جانبه و مشمول، کلیه کسانی که دارای هویت دیجیتال هستند یا دست کم بدان احساس نیاز می کنند را از تبعیض ها و تقسیم بندی های مبتنی بر داده های هویتی می رهاوند. در سایه این عنصر، کاربران بدون دست و پنجه نرم کردن با فرایندهای احراز هویت پیچیده ای که امکان دارد آن ها را از برخی خدمات و تسهیلات محروم کنند، وارد تعامل با سازمان ها و همدیگر می شوند.

۳. سودمندی. هویت های دیجیتال سودمند، دسترسی کاربران به طیف گسترده ای از خدمات، محصولات و تعاملات سودمند را تضمین می کند و در توسعه و استفاده دارای سهولت هستند.

۴. ارائه حق انتخاب. افراد زمانی که بدانند چه سیستم هایی، توانایی استفاده و بهره برداری از داده های شخصی و عمومی آن ها را دارند، حق انتخاب خواهند داشت. ضمن این که در سایه این حق انتخاب، کاربران این امکان را خواهند داشت تا خودشان انتخاب کنند که چه داده هایی را با چه شرکت ها و سازمان هایی و تا چه مدت زمانی به اشتراک بگذارند.

۵. ایمن. امنیت می تواند شامل حفاظت از افراد، سازمان ها، دستگاه ها و زیرساخت ها از سرقت های هویتی، به اشتراک گذاری غیر مجاز داده ها و نقض حقوق بشر باشد.

در حال حاضر، سه نمونه اولیه از سیستم های هویتی در جهان وجود دارند. در سنتی ترین و معمول ترین حالت شاهد نمونه ها و سیستم های «متمرکز» هستیم که در آن، سازمان ها، عموماً دولت ها یا شرکت ها، هویت کاربران را مدیریت کرده و اطلاعات مبتنی بر هویت کاربران را به شیوه خود در سطح سیستم ایجاد و کنترل می کنند. این در حالی است که در مدل های دوم که تحت عنوان سیستم های «فدرالی» فعالیت می کنند، این نقش میان سازمان های مختلف توزیع شده است. سیستم هایی که جدیدترین مدل یعنی مدل «غیر متمرکز» را دنبال می کنند، عمدتاً در فاز آزمایشی قرار دارند و بر این اساس طراحی شده اند تا به افراد، قدرت عمل و کنترل بیشتری برای مدیریت داده های هویتی شان 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 چشم انداز 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 شرح می‌دهد. این که چرا ممکن است 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 چستی یک سیستم مبتنی بر هویت دیجیتال خوب می‌پردازد که می‌تواند پنج عنصر کلیدی ایجاد ارزش برای اشخاص را تأمین کند. ضمن این که در این فصل، نحوه دستیابی به این پنج عنصر نیز مورد بررسی قرار گرفته و کاربرد هر یک در قالب مثالی واقعی تشریح شده است.

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

فصل چهارم شش پیش‌زمینه و اولویت مورد نیاز برای همکاری و مشارکت 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 بررسی 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 عمیق تر آن‌ها مستلزم زمان و فرصت بیشتری است چراکه چنین مفاهیم مهم و گسترده‌ای، مستقیماً با افراد، فناوری‌ها و نیازهای هویتی و دیجیتال آن‌ها در ارتباط هستند.



فصل اول:

موردی برای یک هویت دیجیتال خوب



هویت - شکل دهی 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 اکتسابی مان و مجموعه‌ای از فرهنگ، خانواده، ملیت، احزاب، جنسیت یا هویت‌ها و مشخصات دیگر مان. با وجود این که همه ما این را درک کرده‌ایم، اما هویت هنوز هم به اهمیت خود پایرجاست.

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 (not 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 شکل دهی 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 ساختار شکنی‌های 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 استرگ و روزافزون از کلیه اطلاعاتی است که در خصوص ما وجود دارند، یا پروفایل‌ها و تاریخچه‌ای که از فعالیت‌های مان، رفتارها و تعاملات مان 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 افزایش 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 استانداردهای 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 شکل گیری آن باید با افرادی صورت گیرد که در دنیایی کاملاً 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 میلیارد ها 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 عذیده‌ای 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

هرچه ارتباطات دیجیتال و فعالیت‌های 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 تغییر مان اعم از تاریخ و محل تولد، یا شماره‌های ملی و امثال مارا 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.

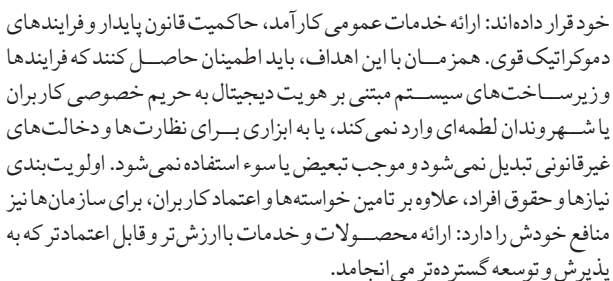
- پروفایل: می‌تواند شامل برخی مشخصات ذاتی نظیر اطلاعات بیومتریک یا مشخصات معین نظیر نام یا شماره‌های ملی افراد باشد.

- 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 می‌زند که اطلاعات مالی، مالیات‌ها، خریده‌ها، 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 روز به روز 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 ارائه دهنده 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.

مراقبت‌های بهداشتی
برای کاربران دسترسی به بیمه، خدمات سلامت: برای نظارت بر دستگاه‌های بهداشتی پوشیدنی‌ها؛ برای سازمان‌های ارائه‌دهنده خدمات سلامت اثبات صلاحیت



رشد ییچیدگی و مسئولیت پذیری

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 ورژن‌های 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 ز 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 می‌تواند 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 توأمان با این تعامل‌پذیری رعایت شود. سیستم‌هایی که

ارزش دادن به کاربر و حفظ اعتماد: در پی تلاش برای دادن راحتی و رفاه بیشتر به کاربران، خدمات شخصی سازی شده، و مدیریت ریسک های در حال رشدی نظیر سرعت های هوشی، ارائه دهندگان خدمات نیاز به حجم بسیار گسترده تری از داده ها 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 مسئولیت پذیری بیشتری نیز خواهد بود تا حقوق کاربران، امنیت آن ها و حریم خصوصی شان رعایت شده و در عین حال، اعتماد آن ها به سیستم نیز حفظ شود. طبیعتاً مدیریت چنین پیچیدگی و در پی آن مسئولیت سنگینی آسان نخواهد بود. درک مختلف سازمان ها، جوامع و کاربران از مفاهیم حریم خصوصی و امنیت نیز این پیچیدگی و دشواری را دوچندان می کند. دولت ها، در حالت کلی توسعه سیستم های مبتنی بر هوش دیجیتال را برای اهداف مشخصی در دستور کار

با اهداف مختلف و چندانگانه‌ای راه‌اندازی شده‌اند، نیاز به داده‌ها و سطوح اعتماد مبتنی بر هویت مختلفی نیز دارند، ضمن این که طراحی و پیاده‌سازی آن‌ها نیز تحت تأثیر 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 این که 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 جامع‌طرح 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 کاملاً مشهود است. کسانی که بتوانند از این انقلاب و نوآوری‌ها به نفع خود استفاده کنند، گوی سبقت را از سایر رقبا خواهند بود و مزایای دگرگون‌شده‌ای را از آن خود خواهند ساخت. کسانی که نتوانند، از قافله عقب خواهند ماند. در غیاب تلاش‌های متفکرانه 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 تأثیر مستقیم دارد. ما باید در اسرع وقت به مساله شمول در سراسر جهان پاسخ دهیم تا از ادامه تشکیل زیرساخت‌های نابرابر و دوکلاس 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 این که 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 در مان 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 بیمارمحورتری 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 تأثیر 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 تأیید 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 بخشد. 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 غیر قابل 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 مورد نیاز زانیز نمی‌دهد. ضمن این که، استفاده کنندگان از محصولات کشاورزی نیز به شدت تمایل دارند منشأ 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 تأمین را معرفی کنند. چنین زنجیره‌هایی، شفافیتی خارق‌العاده در مورد چرخه حیات محصولات در اختیار کاربران قرار می‌دهند. شفافیت در مورد منشأ محصولات، نقل و انتقالات و سفر آن‌ها و تحولاتی که در چرخه حیات و در زنجیره تأمین 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. پر واضح است که چنین مدلی، انگیزه‌های مورد نیاز برای پیشرفت را در سرسراکوسیستم جهانی تأمین 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 در صدد 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، پسوندها و غیر صورت می‌گیرند و هویتی را احراز می‌کنند که قبلاً تثبیت شده است.

پنج پارامتر یک هویت خوب

در نشست سالانه مجمع جهانی اقتصاد سال ۲۰۱۸ در داووس، مجموعه‌ای متشکل از دینفغان، 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 می‌تواند 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. متناسب با هدف. یک هویت دیجیتال خوب راهکاری قابل اعتماد برای افراد است تا بتوانند نسبت به هویتی که ادعا می‌کنند جلب اعتماد کنند، و در سایه این هویت به آزادی‌ها و حقوق خود دست یافته یا توانایی شرکت 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 بهره‌جویند؛ 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 آن‌ها را دشوار و محدود ساخته است.

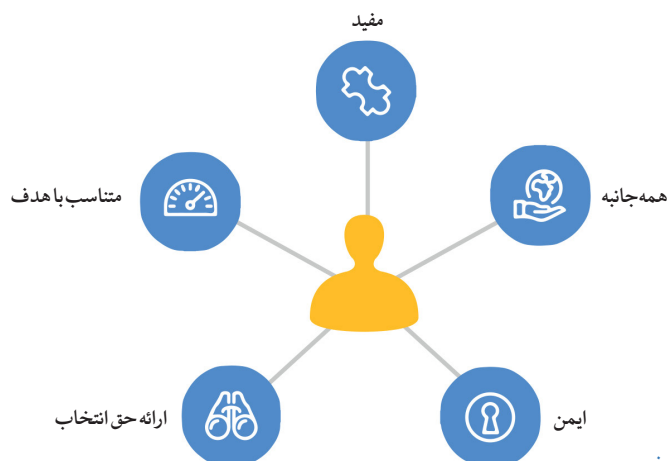
۴. ارائه حق انتخاب. افراد، در صورتی که بتوانند سیستم‌های استفاده کننده از داده‌های هویتی خود را شناسایی کرده و از اهداف آن‌ها سر در بیاورند دارای حق انتخاب خواهند بود. این‌که قادر باشند خود تصمیم بگیرند که کدام داده‌ها، در اختیار کدام سیستم‌ها قرار گیرد و از این داده‌ها با چه هدفی و برای چه مدت زمانی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

۵. ایمن. امنیت شامل حفاظت از افراد، سازمان‌ها، دستگاه‌ها و زیرساخت‌ها از سرقت‌های هویتی، به اشتراک‌گذاری‌های غیر مجاز و نامعتبر داده‌ها و نقض حقوق بشر است. چنین امنیتی در حال حاضر به شکا حقیقی و جامع پیاده‌سازی نشده است، چرا که داده‌های دیجیتال هویتی، هنوز به شکل قابل استفاده و استاندارد گردآوری نشده‌اند و اطلاعات، در سراسر حوزه دیجیتال به شکل ناهمگون پراکنده‌اند.

سیستم‌های هویتی امروز: سه طرح

سیستم‌های هویتی امروز و سیستم‌های هویتی در حال ظهور فردا، عموماً به سه دسته کلی تقسیم می‌شوند: متمرکز، فدرالی و غیر متمرکز. همان‌طور که از عنوان آن‌ها نیز برمی‌آید، زیرساخت هر یک از این مدل‌ها، پیاده‌سازی برای پذیرش و جلب اعتماد، چالش‌ها و مزایای هر یک از آن‌ها برای افراد و کاربران است که آن‌ها را از سایرین متمایز می‌سازد.

همان‌طور که انتظار می‌رود، سنتی‌ترین و معمول‌ترین طرح برای مدل هویتی مدل متمرکز است، که در آن 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 میان‌سازمان‌ها یا شرکت‌های مختلفی تقسیم شده است. سیستم‌هایی که جدیدترین مدل یا همان مدل غیر متمرکز را دنبال می‌کنند، به دنبال دنیایی آرمانی برای کاربران هستند که در آن، افراد خود روی هویت‌های دیجیتال و داده‌های مربوط به آن کنترل دارند و اطلاعات هویتی خود را شخصاً مدیریت می‌کنند.



شکل شماره ۲: پنج عنصر اصلی یک هویت خوب

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 آی دی سوئد؛ سیستم احراز هویت بریتانیایی گاو. یوکی و ریفای	نمونه آزمایشی آموزش 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	عموم‌الاری 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 ارائه‌دهندگان 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 ارائه‌دهنده 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-آی دی استونی یا سیستم احراز هویت بیومتریک ادهار هندوستان، یا یک سازمان بخش خصوصی نظیر یک سیستم بانکداری و یا یک شرکت ارائه‌دهنده 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 و ویژه خود عبور می‌دهند.

سیستم‌های هویتی دولت‌ها یا سیستم‌هایی که توسط ارائه‌دهندگان 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، به ویژه در مورد تراکنش‌های باریسک بالا، با

چنین سیستم‌هایی اقدام کنند. در سیستم‌هایی که فرایندهای اثبات هویت ناکارآمد، 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 بزنند. هنوز هم بسیاری از پلتفرم‌های دیجیتال در حال توسعه سیستم‌های تایید هویت و اعتبارسنجی دیجیتال خود هستند تا بتوانند طیف گسترده‌تری از کاربران و ارائه‌دهندگان خدمات را به سمت خود جذب کنند. وی‌جت 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 سر بلند بیرون بیایند، این امکان را خواهند داشت تا به خدمات و محصولات ارائه شده توسط ارائه‌دهندگان 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 پیاده‌کند 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 ارائه‌دهندگان و مالکین سیستم‌های هویتی، با نهادها دولتی و بخش خصوصی نیز دست‌دوستی 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 تعامل پذیری 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 غفلت می‌تواند در راه روی برخی سوء استفاده‌ها نظیر نظارت‌های غیر مجاز، 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 عموماً دارای دو عضو یا دو شرکت کننده است. دو عضو که کاملاً نیز یکدیگر را می‌شناسند. اما در اکوسیستم‌های هویتی مدرن امروز، تعداد زیادی عنصر نقش آفرین 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
- کنترل‌کننده 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 یارد دسترسی به محصولات، خدمات و یا داده‌ها به هویت‌های دیجیتال وابسته‌اند.
- متولیان یا پشتیبانان، که هویت‌های دیجیتال را قادر می‌سازند تا وارد عمل شوند.
- ورگولاتورها، 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 به‌شناسایی 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 برای مسافرت‌های برون مرزی طراحی و ارائه شده‌اند. در حالت کلی، سازمان‌ها 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 معمولاً 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 تعامل پذیری، 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 غالباً 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 با 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

آدرس دهی به الزامات غیر متمرکز سازی آماده شوند. تخصیص مسئولیت برای جبران و مدیریت ریسک‌ها و نشست‌های اطلاعاتی احتمالی در این قبیل سیستم‌ها نیز از پیچیدگی بالایی برخوردار است. احتمالاً، برای این‌که بتوانند به روشی صحیح از این سیستم‌های هویتی استفاده کرده و در قبال داده‌های خود مسئولیت‌پذیر باشند، نیاز به آموزش خواهد بود.

دیپلم‌ها و صدور سایر کواهینامه‌های 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 صورت 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، مستقیماً به نحوه اثبات هویت و فرایندهای مدیریت داده برمی‌گردد که این نیز به نوبه 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 برمی‌گزینند، اعتماد بیشتری به سیستم خواهند داشت تا افرادی که با سازمان‌ها یا کاربران شخصی طرف هستند.

نقاط قوت

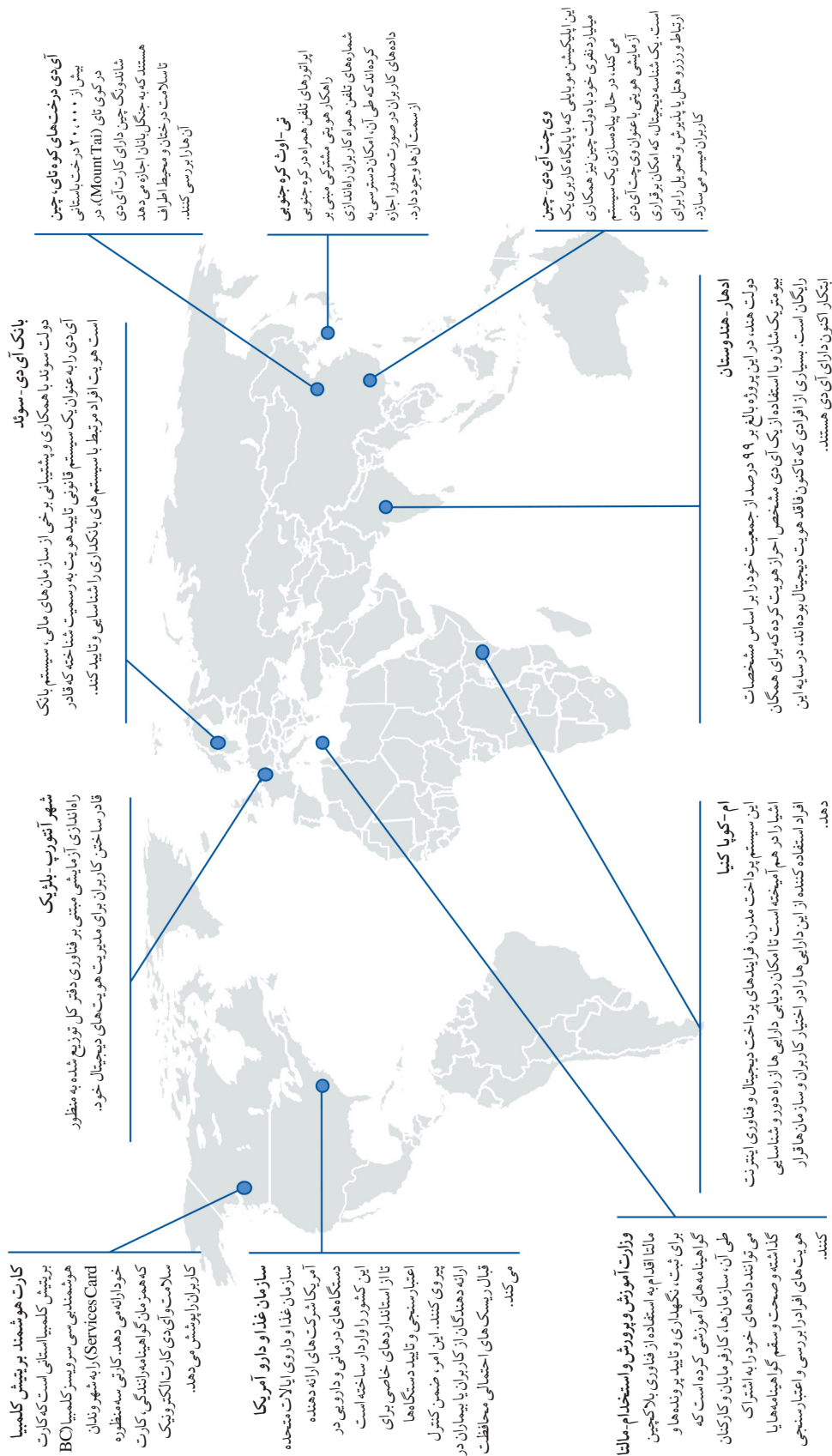
مهم‌ترین نقطه قوت یک سیستم هویتی غیر متمرکز کنترل کاربران روی داده‌ها و شفافیتی است که به آن‌ها ارزانی می‌کند. کنترل روی این‌که کدام داده‌های هویتی می‌تواند به اشتراک گذاشته شوند، با چه سازمان‌ها و افرادی به اشتراک گذاشته شوند و این به اشتراک گذاری تا چه زمانی می‌تواند ادامه پیدا کند. ضمن این‌که سیستم‌های 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 ایجاد ارزش برای آن‌ها می‌انجامد. به علاوه، تعامل‌پذیری یکی از ماهیت‌های عمده و منحصر به فرد 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 فایز از قراردادها و چارچوب‌های قانونی بانک‌ها و دولت‌ها وارد تراکنش می‌شوند. بسیاری از مدل‌های اعتمادی دولت‌ها و بانک‌ها برای سیستم‌های مترکز 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، هر چند 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 مترکز 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

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



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 این که هویتی دیجیتال به افراد بخشیده‌اند، اما نمی‌توانند دسترسی کاربران به برخی خدمات و محصولات مورد نیازشان را تأمین 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 افزون‌تر 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 مورد نیاز 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 این که منظور از خوب، به معنی واقعی کلمه چیست. ضمن این که 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 خط‌مشی‌ها 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 توانمند تأمین 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.

تجارب دسترسی 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، لزوماً بهترین راهکارها را نشان نمی‌دهند، اما می‌توانند در شکل‌گیری بینش در شما کمک کننده باشند.

شکل شماره ۵: پنج عنصر مورد نیاز 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 هیچ گونه خطایی در داده‌های هویتی وجود ندارد. این دقت در تمام جزئیات مهم است و باید به‌روزرسانی شود.

منحصر به‌فرد بودن: شکی نیست که در میان طیف گسترده‌ای از کاربران یک سیستم هویتی، هر یک از افراد منحصر به‌فرد هستند. نیاز به منحصر به‌فرد بودن به ویژه در تراکنش‌هایی که سطح بالایی از ریسک را تجربه می‌کنند غیر قابل 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.

مقیاس پذیری: سیستم‌ها باید بتوانند همسو با ارتقای انتظارات و تقاضا رشد کنند.

این عنصر چرا اهمیت دارد؟

دقت و منحصر به‌فرد بودن پیش‌نیازهای تایید هویت و احراز هویت یک‌فرد 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 منحصر به‌فرد بودن

منحصر به‌فرد بودن، در عین حال که به کاهش تقلبات و تخلفات هویتی می‌انجامد، هویت‌های دیجیتال را قابل اطمینان‌تر نیز می‌کند.

راه‌های زیادی برای تثبیت و توسعه منحصر به‌فرد بودن هویت‌های دیجیتال بین توده کاربران وجود دارد. یک راهکار جامع که امروزه نیز که مورد استفاده قرار می‌گیرد، اعطای نام‌های کاربری منحصر به‌فرد به کاربران، درست مانند آنچه که در حساب‌های کاربری یا در کارت‌های اعتباری و... مشاهده می‌کنید و تلفیق این نام‌های کاربری با رمزهای به اشتراک گذاشته است و در ادامه، گردآوری و ثبت مجموعه‌ای از داده‌های چندگانه اعم از لوکیشن، آی‌پی‌آدرس و یا تاریخچه فعالیت کاربران و ترکیب آن‌ها با این گذرگاه‌ها و نام‌های کاربری است. روش رایج دیگری که وجود دارد، استفاده از داده‌ها یا مشخصات بیومتریک کاربران است. برخی از ویژگی‌های منحصر به‌فرد و ذاتی افراد مانند ویژگی‌های چهره، اثر انگشت یا اسکن‌های عنبیه جزو همین مشخصات بیومتریک هستند.

با این حال، علیرغم این که مشخصات بیومتریک کاربران دارای تضمین هویتی بالایی هستند، اما مستلزم احتیاط، آموزش و ورزیدگی عملیاتی هستند. در صورتی که طراحی ضعیف باشد، ممکن است به محرومیت یا حذف کاربران از سیستم بیانجامد. کیفیت اثر انگشت‌های دریافتی از کاربران ممکن است در طول زمان افت پیدا کند. ضمن این که در مورد کارگرانی که با دست کار می‌کنند، افرادی دارای زخم در انگشتان خود هستند یا از نقص عضو رنج می‌برند، چالش‌های جدی مواجه سیستم احراز هویت و تایید هویت بیومتریک خواهد بود تا زمانی که این قبیل مشکلات به نحو درست پاسخ داده شوند. با توجه به این که داده‌های بیومتریک کاربران از جمله اطلاعات منحصر به‌فرد، قابل شناسایی، حساس و شخصی کاربران هستند، الزامات و ملاحظات امنیتی و حریم خصوصی پیرامون آن‌ها باید به شکل کاملایی عیب و نقصی پیاده‌سازی شوند.

توصیه می‌شود که تلفیقی از این راهکارها را به کار ببندید یا بسته به نوع تعاملات، سطح ریسک‌پذیری سازمان، الزامات انطباقی و رگولاتوری و سطح اطمینان از

داده‌ها و تراکنش‌ها مدل‌های مختلفی را برگزینید. به عنوان مثال، برای دریافت ویزای مسافرتی داده‌های مورد نیاز، در میان سایر داده‌های هویتی ممکن، عبارت خواهند بود از نام، تاریخ تولد، تاریخچه سفری، و برخی مشخصات بیومتریک نظیر اثر انگشت و تصویر چهره کاربران. در حالت کلی، برای کسب اطمینان از صحت و سقم و اعتبار داده‌ها، بهترین رویکرد این است که داده‌های منحصر به‌فرد را در اولویت قرار دهید.

مشارکت‌های دولتی - خصوصی

سیستم‌های هویتی نیازمند نوآوری‌های مبتنی بر فناوری، چارچوب‌های رگولاتوری، پذیرش و اعتماد عمومی گسترده و طراحی هستند که به سیستم انطباق با نیازهای کاربران و پایداری مالی در دراز مدت بدهد. چنین سیستم‌هایی، کاندیداهایی ایده‌آل برای مشارکت‌های دولتی - خصوصی خواهند بود که نقش همه افراد در آن‌ها از پیش تعیین شده است و انگیزه‌های مشارکت نیز کاملاً واضح و مبرهن است. این مشارکت می‌تواند شامل مواردی اعم از تسهیم مسئولیت‌های مالی، همکاری با هم برای طراحی کاربر محور، مالکیت مشترک سیستم‌های مبتنی بر هویت دیجیتال و داده‌ها و دستاوردهای آن‌ها، شناخت متقابل از هم و تعامل‌پذیری بین سیستم‌ها و در نهایت ساختن اکوسیستمی باشد که ارزش بیشتری را برای طرفین ایجاد می‌کند.

مدل کسب و کار پایدار

سیستم‌های مبتنی بر هویت دیجیتال مستلزم قابلیت‌های مالی بلندمدت و طول عمر عملیاتی مفید هستند و در همین راستا، مدل‌های کسب و کاری پایدار فراوانی نیز در دست ظهور و توسعه‌اند. مثال‌های بارزی که می‌توان عنوان کرد، کنسرسیوم‌های مبتنی بر اعتماد و ارائه دهندگانی هستند که هزینه‌ها و داده‌های هویتی خود را با یکدیگر به اشتراک گذاشته‌اند تا بتوانند برای کاربرانشان ایجاد ارزش کنند. این به اشتراک‌گذارندگان هم می‌توانند شامل سازمان‌ها و دولت‌ها شوند و کاربران را مورد خطاب قرار دهند و تعداد آن‌ها نیز هر روز رو به فزونی می‌گذارد. با این حال، این نکته نیز مهم است که انگیزه‌های مالی این مدل‌های کسب و کار حقوق افراد را پامال نکنند و حق انتخاب و کنترل آن‌ها روی داده‌هایشان را در معرض ریسک قرار ندهند. برای این که سیستم‌های هویتی در طول زمان پایدار باقی بمانند، نیازمند تغییر زیرساخت‌ها و مدل‌های کسب و کاری خود مطابق با تحولات تقاضای کاربران خواهند بود تا بتوانند با عملکرد و تجربه‌های نوین کاربران سازگار باشند. در ضمن، مدل‌های کسب و کار 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.

ثبت مالی: نادرا (NADRA) در پاکستان

اداره ملی ثبت احوال پاکستان، آی‌دی کارت‌های رایگانی برای شهروندان کم‌بضاعت 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 کارمزد های 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 کارمزد ها 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 کم‌با حذب 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: هیچ‌کس 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 این که 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

این که 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 آن چه که نیاز دارند دسترسی داشته باشند. گزینه‌های نام‌نویسی و ثبت‌نام دیجیتال می‌توانند در شمول کاربران را 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 مورد نیاز 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 کاربران 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 این که طراحان نیز باید این موضوع را مدنظر قرار دهند که چگونه می‌توانند از فناوری‌های مدرن در راستای ارتقای شمول بهره‌جویند، در عین این که 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 4G 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، به ویژه در مورد اطلاعاتی که ممکن است سبب آسیب‌رسانی 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 این که داده‌های هویتی کاربران رد شوند یا اعتماد اشخاص ثالث وابسته به ارائه دهندگان به برخی از داده‌ها و هویت‌های دیجیتال باعث بروز تبعیض میان کاربران شود بالا خواهد بود. این استانداردها می‌توانند به شکل فعّالانه‌ای حفره‌ها و شکاف‌های احتمالی موجود در سیستم‌های هویتی را که به محرومیت یا تبعیض می‌انجامد شناسایی کرده و برطرف کنند. استانداردهایی که به منظور حفاظت از کاربران و رضایتمندی آن‌ها طراحی و ارائه شده‌اند و آن‌ها را قادر می‌سازند 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 اشیا به ارائه دهندگان خدمات پرداخت کمک می‌کنند تا در پمپ بنزین‌ها کاربران و پرداخت‌های آن‌ها را مدیریت کنند. ضمن این که این سنسورها به کاربران این امکان را می‌دهند تا صورت حساب‌های خود را با استفاده از کیف پول‌های موبایلی‌شان پرداخت کنند. به علاوه، این قابلیت نیز وجود دارد تا با ایجاد پروفایل‌های هویتی، به خدمات و محصولات مالی نیز دسترسی داشته باشند.

ثبت نام آسان: ادهار در هندوستان

به نظر شما چطور می‌توان بیش از ۱٫۳ میلیارد کاربر را در یک سیستم هویتی ثبت نام کرد؟ سیستم هویتی بیومتریک ادهار که توسط دولت هندوستان راه اندازی شده است، در حال ثبت نام طیف گسترده‌ای از کاربران و شهروندان این کشور است و برای ثبت نام، مدارک و مشخصات گسترده‌ای را نیز می‌پذیرد. در ضمن، این سیستم برای افرادی که سابقاً بر این فاقد هویت دیجیتال بوده‌اند نیز برخی گزینه‌های پیشنهادی ارائه می‌دهد. گوشی‌های تلفن همراه، وظیفه ثبت نام بخش 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 ثبت نام، 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 ثبت نام کرده‌اند. با این وجود، هنوز هم مشاجرات 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 سیستم هویتی خوب باید بتواند دسترسی افراد به طیف گسترده‌ای از محصولات، خدمات و تراکنش‌های دیجیتال را فراهم کند و کاربردپذیر باشد.

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

سهولت در استفاده: سهولت در استفاده بیشتر به فرایندهای احراز هویت و

تایید هویت در سیستم‌های هویتی برمی‌گردد و رعایت کم‌ترین میزان اصطکاک ممکن در این فرایندها.

تعامل‌پذیری و پرتابل بودن: سیستم‌های 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 است که در این صورت، انگیزه برای استفاده از چنین سیستم‌های 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 می‌شود. با هویت‌های دیجیتالی که در طول تمامی حوزه‌ها پذیرفته شده‌اند و مرزهای جغرافیایی را پشت سر گذاشته‌اند، افراد به هویت‌های کمتری برای انجام تعاملات و تراکنش‌های خود نیاز خواهند داشت. همین هویت‌های کمتر، به نوبه خود، به معنی سیلوهای مبتنی بر داده کمتر، تکه تکه شدن‌های دیجیتال کمتر و در حالت کلی ریسک‌ها و ناکارآمدی‌های کمتر است.

منظور از خوب چیست؟

خدمات دیجیتال غالباً پافراتر 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 قابلیت‌های برخوردار نیستند. به عنوان مثال، زمانی که در صدد اجاره یا خرید یک آپارتمان برای خود در یک کشور خارجی هستید، ممکن است صاحبخانه قبض برق یا تاریخچه اعتباری شما را قبول نداشته باشد.

به رسمیت شناختن مشترک یکدیگر، که طی آن مدارک و گواهی‌نامه‌ها یا استانداردهای ارائه شده از سوی یک طرف توسط سایر طرفین ارائه دهنده خدمات یا هویت‌ها مورد اعتماد قرار می‌گیرد و به رسمیت شناخته می‌شود، می‌تواند همکاری‌ها و تعاملات را بهبود بخشیده، سرعت بیشتری بدهد و در عین حال هزینه‌ها و اصطکاک‌های تعاملان برون مرزی و برون حوزه‌ای را نیز به شدت کاهش دهد. سیستم‌های تعامل‌پذیر، که قابلیت تعامل و تبادل اطلاعات با یکدیگر را دارند و به هم اعتماد دارند، راحتی را افزایش می‌دهند. با این حال، طراحان هنوز هم باید ریسک‌هایی را که از این تعامل‌پذیری ناشی 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 این که هر تراکنشی نیاز به هویت دیجیتال ندارد، اما زمانی که هویت‌های دیجیتال بسیاری از فرایندها و تراکنش‌ها را تسهیل می‌کنند، افراد تمایل بیشتری برای استقبال از آن‌ها خواهند داشت. این سهولت و راحتی برای کاربران، مستلزم بازنگری در سبک زندگی آن‌ها، رفتارهای آن‌ها و هنجارهای فرهنگی‌شان دارد تا انگیزه‌های احتمالی کاربران برای استفاده 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 آن چه که امروز برای کاربران ارزشمند است، فردا دیگر نباشد. برای سیستم های مبتنی بر هویت دیجیتال، ادامه ارائه ارزش به کاربران، مستلزم نظارت و ارزیابی مداوم نیازها و انتظارات آن ها در طول زمان است.

اصطکاک مناسب

تراکنش های پیچیده ای که از ریسک بالایی برخوردار هستند، ممکن است به ارزیابی ها و طیف گسترده ای از اسناد و داده ها نیاز داشته باشند، اما در این میان، برخی از تراکنش ها نیز وجود دارند که به ارزیابی ها و داده های به مراتب کمتری نیاز دارند و فرایندهای احراز هویت و تایید هویت در مورد آن ها ساده تر است. زمینه و موارد کاربردی می تواند سطح سخت گیری و اصطکاک را برای تایید هویت و احراز هویت مشخص کند. در برخی موارد، مشارکت های بخش خصوصی و دولتی می توانند با کاهش فرایندهای احراز هویت و تایید هویت کاربران، اصطکاک موجود در زیرساخت های خدماتی را کاهش دهند.

مثال هایی از دنیای واقعی

عبور از مرزها و شناخت متقابل: eIDAS، اتحادیه اروپا
سیستم رگولاتوری eIDAS اتحادیه اروپا، استانداردهایی را برای امضاهای دیجیتال، گواهی نامه های واحد شرایط بودن دیجیتال، مهر و موم های دیجیتالی، تایم استمپ ها و سایر فرایندها و مکانیسم های تایید و احراز هویتی تبیین کرده است که به سازمان های مستقر در اتحادیه اروپا کمک می کند تا از سیستم های هویتی و فرایندهای اعتبارسنجی در کمال امنیت و اطمینان استفاده کنند. بدیهی است که چنین رویکردی اعتماد به تراکنش ها و تعاملات برون مرزی را نیز ارتقا خواهد بخشید، تعامل پذیری را افزایش خواهد داد، هویت های تکراری را از اکوسیستم حذف کرده و کاهش خواهد داد و سیستم های مبتنی بر هویت دیجیتال را در اقصی نقاط جهان و در اغلب حوزه ها قابل استفاده خواهد ساخت.

ادغام با زندگی روزمره: تی-او، کره جنوبی
اپراتورهای قدرتمند تلفن همراه در کره جنوبی، یک راهکارهای مبتنی بر هویت دیجیتال مشترک راه اندازی کرده اند. این شبکه، پس از این که مشتریان مجوز ورود به آن را پیدا می کنند، شماره تلفن کاربران و سایر داده های هویتی مربوط به آن ها را ثبت کرده و به اشتراک می گذارند. کاربران با وارد کردن یک پین کد در گوشی های تلفن همراه شان، از فرایند تایید هویت این سیستم عبور کرده و به راحتی می توانند تراکنش های خود را انجام دهند. این سهولت و راحتی، به پذیرش سیستم به شکل معجزه آسایی کمک کرده است، به طوری که بالغ بر ۹۹ درصد از سایت های کره جنوبی، و بیش از ۳۰،۰۰۰ ارائه دهنده خدمات نظیر بانک ها، ارائه دهندگان محتوا و رسانه های اجتماعی آن را پذیرفته و مورد استفاده قرار داده اند. بیش از ۱۵ میلیون کاربر فعال ماهانه تراکنش های خود را از طریق این سیستم هویتی جذاب انجام می دهند و حجم تراکنش های سالانه آن را به رقم ۶۵۰ میلیون دلار رسانده اند.

۴. ارائه حق انتخاب

اصول انتخابی برای یک سیستم هویتی عبارتند از:

شفافیت: در سایه این شفافیت، کاربران قادر خواهند بود تا افراد و سازمان هایی که در پی گردآوری و افشای اطلاعات هویتی شان هستند را شناسایی کرده و در مورد این که چگونه این داده ها پردازش می شوند و مورد بهره برداری قرار می گیرند، یا برای چه اهدافی از آن ها استفاده می شود آگاهی می یابند.

حریم خصوصی: سیستم های هویتی باید بتوانند حریم خصوصی افراد را در فناوری ها و فرایندها تامین کنند. ضمن این که افراد نیز باید بتوانند در مورد این که که کسانی قابلیت استفاده از داده های هویتی آن ها را دارند، برای چه اهدافی

می توانند از این داده ها استفاده کنند و تا چه زمانی این دسترسی می تواند ادامه داشته باشند حق انتخاب داشته باشند و هر زمان که نیاز داشته باشد، داده ها را به ورزسانی کرده یا امحا نمایند.

حفاظت از داده ها: طراحی مبتنی بر فناوری، کنترل های عملیاتی و مدیریت های رگولاتوری، همه و همه باید به نحوی باشند که داده های هویتی کاربران را از افشا، نقص، نشت و یا نابودی مصون دارند.

کنترل کاربری: این که کاربران بتوانند در مورد نحوه بهره برداری از داده های هویتی خود، میزان دسترسی و هدف دسترسی حق انتخاب داشته باشند و فرایندهای گردآوری، پردازش و استفاده از داده ها را رصد کنند بسیار مهم است. هر چند که این کنترل، هر چه بالاتر می رود چالش ها، ریسک ها و فرصت های بیشتری را نیز پیش روی کاربران قرار می دهد.

این عنصر چرا اهمیت دارد؟

طراحی یک سیستم مبتنی بر هویت دیجیتال مدرن می تواند حقوق افراد را که در اعلامیه جهانی حقوق بشر در سال ۱۹۴۸ میلادی نیز توصیف شده، پایمال کرده یا ضمنت کند. در حال حاضر، شاهد تقاضای فزاینده کاربران برای افزایش کنترل روی داده های شخصی شان هستیم. در سیستم هویتی که بتواند به این تقاضا پاسخ دهد، با اعتمادی پرشتاب رو به رو خواهد شد، خطر ابتلا به سوء استفاده یا دستکاری را به حداقل خواهد رساند، و از پذیرشی فوق العاده لذت خواهد برد. در این میان، رگولاتورها نیز توانان روی حریم خصوصی و امنیت متمرکز شده اند.

منظور از خوب چیست؟

خودمدیریتی (Self-management)

توانمندسازی افراد برای مدیریت حرفه ای داده ها و هویت های دیجیتال خود، یک ابزار حریم خصوصی قدرتمند است که به آن ها اجازه می دهد تصمیم گیری کنند چه کسانی می توانند به داده های آن ها دسترسی داشته باشند یا آن ها را به اشتراک بگذارند، هر گونه تغییر در داده ها یا سیستم را شناسایی کنند، و به دیگران حق پردازش داده ها و نتیجه گیری بدهند یا آن ها را رد و منع کنند. کاربران باید در تمام تراکنش ها حق انتخاب باشند تا بتوانند تراکنش ها و گزینه هایی را برگزینند که حقیقتاً به آن نیاز دارند. با این حال، گاهی ممکن است نیاز به حق انتخاب، با نیازهای امنیتی و حمایتی دیگری نیز عین شده باشد. نیازهایی از قبیل نیاز به بررسی های جرایم سایبری، امنیت ملی یا امثال آن. هنگامی که کاربران از به اشتراک گذاری داده های هویتی خود مزایای مستقیمی را دریافت می کنند؛ مانند دریافت تخفیف از فروشگاه ها و غیره، لازم است که هر دو هم به اشتراک گذاری را مدنظر داشته باشند، هم مزایا و دستاوردهای آن را، و هم ملاحظات امنیتی و حریم خصوصی آن را. رابط های دیجیتال و فرایندهایی که به کاربران کمک می کنند 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 ریسک های بالقوه این افشای اطلاعاتی را مدنظر قرار دهند. در غیر این صورت، ممکن است منجر به آسیب رسیدن به کاربران، عدم تمایل آن ها و افت پذیرش سیستم شود.

حمایت های قانونی

مقررات، به ویژه آن دسته از مقررات که حفاظت از داده ها و چارچوب های حریم خصوصی را دنبال می کنند، یک پیش شرط لازم و ضروری برای پیاده سازی سیستم های هویتی هستند. ممکن است رگولاتورها، به دنبال پیاده سازی سیستم های مبتنی بر هویت شفاف و شکل دهی هویت های دیجیتال به شکلی باشند که در بالا نیز عنوان شد. این در حالی است که عموم دولت ها و بخش های خصوصی نیز به دنبال سطح بالایی از حریم خصوصی، به ویژه در مورد داده هایی هستند که امکان نشت آن ها به ملل خارجی وجود دارد. بر همین اساس، طراحان باید چارچوب های رگولاتوری و یژه هویتی، داده های 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 موردنظر 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 این که بتوانند به حقوق خود آگاه بوده، توانایی استفاده از آن را داشته باشند و کنترل داده‌های خود را شخصاً 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. قطعاً 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 آگاهی‌قلمداد شود.

حریم خصوصی در طراحی

حریم خصوصی، فاکتور بسیاری مهمی است که باید در طراحی، ساخت و ساز و اجرای فرایندهای یک سیستم مبتنی بر هویتی دیجیتال نهادینه شده باشد. این نهادینه شدن، به مفهوم رویکردی کاربرمحور به سمت حریم خصوصی است که شامل گردآوری کم‌ترین حجم داده‌های هویتی ممکن برای هر استفاده موردی، کاهش حداقل امکان فرایندهای مربوط به پردازش این داده‌ها و تأیید 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 این که به کاربران، این امکان را می‌دهد تا افراد دارای دسترسی به داده‌های هویتی موجود، هدف آن‌ها از این دسترسی و میزان و مدت زمان این دسترسی را رصد کرده و آن‌ها را رد یا تأیید 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. به عنوان مثال، در حال حاضر آدرس‌های ایمیل کاربران و آی‌پی‌های آن‌ها در این مجموعه جای داده می‌شوند. ضمن این که 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 یارد دسترسی باشد. ضمن این که 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 تأیید 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 این که 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 این که چه مقاماتی از دولت در حال بازیابی یا بازرسی پرونده‌های هویتی آن‌ها است کسب اطلاع کنند.

غیرمتمرکزسازی زیرساخت 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 شخصاً 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 این که بسیاری از سازمان‌ها نیز در این پروژه آزمایشی 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 این که 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 حساسی 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 سیستم هویتی، از افراد و کاربران آن گرفته تا اشخاص ثالث وابسته، عنصری حیاتی است چرا که در سایه این امنیت می توان تهدیدها و جرایم سایبری نظیر سرقت های هویتی را کاهش داد و جلوی پیامدهای ناخواسته ای همچون نقض حقوق بشر را گرفت. یک سیستم ایمن که از داده ها محافظت می کند، به افراد این امکان را می دهد تا در همه سطوح اجتماعی و اقتصادی بالاترین میزان سود را دریافت کنند.

با توجه به دنیای درهم امروز که دستگاه های متصل در همه ابعاد زندگی روزمره افراد و سازمان ها نفوذ کرده اند، اهداف فزاینده جدیدی پیش روی هکرها و مهاجمین سایبری قرار گرفته است. هویت های دیجیتال قابل تایید می توانند در کنار دستگاه های اجرایی، امنیتی و نظارتی، در به حداقل رساندن آسیب هایی که ممکن است متوجه افراد و سازمان ها شوند نقش داشته باشند.

منظور از خوب چیست؟

افشای حداقلی

سیستم های هویتی باید به گونه ای طراحی شده باشند که کاربران را به افشای حداقل اطلاعات مورد نیاز برای تایید و احراز هویت وادار کنند. در صورتی که دست کاربران از کنترل داده های شخصی و هویتی شان کوتاه باشد، این سیستم های هویتی خواهند بود که ملزم به کنترل داده ها و افشای حداقل داده های مورد نیاز برای فرایندهای تایید هویت و انجام تراکنش ها هستند. به عنوان مثال، یک آی دی کارت رسمی، ممکن است هنگام تایید سن شما آدرس تان را نیز نمایش دهد که نیازی به آن نیست و باید اصلاح شود.

آموزش

آموزش داده کاربران برای این که بتوانند داده های خود را به بهترین شکل ممکن مدیریت و کنترل کنند، ریسک های احتمالی متوجه هویت های دیجیتالشان را شناسایی کرده و کاهش دهند و در عین حال در مقابل جرایم سایبری ناگوارای نظیر تقلب، سرقت های هویتی یا سوء استفاده از داده ها نیز بایستند.

ترمیم

حتی بهترین سیستم های هویتی نیز ممکن است در برخی مواقع دچار ایراد و اختلال شده و داده های حساس کاربران را در معرض افشا قرار دهند. این که سیستم بتواند بلافاصله پس از بروز اختلال یا حادثه خود را بازیابی کرده، با پشتیبانی سازمانی و مالی ترمیم های لازم برای پسگویی 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 کاربران و سازمان ها خواهد شد.

مثال هایی از دنیای واقعی

امنیت و حفاظت: ایتس می (Itsme)، بلژیک

پلتفرم هویت دیجیتال ایتس می از فرایند تایید هویت چند منظوره ای استفاده می کند که شامل داده های بیومتریک است و امنیت را ارتقا می بخشد. فرایند تایید هویت این پلتفرم به عنصر نیاز دارد: یک گوشی تلفن همراه که به کاربر متصل باشد، یک سیم کارت که امنیت آن توسط اپراتورهای تلفن های همراه ضمانت شده باشد، و کد مخصوص هر کاربر که توسط ایتس می برای وی صادر شده و منحصر به فرد 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 ارزش‌آفرینی برای کاربرانشان، از قافله مدیریت عقب نمانند. در این فصل، قصد داریم برخی از روندهای مهم هویت‌های دیجیتال، چالش‌ها و فرصت‌هایی را که احتمال دارد سازمان‌ها، ارائه‌دهندگان، سیاست‌گذاران و طراحان سیستم‌ها در آینده‌ای نه چندان دور با آن‌ها مواجه شوند در بوته بحث و بررسی قرار دهیم.

روندها

غیر متمرکزسازی 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 غیر متمرکز. فناوری‌ها و معماری‌های جدید، از قبیل فناوری دفتر کل توزیع شده، می‌توانند نقش تعیین‌کننده‌ای 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 ارائه‌دهندگان 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 پافراتر از محدوده‌های جغرافیایی می‌گذارند و مرزها را در می‌نوردند، 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 ارزش‌آفرینی برای آن‌ها 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. دوقلوهای دیجیتال، به

مفهوم یک قلو 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 این که 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 فناوریانه، روندهای نوظهور و تاکید روی تجربه کاربری و ارزش‌آفرینی برای افراد ظهور کنند؟

بهبود تجربه کاربری. هرچه سازمان‌ها، شرکت‌ها و ارائه‌دهندگان 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 عقب‌نماندن از قافله، بیشتر روی اعتماد کاربران، تجربیات آن‌ها از سیستم‌های طراحی شده و ارزش‌آفرینی 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. بیابید 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 بیشماري 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.

بی تفاوتی کاربران. یکی از نتایج بارز توسعه بیش از حد سیستم های مبتنی بر هویت دیجیتال، ظهور بیش از اندازه چنین سیستم هایی و گزینه های بیشماری از کنترل های اطلاعاتی و مدیریتی برای کاربران، سرریز شدن داده ها است. در چنین حالتی است که افراد از مدیریت و کنترل بیش از حد داده های خود خسته شده و نسبت به رفتارها یا فرایندهایی که ممکن است امنیت، حریم خصوصی، داده ها یا حتی هویت های آن ها را تهدید کند بی تفاوت عمل کنند.

ریسک ها و مسئولیت ها. هر چه یک حوزه توسعه بیشتری می یابد، بازیگران جدیدی نیز به آن ملحق می شوند، و این جا است که مالکیت و مسئولیت پذیری ریسک ها شفافیت بیشتری می طلبد و نیاز به مدیریت بیشتر احساس می شود. پیامدهای ناخواسته طراحی ضعیف. طراحی ضعیف یک سیستم هویتی، نه تنها می تواند به کارایی و راندمان ضعیف بیانجامد، بلکه به افراد نیز آسیب می رساند. به عنوان مثال، یک هویت دیجیتال ناکارآمد که به صورت غیر حرفه ای و ضعیف طراحی شده است، می تواند در راه روی نظارت های غیرقانونی و جاسوسی باز کند. کلیه تصمیمات طراحی باید با در نظر گرفتن پیامدهای منفی ممکنه صورت بگیرند و جای هیچ گونه اهمال کاری وجود ندارد.

فرصت ها

هویت های دیجیتال و سیستم های مبتنی بر این هویت های دیجیتال، نه تنها می توانند برای کاربران مفید واقع شوند بلکه برای جامعه نیز فرصت هایی را در پی دارند. **دنیای دیجیتالی پرتابل، امن تر و قابل اعتمادتر.** یک هویت دیجیتال راحت و قابل اعتماد، نه تنها شما، داده های هویتی و شخصی و دارایی هایتان را ایمن نگه می دارد، بلکه دری به سمت امنیت و اعتماد نیز می گشاید. امنیت و اعتمادی که شبکه ای بسیار گسترده تر از تعاملات رودرروی سابق رقم می زند و مرزهای جغرافیایی و اجتماعی را در می نورد.

سادگی، کارایی و اعتماد در به اشتراک گذاری داده ها. در سایه هویت های دیجیتالی که ساده و راحت هستند، قابل اعتمادند و به افراد حق انتخاب و کنترل روی داده های شان را می دهند، شرکت ها و سازمان ها نیز از منابع اطلاعاتی هنگفتی بهره مند خواهند شد که می توانند به بسیاری از آما و اهداف آن ها جامه عمل بپوشانند. شرکت هایی که تاکنون به سیلوهای اطلاعاتی محدود و تکه تکه سنتی وابسته بوده اند و اکنون، به سهولت هر چه تمام، دریایی از داده های به اشتراک گذاشته شده و ایمن را پیش روی خود دارند. دادن حق انتخاب و کنترل داده ها به افراد، آن هم در شرایطی که همه روزه به فناوری ها و نوآوری های جدیدی دست می یابیم و مشارکت ها و تعاملات بین سازمانی نیز روبه فزونی گذاشته است، منجر به برداشته شدن بار انطباق خواهد شد و با حذف تکرار از فرایندهای تایید هویت در سطح سازمان ها، کارایی را ارتقا بخشیده و هزینه ها و اصطکاک ها را خواهد کاست.

مشارکت های بیشتر برای سیستم هایی بهتر. نیاز به تعامل پذیری و تجربه کاربری یکپارچه، فرصت هایی را پیش روی بخش های خصوصی، دولت ها و جامعه مدنی قرار می دهد تا بتوانند با یکدیگر کار کنند. با کاهش سیستم های هویتی و عاری از تعامل پذیری، افراد و سازمان ها قادر خواهند بود هزینه ها را کاهش داده و فرصت های جدیدی برای تجربه دیجیتال بهتر بیابند.

ارزشی گسترده برای کاربران. مدل ها و الگوهای اعتمادی مدرن این قدرت را دارند تا تعاملات و تراکنش هایی همه روزه و با حداقل ریسک برای کاربران رقم بزنند. تراکنش هایی که دارای کمترین هزینه و در عین حال بالاترین کارایی و راحتی هستند. ضمن این که دسترسی افراد به طیف گسترده و روزافزونی از خدمات، تراکنش ها و شبکه ها نیز به منزله ارزش آفرینی برای آن ها در سطحی وسیع است. **انگیزه ها و رفتارهای بهتر.** هویت های دیجیتال، به ویژه در مورد کودکان می تواند انگیزه ای برای رفتار بهتر و پایدار باشد. به عنوان مثال، سازمان ها و دولت ها می توانند از هویت های دیجیتال برای بررسی کارگران معدن استفاده کنند تا اطمینان حاصل شود که از هیچ کودک کاری در این معادن استفاده نمی شود. **ردیابی در زنجیره های تامین.** زمانی که هویت های دیجیتال با تولیدات کشاورزی

یا سایر محصولات پیوند می خورد، اعتماد در تمام سطح زنجیره تامین به ویژه در نقاط اند-تو-اند آن افزایش پیدا می کند. دلیل این افزایش اعتماد نیز این است که افراد می توانند در مورد صحت و سقم منبع محصولات، نحوه و محل تولید آن ها، به بار آوری و نقل و انتقال و غیره آن تحقیق کنند.

انقلاب صنعتی چهارم. رسالت انقلاب دیجیتال چهارم، ادغام بی کم و کاست و یکپارچه فناوری های دیجیتال برای بهبود زندگی ما است. هویت های دیجیتال ایمن، موثر، راحت، پایمند به حریم خصوصی و همه جانبه به این ادغام کمک خواهد کرد.

فصل چهارم:

اولویتهایی برای مشارکت بخش خصوصی و دولت



مجمع جهانی اقتصاد، به عنوان سازمانی بین المللی برای مشارکت های بخش خصوصی و دولتی پلتفرمی برای دست اندرکاران و ذینفعان معرفی کرده است تا در خلال آن به بحث در مورد ایده های خود بپردازند، اولویت ها را مشخص کنند و به شکل گیری بهتر هویت های دیجیتال در آینده ای نه چندان دور کمک کنند.

در حالت کلی، ذینفعان هویت های دیجیتال از بخش های خصوصی، دولت ها، کسب و کارها و جامعه مدنی، شش اولویت برای پیشبرد مشارکت در حیطه هویت های دیجیتال تعیین و تبیین کرده اند:

تمرکز روی ارزش آفرینی برای کاربران. تخصیص یک هویت دیجیتال به تمام افراد جامعه به تنهایی نمی تواند خوب یا کافی باشد. مابرا همان انتخاب میان بد و بدتر است و به عبارت ساده تر، نداشتن هویت، از داشتن یک هویت بد به مراتب بهتر است. طراحان سیستم های هویتی و سیاست گذاران ملزم هستند تا روی دستاورد حقیقی این سیستم ها تمرکز کنند: پذیرش مبتنی بر تقاضای هویت هایی که پنج عنصر مورد نیاز برای ارزش آفرینی در خود دارند و دسترسی بهتر به خدمات، امنیت مضاعف و تراکنش های آنلاین کارآمد را برای افراد به دنبال می آورند.

قابل حساسرسی. چگونه می توان میزان ارزش ایجاد شده برای کاربران توسط یک سیستم هویتی را اندازه گیری کرد و معیار سنجش این قبیل سیستم ها چیست؟ چطور می توان آن ها را قابل حساسرسی و سنجش نگه داشت؟ بدیهی است که پاسخ به این سوالات بسته به حوزه ها و عملکردها متفاوت خواهد بود و در طول زمان نیز تحول و تکامل خواهد یافت. اما آن چه که از اهمیت بالایی برخوردار است، توسعه معیارهای مشترک برای سیستم ها، کشورها و جنبش های فرامرزی ارزش آفرین برای کاربران است.

حکومت یا مدیریت. اکوسیستم های جدید هویتی نیاز به مدل های حکومتی جدید نیز دارند تا بتوانند نظارت مستقل و قابل حساسرسی بودن به لحاظ فرامرزی را حفظ کرده و ساز و کارهایی را برای تحقق انطباق، مدیریت مسئولیت ها و ارائه منابع در صورت لزوم تعریف کند. هدف از مشارکت ها باید تعریف و تعیین چارچوب هایی به اندازه کافی انعطاف پذیر به منظور تکامل در طول زمان باشد.

نظارت. هویت های دیجیتال خوب به اراده سیاسی قوی، توجه دولت ها، صاحبان کسب و کارها و رهبران جامعه مدنی نیاز دارند. درک مشترک از اصول می تواند به سیاست گذاران، رهبران سازمان ها و طراحان کمک کند تا شیوه های استاندارد و هماهنگی در پیش بگیرند. روایت متقابل بخش های مختلف از هویت های دیجیتال می تواند تا حد زیادی کمک کننده باشد.

مشارکت ها. هویت های دیجیتال ریسک تکه تکه شدن و انزوای همواره به پدک می کشند، مگر این که سازمان و دست اندرکاران صنعت به دنبال مشارکت و استفاده از راهکارها و شیوه هایی برای ایجاد انگیزه، توصیف اولویت های مشترک و تعامل پذیری باشند.

نوآوری. این که کدام یک از شیوه ها، اعم از پروژه های فانوس دریایی (lighthouse projects) که روی استفاده های موردی خاص تکیه می کنند یا سندباکس های چابک (agile sandboxes) که بر فرضیات آزمایشی تاکید دارند و یا سایر راهکارها و متدها این قابلیت را دارند تا هماهنگی لازم و تعادل مورد نیاز بین سرعت رشد فناوری های مدرن و نیازهای کاربران را حفظ کنند از اهمیت بالایی برخوردار است. چرا که در این صورت سازمان ها قادر خواهند بود در کنار هم بهتر مشارکت کرده و در سایه اولویت های مشترک، به نتایج مطلوبی دست یابند. ضمن این که یکی از مهم ترین دستاوردهای این نوآوری ها و مشارکت ها، کتابخانه ای موفق از آزمایش هایی است که هریک دانشگاهی برای آیندگان هستند.

زمینه های فعالیت مشترک

به عنوان نتیجه گیری، لیستی از اولویت ها را تدارک دیده ایم که می توانند به هویت های دیجیتال خوب و به معنای واقعی کلمه کار بر محور منجر شوند.

سیاست و حکومت

- ساز و کارهای احراز هویت و سیاست های متناسب با سطح اطمینان مورد نیاز
- چارچوب های حقوقی مناسب برای حریم خصوصی، امنیت سایبری و حفاظت از داده ها

- سیاست های ملی هویت دیجیتال که با استراتژی های گسترده تری برای امنیت سایبری، ایمنی بیماران، توسعه اقتصادی و امثال آن در هم می آمیزند.
- سیاست های کاربر محور و فرایند هایی برای ارائه دهندگان بخش خصوصی
- گردآوری، پردازش و استفاده شفاف از داده ها به منظور حمایت از اعتماد کاربران
- نظارت مستقل بر هویت های ملی و چارچوب های حفاظت از داده ها
- یک چارچوب جهانی مشترک برای حکومت فرامرزی
- مدیریت سیاست ها و عملکردها در میان دولت ها، کسب و کارها و سایر سازمان ها

جامعه خوب و عمومی

- تعریف و درک مشترک از یک هویت دیجیتال خوب و ارزش آفرینی برای کاربران
- سرمایه گذاری روی تحقیقات به منظور دستیابی به سناریوهای مبتنی بر هوش مصنوعی یا اینترنت اشیاای مرتبط با هویت دیجیتال
- معیارها، ابزارها و استفاده موردی مناسبی را ارزش یک هویت دیجیتال خوب را نشان می دهند.
- تعریف یک هویت دیجیتال خوب برای یک جامعه آماری خاص از کاربران، دامنه ها و استفاده های موردی

قابلیت ها

- مشارکت بین دولت ها، بخش های خصوصی و جامعه مدنی به منظور آگاه سازی افراد از حقوق، ریسک ها و وظایفشان و همچنین ساز و کارهای مسئولیت پذیری موجود پیرامون هویت های آن ها
- چارچوب های پاسخگویی و حساسرسی مشترک
- به اشتراک گذاری متدولوژی و توانمندسازی سیاست گذاران و دست اندرکاران
- توسعه بازارهای بیمه همسو با تکامل هویت های دیجیتال و رشد ریسک ها
- حمایت های حقوقی و غیر حقوقی به منظور کمک به کاربران در مواقع نیاز

نوآوری و طراحی راهکارها

- نهادینه کردن سیاست های امنیتی و حریم خصوصی در خطوط مشی کسب و کارها و راهکارهای مبتنی بر فناوری
- تست بدها (testbeds) و سندباکس های چابک برای اولویت بندی چالش های متوجه ارزش کاربران، نظیر امنیت و تعامل پذیری
- نوآوری در تحولات فرایندهای آنالوگ و دیجیتال و همچنین ادغام، نظیر دوقلوهای دیجیتال
- پاسخگویی به رشد فزاینده داده های شخصی قابل شناسایی کاربران، به ویژه زمانی که پای اینترنت اشیا به میان می آید.

توسعه برنامه

- اولویت بندی استفاده های موردی بر اساس بالاترین پتانسیل آن ها در کاهش اصطکاک و ارزش آفرینی برای کاربران
- طراحی و پیاده سازی مشترک و توانمندسازی راهکارها توسط ذینفعان چندگانه زیر سایه مشارکت های بخش خصوصی و دولتی
- شناسایی نمونه های آزمایشی و فرصت های پیاده سازی نمونه های موفق در مقیاس گسترده عملی زیر چتر مشارکت
- مشارکت با جامعه مدنی به منظور شناسایی ارزش های 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 کاملاً 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 آن چه که «خوب» نامیده می‌شود دست پیدا کنند. اگرچه ممکن است این نقشه راه برخی مسیرهای پریچ و خم، 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 حیاتی اند؛ 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 پایداری 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.

آن چه 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

۳	۲	۱
بازگویی ارزش در آینده	طراحی و ساخت سیستم‌های کاربر محور	شروع
۳-۱ در نظر داشتن نیازهای در حال توسعه برای جلوگیری از تبعیض	۲-۱ حداکثر ارزش کاربری و عملکرد	۱-۱ مشخص کردن کاربران
۳-۲ آمادگی برای مقابله با چالش‌های ناشی از نهادهای حقوقی، دستگاه‌ها، منابع طبیعی و غیره	۲-۲ وارد کردن فضای فناوری، صنعت، فرهنگی و حوزه بازار	۱-۲ در نظر گرفتن زمینه‌ها
۳-۳ آمادگی برای رودررویی با نهادهای مجازی، هوش مصنوعی و غیره	۲-۳ شناسایی و انتخاب بهترین الگو	۱-۳ تصویر برداری از چشم‌انداز
۳-۴ در نظر گرفتن پیامدهای ناشی از فناوری‌های نوین	۲-۳ شناسایی و انتخاب بهترین رویکردها برای انطباق و امنیت	۱-۴ تعیین شرکای بالقوه اکوسیستم
	۲-۵ کاهش خطرات و حل و فصل مشکلات	۱-۵ مشورت با کاربران بالقوه
		۱-۶ ایجاد یک روایت
		۱-۷ آموزش
		۱-۸ برنامه‌ریزی برای به اشتراک گذاری ریسک‌ها
		۱-۹ یافتن فرصت‌های جدید برای ثبات

۱. شروع

۱-۱ **مشخص 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 این که 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 باز مینه‌ها 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 وامی‌دارد.

۱-۳ **تصور برداری 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 بازیگری 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 تأیید 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، معمولاً ناچار هستند تا سفر ایجاد سیستم‌های هویتی را با آموزش سیاست‌گذاران 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 اشتراک‌گذاری ریسک‌ها.** سیاست‌گذاران و رهبران سازمان‌ها شاید به دنبال دسترسی به راه‌های جلوگیری از ریسک‌هایی باشند که اکوسیستم‌های 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 معمولاً 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 می‌تواند سودآوری و موفقیت برای سیستم‌های هویتی در پی داشته باشند. این مدل‌ها، معمولاً به اشتراک‌گذاری هزینه‌ها و ریسک‌ها میان ذینفعان و سازمان‌های مختلف و ارائه طیف گسترده‌ای از خدمات نوین و متنوع، برای سیستم‌های هویتی درآمذایی می‌کنند. در کره جنوبی، شرکت‌های بخش خصوصی منافع و سودآوری زیادی از راه‌اندازی و مشارکت در راهکار هویتی تی‌اوت (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 تازمانی که به حقوق کاربران احترام بگذارد و حریم خصوصی آن‌ها را رعایت کند، می‌تواند به درآمذایی بیانجامد. ضمن این که 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 منحصر به فرد 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

۱-۲ 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 مورد نیاز 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 شرکت کنندگان در اکوسیستم، و برقراری ارتباط موثر با آن‌ها، می‌تواند به پذیرش و توسعه بیش از پیش سیستم کمک کند.

- **پیوند هویت‌های انسانی به غیر انسانی.** 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 پایداری 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 مورد نیاز، 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.** این که حریم خصوصی برای افراد با توجه به فرهنگ آن‌ها، ارزش‌های شخصی‌شان و نوع تراکنش‌های مورد نیاز به چه مفهوم است، دارای اهمیت است. ضمن این که این باید در نظر داشت این حریم خصوصی، به مرور 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.

- **صرفاً 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 کاربران نیز محافظت کند. چنین سیستمی باید بتواند سیاست‌هایی را برای مسئولیت‌پذیری در استفاده، به اشتراک گذاری و مدیریت داده‌ها تبیین کند.

- **تحقق انعطاف‌پذیری و چابکی.** سیستم‌های هویتی حال حاضر دنیا، با برخی چالش‌های 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 آسیب، 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 غیرمجاز 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. این که 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 این که این آموزش‌ها باید روشن و به اندازه کافی جذاب باشند تا کاربران را ورطه بی تفاوتی 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 قبلاً به آن‌ها اشاره کردیم، این قابلیت و قدرت را دارند تا پافراتر از حوزه‌ها و مرزهای جغرافیایی گذشته، و اکوسیستم‌های بسیار وسیع‌تر و متنوع‌تری از سیستم‌های هویتی سابق ایجاد کنند. برای این که 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 این که آن‌ها چه نیازها و انتظاراتی دارند و مهم‌تر این که 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 سطره 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 تأثیر بسزایی داشته باشد.

- **تدارک مدل‌های عملیاتی و حکومتی نوین.** هر چه الگوهای سیستم‌های هویتی به سمت اکوسیستم‌های بزرگ‌تر پیش می‌رود، طراحان و عملیات‌ایزوله 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 منحصر به فردی 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 می‌رسند، 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 باشند 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.** همان‌طور 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 روزه‌به‌روز 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

۱-۳ **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 سرنوشتی 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 پامال شدن حقوق افراد بیانجامد، و همچنین دادن حق انتخاب به افراد برای برگزیدن داده‌های قابل افشا، می‌تواند کمک کننده باشد.

۲-۳ **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 ماجر 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.** هر چه 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.

۴-۳ **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.

