مزایای اینترنت اشیا برای مصرف‌کنندگان چیست؟

IoT نوید آن را می‌دهد که محیط زندگی انسان‌ها، شامل خانه‌ها، دفاتر کاری و وسایل نقلیه را هوشمندتر، قابل سنجش‌تر و تعاملی‌تر کند. اسپیکرهای هوشمند مانند «آمازون اکو» و «گوگل هوم» (Google Home) پخش موسیقی، تنظیم زمان‌بندها یا دریافت اطلاعات را آسان‌تر می‌کنند.

سیستم‌های امنیتی خانه‌ها، نظارت بر اینکه چه چیزی درون و بیرون یک خانه به وقوع می‌پیوند را هم از جهت امنیتی و هم برای دیدن و گفتگو با ملاقات‌کنندگان آسان‌تر می‌کنند. در عین حال، ترموستات‌های هوشمند می‌توانند به انسان‌ها کمک کنند تا خانه‌های خود را پیش از رسیدن به خانه گرم کنند و چراغ‌های هوشمند می‌توانند در هنگام بیرون بودن فرد از خانه نیز جوری برخورد کنند که گویی فرد در خانه است.

فراتر از خانه‌های هوشمند، حسگرهایی وجود دارند که می‌توانند به افراد کمک کنند تا بدانند هوا چقدر دارای آلاینده‌ها یا آلودگی صوتی است. خودروهای خودران و شهرهای هوشمند می‌توانند چگونگی ساخت و مدیریت فضاهای عمومی را دستخوش تغییر کنند. هر چند این نوآوری‌ها ممکن است حریم خصوص انسان‌ها را زیر سئوال ببرد.

برای مصرف‌کنندگان، خانه هوشمند جایی است که با اشیای متصل به اینترنت تعامل برقرار خواهند کرد و این حوزه، یکی از زمینه‌هایی است که غول‌های فناوری مانند آمازون، گوگل و اپل در آن رقابت شدیدی دارند. به عنوان یکی از شناخته شده‌ترین مصادیق این مورد می‌توان به اسپیکرهای هوشمند «آمازون اکو» (Amazon’s Echo) اشاره کرد. هرچند، چراغ‌های هوشمند، دوربین‌ها، ترموستات‌ها و فریزرهای هوشمند نیز وجود دارند. تا هنگامی که بشر هیجان بیشتری از خود برای گجت‌های درخشان جدید بروز دهد، جنبه‌های جدی‌تر و نویی از کاربردهای اینترنت اشیا به ویژه در خانه‌های هوشمند ظهور خواهد کرد.

خانه‌های هوشمند می‌توانند به این موضوع کمک کنند که افراد مسن به طور مستقل و به تنهایی در خانه‌های خودشان زندگی کنند و در عین حال، برای خانواده و دیگر نهادها نیز تعامل با آن‌ها و نظارت بر وضعیت آن‌ها آسان‌تر باشد. در عین حال، توانایی تغییر تنظیمات لوازم خانگی مبتنی بر اینترنت اشیا، می‌تواند به حفظ انرژی و کاهش هزینه‌های مربوط به آن (برای مثال کاهش هزینه‌های وسایل گرمایشی و سرمایشی) کمک کند.

چالش‌های اینترنت اشیا چه هستند؟

اینترنت اشیا، در کنار مزایای بسیاری که دارد، چالش‌هایی را نیز با خود به همراه آورده است. برخی از مهم‌ترین این چالش‌ها، در ادامه مورد بررسی قرار گرفته‌اند.

امنیت اینترنت اشیا

«امنیت» (Security) یکی از مهم‌ترین چالش‌های اینترنت اشیا است. حسگرها در بسیاری موارد داده‌های بسیار حساسی مانند اینکه کاربر در خانه خودش چه اقدامی انجام می‌دهد را گردآوری می‌کنند. امن نگه داشتن این اطلاعات برای کسب و حفظ اعتماد مصرف‌کنندگان مسئله بسیار حیاتی است. اما تاکنون امنیت اطلاعات ثبت شده توسط دستگاه‌های IoT در اغلب موارد بسیار ضعیف بوده است. بسیاری از دستگاه‌های IoT توجه کمی به مبانی امنیت مانند «رمزنگاری» (Encryption) داده‌ها در انتقال دارند.

نقص‌های موجود در نرم‌افزارها – حتی در کدهای قدیمی و به خوبی استفاده شده – معمولا کشف می‌شوند، اما بسیاری از دستگاه‌های اینترنت اشیا قابلیت وصله زدن (Patch) ندارند و این یعنی همواره در معرض خطر هستند. هکرها در حال حاضر به طور فعالانه‌ای دستگاه‌های IoT مانند «مسیریاب‌ها» (Routers) و وب‌کم‌ها را هدف قرار می‌دهند؛ زیرا فقدان امنیت موروثی آن‌ها، قابلیت در خطر افتادن ارثی آن‌ها و به دام بات‌نت‌های عظیم افتادن را آسان ساخته است.

نقص‌ها، دستگاه‌های هوشمندی مانند یخچال‌ها، گازها و ماشین‌های ظرفشویی را برای هکرها دسترسی‌پذیر کرده است. پژوهشگران یک صد هزار وب‌کمی که به راحتی قابل هک بودند را کشف کردند. در عین حالت، کشف شده است که برخی از ساعت‌های هوشمند ویژه کودکان، حاوی نوعی آسیب‌پذیری امنیتی هستند که به هکرها اجازه می‌دهند موقعیت دستگاه را ردیابی، مکالمات را شنود و یا حتی با کاربر گفتگو کنند.

در این وهله است که نگرانی دولت‌ها پیرامون خطرات افزایش پیدا می‌کند. دولت انگلستان راهنماهای خودش را برای امنیت مصرف‌کنندگان دستگاه‌های اینترنت اشیا منتشر کرده است. بر اساس این راهنما، دستگاه‌ها باید رمز عبور یکتا داشته باشند، در عین حال شرکت‌ها باید باید یک نقطه عمومی تماس فراهم کنند تا هر کس بتواند هر گونه آسیب‌پذیری ممکن را گزارش دهند (و روی رفع آن کار کنند)، و کارخانجات باید صراحتا اعلام کنند که هر دستگاهی تا چه زمانی به روز رسانی‌های امنیتی دریافت می‌کند. این مختصرترین فهرست ممکن محسوب می‌شود که البته برای شروع ارائه شده است.

هنگامی که هزینه ساخت اشیای هوشمند کوچک ناچیز باشد، این مشکلات فقط توزیع بیشتری پیدا می‌کنند و رفع کردن آن‌ها سخت‌تر می‌شوند. همه این موارد در کسب و کار نیز اعمال می‌شوند اما سطوح آن‌ها بالاتر است. متصل کردن ماشین‌های صنعتی به شبکه اینترنت اشیا می‌تواند ریسک احتمالی آنکه هکرها این دستگاه‌ها را کشف کنند و مورد حمله قرار دهند افزایش می‌دهد.

جاسوسی صنعتی یا حملات مخرب در زیرساخت‌های حیاتی، هر دو خطرات بالقوه‌ای هستند که اینترنت اشیا در صنعت را تهدید می‌کنند. این یعنی کسب و کارها نیاز به حصول اطمینان از این موضوع دارند که این شبکه‌ها ایزوله و محافظت شده هستند، داده‌های حسگرها به منظور حفظ امنیت آن‌ها و دروازه‌ها، رمزنگاری شده هستند.

وضعیت فعلی فناوری اینترنت اشیا از جهت امنیت، اعتماد کردن به آن را سخت‌تر می‌کند. کمبود امنیت اینترنت اشیا به مانند فقدان یک برنامه‌ریزی امنیتی IoT مداوم در سازمان‌ها است. فکر کردن به سیستم‌های صنعتی که به اینترنت متصل هستند و بدون محافظت رها شده‌اند، نگران کننده است. اینترنت اشیا (IoT) مانند پلی بین دنیای دیجیتال و فیزیکی است و این یعنی هک شدن این دستگاه‌ها می‌تواند عواقب وحشتناکی را در دنیای واقعی داشته باشد. در این میان، در دست گرفتن اختیار یک خودرو بدون راننده، می‌تواند پایانی برای یک فاجعه باشد.

حریم خصوصی و اینترنت اشیا

با وجود حجم انبوه داده‌هایی که حسگرها از همه چیز گردآوری می‌کنند، اینترنت اشیا با مشکلات گسترده حریم خصوصی و امنیت دست و پنجه نرم می‌کند. برای مثال، یک خانه هوشمند مفروض است. این خانه هوشمند می‌تواند بگوید که ساکنان چه زمانی از خواب بیدار می‌شوند (وقتی قهوه‌جوش خودکار فعال می‌شود)، و اعضای خانه چگونه دندان‌های خود را مسواک می‌زنند (به لطف مسواک هوشمند)، ساکنان خانه به کدام کانال رادیویی گوش می‌دهند (به وسیله اسپیکرهای هوشمند)، چه نوع غذایی را می‌خورند (به لطف گاز یا یخچال هوشمند)، کودکان ساکن خانه چه افکاری دارند (به وسیله اسباب‌بازی‌های هوشمند) و چه کسانی به آن خانه رفت و آمد دارند (به کمک زنگ درهای هوشمند). در حالی که شرکت‌ها در جایگاه اول با فروش دستگاه‌های هوشمند کسب درآمد می‌کنند، در جایگاه بعدی با فروش داده‌های کاربران دستگاه‌های خود به کسب درآمد می‌پردازند.

آنچه برای این داده‌ها به وقوع می‌پیوندد، یک مسئله مهم برای حفظ حریم خصوصی افراد است. البته همه شرکت‌های خانه‌های هوشمند، فروش داده‌های مشتریانشان را در مدل کسب و کار خود نمی‌گنجانند؛ اما برخی از آن‌ها این کار را می‌کنند. شایان توجه است که داده‌های اینترنت اشیا را می‌توان با دیگر داده‌ها ترکیب کرد تا تصویری با جزئیات شگفت‌آور از فرد ارائه کرد. پیدا کردن اطلاعات زیاد و شگفت‌انگیز پیرامون یک نفر بر اساس داده‌های یک حسگر کار بسیار ساده‌ای است. در یک پروژه، پژوهشگران با تحلیل مصرف انرژی، سطح کربن مونوکسید و کربن دی‌اکسید، درجه حرارت و رطوبت در طول یک روز در یک خانه، تشخیص داده‌اند که شام فرد چه غذایی بوده است.

اینترنت اشیا، حریم خصوصی و کسب و کار

مصرف‌کنندگان نیاز به درک مبادله‌ای که انجام می‌دهند دارند و اینکه مشخص کنند که آیا از این کار راضی هستند یا خیر. برخی از مشکلات مشابه نیز در کسب و کارها به وقوع می‌پیوندد. برای مثال، آیا تیم اجرایی شرکت از اینکه جلسات خود را در اتاقی که با اسپیکرهای هوشمند و دوربین‌ها تجهیز شده برگزار کنند، خوشحال هستند و از این موضوع رضایت دارند؟ پژوهشی که اخیرا انجام شده حاکی از آن است که چهار مورد از هر پنج شرکت فعال در حوزه اینترنت اشیا، توانایی شناسایی همه دستگاه‌های اینترنت اشیا موجود در شبکه خود را ندارند.

محصولات اینترنت اشیایی که به صورت نامناسبی نصب شده‌اند، می‌توانند به راحتی شبکه‌های شرکت‌ها را برای حملات هکرها باز کنند و یا داده‌ها به سادگی نشت کند. ممکن است اینطور به نظر بیاید که این یک تهدید بدیهی بوده است؛ اما با نگاهی اندکی عمیق‌تر، می‌توان به عنوان مثال حالاتی را تصور کرد که در آن قفل‌های هوشمند یک روز از باز کردن درب دفتر کار فرد برای خود او امتناع کنند و یا ایستگاه آب و هوایی هوشمند موجود در دفتر یک مدیر مهم در سازمان، از طرف هکرها برای ساخت یک «در پشتی» (Backdoor) در شبکه استفاده شود.