فاطمه ربیعی نژاد

امنیت در اینترنت اشیا

امروزه فناوری در حال پیشرفت است و همه برای بهبود وضعیت خود در تلاش هستند. اشیای اطراف ما نیز روزبه‌روز پیشرفته‌تر می‌شوند و به سمت هوشمندشدن حرکت می‌کنند. همان‌طور که در مقاله‌های قبل بررسی کردیم، اتصال اشیا از طریق یک شبکه، مفهوم «اینترنت اشیا» را به وجود می‌آورد. اینترنت اشیا زمینهٔ هوشمندسازی اشیا را فراهم می‌کند که به آسان‌شدن زندگی بشر کمک می‌کند. ممکن است وقتی اسم این فناوری را می‌شنویم، برای راه‌اندازی و استفاده از آن هیجان‌زده شویم، اما باید دقت کنیم و خطرات احتمالی را در نظر بگیریم. اینترنت اشیا به همان اندازه که می‌تواند کمک‌کننده و جالب باشد، ممکن است خطرآفرین نیز باشد و برای ما مشکلاتی به وجود بیاورد. یکی از مهم‌ترین آن‌ها، ایجاد محیط ناامن برای کاربران است. امنیت وضعیتی است که در فضای واقعی و در همه‌جا موردنیاز است. پس در صورت همگانی‌شدن اینترنت اشیا، تأمین امنیت این حوزه نیز اهمیت خواهد داشت.

برای روشن‌ترشدن موضوع به این مثال دقت کنید. امروزه برخی برای خانه‌های خود از درهای هوشمند استفاده می‌کنند. عملکرد این درها چنان است که اگر شکسته شوند یا شخصی به‌جز افرادِ خانه آن‌ها را باز کند، به‌سرعت به نزدیک‌ترین مرکز پلیس هشداری فرستاده می‌شود تا برای امنیت بیشتر اقدام کنند. حال تصور کنید، یکی از بخش‌های این درهای هوشمند توسط سارقان قابل‌نفوذ باشد. آن‌ها می‌توانند قفل را باز کنند و بدون اطلاع پلیس یا صاحب‌خانه وارد شوند. البته این مثال برای یک خانهٔ شخصی بود. می‌دانیم که اگر زمینهٔ نفوذ وجود داشته باشد، بانک‌ها، گاوصندوق‌ها، فروشگاه‌ها و حتی مراکز نظامی دچار مشکل می‌شوند و به خطر می‌افتند.

پس امنیت در اینترنت اشیا بسیار اهمیت دارد. برای بررسی روش‌های افزایش امنیت در اینترنت اشیا، بیایید نحوهٔ عملکرد اینترنت اشیا را مرور کنیم. همان‌طور که در مقاله‌های قبل توضیح دادیم، سامانهٔ اینترنت اشیا چند قسمت دارد: ۱. حسگرها؛ ۲. دستگاه اصلی؛ ۳. فضای ابری. حسگر روی دستگاه نصب شده است و اطلاعات مربوطه را به دستگاه گزارش می‌کند. دستگاه با اتصال به فضای ابری، اطلاعات دریافتی از حسگر را پردازش می‌کند و تصمیم می‌گیرد. مثلاً حسگر حساس به دما، تغییرات دما را به دستگاهِ ترموستات گزارش می‌کند و این دستگاه تصمیم می‌گیرد کدام یک از دستگاه‌های سرمایشی یا گرمایشی را روشن کند. در این حین، از طریق رابط کاربری طراحی‌شده در گوشی تلفن همراه، تمامی مراحل به کاربر گزارش می‌شوند.

برای بهبود وضع امنیت، در اینترنت اشیا، ابتدا باید محل آسیب‌پذیری را در شبکه شناسایی کرد و سپس راهکار ارائه داد. در نگاه اول درمی‌یابیم، اشکال کار در ناامن‌بودنِ ارتباطِ بین حسگرها و دستگاه‌هاست، چرا که آن‌ها از «ارتباطاتِ بدون رمزگذاری» استفاده می‌کنند. بدین ترتیب زمینهٔ نفوذ هکرها فراهم می‌شود. راهکار مدنظر برای حل این مشکل، استفاده از الگوریتم‌های رمزگذاری است، بدین‌وسیله ارتباط بین حسگر تا دستگاه و دستگاه تا فضای ابری، رمزگذاری می‌شود تا امنیت بیشتری در این سامانه برقرار شود.

از دیگر چالش‌های حوزهٔ امنیت، محدودبودن ظرفیت حافظه است که باعث می‌شود قابلیت ذخیره‌سازی و پردازش روی این دستگاه‌ها کاهش پیدا کند. در نتیجه الگوریتم‌های پیچیده روی این دستگاه‌ها اجرا نمی‌شوند. پس برای افزایش امنیت باید از الگوریتم‌های رمزگذاریِ سبک و سریع استفاده کرد.

گاهی رخنه‌گرها(هکرها) برای نفوذ به شبکه، هویت دستگاه را جعل می‌کنند و دستگاه خودشان را به‌جای دستگاه اصلی معرفی می‌کنند. سپس با استفاده از دسترسی‌هایِ دستگاه اصلی، به شبکهٔ اینترنت اشیا وارد می‌شوند. به این کار جعل هویت دستگاه می‌گویند. راهکاری که برای جلوگیری از جعل هویت داده می‌شود، برقراری تنظیمات احراز هویت برای دستگاه‌هاست، به صورتی که هر دستگاه فقط یک مجوزِ دسترسی به شبکه را داشته باشد. به این ترتیب دسترسی مهاجمان به شبکه برای دست‌کاری اطلاعات کاهش می‌یابد. بدین منظور به هر دستگاه نام کاربری و رمز عبور مخصوصی داده شود تا رخنه‌گرها نتوانند هویت دستگاه را جعل و به شبکه نفوذ کنند. البته باید از کاربران درخواست کرد از رمزهای قوی و غیرقابل‌حدس‌زدن استفاده کنند. همچنین، احراز هویت دومرحله‌ای را فعال کنند تا زمینهٔ نفوذ به حداقل برسد.

چالش بعدی، تهدیدهای فیزیکی هستند. اگر اینترنت اشیا همگانی شود، به مدیریت گسترده‌ای در حوزهٔ سخت‌افزار نیاز دارد، چرا که ممکن است حسگرها یا دستگاه‌ها به‌طور طبیعی یا حتی به‌طور عمدی تخریب شوند. به‌خصوص دستگاه‌هایی که در محیط باز نصب

می‌شـــوند، بیشـــتر از همه در معرض این آسیب هســـتند. مثلاً دوربین‌های مداربسته یا حسگرهایی که دسترسی به آن‌ها آسان است، به‌راحتی توسط باد، باران یا حتی خرابکاران آسیب می‌بینند. راهکاری که در برابر این تهدید وجود دارد، این است که ساختمان‌ها یا حتی خود اشـــیا طوری طراحی شوند که حفاظت به بیشـــترین مقدار خود برسد. مثلاً در مناطق بارانی از پوشش‌های ضدآب برای دستگاه‌ها استفاده شود یا دوربین‌ها در قسمتی از ساختمان قرار بگیرند که هم در برابر باران و باد و هم در برابر خطر خرابکاران محافظت شوند. ساختمان‌ها هم قبل از اینکه ساخته شوند، در معماری خود محلی امن برای اشیای هوشمند در نظر بگیرند تا تهدیدهای فیزیکی کاهش یابند.

به‌طور کلی باید گفت، اینترنت اشیا شبکه‌ای شاملِ دســـتگاه‌هایی با قابلیت‌های متفاوت است که در حوزهٔ امنیت به بهبود نیاز دارد. برای این کار باید محل آســـیب‌پذیری را پیدا و سپس راهکاری برای آن ارائه کرد. البته گاهی ممکن اســـت راهکاری ارائه شود که پاسخ‌گو نباشد. هر راهکار باید بارها و بارها آزمایش شود تا بفهمیم چقدر کارساز بوده است؟ و یا آیا روش بهتری وجود دارد یا خیر؟ در آخر باید گفت، اگر اینترنت اشیا غیرقابل‌نفوذ شود و پروتکل‌های امنیتی در آن رعایت شـــوند، آرامش ذهنی افراد را فراهم می‌کند و با توجه به اطلاعات دقیقی که ارائه می‌دهد، می‌تواند وضعیت اشیا و نحوهٔ استفاده از آن‌ها را گزارش کند. این داده‌ها به مشتریان کمک می‌کنند خدمات بهتری ارائه دهند. این فناوری در صورت فراگیرشدن به بهبود زندگی بشر کمک بزرگی می‌کند.