

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

معماری و امنیت در اینترنت اشیا



حمید کوثری

۵	 مقدمه
۷	 فصل اول: معماری اینترنت اشیاء
۸	 (I) اینترنت اشیاء
۱۴	 (II) مقایسه معماری های اینترنت اشیاء
۲۶	 (III) چرا یک معماری مشترک را نمی توان تعریف کرد؟
۳۰	 (IV) موارد مطالعاتی
۳۲	 (V) کاربردها
۳۵	 (VI) نتیجه گیری
۳۵	 (VII) افق های آتی
۳۷	 REFERENCES
۴۵	 فصل دوم: چالش های امنیتی اینترنت اشیاء
۴۶	 (I) تهدیدهای امنیتی اینترنت اشیاء
۵۱	 (II) چالش های امنیتی در حوزه IoT
۵۷	 (III) مکانیزم های اصلی امنیت برای سرویس های IoT
۶۶	 (IV) امنیت فناوری های ارتباطی IoT متداول
۹۸	 (V) مثال هایی از پیاده سازی ها در دستگاه های تجاری
۱۰۵	 (VI) نکات نهایی
۱۱۱	 REFERENCES

مقدمه

اینترنت اشیاء یا IoT مدل شبکه آتی است و نگرشی است که بر مبنای آن وسایل ناهمگن هوشمندانه تر می‌شوند. اینترنت اشیاء به سرعت در حال گسترش است و به بسیاری از حوزه‌های مختلف از جمله مراقبت‌های بهداشتی شخصی، نظارت بر محیط، اتوماسیون خانگی، تحرک هوشمند و نسخه ۴.۰ صنعت رسیده است. در نتیجه، هرچه بیشتر دستگاه‌های اینترنت اشیاء در محیط‌های همگانی و خصوصی مختلف مستقر می‌شوند و به تدریج به اشیای معمول زندگی روزمره تبدیل می‌شوند.

در IoT دستگاه‌های تعبیه شده با اشیای دوردست از طریق اینترنت یا مخابرات میدان نزدیک (NFC) ارتباط می‌گیرند. یک معماری نمونه شامل دستگاهی است که با استفاده از گیت وی‌ها با ابر ارتباط می‌گیرند. توصیف فریمورک IoT مورد استفاده در تعدادی برنامه کاربردی، کاربردهای وسیع و فرآیندهای تجاری در حالت کلی ساده است. مقالات هروری متعددی وجود دارند که در آنها مولفین فریمورک معماری مبتنی بر پارامترهای متنوع مانند پلتفرم‌های IoT جدید، استانداردهای IoT نظیر EPC Global، P2413، نظریه فراکتال، محاسبات مه، IoT جهانی، IoT محلی، فریمورک‌های سه تایی، چهارتایی، پنج تایی و بسیاری ایده‌های نوین دیگر را توصیف می‌کنند.

از طرفی دیگر با گسترش روز افزون اینترنت اشیاء در محیط‌های همگانی و خصوصی مختلف، امنیت سایبری برای جلوگیری از تهدیداتی مانند نشت اطلاعات حساس، حملات انکار سرویس، دسترسی غیر مجاز به شبکه و غیره، تبدیل به یک چالش حیاتی می‌شود. متأسفانه، بسیاری از محصولات تجاری سطح پایین اینترنت اشیاء معمولاً از مکانیسم‌های امنیتی قوی پشتیبانی نمی‌کنند و از این رو می‌توانند هدف - یا حتی وسیله ای - برای تعدادی از

حملات امنیتی باشد. هدف این کتاب ارائه یک نمای کلی از ریسک‌های امنیتی در بخش اینترنت اشیاء و بحث در مورد روش‌های مقابله ممکن است. برای این منظور، پس از معرفی کلی امنیت در حوزه اینترنت اشیاء، ما در مورد مکانیزم‌های امنیتی ویژه‌ای که توسط محبوب‌ترین پروتکل‌های ارتباطی اینترنت اشیاء استفاده شده است بحث می‌کنیم. سپس، برخی از حملات علیه دستگاه‌های اینترنت اشیاء واقعی گزارش شده در منابع رسمی را گزارش و تجزیه و تحلیل می‌کنیم تا نقاط ضعف امنیتی موجود در راه حل‌های تجارت اینترنت اشیاء را نشان دهیم و اهمیت توجه به امنیت را به عنوان بخشی جدایی ناپذیر در طراحی سیستم‌های اینترنت اشیاء مورد توجه قرار دهیم.

با توجه به آنچه گفته شد معماری‌های امنیتی IoT برای مواجهه با چالش‌های آتی نیز باید مورد بازنگری قرار گیرند. از این رو در این کتاب یک مرور جامع درباره معماری‌های کاربردی اخیر IoT و نحوه نقش آفرینی یک معماری مرجع استاندارد IoT برای ارزیابی راه حل‌های مختلف IoT با توجه به مجموعه‌ای از ویژگی‌های امنیتی واجد شرایط، یعنی یکپارچگی، ناشناس بودن، محرمانه بودن، حفظ حریم خصوصی، کنترل دسترسی، احراز هویت، مجوز، تاب آوری و خود سازماندهی ارائه می‌گردد.