

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

معماری و امنیت در اینترنت اشیاء



حمید کوثری

سرشناسه	- کوثری، حمید، ۱۳۶۲
عنوان و نام پدیدآور	معماری و امنیت در اینترنت اشیاء / حمید کوثری.
مشخصات نشر	گرگان: انتشارات نوروزی، ۱۴۰۱، ۱۲۴ ص: مصور، جدول، نمودار؛ ۱۴/۵ × ۲۱/۵ س.م.
مشخصات ظاهری	شابک ۹۷۸-۶۲۲-۰۲-۲۳۵۵-۹ ریال ۱۰۰۰۰۰
شاپاک	و ضعیف فهرست نویسی
یادداشت	فایل کتابنامه: ص. ۱۱۱ - ۱۱۴
موضوع	اینترنت اشیاء
Internet of things	Internet of things -- اینترنت اشیاء -- تدابیر ایمنی
Internet of things -- Security measures	Internet of things -- Security measures
رده بندی کنگره	۸۸۵/TK۵۱۰.۵
رده بندی دیوبی	۶۷۸ /۰۰۴
شماره کتابخانس ملی	۸۹۵۷۵۱۷
اطلاعات رکورد کتابخانس	۹۷۸-۶۲۲-۰۲-۲۳۵۵-۹

معماری و امنیت در اینترنت اشیاء
 ترجمه و تالیف: حمید کوثری
 نوبت چاپ: اول - ۱۴۰۱
 مشخصات ظاهری: ۱۲۴ ص
 قطع: رقعی
 شماره گان: ۱۰۰۰ نسخه
 شماره شابک: ۹۷۸-۶۲۲-۰۲-۲۳۵۵-۹
 چاپ و نشر: نوروزی-۲۵۸-۱۷۳۲۲۴۲۲۵۸.
 قیمت: ۱۰۰۰۰ تومان

حق چاپ برای نویسنده محفوظ می باشد.



نشانی: گلستان، گرگان، خیابان شهید بهشتی، بازار رضاع، ۱۷-۳۳۲۰۰۴۷، آدرس الکترونیکی: Entesharate.noruzi@gmail.com
 سایت انتشارات: www.Entesharate-noruzi.com

فهرست

۵	مقدمه
۷	فصل اول: معماری اینترنت اشیاء
۸	I) اینترنت اشیاء
۱۴	II) مقایسه معماری‌های اینترنت اشیاء
۲۶	III) چرا یک معماری مشترک را نمی‌توان تعریف کرد؟
۳۰	IV) موارد مطالعاتی
۳۲	V) کاربردها
۳۵	VI) نتیجه گیری
۳۵	VII) افق‌های آتی
۳۷	REFERENCES
۴۵	فصل دوم: چالش‌های امنیتی اینترنت اشیاء
۴۶	I) تهدیدهای امنیتی اینترنت اشیاء
۵۱	II) چالش‌های امنیتی در حوزه IoT
۵۷	III) مکانیزم‌های اصلی امنیت برای سرویس‌های IoT
۶۶	IV) امنیت فناوری‌های ارتباطی IoT متداول
۹۸	V) مثال‌هایی از پیاده سازی‌ها در دستگاه‌های 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 مراقبتهاهای بهداشتی شخصی، نظارت بر محیط، اتوماسیون خانگی، تحرک هوشمند و نسخه ۴۰ 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 تعییه شده با اشیای دوردست از طریق اینترنت یا مخابرات میدان نزدیک (NFC) ارتباط می‌گیرند. یک معماری نمونه شامل دستگاهی است که با استفاده از گیت‌وی‌ها با ابر ارتباط می‌گیرند. توصیف فریمورک IoT مورد استفاده در تعدادی برنامه کاربردی، کاربردهای وسیع و فرآیندهای تجاری در حالت کلی ساده ایست. مقالات همروزی متعددی وجود دارند که در آنها مولفین فریمورک معماری مبتنی بر پارامترهای متنوع مانند پلاتفرم‌های 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 سروپس، 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 وسیله‌ای - 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 سنتی IoT برای مواجهه با چالش‌های آتی نیز باید مورد بازنگری قرار گیرند. از این‌رو 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، ناشناسی بودن، محرومانه بودن، حفظ حریم خصوصی، کنترل دسترسی، احراز هویت، مجوز، تاب آوری و خود سازماندهی ارائه می‌گردد.