



۱۵۵۸۶۱۷

اهمیت اینترنت اشیا

مترجم: مهدی اربک رانی

۱۳۹۶

مؤسسه آموزشی تألیفی ارشدان

سرشناسه	:	لی، شان تسای Li, Shancang
عنوان و نام پدیدآور	:	امنیت اینترنت اشیا / مترجم مهدی ازبک‌زایی.
مشخصات نشر	:	تهران: موسسه آموزشی تالیفی ارشدان، ۱۳۹۶.
مشخصات ظاهری	:	۱۷۸ ص.
شابک	:	۹۷۸-۶۰۰-۸۹۹۹-۰۲-۷
وضعیت فهرست نویسی	:	فیفا
یادداشت	:	Securing the internet of things. عنوان اصلی.
موضوع	:	اینترنت اشیا
موضوع	:	Internet of things
موضوع	:	شبکه‌های کامپیوتری — تدابیر ایمنی
موضوع	:	Computer networks -- Security measures
موضوع	:	کامپیوترها — ایمنی اطلاعات
موضوع	:	Computer security
شناسه افزوده	:	ازبک‌زایی، مهدی، ۱۳۵۷ -
رده بندی کنگره	:	الف۹/ل۹۸۵۷/۵/۸۸۵۷ TK۵۱۰۵ ۱۳۹۶
رده بندی دیویی	:	۰۰۴/۶۷۸
شماره کتابشناسی ملی	:	۴۹۹۵۱۰

ارشدان

مؤسسه آموزشی تالیفی ارشدان

نام کتاب:	امنیت اینترنت اشیا
ترجمه:	مهدی ازبک‌زایی
ناشر:	آموزشی تالیفی ارشدان
ویرایش:	اول
نوبت چاپ:	اول ۱۳۹۶
حروفچینی و صفحه آرایی:	www.irantypist.com
طراح و گرافیکست:	www.irantypist.com
شابک:	۹۷۸-۶۰۰-۸۹۹۹-۰۲-۷
شمارگان:	۱۰۰۰
مرکز خرید آنلاین:	www.arshadan.com
مرکز پخش و توزیع:	www.arshadan.net
قیمت:	۰۲۱۴۷۶۲۵۵
	۳۰۰۰۰ تومان

مقدمه مترجم

اینترنت اشیاء به عنوان یکی از موضوعات جدید در علوم کامپیوتر مورد تحقیق قرار گرفته و مبحث مطرح شده در ترجمه حاضر به اصلی‌ترین نگرانی استفاده کنندگان و تولید کنندگان خدمات جدید یعنی امنیت پرداخته است. کمبود منابع فارسی درباره اینترنت اشیاء مشوق اصلی برای ارائه این اثر می‌باشد و مطمئناً متن حاضر در ترجمه خالی از اشکال نمی‌باشد، اما امیدواریم با استفاده از راهنمایی‌های خوانندگان این اثر بتوانیم به افزایش کیفیت و رفع خطاهای احتمالی پرداخته شود، امیدواریم با این اثر به ادبیات تحقیقی درباره امنیت اینترنت اشیاء کمک نموده و همچنین به مصرف کنندگان این فن آوری جدید اطمینان داده شود که موضوعات امنیت و حریم خصوصی مشتریان به عنوان دغدغه‌ای اصلی در حال تحقیق می‌باشد. این اثر یکی از تازه‌ترین کتابهای نشر یافته در سال ۲۰۱۷ می‌باشد و می‌توان تازه‌تر و شاید غامض‌تر بودن برخی از اصطلاحات کاملاً احساس شود، که امیدواریم با ارائه این اثر به این مهم مرتفع گردد.

مهدی ازبک زایی

آذر ۱۳۹۶

Mehdizbakh@gmail.com

m032496f@student.staffs.ac.uk

فهرست مطالب

فصل ۱: ایمن سازی اینترنت اشیا	۱۳
۱-۱. مقدمه	۱۳
۱-۱-۲. مرور پژوهش‌های اخیر	۱۴
۱-۱-۳. الزامات امنیتی	۱۷
۱-۲. الزامات امنیت در معماری IoT	۱۹
۱-۲-۱. لایه حسگر و گره‌های انتهایی IoT	۲۱
۱-۲-۲. لایه شبکه	۲۴
۱-۲-۳. لایه خدمات	۲۶
۱-۲-۴. لایه رابط کاربردی	۲۹
۱-۲-۵. تهدیدات متقابل لایه‌ها	۳۱
۱-۲-۶. تهدیدات ناشی از نگهداری IoT	۳۲
۱-۳. امنیت در بهره برداری از فناوری	۳۲
۱-۳-۱. امنیت در فن آوری های شناسایی و ردیابی	۳۲
۱-۳-۲. امنیت در تلفیق WSN و RFID	۳۳
۱-۳-۳. امنیت در ارتباطات	۳۴
۱-۳-۴. امنیت در شبکه‌ها	۳۶
۱-۳-۵. امنیت در مدیریت خدمات	۳۷
۱-۴. نگرانی‌های امنیتی در برنامه‌های IoT	۳۷
۱-۴-۱. نگرانی‌های امنیتی در سیستم‌های SCADA	۳۸

۴۰	۳-۴-۱. نگرانی‌های امنیتی در IoT اجتماعی
۴۱	۴-۴-۱. محرمانه بودن و امنیت برای مراقبت‌های بهداشتی مبتنی بر IoT
۴۳	۵-۱. خلاصه
۴۵	فصل ۲: معماری امنیت در اینترنت اشیا
۴۵	۱-۲. مقدمه
۴۷	۲-۲. الزامات امنیت در IoT
۴۸	۱-۲-۲. چالش‌های امنیتی داده‌های اینترنت اشیا
۴۹	۱-۲-۲-۱. محرمانه بودن داده‌ها
۵۰	۱-۲-۲-۱. حریم خصوصی
۵۰	۱-۲-۲-۲. اعتماد
۵۱	۲-۲-۲. امنیت در لایه شبکه
۵۱	۳-۲-۲. امنیت در لایه دستگاه
۵۲	۴-۲-۲. امنیت در لایه درویس
۵۳	۵-۲-۲. امنیت در لایه رابط
۵۴	۶-۲-۲. چالش‌های امن IoT
۵۵	۳-۲. تأیید / مجوز ناکافی
۵۵	۱-۳-۲. تأیید اعتبار در IoT
۵۶	۲-۳-۲. مجوز
۵۷	۳-۳-۲. تأیید هویت / مجوز کافی نیست
۵۸	۱-۳-۳-۲. فردی
۵۸	۲-۳-۳-۲. منطقه تجاری
۵۸	۳-۳-۳-۲. توانایی دسترسی به IoT
۵۹	۴-۳-۲. تأیید هویت دستگاه در IoT ناکافی است
۶۰	۴-۲. کنترل دسترسی نا امن
۶۱	۱-۴-۲. سیستم‌های کنترل دسترسی مبتنی بر نقش
۶۱	۲-۴-۲. دسترسی سیستم‌های مبتنی بر لیست
۶۲	۳-۴-۲. دسترسی مبتنی بر قابلیت و توانایی
۶۳	۴-۲-۲. چالش‌ها در کنترل دسترسی
۶۴	۵-۲. تهدیدات برای کنترل دسترسی، حفظ حریم خصوصی و موجود بودن

۶۵	۲-۵-۱. تهدیدات در لایه شبکه
۶۸	۲-۵-۲. تهدیدات در لایه حسگر
۷۱	۲-۵-۳. تهدیدات در لایه عبور و نگهداری IoT
۷۳	۲-۶ حملات مربوط به IoT
۷۳	۲-۶-۱. دسترسی فیزیکی
۷۵	۲-۶-۲. حملات موضعی به وای فای
۷۷	فصل ۳: امنیت و موارد در معرض خطر در اینترنت اشیا
۷۷	۳-۱. ظرفیت کلید مخفی و محرمانگی
۸۱	۳-۲. سند ۱۰۰ روز برای قطعات هوشمند
۸۷	۳-۳. رمز گذاری انتقالی
۸۸	۳-۳-۱. امنیت لایه عمل و نقل
۸۸	۳-۳-۲. لایه سوکت امن
۸۹	۳-۳-۳. HTTPS
۸۹	۳-۳-۴. اعتماد حمل و نقل در IoT
۹۰	۳-۴. واسطه وبی/برایمن
۹۱	۳-۵. نرم افزار یا نرم افزار دایمی امن
۹۴	۳-۶. امنیت لایه فیزیکی
۹۷	۳-۷. خلاصه
۹۹	فصل ۴: تصدیق (سندیت) گره اینترنت اشیا (IoT)
۱۰۰	۴-۱. اهداف حراست در IoT
۱۰۲	۴-۲. سندیت بر اساس کلیدی عمومی
۱۰۵	۴-۲-۱. رمزنگاری متقارن
۱۰۷	۴-۲-۲. AES-CCM
۱۰۸	۴-۲-۳. رمزنگاری کلید عمومی
۱۱۰	۴-۲-۴. زیرساخت کلید عمومی
۱۱۱	۴-۳. شناسایی، رمزگذاری، و نشانه دیجیتال مبتنی بر شناسه
۱۱۱	۴-۳-۱. تأیید هویت مبتنی بر شناسایی
۱۱۵	۴-۳-۲. امضای دیجیتالی
۱۱۸	۴-۳-۳. کلید عمومی خام

۱۲۰	۴-۳-۴. گواهینامه‌های X. 509
۱۲۱	۴-۴. اتصال IP
۱۲۲	۴-۴-۱. امنیت لایه انتقالی (حمل و نقل) دیتاگرام
۱۲۵	۴-۴-۲. پروتکل برنامه محدود
۱۲۵	۴-۵. رمز نویسی سبک
۱۲۶	۴-۵-۱. کارایی ارتباط به هم پیوسته
۱۲۶	۴-۵-۲. قابلیت استفاده برای دستگاه‌هایی با منابع کم‌تر
۱۲۸	۴-۶. چالش‌های امنیتی موجود برای IOT
۱۳۰	۴-۷. نتیجه
۱۳۳	فصل ۱. نیازهای امنیتی در معماری اینترنت اشیا
۱۳۳	۵-۱. مقدمه
۱۳۵	۵-۱-۱. چالش‌های امنیتی در محیط IOT
۱۳۶	۵-۱-۲. لایه حسگر و گره‌های انتهایی IoT
۱۴۰	۵-۲. لایه شبکه
۱۴۳	۵-۳. لایه سرویس
۱۴۵	۵-۴. لایه رابط - کاربردی
۱۴۸	۵-۵. تهدیدها در لایه متقاطع
۱۴۸	۵-۶. تهدیدات ناشی از نگهداری IoT
۱۴۹	فصل ۶: امنیت در توانا کردن تکنولوژی‌ها
۱۴۹	۶-۱. امنیت شناسایی و تکنولوژی‌های ردیابی
۱۵۰	۶-۱-۱. شناسایی
۱۵۰	۶-۱-۱-۱. ردیابی
۱۵۱	۶-۲. امنیت در تلفیق شبکه حسگر بی سیم و RFID
۱۵۶	۶-۳. امنیت در ارتباطات
۱۵۸	۶-۴. پروتکل‌های امنیتی و مسائل مربوط به حفظ حریم خصوصی در پشته 6LoWPAN
۱۵۸	۶-۵. امنیت در مدیریت خدمات

فصل ۷: طرح امنیتی حاضر در اینترنت اشیا	۱۵۹
۷-۱. امنیت اطلاعات و حفظ حریم خصوصی.....	۱۵۹
۷-۲. محرمانگی اطلاعات و مدیریت کلید.....	۱۶۱
۷-۳. بررسی مقالات.....	۱۶۵
فصل ۸: نگرانی‌های امنیتی در اینترنت اشیا اجتماعی	۱۷۱
فصل ۹: امنیت و قابلیت اعتماد برای مراقبت درمانی براساس اینترنت اشیا..	۱۷۳

www.ketab.ir