بسم الله الرحمن الرحیم

اینترنت اشیاء، امنیت
و چالش های پیش روی آن

فرهاد رحمتی

انتشارات ابداع

سرشناسه : قائد رحمتی، فرهاد، ۱۳۶۵ -
عنوان و نام پدیدآور : اینترنت اشیاء، امنیت و چالش‌های پیش روی آن/فرهاد رحمتی.
مشخصات نشر : تهران: نشر ابداع، ۱۳۹۷.
مشخصات ظاهری : ۶۲ ص.
شابک : ۰-۱-۹۵۲۶۹-۶۲۲-۹۷۸:
وضعیت فهرست نویسی : فیپا
موضوع : اینترنت اشیاء
موضوع : Internet of things
موضوع : اینترنت اشیاء -- تدابیر ایمنی
موضوع : Internet of things -- Security measures
رده بندی کنگره : ۱۳۹۷ ۹الف۲ق/QA۷۶/۵۹۱۵
رده بندی دیویی
شماره کتابشناسی ملی ۵۵۱۱۹۹۳

عنوان: اینترنت اشیاء امنیت و چالش های پیش روی آن
ناشر: ابداع
نوبت چاپ: اول ۱۳۹۷
مولف: فرهاد رحمتی
تیراژ: ۱۰۰۰ نسخه
شابک: ۰-۱-۹۵۲۶۹-۶۲۲-۹۷۸
لیتوگرافی: مینیاتور
چاپ: فرشیوه
قیمت: ۹۰۰۰ تومان
آدرس: تهران-میدان انقلاب-خیابان کارگر جنوبی بین خ نظری و روانمهر- بن بست گشتاسب- پلاک ۷- واحد ۱ - تلفن: ۶۶۴۷۲۲۳۰

فهرست مطالب

عنوان **صفحه**

چکیده ۱

فصل اول : کلیات تحقیق

۱-۱. مقدمه ۳

۱-۲. اصطلاحات مرتبط ۷

۱-۲-۱. تشخیص نفوذ ۷

۱-۲-۲. اینترنت اشیاء ۸

۱-۳. بررسی کارهای مرتبط ۱۵

فصل دوم : روش های تشخیص نفوذ در اینترنت اشیاء

۲-۱. تشخیص نفوذ در اینترنت اشیاء ۲۲

۲-۲. استراتژی‌های قرار گرفتن IDS ۲۴

۲-۲-۱. قرار گرفتن IDS به صورت توزیع شده ۲۵

۲-۲-۲. قرار گرفتن IDS به صورت متمرکز ۲۷

۲-۲-۳. قرار گرفتن IDS به صورت ترکیبی ۲۸

۲-۳. روش‌های تشخیص ۳۱

۲-۳-۱. رویکردهای مبتنی بر امضا ۳۲

۲-۳-۲. رویکردهای مبتنی بر ناهنجاری ۳۴

۲-۳-۳. رویکردهای مبتنی بر مشخصه ۳۷

۲-۳-۴. رویکردهای ترکیبی ۳۹

فصل سوم : چالش های امنیتی اینترنت اشیا

۳-۱. چالش های امنیتی و انواع حملات در اینترنت اشیاء ۴۲

۳-۲. مسائل امنیتی در شبکه های حسگر بیسیم (WSNS) ۴۶
۳-۳. حملات انگار سرویس بر لایه های IOT ۴۷
۳-۳-۱. حمله Dos به لایه فیزیکی: ۴۷
۳-۳-۳.حمله DOS به لایه شبکه ۴۸
۳-۳-۴.حملات DOS در لایه انتقال ۴۹
۳-۳-۵.حملات D05 در لایه کاربرد ۵۰
۳-۴. اهمیت داده در اینترنت اشیاء : ۵۰
۳-۵. نبود استاندارد واحد ۵۲
۳-۶.چالش های اینترنت اشیا ۵۳
۳-۶-۱.چالش حریم خصوصی ۵۳
۳-۶-۲.چالش امنیتی ۵۳
۳-۶-۳.چالش هرج و مرج ۵۴
۳-۷.مشخصه های بسیار مرتبط برای امن کردن اینترنت اشیا ۵۵
۳-۸.فایروال و سیاست های تحرک در اینترنت اشیاء ۵۶

چکیده

اینترنت اشیاء (IoT) الگوی جدیدی است که اینترنت و اشیاء فیزیکی را ادغام می‌کند، اشیائی که به دامنه‌های مختلفی از قبیل اتوماسیون منزل، فرآیندهای صنعتی، نظارت بر سلامت انسان و نظارت محیطی تعلق دارند. اینترنت اشیاء حضور وسایل متصل به اینترنت را در فعالیت‌های روزانه‌ی ما عمیق‌تر می‌کند و مزایای زیادی را به همراه داشته و از طرفی چالش‌های مرتبط با مسائل امنیتی را نیز ایجاد می‌کند. در دهه گذشته، اینترنت اشیاء در مرکز توجهات و تحقیقات زیادی قرار داشته است. امنیت و محرمانه بودن، مسایل مهمی برای کاربردهای IOT بوده و همچنان با چالش های بزرگی مواجه است. معماری های اینترنت اشیاء قرار است با جمعی حدود میلیاردها اشیاء سر و کار داشته باشد، که با یکدیگر و با دیگر نهادها، مانند انسان ها و یا نهادهای مجازی تعامل خواهند داشت. همه این تعاملات باید به نحوی محافظت شود، از جمله حفاظت از اطلاعات و تأمین خدمات تمام بازیگران مربوطه و نیز محدود کردن تعداد حوادثی که بر کل اینترنت اشیاء تأثیر می گذارد. با این حال، حفاظت اینترنت اشیاء یک کار پیچیده و دشوار است. تعداد حمله های در دسترس حمله کننده های مخرب با توجه به اتصال جهانی (دسترسی هر کسی) و دسترس پذیری (دسترسی به هر شکل در هر زمان) به عنوان روندهای اصلی اینترنت اشیاء ممکن است گیج کننده باشند. تهدیداتی که می توانند بر نهادهای اینترنت اشیا تأثیر گذارد متعدد هستند، مانند حملات باهدف کانال های ارتباطی مختلف، تهدیدات فیزیکی، محرومیت از خدمات، ساخت هویت، و غیره. در نهایت، پیچیدگی ذاتی اینترنت اشیاء که در آن نهادهای ناهمگن متعدد واقع در زمینه های مختلف می توانند اطلاعات را با یکدیگر مبادله کنند، پیچیدگی های بیشتر طراحی و بکارگیری مکانیزم های امنیتی کارآمد، سازگار و مقیاس پذیر را می طلبد. در این تحقیق به طور خاص روش های تشخیص نفوذ در اینترنت اشیاء و چالش های امنیتی اینترنت اشیا مورد بحث و بررسی قرار گرفته است.

کلمات کلیدی: سیستم تشخیص نفوذ؛ اینترنت اشیاء؛ امنیت سایبری، حملات اینترنتی.