
بسم الله الرحمن الرحيم

عنوان

بررسی تشخیص نفوذ در اینترنت اشیاء

فهرست مطالب

فهرست جداول

چکیده

اینترنت اشیاء 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. به مدت بیش از دو دهه، سیستم‌های تشخیص نفوذ ابزار مهمی برای حفاظت از شبکه‌ها و سیستم‌های اطلاعاتی بوده‌اند. با این حال، استفاده از روش‌های معمولی تشخیص نفوذ در اینترنت اشیاء به دلیل ویژگی‌های خاصی از قبیل وسایلی با محدودیت منابع، پشته‌های پروتکلی خاص، و استانداردها دشوار است. در این مقاله، ما به بررسی تلاش‌های تحقیقاتی انجام شده در زمینه‌ی تشخیص نفوذ برای اینترنت اشیاء می‌پردازیم. هدف ما شناسایی روندهای پیش رو، مسائل باز، و کارهای تحقیقاتی آینده است. ما سیستم‌های تشخیص نفوذ ارائه شده در مقالات پژوهشی را بر اساس ویژگی‌های زیر طبقه‌بندی نموده‌ایم: روش تشخیص، استراتژی قرار گرفتن تشخیص نفوذ، تهدید امنیتی و استراتژی اعتبارسنجی. ما همچنین در مورد احتمالات مختلف برای هر یک از ویژگی‌ها نیز بحث کرده و به تشریح جنبه‌های کارهایی پرداخته‌ایم که روش تشخیص نفوذ خاصی را برای اینترنت اشیاء ارائه کرده‌اند یا استراتژی‌های تشخیص حمله را برای تهدیدات اینترنت اشیاء توسعه داده‌اند که ممکن است در سیستم‌های تشخیص نفوذ قرار داده شود.

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

فصل اول

مقدمه و کلیات تحقیق

۱-۱- مقدمه

تکامل فناوری‌های مختلف از قبیل حسگرها، شناسایی و ردیابی خودکار، محاسبات نهفته، ارتباطات بی‌سیم، دسترسی باند گسترده به اینترنت و سرویس‌های توزیع شده، پتانسیل ادغام اشیاء هوشمند را در زندگی روزانه‌ی ما از طریق اینترنت افزایش می‌دهد. همگرایی اینترنت و اشیاء هوشمندی که می‌توانند به برقراری ارتباط و تعامل با یکدیگر بپردازند، اینترنت اشیاء[1] (IoT) را تعریف می‌کند. این الگوی جدید به عنوان یکی از مهمترین عوامل در صنعت فناوری اطلاعات و ارتباطات[2] (ICT) در سال‌های آینده تشخیص داده شده است (Miorandi و همکارانش، ۲۰۱۲). به گزارش شرکت Gartner، اینترنت اشیاء ممکن است تا سال ۲۰۲۰ دارای ۲۶ میلیارد واحد باشد. سیستم‌های سیسکو پیش‌بینی کرده‌اند که اینترنت اشیاء بین سال‌های ۲۰۱۳ تا ۲۰۲۲ در نتیجه‌ی ترکیب افزایش درآمد و کاهش هزینه‌ها، در آمد ۱۴.۴ تریلیون دلار ایجاد خواهد کرد (Lee و Lee، ۲۰۱۵؛ Bradley و همکارانش، ۲۰۱۳؛ Sicari و همکارانش، ۲۰۱۵؛ Singh و همکارانش، ۲۰۱۴).

بسیاری از حوزه‌های کاربردی از قبیل تدارکات، فرآیندهای صنعتی، ایمنی عمومی، اتوماسیون منازل، نظارت بر محیط و مراقبت از سلامتی ممکن است با استفاده از سیستم‌های اینترنت اشیاء مزایای قابل توجهی داشته باشند (Borgia، ۲۰۱۴). با این حال، ادغام اشیاء موجود در دنیای واقعی با اینترنت می‌تواند تهدیدات امنیتی سایبری را نیز در بسیاری از فعالیت‌های روزانه‌ی ما به همراه داشته باشد. حملات مختلف علیه زیرساخت‌های حیاتی و مهم از قبیل نیروگاه‌های انرژی و سیستم‌های حمل و نقل ممکن است عواقب بسیار وحشتناکی برای تمام شهرها و کشورها داشته باشد. لوازم خانگی ممکن است یک هدف اولیه برای تهدیدات امنیتی و حریم خصوصی خانواده باشد. در مقاله‌ی Notra و همکارانش (۲۰۱۴)، آزمایش‌های انجام شده بر روی سه دستگاه محبوب خانگی، آسیب‌پذیری‌های مختلفی را در رابطه با حریم خصوصی کاربران، فقدان رمزنگاری و احرازهویت نشان می‌دهد. با توجه به استانداردها و پشته‌های ارتباطی مختلف، توان محدود محاسباتی و تعداد بالای وسایل به هم متصل، اقدامات رایج امنیتی در برابر این تهدیدات نمی‌تواند در سیستم‌های اینترنت اشیاء به طور موثری عمل کند. به همین دلیل، توسعه‌ی راه‌حل‌های امنیتی خاص برای اینترنت اشیاء ضروری است تا به کاربران و سازمان‌ها اجازه دهند تمام نقاط ضعف سیستم را شناسایی کنند (Sicari و همکارانش، ۲۰۱۵).

[1] Internet of Things (IoT)
[2] Information and Communication Technology (ICT)