Archive of SID

دهمین همایش پژوهش‌های نوین در علوم و فناوری
Tenth Conference on Recent Research in Science and Technology
تابستان ۱۳۹۶
Summer 2017

مروری بر چالش‌ها و راهکارهای پیشگیری از چالش‌های اینترنت اشیاء

سید میلاد میرمحمدیان[۱]، ساسان برهلیا[۲]، رمضان بابامحمودی[۳]، زهرا آخوندی[۴]

[۱] مدرس موسسه آموزش عالی بصیر
mir.mohammadian@basir-abyek.ac.ir

[۲] مدرس موسسه آموزش عالی بصیر
berehlia@basir-abyek.ac.ir

[۳] مدرس موسسه آموزش عالی بصیر
babamahmoudi@basir-abyek.ac.ir

[۴] دانشجوی لیسانس مهندسی نرم افزار کامپیوتر موسسه آموزش عالی بصیر
z.akhondi3@gmail.com

چکیده

در دنیای مدرن امروز فناوری اطلاعات، مقوله اینترنت اشیاء از اهمیت و ویژگی زیادی برخوردار است. این فناوری دارای مزایای زیادی همانند کاهش هزینه و صرفه‌جویی در وقت و هوشمند شدن اشیا است. همچنین در زمینه‌های مختلف مثل پزشکی و کشاورزی قابل‌استفاده است. بااین‌حال، از معایب آن فناوری نمی‌توان چشم‌پوشی کرد. از بزرگ‌ترین معایب و چالش‌های پیشرو این فناوری امنیت و مقوله کلان داده است. در اینترنت اشیاء، هر دستگاه متصل می‌تواند یک درگاه احتمالی به زیرساخت اینترنت اشیاء یا داده‌های شخصی باشد. نگرانی‌های امنیت و حریم خصوصی داده بسیار مهم هستند، اما با ورود پیچیدگی، نقاط ضعف امنیتی و آسیب‌پذیری‌های احتمالی در مواردی مانند قابلیت همکاری، ترکیبات و تصمیم‌گیری‌های خودگردان، خطرات احتمالی مربوط به اینترنت اشیاء سطح جدیدی به خود گرفته‌اند. این مقاله، به بررسی اینترنت اشیا، مزایا و چالش‌های پیشروی آن و معرفی برخی راه‌حل‌ها با این چالش‌ها پرداخته‌شده است. همچنین، با توجه به چالش‌های کلیدی همانند امنیت و کلان داده، جمع‌بندی کلی جهت مقابله با این چالش‌ها پرداخته شده است.

کلمات کلیدی: اینترنت اشیاء، کلان داده، امنیت، استاندارد واحد.

۱. مقدمه

اینترنت اشیا[۱] ازجمله موضوعات داغ این روزهای عرصه فناوری است که دومین تحول بزرگ معرفی‌شده است. اینترنت اشیاء یا همان IoT، مفهومی که اولین بار در سال ۱۹۹۰م توسط مارک ویزر در موسسه فناوری ماساچوست مطرح‌شده و در سال ۱۹۹۹توسط کوین اشتون مطرح گردید. تغییرات در جهان امروز ناشی از تغییرات علم و فناوری است. این تغییرات در

[1] Internet of Things (IoT)

www.SID.ir

Archive of SID

تمامی محورهای زندگی ما اثر مستقیم داشته و به‌عبارت‌دیگر هرروز شاهد اضافه شدن یک سری مفاهیم و اصطلاحات متنوع هستیم که نشان از نفوذ روزافزون و تأثیرگذاری فزاینده فناوری اطلاعات بر زندگی روزمره است. امروزه بحث‌های زیادی در مورد اینترنت اشیاء صورت گرفته است. نکته کلیدی که در مورد اینترنت اشیاء وجود دارد این است که به ما کمک می‌کند تا از منابع خود مؤثرتر استفاده کنیم، منابع و انرژی کمتری را هدر دهیم، با دقت بیشتری منابع خود را مدیریت کنیم و با کمک اطلاعات و فناوری مؤثرتر ارتباط برقرار کنیم. همان‌طور که می‌دانیم هرروزه ماشین‌های جدید و سامانه‌های آنلاین جدید اطلاعات زیادی را به سامانه‌های اطلاعاتی مرکزی ارسال می‌نمایند. اینترنت اشیا در حوزه‌های مختلفی مثل کشاورزی، پزشکی، صنعت و در راهنمایی رانندگی قابل‌استفاده است. بحثی که بسیار مهم است بحث امنیت و مدیریت کلان داده‌های تولیدشده و تأمین انرژی برای این وسایل هست. در سال ۱۹۹۹ که ایده اینترنت اشیا توسط کوین اشتون مطرح شد، تگ RFID به‌عنوان بستر ایجاد ارتباط در نظر گرفته شده است. درحالی‌که در زمان حاضر شبکه‌های بی‌سیم، شبکه محلی و شبکه های سلولی به‌عنوان بسترهای ارتباطی در نظر گرفته می‌شود. از این رو، در زمان حاضر WIFI ازجمله مهم‌ترین بسترهای ارتباطی در نظر گرفته شده است [1, 2, 3, 4].

در ادامه این مقاله، بخش دوم به بررسی اینترنت اشیاء و قابلیت‌های آن پرداخته شده است. بخش سوم به بررسی کامل چالش‌های اینترنت اشیاء ازجمله کلان داده و امنیت بررسی‌شده است. بخش پنجم راه‌کارهای مقابله با چالش‌های اینترنت اشیاء بررسی‌شده است. درنهایت بخش ششم، به نتیجه‌گیری مقاله اشاره دارد.

۲. اینترنت اشیاء

در سال‌های اخیر درزمینه‌ی ارتباطات راه دور بی‌سیم یک موضوع جدیدی به نام اینترنت اشیاء به وجود آمده است که توسط اشتون در سال ۱۹۹۱ در یک سخنرانی معرفی‌شده است. او جهانی را توصیف کرد که در آن هر چیزی، ازجمله اشیا بی‌جان برای خود هویت دیجیتال داشته باشند و به کامپیوترها اجازه دهند آن‌ها را سازمان‌دهی و مدیریت کنند. اینترنت اشیاء سطح ارتباطات را کاملا افزایش داده، زیرساخت‌های فیزیکی را با زیرساخت‌های فناوری اطلاعات اتصال می‌دهد. همچنین، اجازه می‌دهد تمامی اشیا به اینترنت وصل، هوشمند شده و به تبادل داده بپردازند. درواقع در مفهوم اینترنت اشیاء، بسیاری از اشیایی که در محیط ما قرار دارند به یک شبکه متصل می‌شوند اینترنت اشیاء فکر کردن به‌صورت سنتی را در هم می‌شکند، زیرساخت‌های فیزیکی را با زیرساخت‌های فناوری اطلاعات اتصال می‌دهد و اجازه می‌دهد تمامی اشیا به اینترنت وصل شوند درواقع به سمت هوشمندی حرکت می‌کند و قدرت پردازش را به دست می‌آورد. وقتی همه‌چیز به هم متصل می‌شوند، اشیاء بی‌جان هم صاحب ذهن می‌شود و تجهیزات هم قابلیت تبادل داده و هوشمندی پیدا می‌کنند. این پدیده باعث می‌شود تا تفاوت بین انسان و ماشین محو شود. این نکته قابل‌تأمل است که به درک درستی از شیء در این فناوری برسیم. درواقع در مفهوم اینترنت اشیاء، بسیاری از اشیایی که در محیط ما قرار دارند در یک قالب مشخص به یک شبکه متصل می‌شوند. اینترنت اشیاء، شبکه‌های از اشیاء فیزیکی و مجازی متصل به اینترنت است که در آن اشیا می‌توانند فیزیکی و مجازی باشند اما امکان دستیابی به آن از طریق اینترنت فراهم می‌گردد. اشیاء متصل شده از فناوری‌های تعبیه‌شده درون خود نظیر حسگرها استفاده می‌نمایند تا بتوانند چیزی را حس کرده و احساس خود را مبادله نمایند. این قابلیت، نظام تصمیم‌گیری را در حوزه‌های مختلفی تحت تأثیر خود قرار خواهد داد [1, 2, 4].

پس از اتصال اشیاء به شبکه، امکان ارسال داده و تعامل به کمک تگ‌های شناسایی فرکانس‌های رادیویی و امواج وای فای فراهم می‌گردد و تمامی این اتفاقات به‌صورت بلادرنگ انجام خواهد شد. فرآیند ارسال داده‌ها در فناوری اینترنت اشیاء بدین ترتیب است که به سوژه مورد نظر یک شناسه یکتا و یک پروتکل اینترنتی تعلق می‌گیرد و سپس داده ردوبدل شده و در زمان از قبل تعیین‌شده آن‌ها را ارسال می‌کنند، در مرحله آخر هم امکان تبادل داده بدون دخالت انسان فراهم می‌شود. از اهمیت این فنّاوری این است که تا سال ۲۰۲۰بیش از ۴۰ هزار هگزا بایت داده توسط حسگرهای تعبیه‌شده درون اشیاء فیزیکی متصل به اینترنت تولید می‌گردد. پیش‌بینی‌شده است این حجم اطلاعات بیش از ۹۰٪ داده‌هایی است که تاکنون در دنیا تولیدشده است. در اینترنت اشیا بحث شهر هوشمند و رایانش ابری مطرح می‌شود، شهر هوشمند همان هدف ما از استفاده از اینترنت اشیا است مثل هوشمند کردن سطل زباله در کوچه‌ها و اتصال آن‌ها به سرور مرکزی است تا از نقص‌های

www.SID.ir

Archive of SID

موجود مثل مصرف برق با کمک جایگزین کردن انرژی لازم با نیروی خورشیدی جلوگیری کرده، در صورت بروز خطا از سرور مرکزی برای رفع خطا استفاده کرده و نیاز به مصرف زمان و پذیرش مشکلات احتمالی را از بین می‌برد [1, 2, 4].

از دیدگاه فنی، اینترنت اشیاء حاصل یک فناوری جدید نیست، در حقیقت چندین پیشرفت فنی قابلیت‌هایی را شکل می دهد که به کمک آن بین دنیای مجازی و حقیقی ارتباط برقرار می‌کنند. این قابلیت‌ها بدین شرح‌اند [3, 5, 6]:

ارتباط و همکاری: لوازم و دستگاه‌ها باقابلیت شبکه‌بندی منابع اینترنتی از فناوری‌ها و استانداردهای شبکه‌ای بی‌سیم، ZigBee، بلوتوث، وای فای (جمله این قابلیت‌ها WPANS) و سایر فناوری‌های تحت توسعه‌های جدید، به‌ویژه موارد مربوط به شبکه‌های بی‌سیم حوزه شخصی استفاده کنند. ماژول ZigBee شامل یک رادیو، یک ریزپردازنده و یک پروتکل ساده است و بلوتوث متشکل است از یک طیف جهش فرکانس که اجازه می‌دهد دو دستگاه به‌صورت بی‌سیم به یک‌دیگر متصل شوند و عملکردی راحت و ایمن دارد.

آدرس پذیری: لوازم می‌توانند از طریق سرویس‌های کشف، بررسی و نام‌گذاری تعیین موقعیت گردند و بنابراین با کمک IoT در شبکه اشیاء دور (به‌صورت کنترلی) قابل ادغام شوند و به‌این‌ترتیب قابلیت شناسایی را پیدا می‌کنند. در این راه RFID[۲] بسیار مؤثر است.

حسگری: دستگاه‌ها اطلاعات پیرامونشان را با استفاده از حسگرها جمع‌آوری می‌کنند، آن را ثبت کرده و مستقیم نسبت به آن‌ها واکنش نشان می‌دهند که برای این کار به راهکارهایی مثل وجود سخت‌افزار مناسب نیاز داریم.

پردازش اطلاعات جاسازی‌شده: مشخصه‌های دستگاه‌های هوشمند شامل قابلیت پردازش و قابلیت ذخیره ساز بودن است.

بنابراین باید در طراحی سیستم IoT قابلیت های امنیتی و قابلیت طراحی تکنیکی و قابلیت بهره وری در محیط های گسترده و تجاری را باید لحاظ کرد.

۳. چالش‌های اینترنت اشیاء

در اینترنت اشیا مشکلاتی وجود دارد که ازجمله آن به داده عظیم تولیدشده و مدیریت آن می‌توان اشاره کرد. این بخش به بررسی مشکلات پیشروی اینترنت اشیاء پرداخته است.

۱،۳. تامین انرژی

در ابتدای وجود اینترنت اشیا یکی از مهم ترین چالش ها چالش تامین انرژی برای تعداد زیاد اشیا متصل به شبکه بود. انرژی برق و سایر انرژی های تجدید پذیر با توجه به حجم محدود و اهمیت این منابع گزینه مناسبی نبودند. امروزه با رشد فناوری با فناوری‌هایی مثل انرژی باد و خورشیدی امکان مصرف کمتر از انرژی های تجدید ناپذیر فراهم شده و دستگاه‌هایی با مصرف کمتر تولید شده اند و همین موضوع موجب می‌شود تامین انرژی دیگر نقص بزرگی در نظر گرفته نشود [5, 7, 8]. دستگاه‌های متصل به شبکه اینترنت اشیا باید بتوانند بدون تعویض باتری و نقص‌های سخت‌افزاری به مدت طولانی خدمت‌دهی کنند و همین موضوع موجب شد در تولید باتری و سایر تجهیزات فیزیکی به کیفیت توجه بیشتری شود.

۲،۳. مدیریت داده‌ها

در هر صنعتی مدرن مدیریت داده نقش کلیدی دارد و موجب حفظ عملکرد سیستم می‌شود. اینترنت اشیا یک سیستم گسترده و پویاست و مدیریت خیل داده‌های تولیدشده در آن مهم است. به علت پویا بودن و گستردگی اینترنت اشیا مدیریت آن به یک پایگاه پویا نیاز دارد تا واسطی بین داده‌ها و برنامه‌ها و دیگران باشد. همین ویژگی‌ها باعث می‌شود که پایگاه داده سنتی در اینترنت اشیا منسوخ شود. پس در طراحی مدیریت داده در شبکه اینترنتی از یک پلت فرم مناسب داده برای اینترنت اشیاء، مفاهیم ارتباطات، فرآیندها و ذخیره‌سازی باید به‌درستی تعریف شوند و باید تأمین‌کننده انعطاف‌پذیری، امنیت و حاکمیت، قابلیت‌های مدیریتی، استانداردهای اشیا و مقیاس‌پذیری باشد. چارچوب مدیریت داده‌ها شامل یک‌لایه داده محور و

[2] Radio-frequency identification (RFID)

www.SID.ir

Archive of SID

یک واسط برای اتصال عضوهای شبکه اینترنت اشیا است. لایه داده محور شامل تمام موجودیت‌های مجازی یا واقعی شبکه است که مولد داده هستند. این اطلاعات در مراکز داده نگهداری می‌شوند و امکان عملکرد سیستم به‌صورت بلادرنگ را ایجاد کرده و امکان پردازش درخواست‌ها را ایجاد می‌کند در ضمن این مخازن توسط کاربران قابل‌دسترسی هستند. لایه واسط هم وظیفه تحلیل ریسک و بررسی تقاضای کاربر و سازمان‌ها و زمان آن و اینکه کدام منبع باید استفاده شود را بر عهده دارد [9].

همچنان برای مدیریت با چالش‌های بزرگی روبه‌رو هستیم که شامل چالش‌های اینترنت اشیا است. این چالش‌ها شامل چالش‌هایی مثل وسعت شبکه و تنوع دستگاه‌های متصل به شبکه، هماهنگ کردن و مدیریت دستگاه‌های متصل، تفسیر داده های اجزای مختلف متصل به شبکه، ذخیره و صرفه‌جویی در مصرف انرژی که نه‌تنها در ساختار سخت‌افزاری و سیستمی بلکه در ساختار نرم‌افزار هم یک فاکتور مهم به شمار می‌آید. واکنش و ارتباط اجزا هم یکی از چالش‌هاست زیرا ارتباط بی‌سیم از فاصله چند سانتی‌متری کفایت خواهد نمود اگر شیء در تماس با شیء دیگر باشد و یا کاربر موبایلش را در مقابل آن قرار دهد یعنی حالاتی که چنین فواصل کوتاه مطرح هستند. در فواصل کوتاه انرژی بسیار کمی لازم است و آدرس یابی شیء ساده است اما در فواصل زیاد شرایط پیچیده می‌شود [9].

۳،۳. کلان داده[3]

با گذر زمان و افزایش ورود فناوری به زندگی انسان‌ها و استفاده در کاربردهایی مثل صنعت و داده‌هایی که تولید می‌شوند چالش بزرگی ایجاد شد. از این رو، این حجم عظیم از داده که تولید می‌شوند در کجا ذخیره‌شده و چگونه پردازش شوند. در اینترنت اشیا که یک شبکه عظیم از انواع دستگاه‌ها مثل کامپیوتر و ساعت و یخچال و سایر دستگاه‌ها که هوشمند می‌شوند. بحث مدیریت و پردازش کلان داده‌های با استانداردهایی متفاوت که در حال افزایش هستند مشکل بزرگی محسوب می‌شود. داده‌های بزرگ معمولاً به مجموعه از داده‌ها اطلاق می‌شود که اندازه آن‌ها فراتر از حدی است که با نرم‌افزارهای معمول بتوان آن‌ها را در یک‌زمان برنامه‌ریزی شده اخذ، مدیریت و پردازش کرد و به‌مرور بزرگ‌تر شود. در سال ۲۰۰۱ موسسه گارتنر (گروه متا) سه بعد از چالش‌ها و فرصت‌های پیش رو در حوزه رشد داده‌ها را مطرح کرد که شامل افزایش حجم، سرعت و شتاب و تنوع هستند [10, 11].

افزایش حجم: افزایش در میزان داده

سرعت و شتاب: افزایش سرعت تولید داده‌های ورودی و خروجی

تنوع: افزایش محدوده تنوع و منابع داده‌ها

۴،۳. استاندارد واحد

در اینترنت اشیا اجزای مختلفی همانند وسایل خانه با به‌کارگیری سنسورهایی که در آن‌ها جاگذاری می‌شود، می‌توانند اطلاعات مختلفی تولید کنند که برای مدیریت این وسایل باید همگی به استاندارد واحد پایبند باشند. امروزه باوجود سیستم‌عامل‌های گوناگون و شرکت‌های مختلف که باهم در حال رقابت‌اند مثل مایکروسافت، سامسونگ و ای‌بی‌ام رسیدن به استاندارد واحد سخت به نظر می‌رسد. برای مثال شرکت سامسونگ پلتفرم Artik را عرضه کرده درحالی‌که مایکروسافت در راستای اینترنت اشیا سرویس آژور را عرضه می‌کند و هرکدام سیستم رایانش ابری خاص خود رادارند و نیز آن را برای شرکت خود به‌صورت متن باز عرضه نموده اند [12, 13].

استانداردهای IoT بسیاری برای سهولت بخشیدن به کار سرویس‌دهندگان و توسعه‌دهندگان اپلیکیشن معرفی شده‌است. استانداردهای ارتباطی پایه مانند 6LoWPAN، عموماً مورد استفاده قرار می‌گیرند. شکل ۱ پشته پروتکل IoT را به همراه پروتکل‌های ارتباطی پایه نشان می‌دهد. پروتکل‌های IoT در چهار گروه دسته‌بندی می‌شوند: پروتکل‌های اپلیکیشن، پروتکل های کشف خدمات، پروتکل‌های زیرساخت و سایر پروتکل‌های مؤثر. با این وجود، لازم نیست همه این پروتکل‌ها باهم همراه شوند تا اپلیکیشن خاصی را تحویل دهند. علاوه‌براین، بسته به نوع اپلیکیشن ممکن است به پوشش‌دهی از برخی از

[3] Big Data

www.SID.ir

Archive of SID

استانداردها در آن‌ها نیازی نباشد. پروتکل‌های ارتباطی پایه در IoT، به عنوان استاندارد پروتکل درنظر گرفته می‌شوند؛ این پروتکل‌ها عبارتند از پروتکل صف‌بندی پیشرفته پیام[۴]، انتقال دورسنجی صف پیام[۵]، خدمات کشف داده[۶]، انتقال حالت بازنمودی[۷]، پروتکل مسیریابی[۸] و پروتکل انتقال ابرمتن[۹] [12, 13].

ش	پشته پروتکل اینترنت اشیاء (چهار گروه)	موقعیت پروتکل های ارتباطی پایه در پشته پروتکلی IoT و معماری لایه ای			معماری لایه ای IoT (مدل ۵ لایه)
۱	پروتکل های اپلیکیشن	CoAp	MQTT-SN	AMQP	لایه اپلیکیشن
		DDS	HTTP	REST	
۲	پروتکل های کشف خدمات	mDNS	DNS-SD		لایه شبکه
۳	پروتکل های زیرساخت	RPL			
		6LoWPAN	IPv4	IPv6	لایه تطبیق
		IEEE 802.15.4			لایه پیوند داده
		LTE-A	EPC Global	IEEE802.15.4	لایه فیزیکی
۴	پروتکل های مؤثر	IEEE188.3	IPSec	IEEE1905.1	

شکل ۱: پشته پروتکل IoT به همراه پروتکل‌های پایه ارتباطی

شکل ۲: چالش‌های تحقیقاتی اصلی در اینترنت اشیاء

[4] Advanced Message Queuing Protocol (AMQP)
[5] Message Queue Telemetry Transport (MQTT)
[6] Data Distribution Service (DDS)
[7] Representational State Transfer (REST)
[8] Recognition of Prior Learning (RPL)
[9] Hypertext Transfer Protocol (HTTP)

www.SID.ir

Archive of SID

۵،۳. امنیت

در اینترنت اشیاء، هر دستگاه متصل می‌تواند یک درگاه احتمالی به زیرساخت IoT یا داده‌های شخصی باشد. نگرانی‌های امنیت و حریم خصوصی داده بسیار مهم هستند، اما با ورود پیچیدگی، نقاط ضعف امنیتی و آسیب‌پذیری‌های احتمالی در مواردی مانند قابلیت همکاری، ترکیبات و تصمیم‌گیری‌های خودگردان، خطرات احتمالی مربوط به IoT سطح جدیدی به خود گرفته‌اند. از آن‌جایی که پیچیدگی موجب به‌وجود آمدن آسیب‌پذیری‌های جدید در خدمات می‌شود، خطرات نقص حریم‌خصوصی در IoT افزایش می‌یابد. در اینترنت اشیاء، اکثر اطلاعات موجود مربوط به اطلاعات شخصی ما از قبیل تاریخ تولد، مکان، بودجه و غیره هستند. این یک ویژگی چالش‌برانگیز ابرداده است و حرفه‌های مربوط به امنیت باید تضمین‌کننده درنظرگرفته شدن خطرات احتمالی به مجموعه داده‌ها باشند. پیاده‌سازی اینترنت اشیاء باید مورد تایید قانون، اخلاق، جامعه و سیاست باشد و درآن چالش‌های قانونی، رویکردهای سیستمی، چالش‌های تکنیکی و چالش‌های تجاری درنظر گرفته شود. این بخش برروی طرح پیاده‌سازی تکنیکی معماری امنیتی IoT تمرکز دارد. امنیت در IoT باید از ابتدایی‌ترین مرحله طراحی تا خدمات درحال اجرا پاسخ داده شود. چالش‌های تحقیقاتی اصلی در سناریوی IoT، شامل محرمانگی داده، حریم خصوصی و اعتماد می‌شود که در شکل ۲ مشخص شده است [13, 14].

برای بهتر نشان دادن الزامات امنیتی در IoT، معماری چهار لایه‌ای برای آن درنظر گرفته‌ایم: لایه حسگر، لایه شبکه، لایه خدمات و لایه اپلیکیشن. هر لایه قادر است کنترل‌های امنیتی متناظری مانند کنترل دسترسی، احرازهویت دستگاه، یکپارچگی و محرمانگی داده در انتقال، دردسترس بودن و قابلیت ضد ویروس و حملات فراهم کند. در جدول ۱، مهم‌ترین نگرانی‌های امنیتی در IoT خلاصه شده‌است. الزامات امنیتی بستگی به نوع فناوری حسگر، شبکه و لایه‌ها دارند [14].

جدول ۱: نگرانی‌های امنیتی در اینترنت اشیاء

نگرانی‌های امنیتی	لایه اپلیکیشن	لایه خدمات	لایه شبکه	لایه حسگر
پل ارتباطی وب نا ایمن	√	√	√	
احرازهویت/صدوراجازه ناکافی	√	√	√	√
خدمات شبکه نا امن		√	√	
کمبود رمزنگاری انتقال		√	√	
نگرانی‌های حریم خصوصی		√	√	√
پل ارتباطی ابر غیرایمن	√			
پل ارتباطی موبایل غیرایمن	√		√	√
پیکربندی امنیت ضعیف	√	√	√	
نرم‌افزار/ firmware نا امن	√		√	
امنیت فیزیکی ضعیف			√	√

امنیت شبکه حسگر بی‌سیم یکی از عوامل مهم امنتی در IoT است. ازاین‌رو، شبکه‌های بی‌سیم معمولاً از مدل ۷ لایه اتصال سیستم‌های باز یا همان مدل OSI، به‌شکل بالا به پائین پیروی می‌کنند. تهدیدات امنیتی مربوط به این لایه‌های پروتکل، عموماً در یک سطح لایه و با احتساب یکپارچگی، اعتبار، دردسترس بودن و محرمانگی درنظر گرفته می‌شوند که شکل ۳ این را به خوبی نشان داده است [13, 14].

www.SID.ir

Archive of SID

تقاضای امنیتی	اهداف مشخص
اعتبار	برای متمایز کردن کاربران مجاز از کاربران غیرمجاز
محرمانگی	برای محدود کردن دسترسی به داده های محرمانه تنها برای کاربران مجاز
یکپارچگی	جهت تضمین دقت و صحت اطلاعات انتقال یافته
دردسترس بودن	جهت حصول اطمینان از اینکه کاربران مجاز بتوانند در هر زمانی به خدمات دست یابند

شکل ۳: متدولوژی‌های امنیتی بی‌سیم

۴. راه‌کارهایی بر حل چالش‌ها

فناوری اینترنت اشیا همواره در حوزه IT مطرح بوده و برای بهره‌وری از آن نیاز به حل چالش‌هایش داریم. حل چالش‌ها به این دلیل است که این فناوری گسترش یافته و به طور وسیع‌تری مورد استفاده قرار گیرد. امنیت از مهم‌ترین مشکلات مطرح شده در اینترنت اشیاء است. ازاین‌رو، این بخش به بررسی راهکارهایی برای بهبود امنیت اینترنت اشیاء پرداخته است.

۱،۴. سیستم immunology

این سیستم یکی از روش‌های مطرح‌شده برای حل مشکل امنیت است. این سیستم دارای ۵ فیلتر است و بیشتر فیلترها روی فیلتر کشف تهدید امنیت اجرا می‌شوند. ازاین‌رو، کشف ویروس‌ها به مکان‌هایی که امنیت آن‌ها با چالش روبرو شده است از اصلی‌ترین کارهای این بخش است. این سیستم تلاش دارد با عبور سیستم از این ۵ مرحله، امنیتی پویا ایجاد کند. شکل۴، فیلترهای امنیتی این سیستم راه نشان داده است [15].

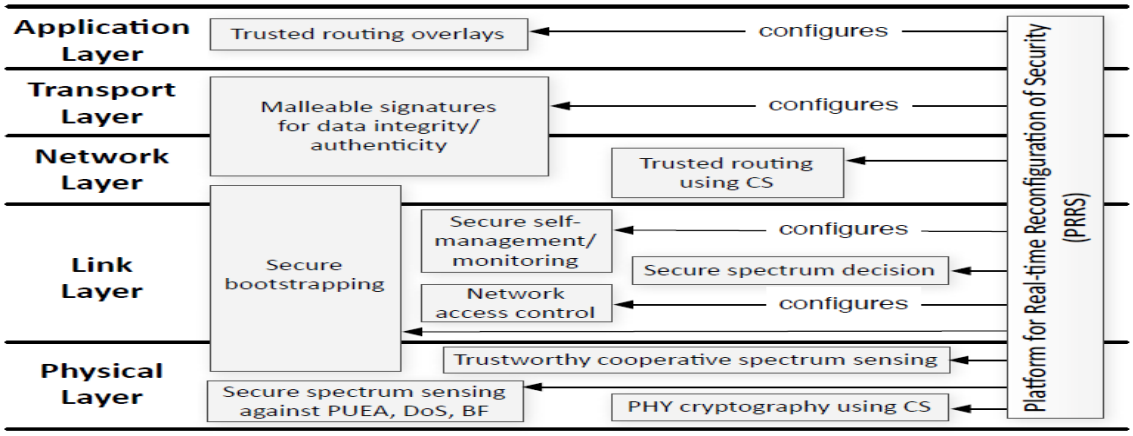
شکل ۴: معرفی فیلترهای روش مبتنی بر immunology

۲،٤. سیستم RERUMP

این سیستم هم از روش‌های حل بحران امنیت است. در این روش که توسط اتحادیه اروپا مطرح‌شده و مدل هفت لایه OSI را هم پوشش می‌دهد یک سیستم چند لایه ای را به صورت قسمت‌های مجزا قسمت بندی کرده و قسمت‌های مختلف لایه‌ها را بررسی می‌کند. این سیستم بیشتر توجه خود را به لایه‌های پایین معطوف می‌کند. شکل ۵ ساختار و روند این سیستم را نشان داده است [1, 5].

www.SID.ir

Archive of SID



شکل ۵: پیاده سازی روش RERUMP روی مدل OSI [1]

۳،۴. راهکارهای چالش‌های پیاده‌سازی امنیت IoT

برخی از تولیدکنندگان دستگاه‌های IoT که در این تجارت تازه‌کار هستند، دارای مکبودهایی در تخصص امنیت بوده و نمی توانند از پس هزینه‌های استخدام متخصصان امنیت برآیند. به‌همین‌خاطر، به مکانیزم‌های امنیتی ابتدایی در عناصر سخت افزاری و نرم‌افزاری خود اکتفا می‌کنند. درنتیجه، دستگاه‌های تولیدشده آن‌ها دارای آسیب‌پذیریهای امنیتی بسیار زیادی است. بسیاری از شرکت‌های تولیدکننده دستگاه‌های IoT تلاش کم و ناچیزی در عرصه تحقیقات و توسعه‌های ارتقاء امنیتی محصولات خود دارند و هدف آن‌ها تنها ارزان بودن محصول است [16, 17].

مجازاً تمامی دستگاه‌هایی که قابلیت اتصال به اینترنت را دارند، دارای سیستم‌عامل‌های جاسازی‌شده‌ای در نرم‌افزار دائمی خود هستند. با این وجود، با این دید که این دستگاه‌ها کوچک و ارزان طراحی شده‌اند، سیستم‌عامل‌هایشان بدون اهداف امنیتی طراحی شده‌است. درنتیجه، اکثر آن‌ها دارای آسیب‌پذیری هستند [16, 17].

درطبیعت همگن توسعه IoT (مانند شبکه‌های حسگر بیسیم؛ که در آن تمامی گره‌ها به استثنای گره چاهک همگی یکسان هستند) خطرات امنیتی زیادی وجود دارد. زیرا اگر مهاجم موفق به شناسایی آسیب‌پذیری‌های یک گره شود، می‌تواند با استفاده از آن سایر گره‌ها و حتی گره‌هایی که طراحی یکسانی دارند و از یک پروتکل استفاده می‌کنند را درمعرض خطر قرار دهد. از آن‌جایی که تعداد دستگاه‌های متصل افزایش می‌یابد، تکنیک‌های به‌کارگیری نقاط ورود یا آسیب‌پذیری‌ها برای حمله نیز افزایش می‌یابد. به‌دلیل وجود ابزارها و حقه‌هایی که به‌دلیل طراحی ساده برخی از دستگاه‌ها پدید آمده‌است، دیگر نیاز نیست که یک مهاجم برای هک کردن دستگاه‌ها مهارت بالایی داشته باشد. مجرمان سایبری قادرند که دستگاه‌هایی که دارای طراحی ضعیف هستند را مجدداً برنامه‌نویسی کرده و از آن‌ها برای دزدیدن اطلاعات حساس استفاده کنند [16, 17].

تعداد بسیار زیادی از دستگاه‌های IoT که در چارچوب‌های سختی توسعه یافته‌اند ممکن است سال‌ها بدون مراقبت در مکانی ساکن باشند و باتوجه به طبیعت آن چارچوب ممکن است پیکربندی یا ارتقاء آن‌ها کاری دشوار باشد. برای برخی اپلیکیشن‌ها که شامل تعداد بسیار زیادی از دستگاه‌ها هستند، این دستگاه‌ها بدون تدارکات ارتقاء و به‌روزرسانی طراحی می‌شوند؛ این امر می‌تواند به‌دلیل به‌وجود آمدن پیچیدگی‌های اساسی به‌سبب زیاد بودن تعداد دستگاه‌ها باشد. از طرف دیگر، اشیاء غیرقابل ارتقاء دیگری نیز وجود دارد که ممکن است هر چندسال یک‌بار جایگزین شوند که دارای چرخه عمرطولانی هستند؛ مانند یخچال‌ها و ماشین‌های هوشمند. بعضی از این اشیاء ممکن است حتی بیشتر از خود شرکت‌ها عمر کنند و درنتیجه دیگر پوششی ازطرف شرکت وجود نخواهدداشت. واضح است که مکانیزم‌های امنیتی این دستگاه‌ها در سناریوی ذکرشده منقضی شوند و درنتیجه نگرانی‌های امنیتی افزایش یابد [16, 17].

دربعضی از اپلیکیشن‌ها ممکن است که توسعه دستگاه‌ها در مکان‌هایی صورت گیرد که فراهم کردن امنیت فیزیکی در آن‌جا کاری دشوار باشد. در این‌گونه موارد، موجودیت‌های مخرب به‌صورت فیزیکی آن‌ها را دراختیار می‌گیرند تا بتوانند مهندسی معکوس را در آن‌ها اعمال کرده و به اطلاعات حساس آن دست‌یابند [16, 17].

www.SID.ir

Archive of SID

اینترنت اشیاء طراحی شده‌است تا به کمک اینترنت، اتصال بدون درزی (یک‌پارچه‌ای) میان دستگاه‌های متنوع در سیستم‌ها و زیرسیستم‌های مختلف فراهم کند. به‌همین ترتیب یک ماشین لباس‌شوئی موردحمله قرارگرفته می‌تواند جهت ارسال هرزنامه های خطرناک (ازطریق اتصال Wi-Fi) در سراسر جهان مورد استفاده قرار گیرد. جدول ۲ نگاهی به عوامل تهدید آمیز اینترنت اشیاء بر اساس کلاس‌بندی مختلف را بررسی کرده است [16, 17].

جدول ۲: طبقه‌بندی عوامل تهدیدآمیز اینترنت اشیاء

عامل تهدیدآمیز	کلاس	مثال‌های معمول
ویژه بدون هدف	نرم‌افزار	ویروس‌های کامپیوتری، کرم‌ها، تروجان‌ها، بمب‌های منطقی
کارمندان	داخلی	کارمندان ناراضی، پیمان‌کاران، گاردهای امنیتی
جرایم و مجرمان سازمان‌دهی شده	خارجی	مجرمانی که اطلاعات آسیب‌پذیر را هدف قرار می‌دهند؛ مثل شماره کارت اعتباری و حساب‌های بانکی
شرکت‌ها	خارجی	شرکت‌ها، آژانس‌های دولتی، شرکا، رقبا
انسان	غیرعمد	تصادفات، بی‌دقتی
انسان	عمدی	دخلی، خارجی
بلایای طبیعی	فاکتورهای غیرانسانی	سیل، آتش‌سوزی، رعدوبرق، زلزله، شهاب

۴،۴. استفاده از Cloud IoT

در اینترنت اشیا همان‌طور که گفته شد یکی از چالش‌ها بحث داده‌های عظیم و مشکل ذخیره‌سازی آن بود و برای حل این مشکل بحث استفاده از رایانش ابری در اینترنت اشیا مطرح شد که به آن Cloud IoT می‌گویند. رایانش ابری مدلی است که شامل مجموعه‌ای از منابع رایانشی(مثل سرورها و فضای ذخیره سازی و سرویس ها) است و هدف آن دسترسی آسان و بدون زحمت به این منابع است و شامل مدل‌های عمومی(دسترسی عموم مردم به آن و وجود یک سازمان مالک و پشتیبان)، خصوصی(در انحصار یک شرکت یا سازمان خاص)، ابرگروهی(استفاده چند سازمان به سیستم و یک سازمان پشتیبان) و ابر آمیخته می‌باشد. در این طرح هدف ما افزایش سطح کیفیت خدمت‌دهی به مشتریان است و برای رسیدن به این مهم باید بین عرضه کننده خدمات و مشتریان یک سری توافقات در مورد سطح خدماتی مورد نیاز و دیگر موارد انجام شده باشدو یک مالک و پشتیبان وجود داشته باشد تا سیستم رایانش ابری را پشتیبانی کند. البته برای جلوگیری از مشکلات احتمالی و خدمت‌دهی مناسب ضروری است که بیش از یک پشتیبان داشته باشد. این روش بسیار مناسب است و هنوز در حال تکمیل است [18].

۵،۴. زیرساخت ارتباطی

با پیاده‌سازی اینترنت اشیا و تبادل داده در آن به زیرساخت ارتباطی قوی نیازمندیم. دلیل اهمیت وجود زیرساخت ارتباطی قوی با پهنای باند بالا، حجم بالای دستگاه‌های متصل و انبوه داده‌های اطلاعاتی تولید شده که باید مبادله شوند می باشد تا بتوان در کوتاه‌ترین زمان ممکن بیشترین داده را منتقل کرد. در بحث شبکه که یک زیرساخت محسوب می‌شود انتخاب نوع شبکه مورد استفاده(بی‌سیم، سلولی و محلی) با توجه به سطح خدمات مورد نیاز در اینترنت اشیا هم اهمیت بسیاری دارد [19].

www.SID.ir

Archive of SID

۵. نتیجه‌گیری

خدمت‌گذاران فناوری اطلاعات برای توسعه کار و اقتصاد شرکت‌های خود سعی در بهبود فناوری اینترنت اشیاء را دارند. به همین دلیل اینترنت اشیاء را می‌توان انقلاب صنعتی قرن بیست و یک در نظر گرفت. اینترنت اشیا دارای مزایا و کاربردهای زیادی است. ازاین‌رو، می‌تواند موجب افزایش توانایی مدیریت انسان بر اشیا هوشمند شده و با به‌کارگیری از آن در صنعت موجب رشد روزافزون و سودآوری آن شود. با این حال، اینترنت اشیاء با چالش‌های عظیمی روبه‌رو است. از این رو، با وجود رشد اینترنت اشیاء، محققان فناوری اطلاعات باید به دنبال راهکارهایی جهت بهبود چالش‌های IoT باشند. این چالش‌ها شامل داده‌های عظیم تولیدشده، مدیریت اشیاء، نبود استاندارد جهانی، ارتباطات اشیاء و امنیت هستند. این مقاله باهدف بررسی مزایا و چالش‌های پیشروی اینترنت اشیا عمل کرده است. همچنین، با ارائه راه‌حل‌هایی به مقابله با مشکلات و تهدیدات اینترنت اشیاء بررسی کرده است. در آینده می‌توان با تحقیق بر روی مکانیزم‌های امنیتی همانند حریم خصوصی و محرمانگی داده‌ها و استانداردهای اینترنت اشیاء به بهبود و توسعه نگرانی‌های امنیتی و کلان داده دست یافت.

مراجع

[1] Kopetz, H. (2011). Internet of things. In *Real-time systems* (pp. 307-323). Springer US.

[2] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805.

[3] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), 1645-1660.

[4] Weber, R. H., & Weber, R. (2010). *Internet of things* (Vol. 12). New York, NY, USA:: Springer.

[5] Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497-1516.

[6] Yan, L., Zhang, Y., Yang, L. T., & Ning, H. (Eds.). (2008). The Internet of things: from RFID to the next-generation pervasive networked systems. CRC Press.

[7] Uckelmann, D., Harrison, M., & Michahelles, F. (2011). An architectural approach towards the future internet of things. In *Architecting the internet of things* (pp. 1-24). Springer Berlin Heidelberg.

[8] Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, *58*(1), 49-69.

[9] Padiya, T., Bhise, M., & Rajkotiya, P. (2015, May). Data Management for Internet of Things. In *Region 10 Symposium (TENSYMP), 2015 IEEE* (pp. 62-65). IEEE.

[10] O'Leary, D. E. (2013). BIG DATA', THE 'INTERNET OF THINGS'AND THE 'INTERNET OF SIGNS. *Intelligent Systems in Accounting, Finance and Management*, *20*(1), 53-65.

[11] Bessis, N. (2014). *Big data and internet of things: a roadmap for smart environments* (Vol. 546). C. Dobre (Ed.). Springer International Publishing.

[12] Dabbagh, M., & Rayes, A. (2017). Internet of Things Security and Privacy. In *Internet of Things From Hype to Reality* (pp. 195-223). Springer International Publishing.

[13] Mainetti, L., Patrono, L., & Vilei, A. (2011, September). Evolution of wireless sensor networks towards the internet of things: A survey. In *Software, Telecommunications and Computer Networks (SoftCOM), 2011 19th International Conference on* (pp. 1-6). IEEE.

[14] Li, F., & Xiong, P. (2013). Practical secure communication for integrating wireless sensor networks into the internet of things. *IEEE Sensors Journal*, *13*(10), 3677-3684.

[15] Liu, C., Zhang, Y., Zeng, J., Peng, L., & Chen, R. (2012, May). Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology. In *Natural Computation (ICNC), 2012 Eighth International Conference on* (pp. 874-878). IEEE.

[16] Robles, R. J., Kim, T. H., Cook, D., & Das, S. (2010). A review on security in smart home development. *International Journal of Advanced Science and Technology*, *15*.

[17] Han, D. M., & Lim, J. H. (2010). Smart home energy management system using IEEE 802.15. 4 and zigbee. *IEEE Transactions on Consumer Electronics*, *56*(3).

[18] Sehgal, A., Perelman, V., Kuryla, S., & Schonwalder, J. (2012). Management of resource constrained devices in the internet of things. *IEEE Communications Magazine*, *50*(12).

[19] Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, *54*, 1-31.

www.SID.ir

Archive of SID

A Review of Challenges and Solutions to Preventing IOT Challenges

Seyed Milad Mirmohammadian
Department of Computer, Faculty of Engenniring, University of Basir, Qazvin, Iran, E-mail: mir.mohammadian@basir-abyek.ac.ir

Sasan Berehlia
Department of Computer, Faculty of Engenniring, University of Basir, Qazvin, Iran, E-mail: berehlia@basir-abyek.ac.ir

Ramzan Babamahmoudi
Department of Computer, Faculty of Engenniring, University of Basir, Qazvin, Iran, E-mail: babamahmoudi@basir-abyek.ac.ir

Zahra Akhondi
Department of Computer, Faculty of Engenniring, University of Basir, Qazvin, Iran, E-mail: z.akhondi3@gmail.com

Abstract. In the modern world of information technology, the IOT is of particular importance. This technology has many benefits such as reducing costs and saving time and objects Intelligence. It can also be used in various fields such as medicine and farming. However, the disadvantages of this technology cannot be ignored. The biggest disadvantages and challenges of this technology are security and big data problems. In IOT, any connected device can be a potential gateway to the IOT infrastructure or personal data. Security and privacy concerns are critical, but with the introduction of the issue of complexity, the potential risks of the Internet of objects, security vulnerabilities and potential vulnerabilities have taken on a new form of possible risks. These risks appear in many cases such as interoperability, combinations and autonomous decisions. This paper describes IOT, its advantages and challenges and introduces some solutions to these challenges. Also, according to the key challenges like the security and big data issues, in this paper, a general solution is proposed for these issues.

Keywords: Internet of Things, Big Data, Security, Unified Standard.

www.SID.ir