ISSN: 2475-3673
http://www.Racj.ir

مجله علمی پژوهش در علوم رایانه (سال پنجم)
شماره ۱۸ / تابستان ۱۳۹۹ / ص ۳۸- ۱۵

بررسی و مقایسه امنیت، اهداف، راه‌کارهای امنیتی و ارائه چهارچوب امنیتی در اینترنت اشیاء

ساسان برهلیا[۱]، محمدباقر حق پرست[۲]، بردیا علاالدینی[۳]، امیرحسین جورسرایی[۳]

[۱] کارشناسی ارشد نرم‌افزار کامپیوتر، مدرس دانشگاه شهید شمسی‌پور.

[۲] فارغ التحصیل کارشناسی ارشد نرم‌افزار، دانشگاه آزاد اسلامی قزوین.

[۳] دانشجوی کارشناسی نرم‌افزار، دانشگاه شهید شمسی‌پور.

نام نویسنده مسئول:
ساسان برهلیا

تاریخ دریافت: ۱۳۹۹/۳/۱۲
تاریخ پذیرش: ۱۳۹۹/۵/۲۷

چکیده

اینترنت اشیاء یک توانمندسازی مبتنی بر هوش را به ویژگی‌های جهان مدرن امروزی مانند شبکه‌ها، سازمان‌ها افزوده است. درواقع یک توسعه ساده از اینترنت یا شبکه ارتباطی نیست بلکه ویژگی‌های هردو این‌ها را دارد. اینترنت اشیاء با استفاده از حسگرهای فعال‌کننده و فناوری ارتباطات داده‌ها که در اشیاء فیزیکی جاسازی می‌شود که امکان ردیابی، هماهنگی یا کنترل اشیاء را از راه شبکه یا اینترنت فراهم می‌کند. برای به تحقق رسیدن اینترنت اشیاء در جایگاه جهانی، چالش‌های آن را باید برطرف نمود. امنیت، استانداردسازی و ارتباطات اشیاء از مهم‌ترین چالش‌های این قول دنیای فناوری اطلاعات است. در این مقاله به مفهوم اینترنت اشیاء، معماری چندلایه، چالش‌ها، تهدیدها، ارائه راه‌حل برای حملات امنیتی در لایه حفره‌های امنیتی، محدودیت‌های پیش روی این تکنولوژی و ارائه یک چهارچوب امنیتی پرداخته‌شده است. ازاین‌رو، این مقاله با توجه به مقوله امنیت اینترنت اشیاء به بررسی و ارزیابی تهدیدات و آسیب‌پذیری‌های اینترنت اشیاء، نگرانی‌های امنیتی لایه‌ها، تکنیک‌های امنیتی، چهارچوب امنیتی و بررسی مکانیزم‌های امنیتی پرداخته است. نتایج در طرح پیشنهادی چهارچوب امنیتی، اشاره به توسعه رابطه مطمئن در امنیت معماری و ارتباطات اشیاء دارد. بااین‌حال، توسعه مکانیزم‌های حریم خصوصی، محرمانگی و یکپارچگی داده‌ها می‌تواند باعث بهبود امنیت اینترنت اشیاء شود.

واژگان کلیدی: اینترنت اشیاء، امنیت، مکانیزم امنیتی، امنیت اینترنت اشیاء.

ISSN: 2475-3673
http://www.Racj.ir

مقدمه

اینترنت اشیاء[1] مفهومی چالش برانگیز و جذاب در دنیای فناوری اطلاعات تلقی می‌شود. فناوری اینترنت اشیاء، برای اولین بار توسط کوین اشتون در سال ۱۹۹۹ ارائه شده است. وی جهانی را توصیف کرد که در آن هر چیزی، از جمله اشیاء بی‌جان، برای خود هویت دیجیتال داشته باشند و به کامپیوترها با توجه به دنیای اینترنت اجازه دهند آن‌ها را سازماندهی و مدیریت کنند. اینترنت، در حال حاضر تمامی مردم جهان را به هم متصل می‌کند. با این حال، با مفهوم اینترنت اشیاء تمام اشیاء به هم متصل می‌شوند. ازاین‌رو، اینترنت اشیاء یک انقلاب تکنولوژیکی از حسگرهای بی‌سیم تا تکنولوژی نانو، یک معماری بر اساس ابزارهای ارتباطی داده‌ها است [۱، ۲].

فناوری اینترنت اشیاء با هدف اینکه همه انسان‌ها و اشیاء بی‌جان بتوانند در هر زمان و هر مکانی، با هر شیء و هر شخص دیگری با استفاده از هر شبکه و سرویسی، ارتباط برقرار کنند. مقوله‌ای که در این میان نگرانی را به همراه دارد، مباحث امنیتی اینترنت اشیاء است. با توجه به چالش‌های پیشرو اینترنت اشیاء همانند ارتباطات، استانداردها و معماری‌ها، امنیت به جدی‌ترین چالش برای خدمت‌گذاران فناوری اطلاعات بدل شده است. به‌عنوان یکی از عناصر حیاتی در طراحی هر شبکه‌ای، امنیت از بزرگترین موانع در توسعه تکامل اینترنت اشیاء به‌حساب می‌آید [۳].

امنیت یک مفهوم کلیدی و قابل اتکا در جهان هستی به شمار می‌آید. از آغاز زندگی انسان تا به‌حال، امنیت بر اساس حفظ بقا و پایداری در مقابل حملات صورت گرفته است. از این رو، مفهوم امنیت در حوزه فناوری اطلاعات یک نیاز اساسی است که برای رسیدین به این تحقق مکانیزم‌های پیاده‌سازی شده و الگوریتم‌های مختلفی وجود دارد. در مقابل امنیت، ارزیابی تهدیدات امنیتی با توجه به هزینه، زمان، مشکلات و شرایط آن مورد بررسی قرار گرفته است. تضمین ایمن‌سازی حوزه فناوری اطلاعات، در جهت‌های مختلف دارای نقص و یافته‌های جدید است. به همین دلیل، امنیت باید به عنوان یک هنر در راستای علم مورد بررسی قرار بگیرد. امنیت از سه اصل پیشگیری، تشخیص و واکنش در راستای رسیدن به اهداف امنیت اطلاعات تشکیل شده است. این اهداف درمجموع برای رسیدن به هدفی واحد و مشخص یعنی حفاظت اطلاعات و سیستم‌های اطلاعاتی از فعالیت‌های غیرمجاز صورت گرفته است [۴].

این مقاله، به بررسی امنیت اینترنت اشیاء با هدف توسعه اهداف امنیتی در تمامی ابعاد پرداخته است. ابتدا چهارچوب امنیتی اینترنت اشیاء باید مورد توجه قرار بگیرید. در ادامه، نیازهای امنیتی از دیدگاه‌های مختلف همانند استاندارد ITU-T بررسی گسترده‌ای صورت می‌گیرد. همچنین، بررسی و مقایسه کلی در حوزه امنیت و ارائه راهکارهایی جهت بهبود امنیت اینترنت اشیاء صورت می‌گیرد.

در ادامه مقاله، بخش دوم به بررسی کارهای گذشته از قبیل مفهوم اینترنت اشیاء، معماری ۴ لایه و چالش‌های پیشرو این فناوری پرداخته است. در بخش سوم، به بررسی امنیت و استاندارد امنیتی پرداخته‌شده است. بخش چهارم به ارزیابی و مقایسه-ای کامل بر روی تمام ابعاد امنیتی اینترنت اشیاء صورت گرفته است. همچنین، راهکارهایی جهت بهبود امنیت اینترنت اشیاء پیشنهادشده است. همچنین، علاوه بر این یک چهارچوب امنیتی IoT ارائه شده است. در نهایت بخش پنجم، نتیجه‌گیری این پژوهش پیش‌رو را بررسی کرده است.

کارهای مرتبط

هدف اصلی این پژوهش بررسی امنیت در اینترنت اشیاء است. از این رو، ابتدا باید مفهوم اینترنت اشیاء به صورت کامل ارائه شود. این بخش، در ابتدا به بررسی کامل مفهوم اینترنت اشیاء می‌پردازد. در ادامه، به بررسی معماری و چالش‌های پیشرو این فناوری اشاره می‌کند. در نهایت، مفهوم اولیه امنیت بررسی خواهد شد.

[1] Internet of Things

ISSN: 2475-3673
http://www.Racj.ir

اینترنت اشیاء

در سال‌های گذشته گروهی از محققان و سازمان‌ها به شفاف‌سازی واژه اینترنت اشیاء پرداخته‌اند. اینترنت اشیاء جهانی است که اشیاء فیزیکی با اطلاعات شبکه یکپارچه می‌شوند. از این رو، می‌توانند به شرکت‌کنندگان فعال در حوزه فرآیندهای کسب‌وکار تبدیل شوند. همچنین، اشیاء از حالت فیزیکی به حالت مجازی تبدیل می‌شوند که نشان‌دهنده یک هویت اصلی در اتصال به اینترنت است. به همین دلیل، IEEE[۲] یک تعریفی برای اینترنت اشیاء ارائه داده است اما هنوز هیچ توافق مشترکی برای تعریف اینترنت اشیاء صورت نگرفته است [۱، ۲، ۳].

با گسترده شدن استفاده مردم از اینترنت و الزام خودکارسازی و هوشمندسازی محیط اطراف، پدیده نوینی به نام اینترنت اشیاء شکل گرفته است. فرض کنید اگر رایانه‌هایی وجود داشت که همه چیز را درباره همه چیز می‌دانست و بدون هیچ کمکی داده‌هایی را که خود جمع‌آوری کرده بود به کار می‌برد، در آن صورت همه چیز قابل ردیابی و اندازه‌گیری بود و بدین صورت تا حد زیادی از اتلاف وقت، انرژی و هزینه جلوگیری می‌شد. همچنین اگر چیزی برای تعویض، تعمیر یا راه‌اندازی لازم بود به راحتی شناسایی می‌شد و اشیاء، به تنهایی قادر به اجرای وظایف خود بودند. وقتی صحبت از اتصال به میان می‌آید، بیشتر رایانه، تبلت و گوشی هوشمند مورد توجه قرار می‌گیرند، اما اینترنت اشیاء جهانی را توصیف می‌کند که در آن همه چیز به صورت هوشمند به یک‌دیگر متصل می‌شوند و باهم ارتباط برقرار می‌کنند، وبه یک سیستم اطلاعاتی بزرگ تبدیل می‌شوند [۱، ۲، ۳].

ازجمله پیامدهای اینترنت اشیاء افزایش امنیت، سلامت، ارائه خدمات و بهره‌وری بالا برای سازمان‌های بشری است. از سوی دیگر، چالش‌هایی در محیط محرمانگی شخصی، امنیت سایبری، به وجود آمدن شناخت دیجیتالی و ساختار ناهمگون داده‌ها و انکار سرویس را در پی دارد. طبق گزارش‌های مرکز تحقیقاتی پو در می سال ۲۰۱۴ اینترنت اشیاء تا سال ۲۰۲۵ رشد فزاینده‌ای خواهد داشت و پیش‌بینی می‌شود تا سال ۲۰۲۰ به ۳۰ میلیارد دستگاه که حاوی این تکنولوژی باشند، می‌رسد. کار-برد اینترنت اشیاء برای شرکت‌ها، فروشگاه‌های خرده فروشی دربخش انرژی و قدرت به‌عنوان راه‌کارهای اصلی محسوب می‌شود. [۱، ۲، ۳].

سه فاز اصلی برای به ثمر رسیدن مرحله نخست اینترنت اشیاء وجود دارد. در فاز نخست اشیاء برای ما و یک‌دیگر قابل‌شناسایی می‌شوند و به‌تدریج آدرس خاص در شبکه به خود اختصاص می‌دهند. در این فاز هر شئ اطلاعات خاصی را در خود نگهداری می‌کند. از طرفی، این افراد هستند که باید با استفاده از ابزارهایی همانند گوشی‌های هوشمند خود این اطلاعات را تهیه کنند. در فاز دوم هر وسیله می‌تواند اطلاعات را در موعد تعیین‌شده برای کاربر ارسال کند. از همین رو، پس از ارتباط میان اشیاء و انسان نوبت به ارتباط اشیاء با یکدیگر است. در فاز سوم اشیاء بدون دخالت انسان با یکدیگر ارتباط برقرار می‌کنند. با تکمیل این سه فاز مرحله نخست تکامل اینترنت اشیاء به اتمام می‌رسد [۳، ۵].

پلتفورم اینترنت اشیاء یکی از مفاهیم کلیدی در IoT به‌شمار می‌آید. شناسایی خودکار رادیویی[۳]، فناوری‌های ارتباطات بی‌سیم، شبکه‌های حسگر و شبکه تجهیزات تعبیه‌شده، شبکه اصلی اینترنت اشیاء را تشکیل می‌دهد. براساس پیشرفت‌های سریع در ارتباطات، بسیاری از شبکه‌های حسگرهای بی‌سیم[۴] و RFID به‌وسیله مکانیزم‌های IoT می‌توانند با یکدیگر در هر مکان و زمان، به هر روشی یکپارچه شوند [۵، ۶].

عناصر اصلی تشکیل دهنده اینترنت اشیاء شامل اشیاء، دستگاه، گذرگاه‌ها، حسگرها و برنامه‌های کاربردی (اپلیکیشن‌ها) هستند. شکل ۲، انواع ارتباط در دستگاه‌های اینترنت اشیاء با توجه به عناصر تشکیل دهنده در IoT را نشان می‌دهد [۱، ۳].

اشیاء: با توجه به مفهوم این فناوری، یک شئ می‌تواند شئ‌ای از دنیای فیزیکی (اشیاء فیزیکی) یا دنیای اطلاعات (اشیاء مجازی) باشد. ازاین‌رو، اشیاء این توانایی را دارد که در یک شبکه ارتباطی، یکپارچه شده و شناسایی شود.

دستگاه: وسیله‌ای که دارای توانایی‌های اجباری ارتباطی و توانایی‌های اختیاری حس کردن، تحرک، گرفتن داده، ذخیره داده و عملیات بر روی داده است. دستگاه انواع متفاوت اطلاعات را جمع‌آوری کرده و آن‌را در اختیار شبکه‌های اطلاعاتی و ارتباطی می‌گذارد تا پردازش‌های دیگر انجام شود.

---

[2] The Institute of Electrical and Electronics Engineers
[3] Radio-frequency identification (RFID)
[4] Wireless sensor networks (WSN)

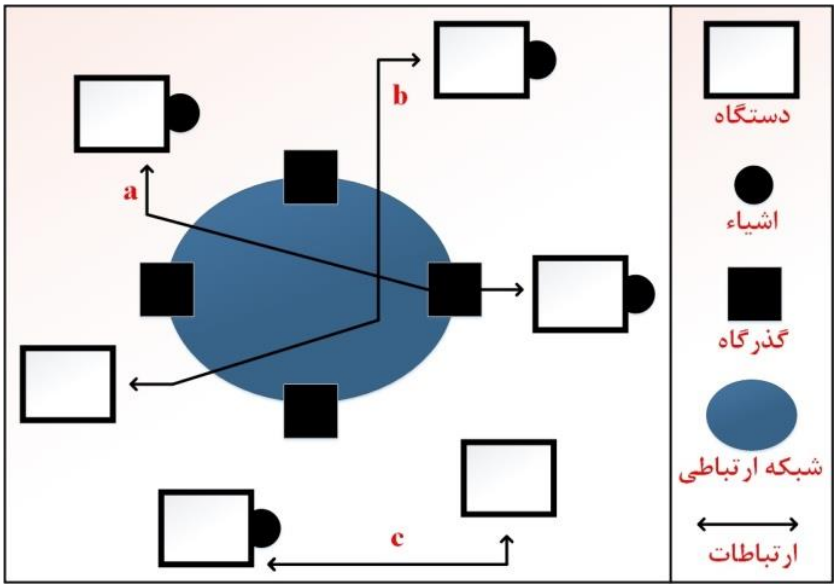
ISSN: 2475-3673
http://www.Racj.ir

گذرگاه‌ها: دستگاه‌هایی که میانجی یا حد واسط ارتباط‌های بی‌سیم هستند و استفاده اشیاء خاص را از منابع به حداقل می‌رسانند.

گذرگاه‌ها: به کاربران، امکان مدیریت منابع مورد استفاده را می‌دهند. همچنین، ارتباط میان دروازه‌ها و اشیاء از طریق معماری‌های زیادی قابل اعمال است.

حسگرها: علاوه بر شناسایی دستگاه‌های دیگر، به دستگاه‌هایی جهت دریافت وضعیت فیزیکی و شرایط محیطی پیرامون نیز نیاز است. این دستگاه‌ها حسگرها هستند که می‌توانند شرایط و وضعیت را درک کرده و داده‌ها را جمع‌آوری کنند. این داده ها می‌توانند از جنس دما، رطوبت، موقعیت مکانی، سرعت باد، لرزش، درجه PH و یا مقدار غبار موجود در هوا باشند.

برنامه‌های کاربردی IoT: شامل انواع مختلفی از اپلیکیشن‌ها هستند. مهمترین برنامه کاربردی IoT شامل سیستم انتقال هوشمند، شبکه‌های هوشمند مرتبط با سلامت و خانه‌های هوشمند هستند. این اپلیکیشن‌ها هم می‌توانند بر پایه پلتفرم‌های اپلیکیشن‌های اختصاصی باشند و هم می‌توانند بر روی پلتفرم‌های حاوی اپلیکیشن خدمات معمول و رایجی بسازند که قابلیت-های ممکن‌سازی عمومی همانند احرازهویت، مدیریت دستگاه، شارژ کردن و حسابداری را فراهم می‌کنند.



شکل ۲: انواع ارتباط در دستگاه‌های اینترنت اشیاء

معماری اینترنت اشیاء

برای نشان دادن ساختار اینترنت اشیاء و بخش‌های مختلف آن به‌صورت مجزا از معماری اینترنت اشیاء استفاده می‌شود. برخلاف اینترنت که غیرقابل‌کنترل است، IoT نیاز به مدیریت دارد. به همین دلیل معماری اینترنت اشیاء با معماری‌های شبکه-های کامپیوتری مثل معماری ۷ لایه OSI[5] متفاوت است. با وجود تعاریف مبهم از این فناوری، معماری آن به‌صورت عمومی پذیرفته‌شده است. معماری عمومی اینترنت اشیاء یک ساختار ۴ لایه است که شامل لایه ادراک، لایه شبکه، لایه میان‌افزار و لایه کاربرد است. شکل ۳، معماری چهار لایه اینترنت اشیاء را نشان می‌دهد [۵، ۷، ۸].

لایه ادراک: لایه ادراک در اینترنت اشیا مشابه لایه فیزیکی OSI است که از حسگرهای مختلف (برای مثال RFID، زیگ‌بی[6]، کیوآر کد و مادون قرمز)، دستگاه‌ها و المان‌های محیطی تشکیل شده است. این لایه عموماً با مدیریت کلی دستگاه سروکار دارد، یعنی شناسایی و جمع‌آوری اطلاعات خاص توسط هر دستگاه حسگر به‌دست می‌آید. این اطلاعات از طریق لایه شبکه به دلیل ارتباطات مطمئن آن به سیستم پردازش داده مرکزی منتقل می‌شود.

[5] The Open Systems Interconnection model (OSI model)
[6] Zigbee Protocol

ISSN: 2475-3673
http://www.Racj.ir

شکل ۳: معماری چهار لایه اینترنت اشیاء [۸]

لایه شبکه: عملکرد این لایه مشابه لایه OSI در شبکه است. این لایه به دودسته توانایی تقسیم می‌شود. ابتدا توانایی شبکه، که به کاربرد آن در ارتباط با کنترل اتصال شبکه مانند: کنترل دستیابی، مبدأ انتقال، احراز هویت، صدور مجوز و حسابرسی (AAA[۷]) می‌توان اشاره کرد. دیگری توانایی انتقال است که نقش مهمی در انتقال ایمن بر عهده دارد. علاوه بر این که از اطلاعات محرمانه نگه‌داری می‌کند. از طریق ارتباط‌هایی همچون WIFI، RFID، مادون‌قرمز و یا ماهواره، اطلاعات را به سیستم پردازش داده مرکزی منتقل می‌کند. به همین منظور، مسئول انتقال اطلاعات از لایه ادراک به لایه بالاترمی باشد.

لایه میان‌افزار: دستگاه‌ها در سیستم اینترنت اشیاء، زمانی که به یک‌دیگر متصل هستند و با یکدیگر ارتباط دارند انواع مختلف خدمات را تولید می‌کنند. لایه میان‌افزار دارای دو کاربرد ضروری و مهم است، این دو کاربرد شامل مدیریت خدمات و دسته‌بندی و ذخیره اطلاعات لایه پایینی در پایگاه‌داده هستند. علاوه‌براین، این لایه قابلیت بازیابی پردازش و محاسبه اطلاعات را دارد. همچنین، می‌تواند بصورت خودکار و بر اساس نتایج محاسباتی تصمیم‌گیری کند.

لایه کاربرد: لایه کاربرد یا کاربر نهایی شامل اپلیکیشن‌های IoT و مسئول مدیریت آن‌ها بر اساس اطلاعات پردازش شده در لایه میان‌افزار هستند. اپلیکیشن‌های IoT می‌توانند در زمینه پست هوشمند، سلامت هوشمند، زندگی مستقل هوشمند، حمل و نقل هوشمند و سایر زمینه‌های گسترده این فناوری باشند. درواقع، این لایه نقطه ارتباط کاربر نهایی با سیستم است، یعنی کاربر با استفاده از اپلیکیشن‌های خود می‌تواند اقدام به درخواست، ثبت یا ویرایش خدمات و اطلاعات کند.

چالش‌های اینترنت اشیاء

براساس تحقیقات انجام شده، این بخش درباره‌ی چالش‌های موجود در توسعه IoT توسط اولویت‌های مهم مورد بحث قرار گرفته‌است. در ادامه به پنج چالش فنی و مدیریتی شامل مدیریت داده، داده‌های استخراجی، حریم خصوصی، نبود استاندارد واحد، هرج و مرج (آشفتگی) و سیستم امنیتی پرداخته شده است.

چالش در مدیریت اطلاعات

دستگاه‌های IoT تعداد زیادی از داده‌ها را تولید می‌کنند که باید پردازش و ذخیره‌سازی شوند. از طرفی هم مرکز داده آمادگی لازم برای مقابله با ماهیت ناممکن داده‌های فرعی و سازمانی را ندارد. تعداد کمی از شرکت‌ها قادر به سرمایه گذاری در ذخیره‌سازی داده‌ها خواهند بود. در نتیجه آن‌ها داده‌ها را براساس اختیارات و ارزش‌های خود برای عملیات یا پشتیبانی اولویت-

[7] Accounting, Authorization, and Authentication (AAA)

ISSN: 2475-3673
http://www.Racj.ir

بندی می‌کنند. همچنان که استفاده از دستگاه‌های IoT بیشتر می‌شود، پهنای باند بیشتری را اشغال می‌کنند. ازاین‌رو، مراکز داده‌ها نیز جهت بهبود کارایی پردازش و پاسخگویی باید از تقسیم بندی بیشتری برخوردار شوند [۹، ۱۰، ۱۱].

چالش استخراج داده

هرچه داده‌های بیشتری برای پردازش و تجزیه و تحلیل در دسترس باشند، استفاده از ابزارهای استخراج داده از اهمیت بیشتری برخوردار می‌شود. این داده‌ها تنها شامل داده‌های گسسته سنتی نمی‌شوند؛ بلکه شامل داده‌های جریانی تولید شده از سنسورهای دیجیتالی است. تکنیک‌های سنتی استخراج داده برای داده‌های تصویری و ویدئویی بدون ساختار مشخص به‌طور مستقیم قابل استفاده نیست. برای استخراج داده‌های جریانی از شبکه‌های حسگر به ابزار استخراج داده‌های پیشرفته‌ای نیاز داریم و این در حالی است که با فقدان (کمبود) تحلیل گران داده روبرو هستیم [۹، ۱۰، ۱۱].

چالش حریم خصوصی

دستگاه‌های IoT می‌تواند اطلاعات گسترده‌ای را در مورد موقعیت، حرکات، شرایط کاربران به دست آورند که این امر موجب ایجاد نگرانی‌های بسیاری در زمینه حفظ حریم خصوصی می‌شود. تا زمانی که داده‌های تولید شده توسط IoT هدف بهبود کیفیت زندگی مردم و نیز کاهش هزینه‌های خدمه از طریق عملیات موثر را مدنظر قراردهند حفاظت از حریم خصوصی کاربران برای اغلب ارائه‌دهندگان خدمات IoT غیرممکن است. با این وجود دستگاه‌های IoT همچنان به سمت هوشمندسازی پیشروی می‌کنند و اعتبار IoT به حفاظت از حریم خصوصی کاربران وابسته است [۹، ۱۰، ۱۱].

چالش نبود استاندارد واحد

زمانی‌که استانداردهای بنیادی اینترنت ایجاد شدند افرادی کنترل این استانداردها را در دست داشتند که خواسته واقعی-شان شکل گیری استانداردهای جهانی بود، اما اینترنت امروزه در کنترل شرکت‌هایی است که هرکدام می‌خواهند از این استانداردها بهره بگیرند و با استفاده از آن‌ها رقبا را شکست دهند. هم چنین اینترنت دردست دولت‌هایی است که در اصل می-خواهند بر همه چیز نظارت داشته باشند، در چنین وضعیتی دولت‌ها و شرکت‌ها چگونه می‌خواهند بر سر استانداردهای جهانی به توافق برسند؟

در اینترنت اشیاء استاندارد یعنی همه چیز هر دستگاه باید به دستگاه‌های دیگر اعلام کند که چه کاری را می‌خواهد انجام دهد. بدون استانداردها نمی‌توان این کار را کرد [۹، ۱۰، ۱۱].

چالش‌های هرج و مرج (آشفتگی)

در حال حاضر هنوز هم استانداردهایی همانند استانداردهای رقابتی، امنیتی، مسائل مربوط به حریم خصوصی، ارتباطات پیچیده وجود دارد که بر روی تعداد بسیاری از دستگاه‌های ضعیف مورد آزمایش قرارگرفته است. اگر این استانداردها به‌دقت طراحی نشود این دستگاه‌های چندمنظوره و برنامه‌های کاربردی می‌توانند منجر به ایجاد هرج‌ومرج در زندگی شوند. در یک جهان دارای ارتباطات ضعیف یک خطای کوچک به‌تنهایی قادر به سقوط یک سیستم خواهد شد. با این حال، در جهانی که ارتباطات آن قوی است تنها یک خطای کوچک می‌تواند منجر به ایجاد اختلال در کل سیستم شود [۹، ۱۰].

چالش امنیت اینترنت اشیاء

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 حریم خصوصی

ISSN: 2475-3673
http://www.Racj.ir

در IoT افزایش می‌یابد. در اینترنت اشیاء، اکثر اطلاعات موجود مربوط به اطلاعات شخصی از قبیل تاریخ تولد، مکان و بودجه هستند. این یک ویژگی چالش‌برانگیز داده ابری است و حرفه‌های مربوط به امنیت باید تضمین‌کننده خطرات احتمالی به مجموعه داده‌ها باشند. پیاده‌سازی اینترنت اشیاء باید موردقبول قانون، اخلاق، جامعه و سیاست باشد و درآن چالش‌های قانونی، رویکردهای سیستمی، چالش‌های تکنیکی و چالش‌های تجاری درنظر گرفته شوند. 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 [۱۱، ۱۲، ۱۳].

با توجه به مباحث گفته شده، برخلاف اینترنت، IoT به‌صورت بسیار قابل توجه‌ای به اقتصاد جهانی تاثیر بسزایی دارد. می‌توان در این زمینه از حمل‌ونقل، سلامت، شهر و خانه هوشمند، روش زندگی شخصی و اجتماعی یادکرد. به همین دلیل، امنیت و حریم خصوصی نگرانی‌هایی هستند که در IoT، بیش‌تر نیاز به پاسخ‌گویی دارند [۱۱].

پیاده‌سازی امنیت اینترنت اشیاء

برخی از تولیدکنندگان دستگاه‌های IoT که تازه‌کار هستند، دارای کمبودهایی در تخصص امنیت بوده و نمی‌توانند از پس هزینه‌های استخدام متخصصان امنیت برآیند. به‌همین‌دلیل، به مکانیزم‌های امنیتی ابتدایی در عناصر سخت‌افزاری 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 [۱۴، ۱۵].

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. طبیعت همگن توسعه IoT (مانند شبکه‌های حسگر بی‌سیم؛ که در آن تمامی گره‌ها کسان 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 را درمعرض خطر قرار دهد. از آن-جایی 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 [۱۴، ۱۵].

تعداد بسیار زیادی از دستگاه‌های IoT که در چهارچوب‌های سختی توسعه یافته‌اند ممکن است سال‌ها بدون مراقبت در مکانی ساکن باشند و باتوجه به طبیعت آن چهارچوب 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. دربعضی از اپلیکیشن‌ها ممکن است که توسعه دستگاه‌ها در مکان-هایی 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. اینترنت اشیاء طراحی شده‌است تا به کمک اینترنت، اتصال یکپارچه‌ای میان دستگاه‌های متنوع در سیستم‌ها و زیرسیستم‌های مختلف فراهم کند. به‌همین ترتیب یک ماشین لباس‌شویی موردحمله قرارگرفته می‌تواند جهت ارسال هرزنامه‌های خطرناک (ازطریق اتصال Wi-Fi) در سراسر جهان مورد استفاده قرار گیرد [۱۳، ۱۴، ۱۵].

ISSN: 2475-3673
http://www.Racj.ir

امنیت

امنیت از بزرگ‌ترین موانع در طراحی شبکه‌های IoT به حساب می‌آید؛ زیرا به تازگی حملاتی از طریق هکرهای کلاه‌سفید (به منظور آزمایش عملکرد دستگاه IoT و یافتن آسیب‌پذیری‌های آن نسبت به قابل نفوذ بودن) و حملات هکر کلاه سیاه از سوی موجودیت‌های مخرب (که با بکارگیری آسیب‌پذیری‌های شناخته شده سعی در دست‌یابی به اطلاعات شخصی افراد) صورت می‌گیرد. در نتیجه با افزایش این گونه حملات سایبری که IoT را هدف قرار می‌دهند نیاز به استراتژی‌های امنیتی در این حوزه است که باید برنامه‌ریزی و اجرا شود. ازاین‌رو، هدف‌های جدید امنیتی شناسایی شده و در فرایند طراحی دستگاه-های IOT پیاده‌سازی می‌شوند [۱۶، ۱۷].

در این راستا از الگوهای سه‌گانه‌ای به نام CIA[8] استفاده می‌شود که به نام‌های محرمانگی، یکپارچگی و دردسترس بودن هستند. از این رو، با گسترش آن‌ها الزامات امنیتی همانند احرازهویت، کنترل دسترسی، قابلیت عدم‌انکار، راه اندازی ایمن و شناسایی دستکاری دستگاه، امنیت و حریم خصوصی در استاندارد ITU-T مطرح شدند. اغلب در هر مکانیزم امنیتی دو ویژگی حفاظت وکنترل در اولویت هستند اما از آنجایی که در هر سیستم اهداف امنیتی متفاوت است الزامات امنیتی متفاوتی هم در پی دارد. بخش بعدی توضیح مختصری از الزامات امنیتی مذکور را ارائه می‌دهد [۱۶، ۱۷].

محرمانگی: محرمانگی داده تضمین می‌کند که تنها افراد مجاز اجازه دسترسی به داده‌ها را خواهندداشت وهیچ اطلاعات حساسی به افراد غیرمجاز داده نخواهد شد. سطح محرمانگی به سناریو اپلیکیشن و پیاده‌سازی آن بستگی دارد. برای نمونه: سطح محرمانگی آب‌پاچ‌های هوشمند قابل مقایسه با سطح محرمانگی دستگاه‌های صنعت سلامت نخواهد بود در واقع یعنی اطلاعات بیماران باید قوی باشد که دسترسی به این اطلاعات فقط به افراد مجاز محدود شود [۱۸، ۱۹].

یکپارچگی: گاهی دستگاه‌های IoT اطلاعات شخصی کاربران، سرویس‌دهندگان شبکه و تولیدکنندگان دستگاه‌های هوشمند را به صورت محلی روی دستگاه‌ها ذخیره می‌کنند. این اطلاعات حاوی داده‌های مهمی همانند رکوردهای مهم و کلید رمز است. یکپارچگی در واقع حفظ دقت، پایداری، اعتمادپذیر بودن داده‌ها در حین عمل انتقال یا ذخیره‌سازی است [۱۸، ۱۹].

دردسترس بودن: راه حل‌هایی که تضمین می‌کند که کاربران مجاز اجازه حق دسترسی به داده‌های درون یک سرویس و یا یک سیستم مجاز را داشته باشند. اعمال تعمیرات سخت‌افزاری به محض پیدایش یک مشکل، اطمینان از به روز بودن نرم-افزارهای موجود بر روی سیستم، رها بودن از بند هرگونه مغایرت‌های نرم‌افزاری، نگهداری یک بازیابی سریع، انطباق در سناریوها و کپی پشتیبان داده‌ها از جمله راه‌حل‌های در دسترس بودن است [۱۸، ۱۹].

احرازهویت: احراز هویت تضمین می‌کند که هر تراکنشی یا هر تبادل اطلاعاتی از طرف منبعی است که باید باشد. این عمل هر زمان که دستگاهی به شبکه متصل شود صورت می‌گیرد و تضمین می‌کند که هیچ شخص ثالثی با احتمال وجود خطر امنیتی به شبکه متصل نخواهد شد. این امر سبب وجود تایید مبتنی بر امضاء کدگذاری شده‌است که هویت هر منبع سیستم عامل را تایید می‌کند [۱۸، ۱۹].

کنترل دسترسی: کنترل دسترسی تعیین می‌کند که چه کسی اجازه دسترسی به برخی منابع را دارد در واقع یعنی تنها موجودیت‌های مورد اعتماد می‌توانند نرم‌افزار دستگاه را بروز رسانی کنند و به عاملان دستور دهند که عملیات پیکربندی دستگاه را انجام دهند یا به داده‌های حسگر دسترسی داشته باشند. احراز هویت جزء مهمی از کنترل دسترسی است چرا که دسترسی کاربران و دستگاه‌ها باید احراز شود [۱۸، ۱۹، ۲۰].

عدم انکار: عدم انکار مدارکی را فراهم می‌کند که به کاربر اجازه نمی‌دهد تا عملی مانند تبادل پیام را انکار کند. این رویکرد حضور مدرک را از طریق یک شخص ثالث مورد اعتماد (TTP) تضمین می‌کند این مدرک باید تبادل گواهی میان موجودیت‌ها را غیرقابل انکار کند و از فرایند نظارت داده در این رویکرد استفاده می‌شود تا اشیاء در معرض خطر شناسایی شوند [۲۱].

راه اندازی ایمن: راه اندازی ایمن یک دستگاه تمامی اقدامات موجود مبتنی بر اجرای نرم‌افزارهای مختلف بر روی یک دستگاه را در زمان روشن شدن آن دستگاه مسدود می‌کند. ازاین‌رو، عدم تغییر سیستم عامل را تضمین می‌کند. اعتبار و

[8] Confidentiality, Integrity, and Availability (CIA)

ISSN: 2475-3673
http://www.Racj.ir

یکپارچگی نرم‌افزارهای درحال اجرا بر روی آن دستگاه توسط امضاءهای دیجیتالی تایید می‌شوند که رمزنگارانه تولید شده‌اند و نیاز به سخت‌افزار خاصی است. در نتیجه، پیاده‌سازی آنها با استفاده از کدهای امضاء رمزنگاری شده است [۲۱، ۲۲].

شناسایی دستکاری دستگاه: شناسایی دستکاری دستگاه یکی از الزامات امنیتی است که به شناسایی تمامی اقدامات مبنی بر مداخله و دستکاری با یک دستگاه، چه به‌صورت فیزیکی و چه به‌صورت منطقی می‌پردازد. باوجود این‌که برخی از واحدهای ریزپردازنده جدید دارای حافظه پیشرفته و قابلیت‌های حفاظت از کد (که از آن‌ها دربرابر دسترسی‌های غیرقانونی محافظت می-کند) هستند، اما با این حال استفاده از این حفاظت‌های ضد دستکاری همیشه نمی‌تواند حفاظت کافی و موردنیاز را فراهم کند [۲۱، ۲۲].

تعداد بسیار زیادی از دستگاه‌های اینترنت اشیاء مانند حسگرها، در محیط‌های باز توسعه می‌یابند و به مهاجم این امکان را می‌دهند که تماس مستقیمی با آن‌ها داشته باشند. علاوه‌براین، برخی از مهاجمان ماهر ممکن است آن‌ها را برای تجزیه و تحلیل به آزمایشگاه‌های خود ببرند. به‌عنوان مثال‌هایی از این قبیل دستگاه‌ها، می‌توان از گره‌های حسگر و دستگاه‌های پوشیدنی IoT اشاره کرد [۲۱، ۲۲].

امنیت و حریم خصوصی در استاندارد ITU-T

توصیه‌های Y.2066 که در استاندارد ITU-T قرار دارد، شامل لیستی از الزامات امنیتی مربوط به اینترنت اشیاء است. این لیست، پایه مفیدی برای درک محدوده امنیتی موردنیاز در پیاده‌سازی یک موضع IoT فراهم می‌آورد. این الزامات، از یک سو همان الزامات کاربردی درحین دریافت، ذخیره‌سازی، انتقال، جمع‌آوری و پردازش داده‌های اشیاء است و از سوی دیگر خدماتی که شامل این اشیاء هستند را تدارک می‌بینند. این الزامات که مرتبط با تمامی عاملان IoT است عبارت‌اند از [۲۲، ۲۳]:

امنیت ارتباطات: قابلیت ارتباط ایمن، مورد اعتماد و محافظت شده در برابر حریم خصوصی امری ضروری و موردنیاز است؛ چراکه درحین انتقال داده در IoT، باید از دسترسی غیرمجاز به محتوای داده جلوگیری‌شده، یکپارچگی داده‌ها تضمین‌شده و محتوای مربوط به حریم‌خصوصی داده محافظت شود.

امنیت مدیریت داده: قابلیت مدیریت داده به‌صورت ایمن، مورد اعتماد و محافظت‌شده در برابر حریم خصوصی امری ضروری و موردنیاز است. از این طریق می‌توان در حین ذخیره‌سازی یا پردازش داده در IoT، از دسترسی غیرمجاز به محتوای داده جلوگیری کرد. همچنین، یکپارچگی داده‌ها را تضمین و از محتوای مربوط به حریم خصوصی داده حفاظت کرد.

امنیت تدارک خدمات: قابلیت تدارک ایمن، مورد اعتماد و محافظت‌شده در برابر حریم خصوصی امری ضروری است. در این‌صورت از دسترسی غیرمجاز به خدمات و همچنین تدارکات خدمات جعلی جلوگیری شده و اطلاعات خصوصی کاربران IoT مورد حفاظت قرار می‌گیرد.

ادغام تکنیک‌ها و سیاست‌های امنیتی: برای تضمین کنترل امنیت مداوم در دستگاه‌های مختلف و شبکه‌های متفاوت، نیاز به ادغام تکنیک‌ها و سیاست‌های امنیتی مختلف می‌باشد.

اعتباردهی و احرازهویت مشترک: قبل از این‌که دستگاهی (کاربری) به IoT دسترسی پیدا کند، نیاز است که احرازهویت و اعتباردهی مشترکی باتوجه به سیاست‌های امنیتی ازپیش تعیین‌شده میان آن دستگاه و IoT صورت گیرد.

حسابرسی امنیتی: حسابرسی امنیتی باید در اینترنت اشیاء پوشش داده شود. باتوجه به قوانین و مقررات، اپلیکیشن‌هایی که به داده‌های مختلف دسترسی دارند باید تماماً شفاف (بدون ابهام)، قابل ردیابی و تجدیدپذیر باشند. در مجموع، IoT باید حسابرسی‌های امنیتی را در انتقال، ذخیره‌سازی و پردازش داده و همچنین در دسترسی اپلیکیشن‌ها پوشش دهد.

ISSN: 2475-3673
http://www.Racj.ir

جدول ۱: تحلیل حملات ممکن براساس تهدیدات و آسیب‌پذیری‌ها در محیط IoT

گروه		ویژگی‌ها	فواید	تهدیدات	آسیب پذیری	حملات	مکانیزم امنیتی				
							محرمانگی	یکپارچگی	احراز هویت	دردسترس بودن	عدم انکار
سخت افزار	RFID	شناسه منحصربه‌فرد و شناسایی خودکار	تبادل سریع داده میان تگ‌ها	ردگیری، DoS، انکار و کلاهبرداری	دخالت، فساد و حذف	استراق سمع و جعل و تقلب	−	−	−	+	−
	ZigBee	رادیو، ریزپردازنده، پروتکل ساده و سایز کوچک	قابل اعتماد، کاهش مصرف، هزینه پائین	دست‌کاری بسته	هک شدن	تبادل کلید، KillerBee و Scapy	±	+	±	+	±
	بلوتوث	طیف جهش فرکانس	اجازه اتصال بی‌سیم به دو دستگاه، امن	استراق‌سمع، DoS	Bluesnarfing، Bluejacking	نجواگر ماشین، Bluebugging	−	−	±	±	±
	گره حسگر	حسگرها و عاملان	انعطاف-پذیری، تأخیر بالا در ارتباطات	DoS، فرسودگی، بی‌عدالتی و Sybil	Flooding، پروتکل-های مسیریابی	تراکم، دست کاری، تصادم	±	±	+	+	+
زیرساخت	سیمی	کابل، آداپتور شبکه و روتر	امنیت بیشتر قابلیت اعتماد و سهولت بالا	دست‌کاری داده، اخاذی	سیستم سیگنالینگ، دزدی لوازم	پیوند ضعیف، حملات مخرب	+	±	+	+	+
	بی سیم	ارتباط رادیویی، فرستنده و گیرنده	دسترسی مهمان بالا، گسترش شبکه، توانایی همکاری بالا	نقاط دسترسی سرکش، پیکربندی اشتباه	هک شدن، فقدان سیگنال	DoS، شماره‌گیری جنگ، تونل-زنی پروتکل، مرد میانی	±	±	±	+	+
اپلیکیشن هوشمند	شهر هوشمند	نورپردازی خیابان، مدیریت آب و زباله	برنامه‌ریزی شهری، تحویل خدمات، توسعه اقتصاد	شهر هوشمند، دست کاری اطلاعات	شناسایی جعلی زلزله و سیل	اپلیکیشن‌های موبایل، حسگرها	±	±	±	±	−
	شبکه هوشمند	واحدهای هوشمند، انرژی	ذخیره هزینه، استقلال انرژی	امنیت مشتری، امنیت	اعتماد میان دستگاه-	نقاط پایانی دستگاه، حملات	±	±	±	±	±

ISSN: 2475-3673
http://www.Racj.ir

		هوشمند		فیزیکی	های برق	مخرب					
	مراقبت درمانی هوشمند	کارت‌های هوشمند سلامت	ارتقاء امنیت بیمار و جزئیات اطلاعات	دزدی و فقدان، سوءاستفاده داخلی، اعمال غیرعمد	هک شدن	حمله داخلی، حمله سایبری	±	±	±	-	-
	حمل و نقل هوشمند	کنترل ترافیک، پارکینگ، حمل و نقل عمومی	سهولت در استفاده	DoS شهر هوشمند	آفت امنیتی	حملات سایبری	-	-	±	±	±

ارزیابی و مقایسه

رشد و توسعه اینترنت اشیاء در راستای بهبود حفظ امنیت به تحقق می‌پیوندد. در ادامه، این بخش به بررسی امنیت و راهکارهای مقابل با تهدیدات امنیتی از تمامی ابعاد پرداخته است. همچنین به بررسی و مقایسه مقوله مهم امنیت پرداخته شده است و پیشنهاداتی جهت بهبود امنیت اینترنت اشیاء پیشنهاد داده شده است.

حملات براساس تهدیدات و آسیب‌پذیری‌های IoT

اینترنت اشیاء مفهومی است که هر روز تکامل می‌یابد. فناوری‌هایی مانند شبکه‌های حسگر بی‌سیم، RFID و امکانات ابری توسط دستگاه‌های IoT به‌کار گرفته می‌شوند. تابع M2M الگوی اصلی ساخت بلوک‌های IoT است. بعلاوه، الگوی IoT در دامنه‌های زیادی از جمله شهرهای هوشمند، سلامت هوشمند و انتقال هوشمند قابل اعمال است. این دستگاه‌ها باید قادر به برقراری ارتباط با یک‌دیگر و سایر اجسام وحتی انسان‌ها باشند. هر ارتباطی باید ایمن باشد به‌طوریکه به کاربر این اطمینان را بدهد که اطلاعات وی و کانال‌های ارتباطی او ایمن است. با این وجود، حفاظت از IoT وظیفه‌ای چالش برانگیز است [۱۳، ۲۴، ۲۵].

در این حوزه، امنیت چالش قابل توجهی است که باید در IoT درنظرگرفته شود. معماری IoT باید بتواند میلیاردها جسم متصل را مدیریت کند. این سناریو راه‌های دست‌یابی بسیاری برای مهاجمان ایجاد می‌کند؛ چراکه دسترسی و اتصال جهانی از اهداف پایه این فناوری است. اینترنت اشیاء تحت تأثیر سطوح مختلفی از تهدیدات در نواحی سخت‌افزاری، شبکه و اپلیکیشن-های هوشمند قرار خواهد داشت که کانال‌های ارتباطی مختلفی را هدف قرار خواهند داد. مشکلات امنیتی و حریم خصوصی باید در مقیاس‌های بزرگ و دامنه‌های متفاوت در IoT پاسخ‌گویی شوند [۱۳، ۲۴، ۲۵]. جدول ۱ به ارزیابی کاملی از انواع تهدیدات پرداخته است. علایم موجود در مکانیزم‌های امنیتی جدول ۱ بدین معنی هستند؛ علامت - به معنی دارا نبودن، علامت + به معنی دارا بودن و علامت ± هم به معنی دارا بودن و نبودن است [۲، ۲۴، ۲۶، ۲۷، ۲۸، ۲۹، ۳۰، ۳۱، ۳۲].

نگرانی‌های امنیتی در لایه‌ها

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 حریم خصوصی

ISSN: 2475-3673
http://www.Racj.ir

در IoT افزایش می‌یابد. مهمترین نگرانی‌های امنیتی در حوزه IoT در معماری چهار لایه‌ای که شامل لایه حسگر، لایه شبکه، لایه خدمات، لایه اپلیکیشن قرار دارد که به طور مختصر در جدول ۲ به آن پرداخته شده است [۲، ۸، ۱۳، ۳۳].

جدول ۲: نگرانی‌های امنیتی در معماری چهار لایه

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			√	√

لایه حسگر با عناصر پایانی IoT ادغام شده تا اطلاعات دستگاه‌ها را حس و دریافت کند. ازجمله تهدیدات وآسیب پذیری های امنیتی در لایه حسگر در جدول ۳ بیان شده است. همچنین جدول ۴، به بررسی آسیب‌پذیری و تهدیدات امنیتی گره‌های نهایی لایه حسگر، پرداخته است [۱۳، ۳۴].

جدول ۳: آسیب‌پذیری‌ها و تهدیدات امنیتی در لایه حسگر

تهدیدات امنیتی	توضیحات
دسترسی غیرمجاز	دسترسی فیزیکی و حملات منطقی، اطلاعات حساس در گره‌های نهایی دردست مهاجم است.
دردسترس بودن	گره‌های نهایی درصورت قرارگرفتن درمعرض دسترسی فیزیکی یا حملات، دست از کار می‌کشند.
حمله Spoofing	با گره‌های بدافزار و جعل داده، مهاجم خود را به‌عنوان دستگاه، گذرگاه یا گره نهایی جا می‌زند.
تهدید خودخواهی	برخی از گره‌های نهایی برای ذخیره منابع یا پهنای باند دست از کار می‌کشند و شبکه مختل می‌شود.
کد مخرب	ویروس، تروجان یا پیام اوراق که منجر به شکست نرم‌افزار می‌شوند.
DoS	اقدامی درجهت خارج کردن یک منبع گره‌نهایی از دسترس کاربران.
تهدیدات انتقال	تهدیداتی مانند قطع کردن، مسدود کردن، دست‌کاری داده و جعل.
حمله مسیریابی	حمله به یک مسیر روتینگ.

جدول ۴: تحلیل آسیب‌پذیری و تهدیدهای امنیتی در لایه حسگر

آسیب‌پذیری و تهدیدات امنیتی گره‌های نهایی	دستگاه‌های نهایی	گره‌های نهایی	گذرگاه‌های نهایی
دسترسی غیرمجاز	√	√	√
تهدید خودخواهی		√	√
حمله Spoofing		√	√
کد مخرب	√	√	√
DoS	√	√	√
تهدیدات انتقال			√

ISSN: 2475-3673
http://www.Racj.ir

حمله مسیریابی	√	√	√

نتایج جدول ۴ نشان می‌دهد که دسترسی غیرمجاز، کد مخرب، DOS و حمله مسیریابی بیشتر آسیب را در گره‌های نهایی دارد. از این رو، راهکارهایی برای جلوگیری از این حملات باید در لایه حسگر بیشتر مطرح شود.

لایه شبکه زیرساختی برای پوشش‌دهی ارتباطات سیمی یا بی‌سیم درمیان اشیاء است. ازجمله تهدیدات وآسیب پذیری های امنیتی در لایه شبکه در جدول ۵ ذکر شده است. همچنین، جدول ۶ به بررسی آسیب‌پذیری‌ها با توجه به تهدیدات امنیتی در لایه حسگر پرداخته است [۳۳، ۳۴].

جدول ۵: تهدیدات امنیتی در لایه شبکه

تهدیدات امنیتی	توضیحات
رخنه داده	اطلاعات فاش شده در یک محیط غیرقابل اعتماد
کلید خصوصی و عمومی	شامل تمامی کلیدهای شبکه
کد مخرب	ویروس، تروجان یا پیام اوراق که منجر به شکست نرم‌افزار می‌شوند.
DoS	اقدامی درجهت خارج کردن یک منبع گره‌نهایی از دسترس کاربران.
تهدیدات انتقال	تهدیداتی مانند قطع کردن، مسدود کردن، دست‌کاری داده و جعل.
حمله مسیریابی	حمله به یک مسیر روتینگ.

با توجه به بررسی‌های جدول ۵، فاکتور امنیت انتقال بیشترین آسیب‌پذیری را در لایه شبکه دارد. از این رو، بهبود بحث ارتباطات اشیاء در این حوزه باید مورد بهبود و مطالعه بیشتر قرار گیرد. به همین دلیل، می‌توان از معماری اینترنت اشیاء در راستای بهبود امنیت انتقال و ارتباط اینترنت اشیاء استفاده کرد.

جدول ۶: تحلیل آسیب‌پذیری و تهدیدهای امنیتی در لایه حسگر

تهدیدات	حریم‌خصوصی	محرمانگی	یکپارچگی	DoS	PKI	MITM	جعل درخواست
حفاظت فیزیکی	√	√					√
امنیت انتقال		√	√	√	√	√	√
اتصال بیش‌ازحد			√	√	√		
ادغام لایه صلیبی	√	√				√	√

لایه خدمات برای فراهم کردن و مدیریت خدمات موردنیاز کاربران یا اپلیکیشن‌ها است. ازجمله تهدیدات و آسیب پذیری های امنیتی در لایه خدمات در جدول ۷ ذکر شده است [۱۳، ۳۵، ۳۶].

جدول ۷: تهدیدات امنیتی در لایه خدمات

تهدیدات	توضیحات
تهدیدات حریم‌خصوصی	نشت حریم‌خصوصی یا ردیابی مکانی مخرب.
سوءاستفاده از خدمات	دسترسی کاربران غیرمجاز به خدمات یا دسترسی کاربران مجاز به خدمات غیرمجاز.
جعل هویت	هویت گره‌های نهایی IoT توسط مهاجم جعل می‌شود.
دست‌کاری اطلاعات خدمات	اطلاعات موجود در خدمات توسط مهاجم دست‌کاری می‌شود.
انکار	انکار عملیاتی که صورت گرفته است.
DoS	اقدامی درجهت خارج کردن یک منبع گره‌نهایی از دسترس کاربران.

ISSN: 2475-3673
http://www.Racj.ir

حمله بازپخش	مهاجم اطلاعات را مجدداً ارسال می‌کند تا از دریافت‌کننده کلاه‌برداری کند.
حمله مسیریابی	حمله به یک مسیر روتینگ.

لایه اپلیکیشن متشکل از روش‌های تعامل با کاربر یا اپلیکیشن‌ها است. ازجمله تهدیدات وآسیب پذیری های امنیتی در لایه اپلیکیشن در جدول ۸ ذکر شده است. همچنین جدول ۹ به بررسی و تحلیل آسیب‌پذیری‌های تهدیدهای امنیتی در لایه اپلیکیشن پرداخته شده است [۳۷، ۱۳، ۸].

جدول ۸: تهدیدات امنیتی در لایه اپلیکیشن

تهدیدات	توضیحات
پیکربندی از راه‌دور	شکست خوردن پیکربندی در پل‌های ارتباطی
پیکربندی اشتباه	پیکربندی غلط در گره‌های نهایی IoT
مدیریت امنیتی	نشت کلیدها و فایل‌های Log
سیستم مدیریت	شکست خوردن سیستم مدیریت

بر اساس نتایج بدست آمده از جدول ۹، مکانیزم‌های امنیتی به ویژه مکانیزم محرمانگی داده که شامل محرمانگی و یکپارچگی داده می‌شود، از اهمیت بالای برخوردار است. همچنین، بهبود مکانیزم‌های امنیتی در این لایه باعث تسریع کار مشتریان و ارائه‌دهندگان این تکنولوژی می‌شود.

جدول ۹: تحلیل آسیب‌پذیری و تهدید امنیتی در لایه اپلیکیشن

تهدید	دسترسی غیرمجاز	شکست گره	جعل	گره خودخواه	ویروس، تروجان، Spam	حریم-خصوصی
حفاظت امنیت فیزیکی	√	√	√			
آنتی‌ویروس، فایروال				√		
کنترل دسترسی	√	√	√			√
محرمانه	√	√	√			√
یکپارچگی داده		√	√	√	√	
احرازهویت	√	√	√			√
عدم انکار	√	√	√			√

تکنیک‌های امنیتی

جهت بررسی تکنیک‌های امنیتی اینترنت اشیاء، ابتدا باید آن‌ها را از لحاظ ویژگی‌های منطقی و کاربردی طبقه‌بندی کرد. این طبقه‌بندی امنیتی در چهار گروه برنامه کاربردی، ساختار، ارتباط و داده تعریف شده است. شکل ۵ طبقه‌بندی امنیتی اینترنت اشیاء را نشان می‌دهد [۳۸، ۳۹، ۴۰].

برنامه کاربردی: گسترش اینترنت اشیاء بر برخی نواحی برنامه کاربردی بسیار اثر می‌گذارد. برنامه‌های کاربردی براساس نوع دسترسی شبکه، مقیاس، ناهماهنگی، قابلیت برگشت و درگیری کاربر دسته بندی می شوند. همانطور که در طبقه بندی امنیت اینترنت اشیاء نشان داده شده است، چندین تکنیک امنیتی وجود دارد. رایج‌ترین تکنیک‌های امنیتی مورد استفاده

ISSN: 2475-3673
http://www.Racj.ir

شامل تصدیق، مجوز، تخلیه منابع و ایجاد اعتماد است. جدول ۱۰ به خلاصه‌ای از تکنولوژی‌های امنیتی در حوزه اینترنت اشیاء پرداخته است [۴۱، ۴۲، ۳۹، ۴۳].

شکل ۵: طبقه‌بندی امنیتی اینترنت اشیاء

معماری: در حال حاضر هیچ معماری اینترنت اشیاء قابل قبولی در جهان وجود ندارد. چندین نوع تحقیق در خصوص معماری اینترنت اشیاء باخلاصه برنامه و دامنه کاربرد متفاوت به لحاظ تصدیق و مجوز انجام شده است. جدول ۱۱ به انواع معماری‌های امنیتی و دامنه کاربرد پرداخته است [۴۴، ۴۵، ۱۳، ۴۱، ۳۹].

جدول ۱۰: مروری بر تکنولوژی‌های امنیتی در اینترنت اشیاء با تمرکز بر برنامه کاربردی

تکنولوژی	اهداف	مزایا	محدودیت
پیاده سازی ابری با استفاده از پایگاه محاسبه انکا	تعیین روندهای برنامه کاربردی فعلی اینترنت اشیاء و نیاز به ترکیب تکنولوژی-های میان رشته‌ای مختلف	- از حافظه و منابع سیستم به همراه ابرهای خصوصی و عمومی استفاده می‌کند. - تامین منابع برای ابرهای عمومی؛ مانند Microsoft Azure و Amazon ESC	حفاظت از امنیت و حریم-شخصی در ابرهای چندگانه مسئله جدی است.
طرح رمز گذاری مبتنی بر ویژگی جفت نبودن (ABE) بر پایه منحنی بیضوی رمزنگاری (ECC)	- اشاره به مشکلات امنیتی و حریم شخصی در اینترنت اشیاء. - کاهش محاسبه و ارتباط مازاد.	رمزگذاری مبتنی بر ویژگی (ABE) در کنترل دسترسی رمزگذاری مبتنی برمتن و رمز-گذاری پراکنده قابل اجرا است.	- صعودی‌پذیری ضعیف. - انعطاف‌پذیری ضعیف در لغو ویژگی.
طرح تجدید نظر شده اشتراک سری	- دستیابی به صعودپذیری داده. - کاهش مدیریت کلیدی پیچیده مربوط به الگوریتم-های رمزگذاری قراردادی.	با طرح اشتراک سری دستیابی به صعودپذیری امکان‌پذیر می-شود.	- تولید مازادهای محاسباتی که گلوگاه احتمالی می‌آورد. - خرابی سخت‌افزاری منجرب به مسئله تحمل نقص می‌شود.

ISSN: 2475-3673
http://www.Racj.ir

تخمین منبع و مدیریت با استفاده از رایانش به صورت مد.	ارائه مدل تخمین منبع احتمالی مشتری برای مدها.	- اجازه تحویل داده در زمان واقعی را می‌دهد. - خصوصیات ابر را به لبه‌ی IoT اصلی و دیگر گره‌های پایانی	رسیدن به حداقل تاخیر دشوار است.

جدول۱۱: انواع مختلف معماری امنیتی اینترنت اشیاء و دامنه کاربرد

ساختار	دامنه کاربردی	رفع استحکام در شبکه‌های قدیمی
معماری SDN	محیط هوشمند	بهبود امنیت و ساختار مجوز برای سیستم‌های مراقبت‌های بهداشتی بر پایه اینترنت اشیاء
معماری SEA	مراقبت‌های بهداشتی	تسهیل تعامل سیستم‌های حسگر راه دور و داده با تکنولوژی‌های ارتباطی
ساختار شهر هوشمند	شهر هوشمند	تعریف امنیت سرویس‌های ساختار میان افزار اینترنت اشیاء. تحلیل و تمرکز بر سرویس‌های امنیتی که می‌توان در میان اینترنت اشیاء به کاربرد.
معماری سرویس گرا	انتقال هوشمند	ارائه یک ساختار امنیتی صعودپذیری جدید برای امنیت E2E و کنترل دسترسی IoT ارزیابی ساختار در تنظیمات محدود M2M.
معماری امنیت شئ (DSCAR)	شبکه هوشمند	شناسایی دو نوع ساختار اینترنت اشیاء برای یک سازمان سه لایه‌ای متمرکز بر روی ابر و ساختارهای پنج لایه‌ای خود مختار.
چهارچوب سازمان‌دهی‌های مفهومی	سازمان‌های تجاری	اشاره به آسیب‌پذیری‌ها در سیستم‌های قدیمی اینترنت اشیاء
معماری SDN سیاه	شهر هوشمند	برای رفع آسیب‌پذیری در سیستم‌های IoT سنتی

ارتباط: ارتباط اینترنت اشیاء شامل تبادل به اشتراک گذاردن اطلاعات در میان دستگاه‌های اینترنت اشیاء یا بین لایه‌های مختلف اینترنت اشیاء است. با احتمال زیاد اینترنت اشیاء در دامنه‌های بسیار، تمام زیر ساخت ارتباط اینترنت اشیاء از چشم‌انداز امنیتی، ناسازگار و از چشم‌انداز کاربران نهایی، نسبت به از دست دادن حریم شخصی آسیب‌پذیر است. رسانه ارتباط اینترنت اشیاء به عنوان یک مقطع تصمیم برای مهاجمان عمل می‌کند. حملات احتمالی در مجرا به شرح ذیل هستند. تکنیک-های حملات مرد میانی و استراق سمع در طبقه‌بندی ارتباط در اینترنت اشیاء دخیل هستند [۴۶، ۳۹، ۴۰].

داده: حریم شخصی کاربران و اعتماد آنها باید حفظ شود تا اینترنت اشیاء کاملا گسترده و پذیرفته شود. حریم شخصی داده و محرمانه بودن برای روندهای تجاری همچنان مسائل بسیار مهمی هستند و یافتن راه‌حل‌های کاربردی نیز چالش برانگیز است. حریم شخصی داده‌های کاربر باید تضمین شود، زیرا کاربران برای اطلاعات شخصی خود به بالاترین میزان حفاظت نیاز دارند. اعتماد، شامل حفظ حریم شخصی کاربر که داده‌های شخصی کاربر را در بر می‌گیرد. انتقال و محاسبه اعتماد در میان گره‌های مختلف در یک اینترنت اشیاء نامتقارن مسأله‌ای چالش برانگیز است. جدول ۱۲، تهدیدهای امنیتی داده با توجه به لایه‌های اینترنت اشیاء را مرور کرده است [۳۹، ۴۷، ۴۸].

ISSN: 2475-3673
http://www.Racj.ir

جدول ۱۲: خلاصه تهدیدهای امنیتی در داخل هر لایه IoT

لایه‌ها	تهدیدها
فیزیکی	دست‌کاری اجزای سخت
پیوند	برخورد، بی‌عدالتی، فرسودگی، بازپخش، حملات فراداده
شبکه	بی‌توجهی، بررسی ترافیک، سیاه چاله، حملات متادیتا

بررسی چهارچوب امنیتی

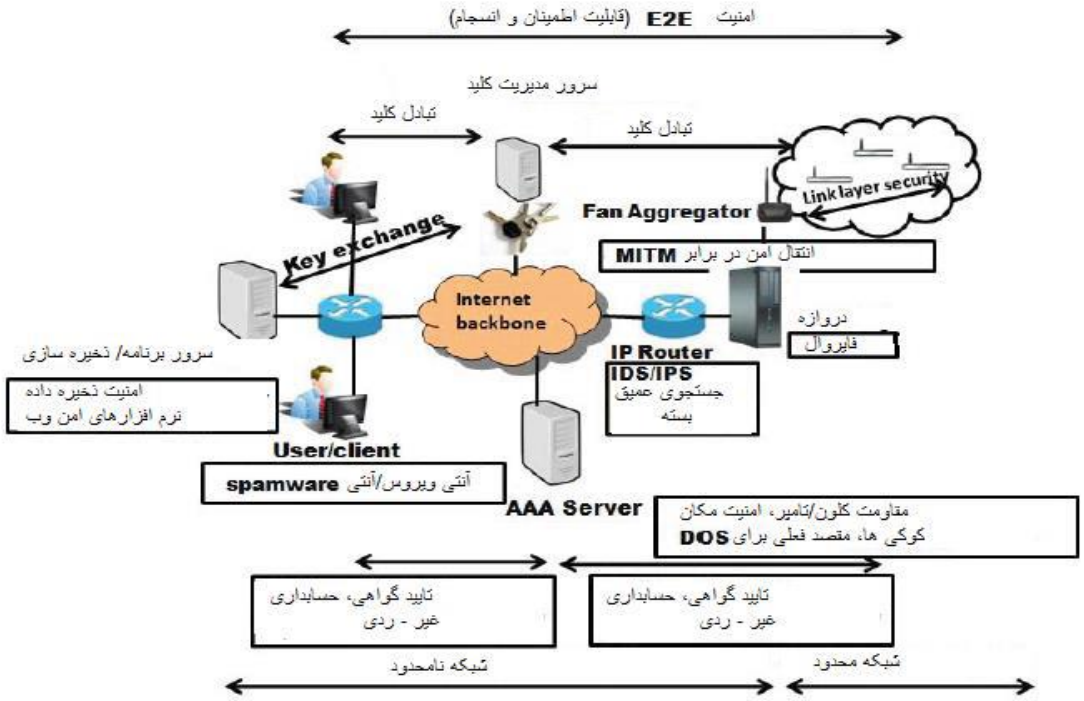
این بخش چهارچوبی ایمن برای جلوگیری از تهدیداتی که در پژوهش مطرح شد معرفی می‌کند. خلاصه‌ای از این دیدگاه را می‌توانید در شکل ۶ مشاهده کنید. در جدول ۱۳، این چهارچوب‌ها به‌عنوان راهکارهایی برای مقابله با تهدیدهای واردشده به هریک از فاکتورهای امنیتی همانند اتصال، تحرک، مقیاس‌پذیری، آدرس‌دهی و شناسایی، محدودیت‌های منبع و تبادل داده آمده است. همچنین، چهارچوب‌های امنیتی شامل امنیت فیزیکی دستگاه یا گره‌نقطه آخر، امنیت راه‌اندازی و ستاپ، احراز هویت، صدور اجازه و حسابداری، انتقال داده و امنیت ذخیره‌سازی، امنیت پروکسی، امنیت مسیریابی و شبکه، امنیت چندلایه و اندازه‌های مشترک امنیتی می‌شود. با این حال، جدول ۱۴، طبقه‌بندی‌ای از عوامل تهدید آمیز در چهارچوب امنیتی اینترنت اشیاء با ذکر مثال‌های کاربردی نشان داده است [۴۹، ۵۰، ۵۱، ۵۲، ۱۳]. علاوه بر این، در ادامه چارچوب امنیتی پیشنهادی بررسی شده است.

جدول ۱۳: چالش‌ها و تهدیدات امنیتی و راهکارهای مقابله با آن‌ها با توجه به چهارچوب امنیتی

زمینه چالش	انواع	حملات و تهدیدها	راهکارها
اتصال	فیزیکی	حملات MITM	استفاده از احراز هویت، صدور اجازه و حسابداری، اطلاع تغییر در سرور یا در دسترس نبودن آن به دستگاه‌ها جهت جلوگیری از درخواست اضافه
	خدمات	حملات انکار خدمات یا DoS	
تحرک	---	حملات DoS، MITM و حملات ردی (انکار)	حفظ تداوم سرویس از طریق مکانیزم‌های انتقال ایمن، احراز هویت، تأیید موجه، قوانین کنترل و حسابداری، تأیید صلاحیت مجدد گره‌ها پس از خلل تداوم سرویس
مقیاس‌پذیری	افقی	حملات DoS	تشخیص دستگاه‌های مجاز و صدور اجازه مختص به آن‌ها و اطمینان حاصل کردن از قابل‌اعتماد بودن گره‌های واسطه
	عمودی	فروچاله[9] و لانه کرمی[10]	
آدرس‌دهی و شناسایی	---	حملات ردی (انکار وظایف) و کلاه‌برداری	استفاده از 6LoWPAN و IPv6 منحصربه‌فرد و همچنین انبار جهانی IP جهت بررسی صحت، سیستم‌های تشخیص نفوذ و الگوریتم‌های پیشگیری و عقب‌گرد
محدودیت منابع	---	دست‌کاری، شبیه‌سازی، نشت اطلاعات، امنیت کاربر و احتمال بروز حملات DoS	استفاده از رمزنگاری تصویری، سخت‌افزار مقاومت در برابر دست‌کاری، مکانیزم‌های انسجام و یکپارچگی و همچنین قطع دسترسی گره مخرب به حافظه و اطلاعات محرمانه
تبادل داده	---	نشت اطلاعات، امنیت کاربر، استهلاک منابع و امکان وجود حملات DoS و MITM	استفاده از رمزگذاری E2E، استفاده از الگوریتم‌های رمزگذاری سبک‌وزن مثل رمزگذاری متقارن و کلید عمومی (PKI) و پارازیت‌ها و کدهای بررسی انسجام

[9] sinkhole
[10] wormhole

ISSN: 2475-3673
http://www.Racj.ir



شکل ۶: چهارچوب امنیتی اینترنت اشیاء [۵۲]

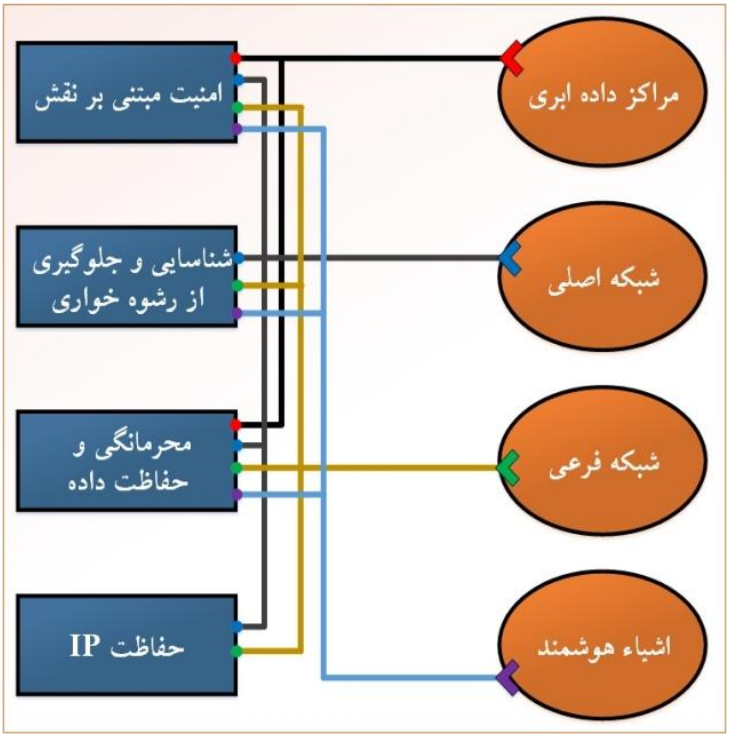
جدول ۱۴: طبقه‌بندی عوامل تهدید آمیز IoT

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 سازمان‌دهی‌شده	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	داخلی، خارجی
بلایای طبیعی	فاکتورهای غیرانسانی	سیل، آتش‌سوزی، رعدوبرق، زلزله، شهاب

ارائه یک چهارچوب امنیتی

چهارچوب امنیتی پیشنهادی همانند یک الگو کاربردی و موثر می‌تواند به‌عنوان ابزار مفیدی در طراحی و پیاده‌سازی پروتکل‌های امنیتی IoT عمل کند. شکل ۷، محیط امنیتی مربوط به یک ساختار منطقی، چهارچوب امنیتی پیشنهادی IoT را نشان می‌دهد. چهارچوب موردنظر شامل سطوح اشیاء هوشمند، شبکه فرعی، شبکه اصلی و مراکز داده ابری است.

ISSN: 2475-3673
http://www.Racj.ir



شکل ۷: الگوی چهارچوب امنیتی پیشنهادی

اشیاء هوشمند: شامل حسگرها، عاملان و سایر سیستم‌های جاسازی‌شده در مرز شبکه است. این بخش، آسیب‌پذیرترین قسمت IoT است. ازاین‌رو، دستگاه‌ها ممکن است در محیط فیزیکی ایمنی حضور نداشته باشند. مهم‌ترین نگرانی در این سطح، فاکتور در دسترس بودن است. اعتبار، یکپارچگی داده‌ها و حفظ حریم خصوصی از دیگر نگرانی‌ها برای مدیران در این سطح است.

شبکه فرعی: این سطح، درارتباط با ارتباطات سیمی و بی‌سیم میان دستگاه‌های IoT است. به‌علاوه، حجم مشخصی از پردازش و تثبیت داده در این سطح صورت می‌گیرد. یکی از مسائل نگران‌کننده اساسی، تنوع بسیار زیاد در پروتکل‌ها و فناوری-های شبکه مورد استفاده در دستگاه‌های IoT و نیاز به توسعه و اجرای یک سیاست امنیتی یک‌دست است.

شبکه اصلی: سطح شبکه هسته، فراهم‌کننده مسیر داده میان پلتفرم‌های مرکزی شبکه و دستگاه‌های IoT است. مسائل امنیتی موجود در این قسمت، آن‌هایی هستند که در شبکه‌های اصلی با آن‌ها مواجه می‌شویم. با این وجود، تعداد بسیار زیاد نقاط پایانی که مدیریت شده و یا با آن‌ها تعاملی صورت می‌گیرد، بار امنیتی قابل‌توجهی را ایجاد می‌کنند.

مراکز داده ابری: این سطح شامل اپلیکیشن‌ها، محل ذخیره‌سازی داده‌ها و پلتفرم‌های مدیریت شبکه است. نگرانی‌های اصلی موجود در این سطح، تعامل‌پذیری، قابلیت همکاری اشیاء و مقوله امنیتی کلان داده[11] است.

در راستای این چهارچوب چهار سطحی، چهار قابلیت عمومی امنیتی شامل امنیت مبتنی بر نقش، شناسایی و مقابله با رشوه‌خواری، محرمانگی و محافظت داده و حفاظت پروتکل اینترنت از عوامل تاثیرگذار در این روند است.

امنیت مبتنی بر نقش: سیستم کنترل دسترسی مبتنی بر نقش[12]، به‌جای توجه به هویت فرد، به نقش وی در سیستم توجه می‌کند. به هر کاربر باتوجه به مسئولیت‌هایش، نقشی به صورت پویا و ایستا اختصاص داده می‌شود. سیستم RBAC استفاده‌های تجاری گسترده‌ای در سیستم‌های شرکتی و همچنین ابر داشته و ابزار قابل فهمی در مدیریت دسترسی به دستگاه-های IoT و داده‌های تولیدی آن‌ها می‌باشد.

[11] Big Data
[12] Role-based access control (RBAC)

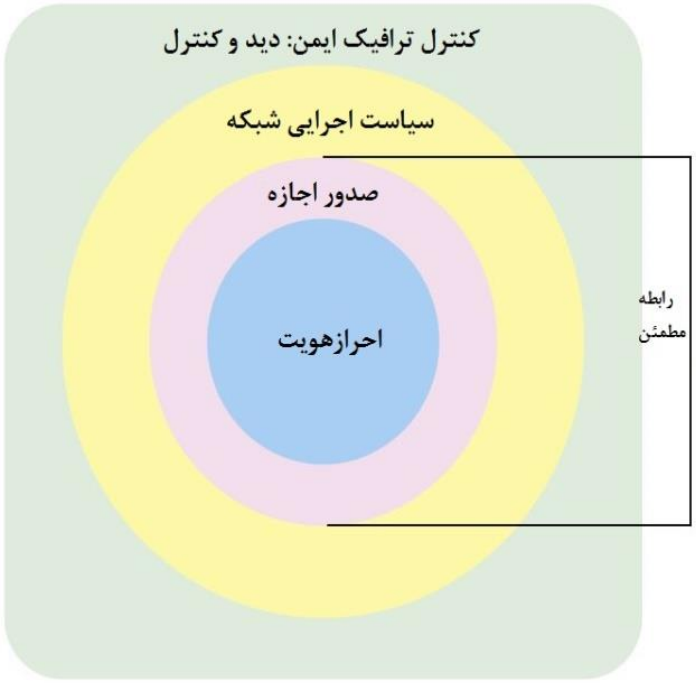
ISSN: 2475-3673
http://www.Racj.ir

شناسایی و مقابله‌با رشوه‌خواری: این تابع اساساً در دستگاه و سطح شبکه فرعی اهمیت دارد، اما به سطح شبکه اصلی نیز رسیده است. تمامی این سطوح، شامل عناصری هستند که در ناحیه خارجی شرکت حضور داشته و توسط وسایل فیزیکی محافظت می‌شوند.

محرمانگی و محافظت داده: این توابع، تمامی سطوح معماری را دربر می‌گیرند.

حفاظت پروتکل اینترنت: حفاظت از داده‌های درحال حرکت دربرابر استراق‌سمع و جاسوسی در تمامی سطوح امری ضروری است.

هدف از این چهارچوب بهبود عناصر امنیتی مهم همانند احراز هویت، صدور مجوز، سیاست اجرایی شبکه و تجزیه و تحلیل ایمن ترافیک است. این عناصر با توجه به طرح پیشنهادی مورد توسعه بهتری قرار خواهند گرفت. هدف از چهارچوب پیشنهادی رسیدن به یک رابطه مطمئن در معماری امنیتی اینترنت اشیاء است. شکل ۸ چهارچوب یک رابطه مطمئن در امنیت IoT را نشان می‌دهد. از این رو، یکی از مفاهیم مهم و مرتبط با این چهارچوب، روابط مطمئن است. در این زمینه، رابطه مطمئن به وضعیتی اشاره دارد که در آن، هریک از طرفین یک ارتباط درمورد هویت و حق دسترسی دیگری اطمینان‌خاطر دارد. عنصر احرازهویت چهارچوب اعتماد، سطح پایه‌ای از اعتماد را فراهم می‌کند که با کمک عنصر صدور اجازه گسترده می‌شود. به عنوان مثال، یک خودرو می‌تواند رابطه مطمئنی با خودروی دیگری از همان فروشنده برقرار کند. زمانی که رابطه مطمئنی میان یک خودرو و شبکه آن ایجاد می‌شود، آن خودرو اجازه دارد که اطلاعات اضافی مانند مقدار کیلومترشمار و یا آخرین رکورد به‌دست‌آمده را به اشتراک بگذارد. در نتیجه، الگوی چهارچوب امنیتی پیشنهادی، می‌تواند چهارچوب ایمن اینترنت اشیاء یعنی داشتن یک رابطه مطمئن را بهبود و توسعه دهد.



شکل ۸: رابطه مطمئن در چهارچوب امنیت IoT

بررسی مکانیزم‌های امنیتی مختلف

مکانیزم‌ها و فاکتورهای امنیتی مهم و بسیاری در حوزه امنیت اینترنت اشیاء وجود دارد. در پژوهش پیش‌رو تعریف و بررسی‌های زیادی بر نوع عملکرد این فاکتورها صورت گرفته است. از مهم‌ترین این فاکتورها جهت مقایسه و بررسی در این بخش می‌توان به فاکتورهایی همانند احراز هویت، محرمانگی، کنترل دسترسی، حریم خصوصی، اعتماد، اجرای سیاست، میان‌افزارهای ایمن و امنیت سیار اشاره کرد. در پژوهشی این فاکتورها و کارهایی که بر اساس این مکانیزهای امنیتی صورت گرفته است، بررسی شده است. از این رو، جدول ۱۵ به بررسی و مقایسه‌ی کاملی از کارهای انجام شده بر اساس فاکتورهای امنیتی

ISSN: 2475-3673
http://www.Racj.ir

پرداخته است. همچنین، جدول ۱۶، به بررسی فاکتورهای امنیتی که به صورت همزمان مورد بررسی قرار گرفته‌اند را نشان می-دهد [۵۳].

جدول ۱۵: بررسی کارهای انجام شده مبتنی بر فاکتورهای امنیتی

فاکتورها	کارهای انجام شده	فاکتورهای مشترک	کارهای انجام شده
احراز هویت	۲۴	احرازهویت و محرمانگی	۲
محرمانگی	۹	احرازهویت و کنترل دسترسی	۵
کنترل دسترسی	۳۱	کنترل دسترسی و محرمانگی	۱
حریم خصوصی	۱۹	حریم خصوصی و کنترل دسترسی	۲
اعتماد	۲۱	حریم خصوصی و احرازهویت	۱
اجرای سیاست	۱۱	اعتماد و کنترل دسترسی	۳
		اعتماد و احرازهویت	۴
میان‌افزارهای ایمن	۱۲	اجرای سیاست و حریم خصوصی	۱
		اجرای سیاست و کنترل دسترسی	۱
امنیت سیار	۱۸	اجرای سیاست و میان‌افزارهای ایمن	۱

نتایج جدول ۱۵ نشان می‌دهد که به ترتیب فاکتورهای کنترل دسترسی، احراز هویت و قابلیت اعتماد بیشتر مورد توجه پژوهشگران جهت توسعه و بهبود امنیت اینترنت اشیاء بوده است. از این رو، می‌توان از این سه فاکتور جهت پژوهش‌های پیش‌رو بیشترین کمک را گرفت. همچنین استفاده از مکانیزم حریم خصوصی، جهت بهبود امنیت بعد از فاکتورهای نام‌برده شده بیشتر مورد توجه قرار گرفته است. با این حال، حریم خصوصی به‌عنوان مهم‌ترین فاکتور امنیتی باید بیشتر مورد توجه قرار گیرد و راهکارهای زیادی جهت توسعه و بهبود امنیت اینترنت اشیاء ایجاد کند.

نتیجه گیری

اینترنت اشیاء به‌عنوان یک انقلاب مدرن در دنیای فناوری اطلاعات تلقی می‌شود. ازاین‌رو چالش‌های پیشرو این فناوری مدرن از قبیل امنیت، استانداردها باید بیشتر موردتوجه محققین قرار بگیرد. در این حوزه، دستگاه‌های IoT می‌توانند به نفع و ضرر کاربران عمل کنند. به همین دلیل مصرف‌کنندگان باید اطمینان از امنیت دستگاه‌ها و اشخاص داشته باشند. این مقاله به بررسی چالش‌ها، تهدیدها، ارائه راه‌حل برای حملات امنیتی در لایه حفره‌های امنیتی و محدودیت‌های پیش روی این تکنولوژی پرداخته است. بااین‌حال، نقص‌های امنیتی موجود در اینترنت اشیاء برای توسعه و پیاده‌سازی IoT در حوزه‌های مختلف بسیار زیان‌آور است. نتایج از بررسی‌ها و مقایسه‌های انجام‌شده این مقاله در تحلیل حملات ممکن بر اساس تهدیدات و آسیب‌پذیری‌ها در محیط IoT، مکانیزم‌های امنیتی می‌تواند به بهبود گروه‌های سخت‌افزار، زیرساخت و اپلیکیشن هوشمند کمک شایانی نماید. همچنین، با به‌کارگیری مکانیزم‌های امنیتی و ترکیب مکانیزم‌ها، می‌توان توسعه امنیت لایه‌های اینترنت اشیاء افزایش داد. از طرفی نتایج از ارائه یک الگوی چهارچوب امنیتی، سعی در ایجاد یک رابطه مطمئن دارد. در آینده، برای رسیدن به یک رابطه مطمئن و بهبود آن، باید فاکتورهای صدور اجازه و احراز هویت توسعه پیدا کند. علاوه بر این، با توجه به بررسی مکانیزهای امنیتی، بهبود فاکتورهای حریم خصوصی، کنترل دسترسی، احراز هویت و قابلیت اعتماد در آینده باید بیشتر موردتوجه پژوهشگران جهت توسعه و بهبود امنیت اینترنت اشیاء قرار گیرد.

ISSN: 2475-3673
http://www.Racj.ir

منابع و مراجع

[1] Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers*, *17*(2), 261-274.
[2] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805.
[3] Hussain, F. (2017). Internet of Things: Building Blocks and Business Models.
[4] Van Tilborg, H. C., & Jajodia, S. (Eds.). (2014). *Encyclopedia of cryptography and security*. Springer Science & Business Media.
[5] Ray, P. P. (2016). A survey on Internet of Things architectures. *Journal of King Saud University-Computer and Information Sciences*.
[6] Stojkoska, B. L. R., & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production*, *140*, 1454-1464.
[7] Bucherer, E., & Uckelmann, D. (2011). Business models for the internet of things. In *Architecting the internet of things* (pp. 253-277). Springer Berlin Heidelberg.
[8] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of things Security: A Survey. *Journal of Network and Computer Applications*.
[9] Borgia, E., Gomes, D. G., Lagesse, B., Lea, R. J., & Puccinelli, D. (2016). Special issue on "Internet of Things: Research challenges and Solutions". *Computer Communications*, *89*, 1-4.
[10] Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431-440.
[11] 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.
[12] Di Pietro, R., Guarino, S., Verde, N. V., & Domingo-Ferrer, J. (2014). Security in wireless ad-hoc networks–a survey. *Computer Communicatio-ns*, *51*, 1-20.
[13] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266-2279.
[14] Bi, Z., Da Xu, L., & Wang, C. (2014). Internet of things for enterprise systems of modern manufacturing. *IEEE Transactions on industrial informatics*, *10*(2), 1537-1546.
[15] Samaila, M. G., Neto, M., Fernandes, D. A., Freire, M. M., & Inácio, P. R. (2017). Security Challenges of the Internet of Things. In *Beyond the Internet of Things* (pp. 53-82). Springer International Publishing.
[16] Ukil, A., Sen, J., & Koilakonda, S. (2011, March). Embedded security for Internet of Things. In *Emerging Trends and Applications in Computer Science (NCETACS), 2011 2nd National Conference on* (pp. 1-6). IEEE.
[17] Raza, S. (2013). *Lightweight security solutions for the internet of things* (Doctoral dissertation, Mälardalen University, Västerås, Sweden).
[18] Gamundani, A. M. (2015, May). An impact review on internet of things attacks. In *Emerging Trends in Networks and Computer Communications (ETNCC), 2015 International Conference on* (pp. 114-118). IEEE.
[19] Abomhara, M., & Køien, G. M. (2014, May). Security and privacy in the Internet of Things: Current status and open issues. In *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on* (pp. 1-8). IEEE.
[20] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146-164.
[21] Alqassem, I., & Svetinovic, D. (2014, December). A taxonomy of security and privacy requirements for the Internet of Things (IoT). In *Industrial Engineering and Engineering Management (IEEM), 2014 IEEE International Conference on* (pp. 1244-1248). IEEE.
[22] Xu, T., Wendt, J. B., & Potkonjak, M. (2014, November). Security of IoT systems: Design challenges and opportunities. In *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design* (pp. 417-423). IEEE Press.
[23] Tamboli, J., Kaneria, R., Patoliya, D., & Ramani, S. (2014). Security in the Internet of Things. *Communication, Cloud and Big Data: Proceedings of CCB 2014*.

ISSN: 2475-3673
http://www.Racj.ir

[24] Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the internet of things: Perspectives and challenges. *Wireless Networks*, *20*(8), 2481-2501.
[25] Kanuparthi, A., Karri, R., & Addepalli, S. (2013, November). Hardware and embedded security in the context of internet of things. In *Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles* (pp. 61-64). ACM.
[26] Massis, B. (2016). The Internet of Things and its impact on the library. *New Library World*, *117*(3/4), 289-292.
[27] Zhang, Y., Shen, Y., Wang, H., Yong, J., & Jiang, X. (2016). On secure wireless communications for IoT under eavesdropper collusion. *IEEE Transactions on Automation Science and Engineering*, *13*(3), 1281-1293.
[28] Ma, H. D. (2011). Internet of things: Objectives and scientific challenges. *Journal of Computer science and Technology*, *26*(6), 919-924.
[29] Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Context aware computing for the internet of things: A survey. *IEEE Communications Surveys & Tutorials*, *16*(1), 414-454.
[30] Bi, Z., Wang, G., & Xu, L. D. (2016). A visualization platform for internet of things in manufacturing applications. *Internet Research*, *26*(2), 377-401.
[31] Barreto, L., Celesti, A., Villari, M., Fazio, M., & Puliafito, A. (2015, August). An authentication model for IoT clouds. In *Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015* (pp. 1032-1035). ACM.
[32] Aman, W., & Snekkenes, E. (2015, December). Managing security trade-offs in the internet of things using adaptive security. In *Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for* (pp. 362-368). IEEE.
[33] Ndibanje, B., Lee, H. J., & Lee, S. G. (2014). Security analysis and improvements of authentication and access control in the internet of things. *Sensors*, *14*(8), 14786-14805.
[34] Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243-259.
[35] Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and challenges for realising the Internet of Things. *Cluster of European Research Projects on the Internet of Things, European Commision*, *3*(3), 34-36.
[36] Choi, J., Li, S., Wang, X., & Ha, J. (2012, June). A general distributed consensus algorithm for wireless sensor networks. In *Wireless Advanced (WiAd), 2012* (pp. 16-21). IEEE.
[37] Ning, H., Liu, H., & Yang, L. T. (2013). Cyberentity security in the internet of things. *Computer*, *46*(4), 46-53.
[38] Covington, M. J., & Carskadden, R. (2013, June). Threat implications of the internet of things. In *Cyber Conflict (CyCon), 2013 5th International Conference on* (pp. 1-12). IEEE.
[39] Akhunzada, A., Gani, A., Anuar, N. B., Abdelaziz, A., Khan, M. K., Hayat, A., & Khan, S. U. (2016). Secure and dependable software defined networks. *Journal of Network and Computer Applications*, *61*, 199-221.
[40] Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011, February). Proposed embedded security framework for internet of things (iot). In *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on* (pp. 1-5). IEEE.
[41] 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.
[42] Yao, X., Chen, Z., & Tian, Y. (2015). A lightweight attribute-based encryption scheme for the Internet of Things. *Future Generation Computer Systems*, *49*, 104-112.
[43] Jiang, H., Shen, F., Chen, S., Li, K. C., & Jeong, Y. S. (2015). A secure and scalable storage system for aggregate data in IoT. *Future Generation Computer Systems*, *49*, 133-141.

ISSN: 2475-3673
http://www.Racj.ir

[44] Moosavi, S. R., Gia, T. N., Rahmani, A. M., Nigussie, E., Virtanen, S., Isoaho, J., & Tenhunen, H. (2015). SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Computer Science*, *52*, 452-459.
[45] Vučinić, M., Tourancheau, B., Rousseau, F., Duda, A., Damon, L., & Guizzetti, R. (2015). OSCAR: Object security architecture for the Internet of Things. *Ad Hoc Networks*, *32*, 3-16.
[46] Hashem, I. A. T., Chang, V., Anuar, N. B., Adewole, K., Yaqoob, I., Gani, A., ... & Chiroma, H. (2016). The role of big data in smart city. *International Journal of Information Management*, *36*(5), 748-758.
[47] Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. *Future Generation Computer Systems*, *56*, 684-700.
[48] Chakrabarty, S., Engels, D. W., & Thathapudi, S. (2015, October). Black SDN for the Internet of Things. In *Mobile Ad Hoc and Sensor Systems (MASS), 2015 IEEE 12th International Conference on* (pp. 190-198). IEEE.
[49] Bagci, I. E., Raza, S., Chung, T., Roedig, U., & Voigt, T. (2013, June). Combined secure storage and communication for the internet of things. In *2013 IEEE International Conference on Sensing, Communications and Networking (SECON)* (pp. 523-531). IEEE.
[50] Jucker, S. (2012). Securing the Constrained Application Protocol. *no. October*, 1-103.
[51] Hartke, K., & Bergmann, O. (2012). Datagram Transport Layer Security in Constrained Environments. *draft-hartke-core-codtls-01 (work in progress)*.
[52] Naccache, D., & Sauveron, D. (Eds.). (2014). *Information Security Theory and Practice. Securing the Internet of Things: 8th IFIP WG 11.2 International Workshop, WISTP 2014, Heraklion, Crete, Greece, June 30-July 2, 2014, Proceedings* (Vol. 8501). Springer.
[53] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146-164.