تامین امنیت دراینترنت اشیابا ارایه روشی استانداردد‌ر مورد فایروال وسیاستهای تحرک

غلامحسین اکباتانی فرد [۱]، سیده حورا فخر موسوی [۲]، مجید مظفری*[۳]

۱-گروه کامپیوتر واحد لاهیجان دانشگاه آزاد اسلامی لاهیجان ایران
۲-گروه کامپیوتر واحد لاهیجان دانشگاه آزاد اسلامی لاهیجان ایران
۳-دانشجو کارشناسی ارشد، گروه کامپیوتر رشت دانشگاه ازاد اسلامی ،رشت ایران

چکیده

اینترنتِ اشیا[۱] (IoT) مفهومی است که اشیاء و روش های ارتباطی مختلفی برای تبادل اطلاعات باهم استفاده می کنند. امروزه IoT بیشتر یک واژه تشریحی از این دیدگاه است که همه چیز باید به اینترنت وصل شود. IoT در آینده به یک مساله اساسی تبدیل خواهد شد، زیرا این مفهوم فرصت هایی را برای سرویس ها و نوآوری های جدید فراهم می کند. همه چیز به هم وصل خواهد شد و اشیاء قادر خواهند بود با همدیگر ارتباط برقرار کنند، در حالی که آنها در یک محیطِ محافظت نشده عمل می کنند. این مورد آخر منجر به یک چالش امنیتی مهم شده است.امروزه، IoT یک نیاز مهم برای استانداردسازی و معماری های نوین است که توضیح می دهند این تکنولوژی چگونه باید پیاده سازی شود و دستگاه های IoT چگونه با یک روش امن باهم ارتباط برقرار کنند. چالش های امنیتی ریشه در این تکنولوژی و چگونگی اکتساب و تغییر اطلاعات توسط آن دارند. در این گزارش یک معرفی از IoT و چگونگی استفاده از آن، و همچنین تهدیداتی که IoT در رابطه با امنیت اطلاعات با آن روبرو است، ارائه شده است. بعلاوه، برخی پیشنهادات نیز درباره چگونگی رفع نیاز اساسی جهت اعتبارسنجی و ارتباط امن در این مقاله برای خواننده فراهم شده است. راه حل های ارائه شده هم مبتنی بر روش های معاصر و هم پروتکل هایی همچون IPSec و DTLS می باشد. این پروتکل ها در محیطی استفاده شده اند که در طول اینترنت و در داخلِ یک شبکه ۶LoWPAN توسعه یافته است.این مقاله علمی مروری به عنوان کارهای آینده حوزه های تحقیقاتی بیان شده است که می تواند به عنوان پایه برای آنها استفاده شود. این حوزه های تخصصی شامل تحلیل های بیشتر برروی آسیب پذیری ها می باشد.

واژگان کلیدی: اینترنت اشیا، IoT، امنیت اطلاعات، پیگی بکینگ،ارتباط امن.

[۱] Internet of things

مقدمه

اینترنت اشیا یک واژه جدید، و در عین حال قدیمی است. قبلا در سال ۱۹۹۹ *کوین آشتون*[۲] در زمانِ یک ارائه در Proctor & Gamble به این مفهوم اشاره کرد. او از این واژه جهت پیوندِ ایده‌ی شناسایی فرکانس رادیویی[۳] (RFID) به اینترنتِ استفاده کرد. بعدها استفاده از این موضوع گسترده شد و شرکت های بزرگ گسترش زیادی را برای IoT پیش بینی کردند [Gartner et al, ۲۰۱۳]. یک پیش بینی این است که تعداد اشیاء متصل شده در جهان یک افزایش سی برابری بین سال های ۲۰۰۹ تا ۲۰۲۰ خواهد داشت، لذا در ۲۰۲۰، تعدادِ ۲۶ میلیارد شیء وجود خواهد داشت که به اینترنت متصل هستند [Gartner, ۲۰۱۳]. دلیل اینکه IoT بسته به دو چیز بسیار بزرگ و کلان شده است: قانون موور[۴] و قانون کوومی[۵]. قانون موور می گوید تعداد ترانزیستورهای روی یک تراشه[۶] تقریبا هر دو سال دوبرابر می شوند [Moore,۲۰۱۵]. این مردم را قادر کرده است کامپیوترهای قدرتمندتری را با تراشه های با همان اندازه توسعه دهند. اینتل، که یک سازنده تراشه نیمه رسانای معروف است، در طول سال ۱۹۷۱ تعدادِ ۲۳۰۰ تراتزیستور برروی یک پردازنده داشت و در سال ۲۰۱۲ پردازنده های فعلی آنها شامل ۱.۴ میلیارد ترانزیستور است [Intel,۲۰۱۵]. این تقریبا یک افزایشِ ۶۱۰۰۰۰ درصدی است که انتظار می رود با همین منوال پیش برود.قانون کوومی بیان می دارد که تعداد محاسبات بر کیلووات/ساعت تقریبا هر سال و هر نیم سال دوبرابر می شود [Koomey et al,۲۰۰۹]. *کوین آشتون*[۷] می گوید این دو قانون با هم ما را قادر می سازند کامپیوترهای قدرتمند و بهینه (از نظر انرژی) بسازیم. با برگرداندن گراف از بالا به پایین برای قانون موور، می توان این تفسیر را کرد که اندازه یک کامپیوتر هر دو سال نصف می شود. با انجام همین کار برای قانون کوومی، این برداشت می شود که مقدار انرژی مورد نیاز برای انجام یک محاسبه با یک نرخ بسیار سریع کاهش پیدا می کند [Ashton,۲۰۱۵]. ترکیب این دو تفسیر به ما می گوید که می توانیم محاسبات یکسانی برروی یک تراشه کوچکتر انجام دهیم، و در عین حال، انرژی کمتری مصرف کنیم- چرا که محاسبات از نظر انرژی بهینه تر می شوند. نتیجه‌ی احتمالی یک کامپیوتر کوچک، قدرتمند و بهینه (از نظر انرژی) است که ما را قادر می سازد سرویس های پیشرفته تری با استفاده از حوزه تراشه کمتر و با صرف انرژی کمتری از قبل ارائه دهیم.تعریف واژه IoT ممکن است کمی سخت باشد، زیرا بسته به اینکه چه کسی واژه را تعریف می کند، ممکن است تعریف های مختلفی داشته باشد . مفهوم پایه‌ایِ IoT عبارت است از متصل کردن اشیاء به هم، به طوری که این «اشیاء» قادر باشند با هم ارتباط برقرار کنند و همچنین، افراد قادر باشند با آنها در ارتباط باشند [Vermesan and Friess,۲۰۱۴]. اینکه این اشیاء چه چیزهایی باشند، بستگی به محیط و حوزه ای که این واژه استفاده شده است و منظور از استفاده از شیء دارد. در

---

۲ Kevin Ashton
۳ radio frequency identification
۴ Moor's law
۵ Koomey's law
۶ chip
۷ Kevin ashton

این گزارش، ما قصد داریم از تعریف ارائه شده توسط بخش استانداردسازی ارتباط راه دور[۸] ITU پیروی کنیم (یک آژانس ملی متحد است که توسط ICT مجوز گرفته است): «یک زیرساختِ جهانی برای جامعه اطلاعات، که امکان سرویس های پیشرفته را از طریق متصل کردن[۹] (فیزیکی یا مجازیِ) اشیاء براساس اطلاعات قابل استفاده و قابل تبادلِ موجود و در حال رشد و تکنولوژی های ارتباطی فراهم می کند». متصل کردن دنیای فیزیکی با دنیای مجازی و اعمال این مفهوم برای همه اشیاء امکان‌های زیادی را در رابطه با امکانِ دسترسی به هر چیز در هر زمان و هرجا آشکار می کند. فراهم کردن امکان‌های جدید تهدیدات جدید، ریسک های امنیتی جدید، و آسیب پذیری های جدیدی را نیز در دنیای اشیا متصل شده به وجود می آورد. اشیا در دنیای فیزیکی چیزهایی هستند که از نظر فیزیکی موجود بوده و از نقطه نظرِ IoT ما قادریم این چیزها را حس کنیم، با آنها کار کنیم و به آنها متصل شویم، اما در دنیای مجازی، «اشیا» چیزهایی هستند که امکان ذخیره، دسترسی و پردازش آنها وجود دارد [ITU,۲۰۱۲].

IoT شامل حسگرهایی برای گرداوری اطلاعات می باشد. حسگرها قبلا در زندگی روزمره استفاده شده اند، با این وجود ممکن است اکثر مردم آن را باور نکنند. تلفن های هوشمند شامل حسگرهای مختلفی از جمله شتاب‌سنج، دوربین، و گیرنده های GPS می باشند. حسگرهای تعبیه شده در جامعه امروزی چیز جدیدی نیستند. *کیون اشتون* گفته است که IoT قبلا اتفاق افتاده است، اما ما نباید آن را در مقایسه با تلفن های هوشمند ببینیم که هم دیده می شوند و هم قابل لمس هستند. RFID یک نمونه از تکنولوژی IoT است، که وجود دارد، اما لزوما دیده نمی شود؛ بنابراین توسعه‌ی IoT ممکن است راه طولانی را بگذارند، بدون اینکه توسط کسی دیده شود.

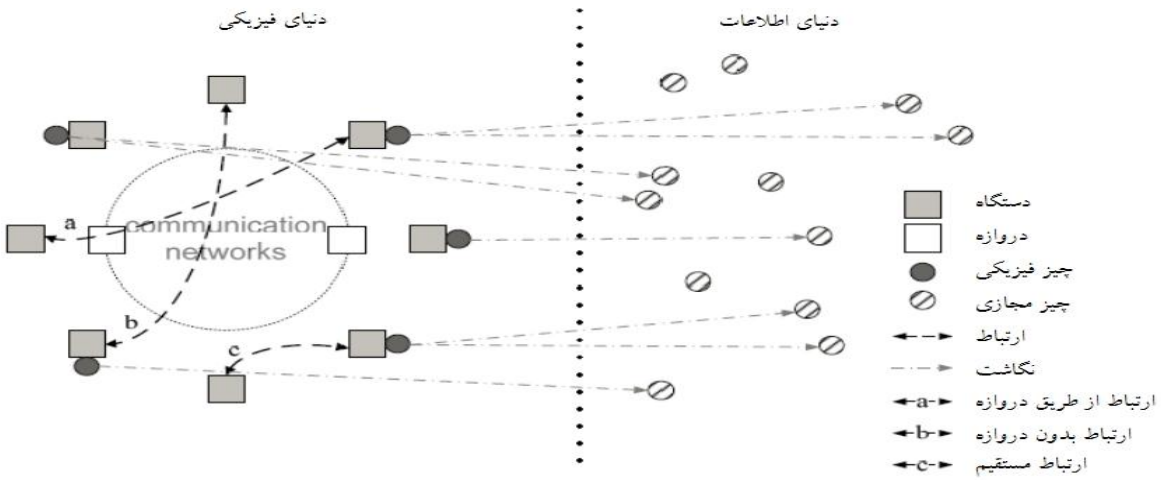
ساختار این مقاله به این صورت میباشد که در بخش ۱سوابقی از اینترنت اشیا ارایه شده است.در بخش ۲ تعریف مسئله ودر بخش ۳ در مورد امنیت اطلاعات مطالبی بیان شده است.در بخش ۴ امنیت اطلاعات مختص اینترنت اشیا آورده شده است.در بخش ۵به موضوع اصلی همان تحرک وفایروال پرداخته شده و یک روش استاندارد سازی پیام ارایه شده است.در تحقیقات و مقالات بعدی خاصیت پیکی بکینگ استاندارد پیام رسانی QLMارایه خواهد شد.در بخش ۶ هم نتیجه گیری مطالب بیان شده است.

۱- سوابق

حیاتی ترین بخش دستیابی به IoT، ارتباط است، زیرا برای متصل کردن دستگاه های مختلف، باید آنها قادر به ارتباط باشند. همه ویژگی های دیگر، همچون حسگری، تحرک ،قابلیت ضبط کردن، ذخیره کردن، و پردازش داده غیرضروری هستند؛ مگر اینکه دستگاه شما یکی از این ویژگی ها را لازم داشته باشد. با این وجود، قابلیت ارتباط، در زمانِ برچسپ گذاری یک دستگاه به عنوان یک دستگاه IoT ضروری است. اینکه این ارتباط چگونه برقرار می شود از اهمیت کمتری

[۸] Telecommunication Standardization Sector
[۹] interconnecting

برخوردار است، چرا که ارتباط واقعی لایه فیزیکی و لایه پیوند داده در داخل IoT را می توان به روش های مختلفی محقق ساخت.



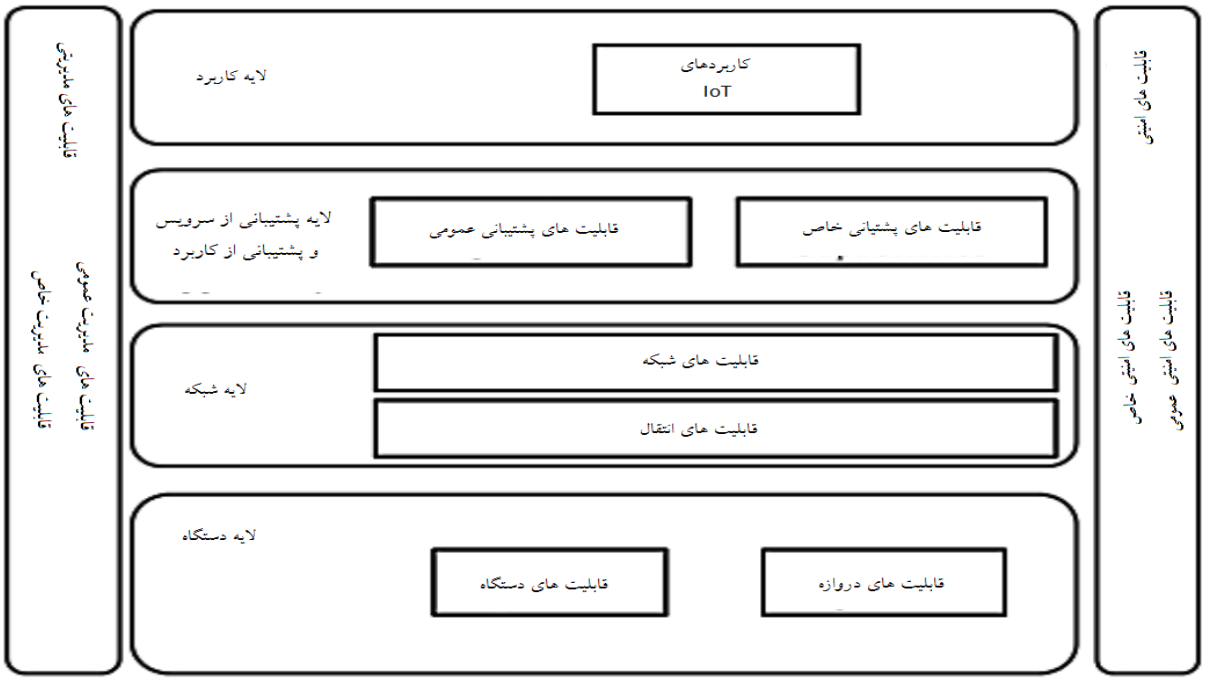
شکل ۱ : نگاهی کلی به اینترنت اشیا (این تصویر با اجازه‌ی مولفین [ITU,۲۰۱۲] استفاده شده است).

حالت C در شکل ۱نشان می دهد که دستگاه ها همیشه نیاز به ارتباط از طریق یک شبکه ارتباطی ندارند. برای مثال، اگر دو دستگاه به هم نزدیک هستند، شاید ارتباط مستقیمِ آنها (مثلا) از طریق یک رادیو با استفاده از تکنولوژی های همچون بلوتوث یا زیگبی[۱۰] آسان تر باشد (این دو پروتکل امکان ارتباط مستقیم را فراهم می کنند). به طور عکس، در حالت A از شکل ۱، یک دستگاه قادر است از طریق یک دروازه و با استفاده از یک پروتکل (مانند IPv۶ برروی یک شبکه شخصی با توان کم (۶LoWPAN)) ارتباط برقرار کند، و سپس دروازه می تواند از طریق پروتکل دیگری همچون (IPv۴) برروی یک شیکه ارتباطی مانند اینترنت ارتباط برقرار کند. حالت B در شکل ۱ دو دستگاه را نشان می دهد که به طور مستقیم به هم وصل شده اند، به طوری که نیازی به دروازه ندارند، که هردو دستگاه به طور مستقیم به شبکه ارتباطی وصل شده اند و لذا با وجود اینکه در دو جای مختلف قرار گرفته اند، قادرند به هم متصل شوند.

۱-۱ مدل مرجع IoT

ITU-T یک مدل مرجع برای IoT تعریف کرده است. این مدل به چهار لایه تقسیم شده است: لایه کاربرد، لایه پشتیبانی از کاربرد و پشتیبانی از سرویس، لایه شبکه و لایه دستگاه (شکل ۲). هرکدام از این لایه ها نیز خود شامل قابلیت های امنیتی و مدیریتی هستند. همانطور که در شکل نشان داده شده است، این قابلیت ها هم شامل قابلیت های خاص، و هم قابلیت های کلی هستند که می توانند از چند لایه عبور کنند. (چند لایه را شامل شوند).

[۱۰] zigbee



شکل۲: مدل مرجع ITU-T برای IoT. گرفته شده از پیشنهادِ ITU-T Y.۲۰۶۰ و استفاده شده با مجوز از مولفین.

۱-۲ واژه ی IoT کجا استفاده می شود؟

واژه IoT در حوزه های مختلفی از جمله، بدن (انسان)، خانه ها، شهرها، صنعت، و محیط های عمومی استفاده می شود.

- در حوزه بدن، IoT امکان حسگری و اتصال را مقدور می سازد، برای مثال، ردیابی فعالیت، وضعیت سلامت و اطلاعات مربوطه دیگر نه تنها زندگی روزمره کاربر، بلکه سلامت او در آینده را از طریق پیشگیری از محیط های بد بهبود می بخشد.
- در رابطه با خانه، IoT اغلب مربوط به نظارت و مدیریت محلی و راه دورِ چراغ ها و وسایل برقی، یا محافظت از گیاهان حیاط از طریق استفاده از یک سیستم آب‌پاشی خودکار است. امروزه، این به یک حوزه بسیار مهم تبدیل شده است، چرا که جاهای بسیاری در حال حاضر با مشکل کم آبی روبرو هستند، لذا رهیافت های سنتی برای آبیاری گیاهان خانه ای و باغچه ها دیگر کارا نمی باشد.
- در رابطه با شهرها، واژه IoT برای توصیف سیستم هایی استفاده می شود که به طور کارایی اطلاعات تولید شده توسط زیرساخت های مختلف را گرداوری و پردازش می کنند. به عنوان مثال می توان به مراکز نظارتی برای چراغ های راهنمایی، چراغ های خیابان، مراقبت دوربین و شبکه نیرو اشاره کرد.

- بهینه سازی عملیات ها، بهره وری عمده، صرفه جویی در منابع، و کاهش هزینه ها معمولا مهمترین اهداف راه حال های IoT اعمال شده در صنعت می باشند. برای مثال، صنعت می تواند از IoT برای مراقبت از دارایی های تجاری، بهبود امنیت محیطی، و حفظ کیفیت و سازگاری در فرایند تولید استفاده کند.
- آخرین (و البته نه لزوما کم اهمیت‌ترین) مورد نظارت محیطی است که IoT می تواند به ما در درک و مدیریت بهتر منابعی که داریم کمک کند. حسگرها می توانند از حیات وحش محافظت کنند، جریان و استفاده از آب را بررسی کنند، آب و هوای محلی را نظارت کنند، استفاده از منابع طبیعی را بررسی کنند، یا قبل و بعد از حوادث طبیعی مردم را از حادثه باخبر کنند.

۲- تعریف مساله

از آنجایی که IoT یک مفهوم نسبتا جدید است، هنوز برای بسیاری از شرکت ها و کارمندان صنعتی به شدت ناشناخته و تعریف نشده است. این دانش محدود ممکن است موجب ترسیدن آنها، ، ناآگاهی کامل از مسائل امنیتی و حریم خصوصی در رابطه با استقرار IoT شود [Weissman,۲۰۱۵]. به همین دلیل است که بسیاری از تاجرها (یا بازاری ها) می خواهند درباره تهدیدات، منافع، معایا، و راه حل های مربوط به امنیت در رابطه با IoT بیشتر بدانند. بعلاوه، آنها می خواهند بدانند چه قابلیتی در امنیت اطلاعات جهت تحقق بخشیدن به امنیت کار (از نظر هزینه) در رابطه با استقرار IoT ضروری است. این دانش وتوانایی باید به انتقال آنها از یک تاجر غیر IoT به یک تاجر IoT کمک کند، چرا که آن، کارکنان و مدیریت را قادر به درک و رفع تردیدات و مسائل مربوط به سرمایه گذاری و ریسک های امنیتی مربوطه می سازد. با این کار، مدیران می توانند یک تحلیل متوازن و سودمند از تطبیق IoT برای یک کاربرد خاص یا چندین کاربرد انجام دهند.

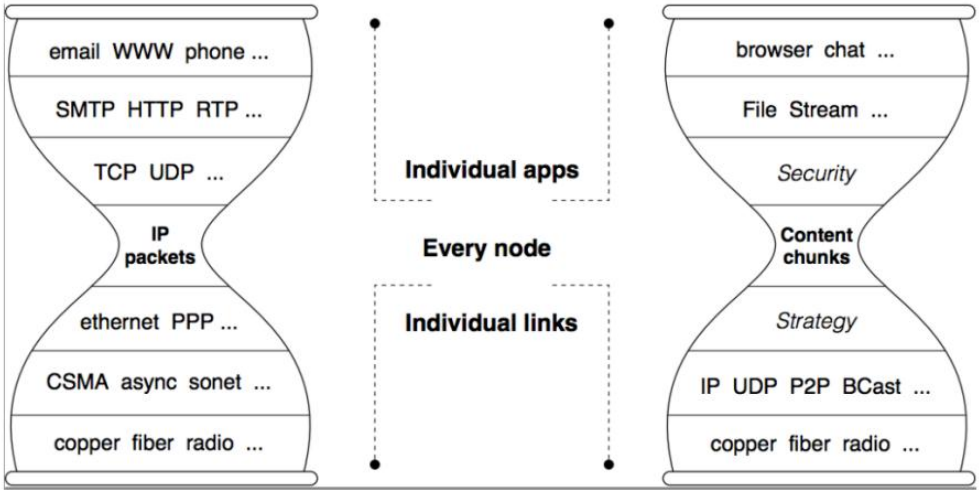
۲-۱ اشیا

مفهوم IoT شامل انواع مختلف تکنولوژی ها و همه روش های مقدور برای ارتباط بین اشیاء (مجازی و فیزیکی) از طریق اینترنت است. گستردگی این مفهوم آن را پیچیده تر می کند، که دلیل آن ناهمگنی مولفه هاست. از آنجایی که هر نوع دستگاهی می تواند از سخت افزار و نرم افزار خاص خود استفاده کند، رنج گسترده ای از سیستم های عامل و برنامه های کاربردی وجود دارد که باید در نظر گرفته شوند. در برخی حالات، ممکن است دستگاه سیستم عامل نداشته باشد، برای مثال، دستگاه هایی وجود دارند که تنها یک رابط شبکه، یک راه انداز، و یک برنامه کاربردی برای تولید داده دارند.

۲-۲ ارتباط

دستگاه های مربوط به فروشندگان مختلف اغلب دارای پروتکل های متفاوتی هستند. در برخی حالات، این پروتکل های شخصی بوده و لذا برای عموم ناشناس هستند. تجربه به ما نشان می دهد که پروتکل های امن نیاز به دیدگاه بازی برای فراهم کردن ارزیابی توانمند، و لذا بدست آوردن مقبولیت و استفاده‌ی گسترده دارند [Forum,۲۰۱۵].

امروزه، دستگاه های IoT به شکل روزافزونی دارای یک اشتراک هستند، و آن استفاده از پروتکل اینترنت (IP) در لایه شبکه از پشته ی پروتکل است. دلیل اینکه این دستگاه ها به طور روزافزون از IP استفاده می کنند، امکان ارتباط از طریق اینترنت است. مدل ساعت شنی معروف[۱۱] (بخش سمت چپ شکل ۳) این مفهوم را به روشنی نشان می دهد، به طوری که همه چیز دربالای IP و IP در بالای همه چیز است [ITU-T,۲۰۱۵]. توجه داشته باشید که بخش سمت راست شکل یک رهیافت دیگر را نشان می دهد که در آن، بسته های داده نامگذاری شده اند، و این بسته های نام گذاری شده مورد درخواست قرار می گیرند.



شکل۳:پشته IP با IP در وسط آن، در مقایسه با آدرس دهی مبتنی بر محتوا با بسته های محتوا در وسط آن. (گرفته شده از شبکه داده نامگذاری شده تحت مجوزهای مشترک خلاق ۳.۰ [Astrand and Yu,۲۰۱۲].

۳- امنیت اطلاعات چیست؟

امنیت اطلاعات یک واژه سایبان مانند برای فرایند ها و متدلوژی های مورد استفاده در حفاظت از اطلاعات، داده ها و سیستم هاست. در رابطه با امنیت اطلاعات، محافظت به معنی پیش گیری از دسترسی، استفاده، افشاء، شکستن، دستکاری یا تخریب بدون مجوز است. امنیت اطلاعات دارای سه اصل اساسی است که باید در نظر گرفته شوند. این سه اصل

[۱۱] hourglass model

عبارتند از قابلیت اعتماد، قابلیت دسترسی، و یکپارچگی [Bosworth et al,۲۰۰۹]. قابلیت جوابگویی[۱۲] به یک اصل مهم تبدیل شده است، و برخی اوقات توسط شرکت های امنیتی در بین این سه اصل قرار می گیرد. این مفاهیم در جدول ۱ شرح داده شده اند.

جدول ۱:اصول استفاده شده در امنیت اینترنت

اصل ها	شرح
قابلیت اعتماد	قابلیت اعتماد مفهومی است که به توانایی حفاظت از داده ها/ اطلاعات در مقابل افرادی که مجوز دسترسی یا مشاهده ندارند، مربوط است.
قابلیت دسترسی	قابلیت دسترسی به توانایی تضمین اعتماد و دسترسی به داده ها/ اطلاعات در زمان نیاز اشاره دارد.
یکپارچگی	یکپارچگی به قابلیت پرهیز از دستکاری بدون مجوز داده ها/ اطلاعات، و در نتیجه اطمینان از دقت و قابلیت اعتماد مربوط است.

Parkerian hexad یک چهارچوب نمونه برای امنیت اطلاعات است. این چهارچوب با حفظ اصول قابلیت اعتماد، یکپارچگی و قابلیت دسترسی، اصول سودمندی[۱۳]، اعتبارسنجی، و مالکیت[۱۴] را اضافه کرده است [Bosworth et al,۲۰۰۹]. این واژه ها در جدول۲ شرح داده شده اند.

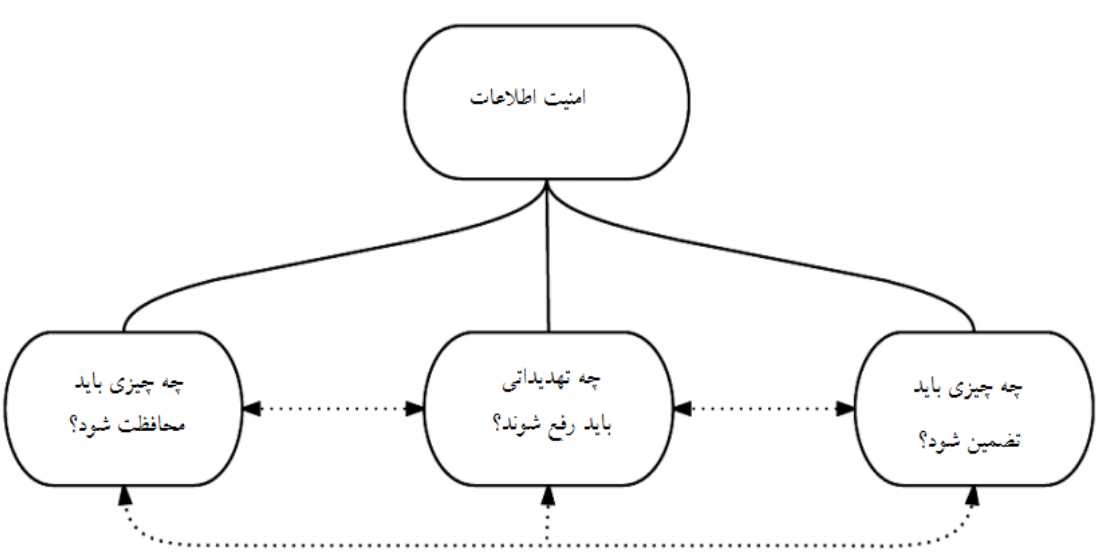
جدول ۲: اصول مربوط به Parkerian hexad

اصول	شرح
سودمندی	سودمندی مفید بودن اطلاعات را شرح می دهد.از دست دادن کلید رمزنگاری برای اطلاعات رمزنگاری شده موجب بی فایده شدن اطلاعات می شود.
اعتبارسنجی	اعتبارسنجی به قابلیت اطمینان از اصل بودن اطلاعات اشاره دارد.
مالکیت	مالکیت یک مفهوم فیزیکی تر است که به از دست دادن مالکیت اطلاعات با ارزش مربوط می شود.

از دست دادن مالکیت ضرورتا به این معنی نیست که قابلیت اعتماد شکسته است. سرقت اطلاعات با ارزشی که رمزنگاری شده است به از دست دادن مالکیت مرتبط است، اما به قابلیت اعتماد ضربه ای نمی زند، زیرا سارق نمی تواند اطلاعات را بخواند. از طرف دیگر، از دست دادن یک فایل با ارزشی که تنها نسخه است، می تواند خطرناک باشد.

[۱۲] Accountability
[۱۳] Utility
[۱۴] possession

چگونگی دستیابی به امنیت اطلاعات ممکن است بسته به اطلاعاتی که باید محافظت شود، متفاوت است. امنیت اطلاعات را می توان به سه سوال تقسیم کرد، تا بهتر بتوان درک کرد کدام مفاهیم باید جهت حفظ اطلاعات مد نظر قرار بگیرند. این سوالات را می توان در شکل ۴ مشاهده کرد. سوالات از این قرارند: «چه چیزی باید محافظت شود؟»، «چه تهدیداتی باید رفع شوند؟» و «چه چیزی باید تضمین شود؟».



شکل ٤: سوالات مربوط به امنیت اطلاعات

۳-۱ چه چیزی باید محافظت شود؟

چه چیزی لازم است از آن محافظت شود؟ آن یک سیستم است یا اطلاعات؟ اگر هدف محافظت از اطلاعات است، باید دانست که آیا اطلاعات محرمانه است، داخلی است، یا برای عموم در دسترس است. اگر اطلاعات عمومی باشند، تنها دسترسی پذیری، قابلیت جوابگویی، ویکپارچگی مرتبط هستند. با این وجود، اگر اطلاعات محرمانه باشند، مفهوم قابلیت اعتماد نیز باید در نظر گرفته شود.

۳-۲ چه چیزی باید تضمین شود؟

این سوال به این مربوط است که کدام یک از این مفاهیم باید تحقق بخشیده شوند. تضمین اینکه سیستم توسط تاثیرات منفی تحت تاثیر قرار نگرفته است، به این معنی است که مطلوب است قابلیت دسترسی تحقق یابد.پاسخ های زیادی برای این سوال وجود دارد و همه پاسخ ها یک یا چند تا از مفاهیم را اعمال می کنند. نمونه هایی در جدول ۳ نشان داده شده اند، و همه این پاسخ ها حداقل به یکی از مفاهیم مرتبط است.

جدول ۳: نمونه پاسخ ها

پاسخ ها	مفهوم (ها)
هیچ شخص نامعتبری نمی تواند به اطلاعات دسترسی پیدا کند.	قابلیت اعتماد
اطلاعات به درستی تحویل داده شده اند.	یکپارچگی، قابلیت جوابگویی
گیرنده می تواند تایید کند که فرستنده چه کسی است	اعتبارسنجی
اطلاعات تحویل داده شده است.	قابلیت جوابگویی، دسترسی پذیری

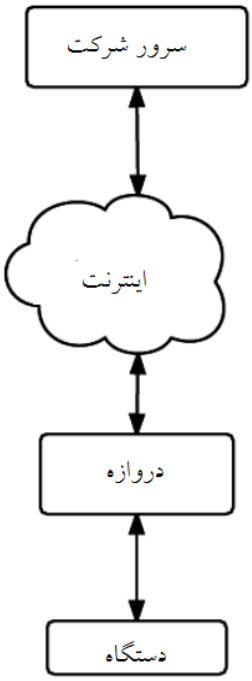
۳-۳ چه تهدیداتی باید رفع شوند؟

این سوال مربوط به این است که چه نوع از تهدیدات مربوط به سیستم/ اطلاعات هستند. آیا تخریب سیستم یا تخریب/ از دست دادن/ تحریف اطلاعات یک تهدید است؟ این تهدیدات تنها مربوط به تهدیدات خارجی نیستند، بلکه تهدیدات داخلی را نیز شامل می شوند. یک تهدید توسط عاملی[۱۵] به وجود می آید که عامل تهدید نام دارد. یک عامل تهدید می تواند تهدیدات عمدی یا تصادفی را منجر شود. عامل های تهدید مختلف منابع مختلف و احتمال حمله مختلف را دارند. یک کاربر که دانش کافی ندارد ممکن است اشتباها اطلاعات را خراب کند. این مساله ممکن است با آگاهی کاربر و از روی عمد نیز رخ دهد.

٤- امنیت اطلاعات در اینترنت اشیا

انجمن جریکو[۱۶] مجموعه ای از نشریات از گروه باز[۱۷] است، که اصولی را در زمان طراحی برای یک آینده de-perimeterised تعریف می کند، که با مفاهیم IoT همخوانی زیادی دارد. De-perimetarisation شامل محافظت از سیستم ها و داده های یک سازمان با همکاری پروتکل های امن، سیستم ها و اعتبارسنجی های سطح داده با حضور یک محدوده خاص بین خود سازمان و دنیای بیرون می باشد [Forum,۲۰۱۵]. در رابطه با IoT، آن یک سناریو را تعریف می کند که یک سازمان برای مثال حسگرهای آب و هوا را نصب کرده است که اطلاعات درباره باد، باران و غیره را گرداوری می کند، و این اطلاعات را به سرور شرکت یا یک ابر[۱۸] جهت بازیابی در آینده ارسال می کند. شکل ۵ این محیط را نشان میدهد.

[۱۵] actor
[۱۶] Jericho Forum
[۱۷] Open Group
[۱۸] cloud



شکل ۵: مثالی از محیط de-perimeterised

برای دستیابی به امنیت اطلاعات در IoT لازم است سیستم ها و داده ها بدون تکیه بر محافظت شبکه پایه، مانند دیوارهای آتش، قادر به محافظت از خود باشند. دیوارهای آتش مانند یک دیوار محافظ جهت امن کردن منابع شرکت در مقابل نفوذگرها عمل می کنند، که در اکثر حالات با IoT مرتبط نیستند. برای سادگی نصب اشیا بیشتر، این اشیا باید قادر به اعمال سطوح سیاست امنیتی خود، حتی در محیط یا شبکه های غیرقابل اعتماد باشند. نیازمندی دیگر این است که مکانیزم های امنیتی ساده و مقیاس پذیر بوده و مدیریت آنها آسان است، که این موضوع تعیین محدوده آنها را ساده کرده است،چرا که همه راه حل ها در همه محیط ها مناسب نیستند [Forum,۲۰۱۵].

تکنیک های زیر برای پذیرفتن معماری de-perimeterised لازم می باشند:

- سیستم اعمال سیاست امنیتی
- سیستم های مدیریت حقوق و شناسه
- رمزنگاری داده ها

٤-١ تهدیدات امنیتی مربوط به اینترنت اشیا

مسائل امنیتی IoT عمدتا به دو ناحیه تقسیم می شوند: تهدیدات مجازی و فیزیکی . تهدیدات فیزیکی با de-perimeterised شدن اشیا بیشتر و بیشتر می شوند. تهدیدات مجازی به شدت با تهدیدات مربوط به هر محیط IT امروزی هم بسته هستند و عمدتا شامل دستیابی به داده ها و اطلاعات یا بدست آوردن کنترل خود دستگاه است. بعلاوه،

بکار بردن روش های استفاده شده در امنیت یک محیط IoT محدودیت دارند، چرا که بسیاری از دستگاه ها از نظر کارایی و توان محدود هستند. از آنجایی که این گزارش اساسا برروی مفهوم امنیت اطلاعات کار می کند، نقطه شروع تحلیل تهدید خود سرمایه است، که همان اطلاعات (داده) می باشد. هیچ عامل تهدیدی شناسایی نشده است، چرا که این تحلیل تهدیدات را به صورت کلی در نظر گرفته و برروی یک تهدید خاص تمرکز نکرده است.
مشخص کردن اینکه کدام تهدیدات به IoT مربوط هستند و با چه آسیب پذیری هایی باید مقابله شود تا هر مولفه ای در محیط IoT امن باشد، با نگاه کردن به نقاط مختلف یک حمله آسان تر است. سه نقطه شناسایی شده حمله عبارتند از: ارتباطی که بین اشیاء اتفاق می افتد، خود دستگاه های IoT، و در حالت سوم، وقتی که یک دروازه استفاده می شود، نقطه گرداوری مرکزی چندین حسگر یا یک کنترلگر برای چندین محرک.

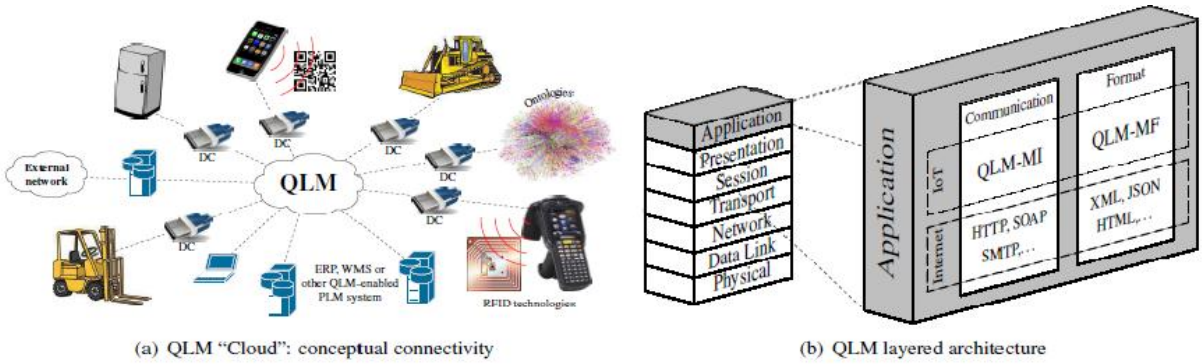
٤-۲ مشخصه های بسیار مرتبط برای امن کردن اینترنت اشیا

کاملا واضح است که اکثر چیزهای مهم در IoT اعتبارسنجی دوجانبه و راهی برای امن کردن ارتباط با هرکدام از «اشیا» هستند. جهت استفاده از مجموعه ای از اشیا، باید نوعی اعتماد بین منابع اطلاعاتی وسینک ها به وجود بیاید. اعتماد جهت باور کردنِ اطلاعاتی که هر چیزی ارسال می کند، نیاز است. در هنگام ارتباط، ما باید مطمئن باشیم که داده ها صحیح هستند، که ابتداء باید مطمئن شویم که ما در یک ارتباط واقعی با یک دستگاه «درست» هستیم و داده های ارسال شده توسط این دستگاه در مسیر رسیدن به مقصد تغییری نکرده اند (یعنی اطمینان از یکپارچگی).
به همین دلیل است که ما برروی اولین گام در فرایند نصب یک محیط IoT، یعنی متصل کردن اشیا، تمرکز کرده ایم. ما می خواهیم قادر به تضمین این باشیم که در حال صحبت با دستگاه درست هستیم، لذا شما در حال ایجاد یک زنجیره اعتماد هستید.

۵- فایروال و سیاستهای تحرک درIOT

اینترنت اشیابرای ارائه یک شبکه که در آن جریان های اطلاعاتی به راحتی می توانند بین هر مجموعه انواع محصولات، دستگاه ها، کاربران و سیستم های اطلاعاتی ارتباط برقرارکنند در نظر گرفته شده است. این دیدگاه به دلیل توسعه پیوسته مفاهیم سیستم های جدید اطلاعاتی و فن آوری ها به واقعیت نزدیک می شود. با این حال، این واقعیت جدید نیاز به توجه ویژه در جنبه های خاصی از اینترنت اشیا مانند امنیت و تحرک است. اول، افراد و شرکت ها امنیت دارایی‌های اطلاعاتی / داده ها را با استفاده از فایروال ها می خواهند، که به ناچار به یک درگیری و به چالش کشیده شدن بین امنیت داده ها و قابلیت استفاده می‌انجامد. دوم، محصولات به طور فزاینده ای در حال تبدیل شدن در قالب تلفن همراه هستند، فعالیت در محیط هایی که در آن تماس با آنها به طور مستقیم با استفاده از آدرس IP شان می تواند مشکل باشد (به عنوان مثال محدودیت های دسترسی). بنابراین در برخی از برنامه های اینترنت اشیا ممکن است فعال کردن ارتباطات دو طرفه از طریق هر نوع فایروال لازم باشد، به عنوان مثال، برای فعال کردن کنترل در زمان واقعی و تعمیر و نگهداری.

در به اصطلاح اینترنت اشیا و سیستم های فیزیکی سایبری (CPS)، کاربران تلفن همراه و اشیاء به صورت پویا به کشف و تعامل با محاسبات ناهمگن، منابع فیزیکی و هچنین داده های مجازی و محیط ها قادر خواهند بود [Gershenfeld et al,۲۰۰۴]. این دیدگاه به دلیل افزایش روزانه مفاهیم و فن آوری ها مانند سخت افزار یا نرم افزار سنسور، معنایی، ابری، مدل سازی داده ها، ذخیره سازی، استدلال، و غیره به واقعیت نزدیک می شود. [Roussos and Kostakos,۲۰۰۹]. میلیاردها دستگاه به اینترنت متصل شده و پیش بینی شده که درسال ۲۰۲۰ به حدود ۵۰-۱۰۰ میلیارد دستگاه برسد. استانداردسازی در نمونه اینترنت اشیا بسیار مهم است زیرا باعث افزایش قابلیت تبادل اطلاعات و توسعه پذیری می شود، اما هنوز هم یک نیاز واقعی برای نسل کافی و به طور کلی سطح نرم افزاری در استانداردهای پیام رسانی اینترنت اشیا وجود دارد. تفسیر اینترنت اشیا ارائه شده واقعی تر است، جایی که اینترنت اشیا به این معنا که "یک سیستم اطلاعاتی عمومی برای دسترسی و هماهنگ سازی هر نوع اطلاعات محصول مرتبط، به طور عمده از طریق اینترنت" استفاده شده است. در این تفسیر، تمرکز به کل چرخه عمر محصول داده می شود، که در آن محصول از طریق مناطق کسب و کار متعدد عمل می کند. در این زمینه، چالش اصلی ارائه رابط استاندارد برای فعال کردن روش های کسب و کار پیچیده و تبادل اطلاعات یکپارچه میان تمام سهامداران کالا و سیستم های درگیر است. طراحی چنین رابط هایی یک گام ضروری به منظور افزایش مدیریت چرخه عمر محصول (PLM) است، در حالی که امکان ایجاد درست یک اینترنت اشیا را ممکن می سازد. با این حال، شرایط مناسب برای یک استاندارد مشترک تبادل داده ها بین سازمان هایی که رسیده اند و یا حتی ارائه شده برای اینترنت اشیا ایجاد نشده است.گسترش تلفن های همراه و دستگاه های محاسبات فراگیر در طول دهه گذشته باعث ایجاد میزبان و تحرک خدمات در اینترنت شده که یک مسئله قابل توجه است. ارائه داده ها به یک میزبان تلفن همراه در سراسر تغییر آدرس شبکه بدون اخلال اتصالات موجود یک چالش اصلی باقی مانده است [Paula et al,۲۰۱۴]. برای حل این مشکل، مردم اقدامات پیشگیرانه را برای اطمینان از امنیت، محرمانه بودن، و یکپارچگی دارایی های اطلاعاتی/ داده ها با استفاده از دیوار آتش و سیستم های پروکسی [Jin et al,۲۰۱۳] که به ناچار به یک درگیری برای به چالش کشیدن بین امنیت داده ها و قابلیت استفاده انجام می دهند. امنیت برای انجام خدمات جدید چالش بیشتری ایجاد می کند، در حالی که قابلیت استفاده به منظور دستیابی به تایید کاربر از آن خدمات نیاز دارد [Chen,۲۰۱۲]. این اساسا درست است که در نظر گرفتن کل چرخه عمر محصول از اطلاعات مربوط به محصول یک منبع ارزشمند برای شرکت هاست و نباید توسط سازمان های دیگر دیده شود. در نظر گرفتن محیط ها با فایروال و سیاست های تحرکی، اجازه دادن به اشتراک گذاری اطلاعات در مد P۲P با وجود حضور فایروال ها، NAT ها، و یا سیستم های مشابه (به عنوان مثال، هنگامی که برای توسعه کنترل زمان واقعی و یا پیش بینی خدمات تعمیر و نگهداری در اینترنت اشیا) ممکن است مفید باشد.



(a) QLM "Cloud": conceptual connectivity (b) QLM layered architecture

شکل ٦: استانداردهای پیام رسانی QLM (QLM-MI و QLM-DF)

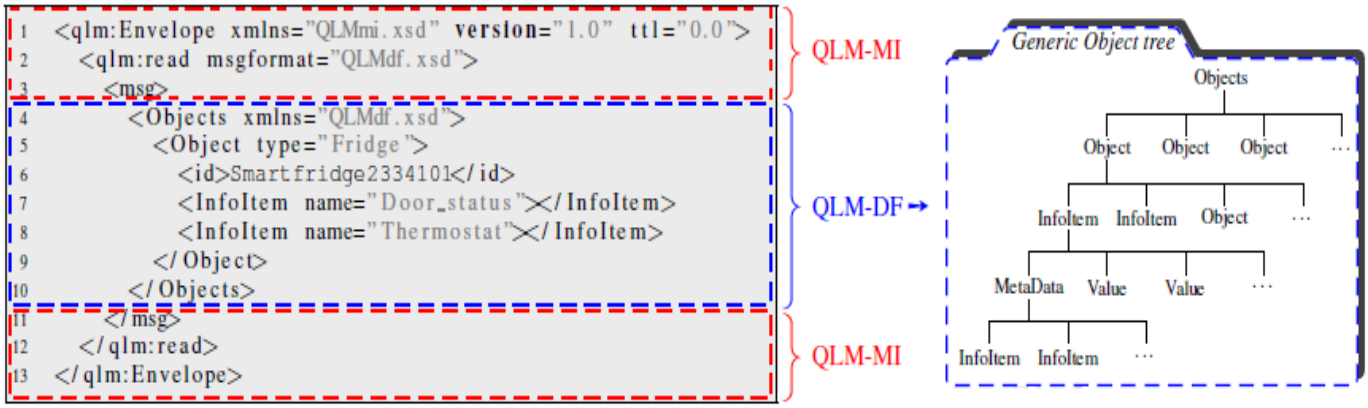
استانداردهای پیام رسانی QLM پیشنهاد می کند که مجموعه ای از رابط ها که قادرند، در میان اشیا دیگر، ارتباطات در زمان واقعی و همچنین ارتباطات دو طرفه با گره های واقع شده در پشت سیستم های فایروال / NAT را قرار دهند. این ویژگی امکان سوء استفاده از قرار دادن درخواست های بیشتر به عنوان بخشی از یک پاسخ به درخواست های قبلی روی همان اتصال را ایجاد می کند. این مفهوم معمولا با عنوان "پیگی بکینگ" اشاره شده است.

۵-۱ استاندارد پیام رسانی QLM

در دنیای QLM، ارتباط بین شرکت کنندگان (به عنوان مثال، محصولات و سیستم های پشت خط) که توسط عبور پیام بین گره ها با استفاده از QLM-MI انجام می شود. "ابر" QLM در شکل۶(a) که عمدا در همان روش برای ابر اینترنتی کشیده شده است. جایی که در آن کاربران اینترنت با استفاده از پروتکل HTTP عمدتا برای انتقال اطلاعات کدگذاری شده HTML که اساسا برای کاربران انسان در نظر گرفته شده استفاده می کنند، QLM-MI برای انتقال اطلاعات مربوط به چرخه عمر که به طورعمده برای استفاده و پردازش توسط سیستم های اطلاعات خودکار در نظر گرفته شده است. در روش مشابه به عنوان HTTP می تواند برای حمل و نقل محموله نیز استفاده شود اگرچه در فرمت های دیگر ازHTML، مانند QLM می توان برای حمل و نقل محموله در تقریبا هر فرمتی استفاده کرد. XML در حال حاضر ممکن است رایج ترین فرمت برای محموله های مبتنی بر متن به دلیل انعطاف پذیری که فراهم می کند باشد که فرصت های بیشتری برای ساختارهای پیچیده داده ای.ارائه می کند، اما از برخی دیگر مانند JSON، CSV نیز می توانید استفاده کنید (شکل۶(b)).

شکل۷: فرمت داده های QLM : "شیء" عمومی یک درخت و به عنوان مثال از یک پیام QLM با تکیه بر آن درخت

QLM-DF تا حدودی همان نقش در اینترنت اشیا را کامل تر انجام می دهد مثل HTML برای اینترنت، به این معنی که QLM-DF مدل توصیفی برای محتوای در اینترنت اشیا است. اطلاعات کد گذاری شده با استفاده از QLM-DF را می توان توسط هر پروتکل تبادل اطلاعات، مانند ،JMS WSDL / SOAP و یا خدمات پیام رسانی ebXML (شکل۵(b)) استفاده کرد.



در کوتاه مدت، QLM-MI و QLM-DF نهادهای مستقل که در لایه کاربردی مدل OSI مقیم هستند، همانطور که در شکل۶ (b) نشان داده شده، که در آن QLM-MI به عنوان سطح ارتباطات مشخص شده و به QLM-DF به عنوان سطح فرمت مشخص شده است.

۵-۱-۱ فرمت داده QLM (QLM-DF)

QLM-DF به عنوان یک هستی شناسی ساده با استفاده از طرح XML، که به اندازه کافی برای نمایش "هر شی" و اطلاعاتی که برای تبادل اطلاعات در اینترنت اشیا مورد نیاز است مشخص شده است. عمدا در یک روش مشابه به عنوان ساختمان داده در برنامه نویسی شی گرا تعریف شده است. به عنوان یک سلسله مراتب با عنصر "اشیاء" و ساختار عنصر بالای آن ساخته شده است. عنصر "اشیاء" می تواند شامل تعدادی از زیر عناصرهای "شی" باشد. شکل ۷ دیدی به هر دو سلسله مراتب عمومی/ درخت شی و نمونه ای از یک پیام QLM است که به ساختار این درخت شی احترام می گذارد. در این مثال، یک شی منحصر به فرد از نوع یخچال (به ردیف ۵ از پیام های XML نگاه کنید) در نظر گرفته شده است. عناصر "شی" می تواند دارای هر تعداد از خواص باشند، که به عنوان اطلاعات آیتم اشاره شده است، و همچنین به عنوان زیر عناصر "شی". در مثال ما، شی یخچال دو اطلاعات آیتم به نام وضعیت درب و ترموستات (به ردیف ۷ و ۸ نگاه کنید). در نتیجه درخت شی شامل هر تعداد از سطوح می باشد. هر شی دارای یک زیر عنصر اجباری به نام "ID" است که به شناسایی شی می پردازد (به ردیف ۶ نگاه کنید). "id" را ترجیحا باید به صورت جهانی منحصر به فرد باشد و یا حداقل برای نرم افزار خاص، دامنه، و یا شبکه ای از سازمان های درگیر منحصر به فرد باشد.

در برنامه نویسی شی گرا، اشیاء توسط سلسله مراتب از همدیگر توسط مرجع و یا اشاره گر آگاه هستند. QLM-DF، نیز مانند مراجع شی که با استفاده ازعنصر شی "ID" ساخته شده اند بوجود آمده اند. با این حال، در اینترنت اشیا، "ID" به یک محل حافظه خاص اشاره نمی کند اما به یک شی اینترنت اشیا که اطلاعاتشان را حتی ممکن است در سیستم های اطلاعات متعدد و سازمان ها پخش کنند اشاره می کند. روش ها و سیستم های مختلف برای کشف چنین اطلاعاتی توزیع شده ای پیشنهاد شده است. ساده ترین مکانیزم شامل URL در شناسه خود است که توسط هوویو و همکاران ارائه

شده است.[Huvio et al,۲۰۰۲]، و سپس برای بازیابی اطلاعات با لینک دادن شی توسط فراملینگ و همکاران پیشنهاد شده است. روش های جدید هنوز برای حل این مسئله توسعه داده شده اند، که از محدوده این گزارش فراتر است.

۲-۱-۵ رابط پیام رسانی QLM (QLM-MI)

QLM-MI برای رفع الزامات متعدد اینترنت اشیا تعریف شده است. یکی از خصایص بارز QLM-MI این است که گره های QLM به هر دو حالت "سرور" و یک "مشتری" عمل می کنند، بنابراین به صورت مستقیم با هم دیگر و یا با سرورهای پشت خط به شیوه P۲P ارتباط برقرار می کنند. نمونه های معمولی از داده های مبادله شده قرائت سنسور، چرخه عمر حوادث، درخواست برای داده های تاریخی، اطلاعیه ها، و غیره هستند. اول، پیام های QLM-MI "پروتکل اگنوستیک" هستند،به طوری که آنها می تواند برای تبادل از HTTP، SOAP، SMTP، FTP و یا پروتکل های مشابه استفاده کنند. مناسب ترین پروتکل برای استفاده به نرم افزار و همچنین مکانیزم های امنیتی از پروتکل ها بستگی دارد. این عدم وابستگی به پروتکل های خاص ارتباطاتی QLM را از بسیاری (و یا بیشتر) از دیگر استانداردهای پیام رسانی اینترنت اشیا متفاوت می کند. دوم، سه عملیات اساسی(نوشتن،خواندن ولغو) اما پایه ای در QLM-MI تعریف شده است.یکی دیگر از ویژگی های مهم QLM-MI این است که پیام های QLM "خود شامل" هستند به این معنا که همه اطلاعات لازم برای فعال کردن دریافت کننده که مسئولیت رسیدگی به پیام که در داخل خود پیام است را بر عهده دارد(مثال: اقدامات برای انجام این کار، آدرس پاسخ به تماس و. . .).

در مقالات بعدی به شبیه سازی و پیاده سازی روش ارایه شده و همچنین به خاصیت پیگی بکینگ (ارتباط دو طرفه ناهمزمان)خواهیم پرداخت.

٦. نتیجه گیری

IoT شامل اشیاء مختلف با قابلیت های متفاوت است که روش مشترکی برای ارتباط جهت امکان انتقال اطلاعات دارند (یک زنجیره ارتباطی از طریق یک شبکه ارتباطی)، که این اطلاعات توسط دو یا چند شیء درک می شوند تا یک فرایند را کاراتر کنند؛ که این کار از طریق کاهش فاکتورهای انسانی و تعامل او انجام می شود.

اشیاء هم شامل اشیاء فیزیکی و هم مجازی هستند، اما محدود به این دو نمی باشد:

- دستگاه های الکترونیکی (مثل کامپیوترها، تلفن های همراه، تلویزیون ها، ماشین‌ها، و ربات ها)
- حسگرها (که از طریق دستگاه ها یا دروازه هم متصل می شوند)

امنیت اطلاعات واژه ای است که برای توصیف فرایندهایی جهت امن کردن داده ها و سیستم ها استفاده می شود. نمونه ای از چنین فرایندی تحلیل یک تهدید یا آسیب پذیری است، که می توان از آن برای شناسایی تهدیدات و در نتیجه،

شناسایی و ارزیابی راه حل های امنیتی برای یک محیط IoT استفاده کرد. براساس تحلیل های ما، گروهی از تهدیدات مجازی و فیزیکی جهت ارائه یک دید کلی از نیازمندی های امنیتی مورد نیاز ارائه شد.

چالش ها و فرصت های جدید با اینترنت اشیا به وجود می آید، که در آن اشیایی از دنیای واقعی شبیه دنیای مجازی است، بنابراین امکان اتصال به هر نقطه، در هر زمان و برای هر چیزی. با این حال، بر اساس تجربه ما با اینترنت اشیا و پیام رسانیهای مختلف و ارتباطات استاندارد مربوط به آن، و همچنین تجربه ما از ایجاد پیاده سازی های متعدد از اینترنت اشیا در حوزه های مختلف، ما ادعا می کنیم که یک نیاز واقعی به اندازه کافی عمومی و کلا قابل اعمال در سطح برنامه اینترنت اشیا استاندارد پیام رسانی وجود دارد.

منابع:

Gartner, "Gartner Says the Internet of Things Installed Base Will Grow to ۲۶ Billion Units By ۲۰۲۰," Gartner, ۱۲ December ۲۰۱۳. [Online]. Available: http://www.gartner.com/newsroom/id/۲۶۳۶۰۷۳. [Accessed ۰۲ April ۲۰۱۵].

G. E. Moore, "Cramming More Components onto Integrated Circuits," [Online]. Available: http://www.cs.utexas.edu/~fussell/courses/cs۳۵۲h/papers/moore.pdf. [Accessed ۲۴ April ۲۰۱۵].

Intel, "Intel Chips," ۷ December ۲۰۱۳. [Online]. Available: http://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/history-intel-chips-timeline-poster.pdf. [Accessed ۲۴ April ۲۰۱۵].

J. G. Koomey, S. Berard, M. Sanchez and H. Wong, "Assesing Trends In The Elecritcal Efficiency Computation Over Time," ۲۰۰۹.

K. Ashton, "Kevin Ashton. The Internet of Things. Seoul, June ۱۹, ۲۰۱۴ - YouTube," ۱۹ June ۲۰۱۴. [Online]. Available: https://www.youtube.com/watch?v=xSYkp۸_Dn۲E. [Accessed ۱۵ April ۲۰۱۵].

O. Vermesan and P. Friess, Internet of Things - From Research and Innovation to Market Deployment, Aalborg Ø: River Publishers, ۲۰۱۴.

ITU Telecommunication Standardization Sector, "ITU-T Recommendation database," ۲۰۱۲. [Online]. Available: http://handle.itu.int/۱۱.۱۰۰۲/۱۰۰۰/۱۱۵۵۹-en?locatt=format:pdf&auth. [Accessed ۱۳ April ۲۰۱۵].

C. G. Weissman, "We Asked Executives About The Internet Of Things And Their Answers Reveal That Security Remains A Huge Concern," Business Insider, [Online]. Available: http://www.businessinsider.in/We-Asked-Executives-About-The-Internet-Of-Things-And-Their-Answers-Reveal-That-Security-Remains-A-Huge-Concern/articleshow/۴۵۹۵۹۹۲۱.cms. [Accessed ۱۰ April ۲۰۱۵].

Jericho Forum, "Jericho Forum Commandments," ۲۰۰۷. [Online]. Available: https://collaboration.opengroup.org/jericho/commandments_v۱.۲.pdf. [Accessed ۱۳ April ۲۰۱۵].

ITU-T, "A Handbook on Internet Protocol (IP)-based Networks and Related Topics and Issues," ۲۰۰۵. [Online]. Available: http://www.itu.int/ITU-T/special-projects/ip-policy/final/IPPolicyHandbook-E.pdf. [Accessed ۱۳ April ۲۰۱۵].

S. Bosworth, E. Whyne and M. Kabay, Computer Security Handbook, Fifth Edition, John Wiley & Sons, ۲۰۰۹.

L. Astrand and T. Yu, "Deprecate DES, RC۴-HMAC-EXP, and Other Weak Cryptographic Algorithms in Kerberos," RFC ۶۶۴۹ (Draft Standard), July ۲۰۱۲. [Online]. Available: https://tools.ietf.org/html/rfc۶۶۴۹. [Accessed ۹ June ۲۰۱۵].

N. Gershenfeld, R. Krikorian, D. Cohen, The Internet of Things, Scientific American. ۲۹۱ (۴) (۲۰۰۴) ۷۶–۸۱.

G. Roussos, V. Kostakos, RFID in pervasive computing: State-of-the-art and outlook, Pervasive andMobile Computing. ۵ (۱) (۲۰۰۹) ۱۱۰–۱۳۱.]

S. Paula, R. Jaina, M. Samakab, J. Pan, Application delivery in multi-cloud environments using software defined networking, Computer Networks, ۶۸ (۲۰۱۴), ۱۶۶–۱۸۶.

X. Jin,L. E. Li, L. Vanbever, J. Rexford, Softcell: Scalable and flexible cellular core network architecture, in: Proc. ۹th ACM conference on Emerging networking experiments and technologies, ۲۰۱۳, ۱۶۳–۱۷۴.

L. Chen, Application perspectives for active safety system based on internet of vehicles, in: Proc. FISITA ۲۰۱۲ World Automotive Congress, ۲۰۱۲, ۱۴۷–۱۵۲.

E. Huvio, J. Gr¨onvall, K. Fr¨amling, Tracking and tracing parcels using a distributed computing approach, in: Proc. ۱۴th Annual conference for Nordic researchers in logistics, ۲۰۰۲, ۲۹–۴۳