اینترنت اشیاء و چالشهای امنیتی آن

محمدرضا مصلحی، گروه مهندسی کامپیوتر- دانشگاه کاشان ، گروه کامپیوتر موسسه آموزش عالی جهاددانشگاهی استان اصفهان
moslehi@acecr.ac.ir
حسین ابراهیم پور کومله،استادیار گروه مهندسی کامپیوتر- دانشگاه کاشان
ebrahimpour@kashanu.ac.ir

Archive of SID

چکیده
اینترنت اشیا(IOT) بعنوان یک فناوری نوظهور با ترکیب دو عرصه ی دیجیتالی و فیزیکی، دسترسی به فناوری اطلاعات را گسترده تر ساخته است. اینترنت اشیاء همچنانکه به سمت فراگیر شدن پیش میرود زندگی انسانها را هر چه بیشترتحت الشعاع خود قرار خواهد داد. برخی از چالشهای مهم مرتبط با توسعه این پدیده موضوع امنیت آن بوده که در تمام لایه های آن و حتی بطور خاص در لایه های منفرد مورد نیاز است. با توجه به ساختار و کاربردهای اینترنت اشیاء و همچنین تهدیدات و چالش های موجود در فضای سایبری نخست نیازهای امنیتی را بررسی کرده و سپس با بررسی برخی روشهای امن سازی اینترنت اشیاء، یک روش با توجه به رویکردهای مورد بحث را پیشنهاد می کنیم.
کلمات کلیدی: اینترنت اشیاء، امنیت، حریم خصوصی، امنیت لایه ای

1- مقدمه

حدود دو دهه است که اینترنت راه خود را به خانه های مردم باز کرده است. با این وجود تغییری که در نحوه ارتباطات ایجاد کرده، شگرف بوده است. اینترنت عادت های روزمره ما همچون خرید، تماس با آشنایان وسفر و ... را دگرگون کرده است. در آینده نفوذ اینترنت به مراتب بیش از امروز خواهد بود و این دانشمندان و نظریه پردازان حوزه فناوری اطلاعات را به فکر ایده پردازی دراینترنت اشیاء انداخته است. اینترنت اشیاء، حضور فراگیر اشیاء متنوع همچون برچسب های RFID، حسگرها، عملگرها، گوشی های هوشمند و ... در اطراف ماست که با شبکه شدن و داشتن آدرس های منحصر به فرد قادرند با یکدیگر تعامل کرده و خدماتی را به ما ارائه دهند. دستگاههایی که هر روز از آنها استفاده می کنیم (مانند یخچال و فریزر، اتومبیل، فن ها ، چراغ ها) و فن آوری های عملیاتی مانند آنچه که در سطح کارخانه یافت می شود، در حال تبدیل شدن به موجودیتهای متصل جهانی هستند. این دنیای اشیاء متصل شده است - جایی که انسان ها با دستگاه ها تعامل داشته و ماشین ها نیز با ماشین های دیگر صحبت می کنند (M2M).

پیش بینی می شود که تا سال 2025 میلادی تعداد وسایل متصل به اینترنت به بیش از 50 میلیارد برسد. [1] اینچند برابر بیشتر از تعداد افراد روی کره زمین خواهد بود و شامل اتومبیلها، وسایل منزل، و حتی البسه شما نیز خواهد شد. با چنین گسترشی موضوع امنیت برای IoT امری چالش بر انگیز خواهد بود، که در ادامه مروری بر نیازمندیهای آن خواهیم داشت.

www.SID.ir

2- اینترنت اشیاء و کاربردهای آن

توسعه انواع جدید حسگرها و فعال کننده ها در ترکیب ارتباطات شبکه ای فراگیر و رو به رشد، مفهوم اینترنت اشیاء را شکل میدهد[2]. عوامل زیادی از جمله کاهش قیمت تجهیزات IoT و تقاضای زیاد کاربران برای خدمات جدید در تکامل اینترنت و IoTدخیل هستند. با توجه به پیشرفتهای اخیر شاهد ساخت تجهیزاتی هستیم که علاوه بر اینکه سیار هستند، پوشیدنی بوده و یا دستگاههای ادغام شده ای با حافظه و قدرت پردازشی بالا و مجهز به تکنولوژیهای حسگر متنوع هستند. افزایش کارایی دستگاههای IoT منجر به ارایه خدمات بیشتر و بهتر به کاربر نهایی خواهد شد. تا چند سال آینده شاهد نفوذ گسترده ی تراشه های با قابلیت ارتباط و حسگری به تمام انواع اشیاء فیزیکی خواهیم بود، که کاربردهایی نظیر موارد زیر را هر چه بیشترگسترش میدهد:

- خانه های هوشمند (کنترل محیطی و لوازم هوشمند)
- شهر هوشمند (کنترل منابع مثلا روشنایی معابر ، مدیریت زباله ، مدیریت آب و انرژی ، کنترل ترافیک و..)
- صنعت (کنترل فرآیند)
- ساختمان سازی (مدیریت ساخت هوشمند)
- افراد (خدمات موقعیت ، مدیریت و نظارت بر سلامت و...)

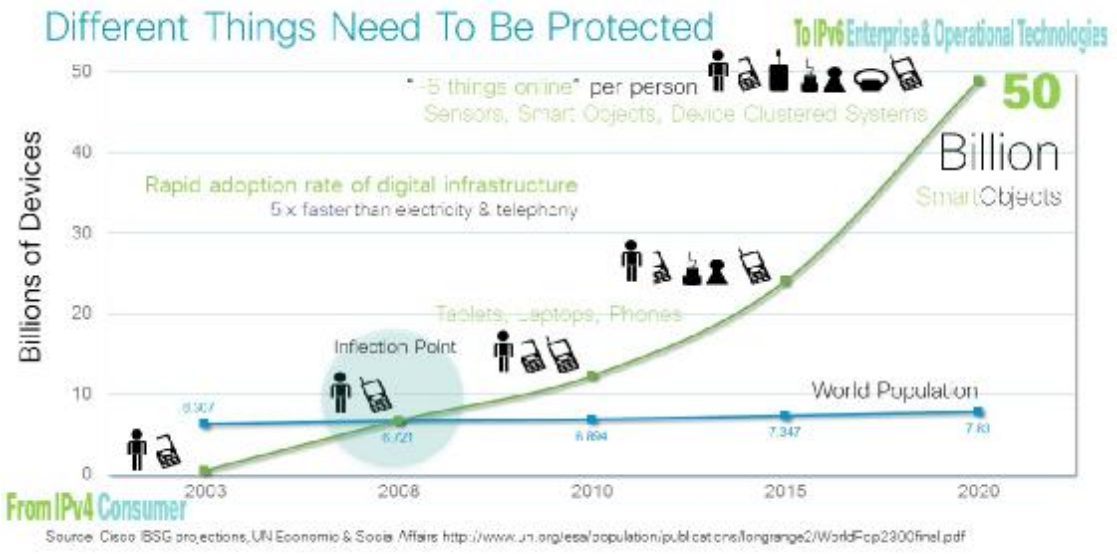
توسعه حسگرها و سیستم های بر اساس IoT، این عوامل را علاوه بر اینکه محبوب تر میکند، باعث میشود در همه جا حضور داشته و هر چه بیشتر شخصی شود. بر طبق پیش بینی گارتنر بیش از 50درصد ارتباطات اینترنتی بین تجهیزات و دستگاههای IoT بوده و با گسترش استفاده از این فناوری که پیش بینی می شود تعداد آنها تا سال 2020 به 30 میلیارد برسد[3] ارزش تجاری آن نیز از 1 میلیارد دلار سال 2015 به 48 میلیارد دلار در سال 2025 خواهد رسید. [1]

3- رشدIoT

در سال 2008 یک نقطه عطف رخ داد، و آن زمانی بود که تعداد اشیایی که به اینترنت متصل بودند از جمعیت انسانی پیشی گرفت. نرخ پذیرش IoT نزدیک به حداقل پنج برابر سریعتر از نرخ پذیرش برق و تلفن است، این موضوع در شکل 1 نشان داده شده است. این برابر با شش شی برای هر فرد روی زمین است [4] .یک روند جالب که به رشد IoT کمک شایانی کرده انتقال اینترنت از نسخه 4 پروتکل IP به نسخه 6 آن پروتکل است. اگر نسخه 4 را مبتنی بر مصرف کننده هایی مثل لپ تاپ ها و تبلت ها با مفهوم فناوری اطلاعات (IT) بدانیم، نسخه 6 این پروتکل مبتنی بر فناوری عملیاتی (OT) از تعاملات ماشین به ماشین ها بوده که شامل حسگرها، اشیای هوشمند و سیستمهای خوشه ای (به عنوان مثال، شبکه هوشمند) است.

Archive of SID

www.SID.ir



شکل 1 رشد IoT

از منظر تکنولوژیکی، سه محرک اصلی در رشد IoT نقش دارند:

- **رایانش فراگیر**: با هوشمندی در اشیایی در لبه، به عنوان مثال، سیستم عامل های سبک وزن مانند TinyOS در سیستم عامل های کامپیوتری بسیار کوچک.
- **استفاده گسترده از IP** : با همگرایی پروتکل ها برای اجرای رویIP به جای حمل و نقل اختصاصی. همچنین پذیرش و پشتیبانی بیشتر از IPv6 در شبکه های حامل.
- **اتصال همه جانبه**: از جمله اتصال سلولی، رادیویی و ثابت. این شامل شبکه های توان پایین، شبکه های مش بی سیم شخصی است که بطور خاص مناسب سنسورها است.

اساسا پیشرفت و توسعه در این تکنولوژی ها امکان توسعه دستگاه های IoT مانند سنسورهایی با قابلیت های محاسبات، ذخیره سازی و شبکه را در فاکتورهای بسیار کوچک با نیازمندیهای کم انرژی فراهم ساخته است. محققان و پیشگامان اولیه، پیشرفت های فن آوری های بی سیم، از جمله رادیو و ماهواره، کوچک سازی و صنعتی شدن دستگاه ها؛ و افزایش پهنای باند، محاسبات و قدرت ذخیره سازی را ترغیب می کنند. همه اینها فرصتی برای کاهش هزینه های مدیریتی و عملیاتی با تبدیل این سیستم ها از پلت فرم های قدیمی، مانند Modbus یا دیگر پروتکل های ارتباطی سریال، به زیرساخت های با قابلیت IP را فراهم میکند.

4- چالش امنیت در IoT

دراین شرایط هرچند این تجهیزات در تمام جنبه های زندگی شخصی حضور داشته و آن را کنترل کرده و از مدلهای تجاری جدید حمایت میکنند و باعث افزایش کارآمدی بسیاری از کاربردها شده و نهایتا سبب بهتر شدن زندگی افراد میشوند، ولی طبیعتا مخاطرات آن نیز بطور قابل توجهی بیشتر بوده و بنابراین به مولفه های امنیتی نیرومندی نیاز است. چنانچه میدانیم نیازمندیهای

Archive of SID
www.SID.ir

امنیتی در اینترنت و تکنولوژیهای ارتباطی و فناوری اطلاعات برای شرکتها و سازمانها قبلا نیز یکی از مسائل چالش بر انگیز بوده ولی چالشها و نگرانی ها در مورد" امنیت IoT" بحرانی تر از قبل میباشد.

موضوع مهم دیگر نبود یک توافق سراسری روی معماری و استانداردهای مورد نیاز در امنیت IoT بوده که این امر خود مانع بکارگیری یکپارچه مکانیزم های امنیتی شده است. توسعه و بکارگیری هر چه بیشتر IoT منجر به افزایش مخاطرات حملات خواهد شد. در این حملات نه تنها موجودیتهای با قابلیت IoT در خطر می افتند بلکه سبب می شود نفوذ گران باالقوه بتوانند از یک مسیر نظارت نشده به اطلاعات حساس حوزه IT سازمان دست پیدا کنند که این مساله خود میتواند راهی به فرآیندهای تجاری شرکت، مالکیتهای معنوی و پایگاه اطلاعات مشتریان باشد [6],[5].

بطور خاص اگر روی رویکرد مهم خانه های هوشمند تمرکز کنیم می توانیم قابلیت رخنه به حریم خصوصی را با در نظر گرفتن داده های صریح و مستقیما مرتبط با افرادی که در خانه زندگی میکنند را محدود کنیم. هر چند فعالیت این افراد میتواند بطور غیر مستقیم وبا بررسی فعالیتهای فیزیکی و شبکه ای تجهیزات و دستگاههای داخل خانه دنبال شود.

در رابطه با خانه های هوشمند شاهد همکاری موجودیتها و تکنولوژیهای متفاوت و مختلف IoT هستیم که برای تعریف پارامترهای امنیتی لازم نیازمند دیدگاهها و راه حلهای جدید بوده و لازم به ذکر است که در اینجا نیز توافق واستانداردهای قوی وجود ندارد.

امنیت فضای سایبری با سه مولفه محرمانگی ، صحت و قابلیت دسترسی تعریف شده که میتواند بعنوان نیازهای پایه امنیت IoT نیز در نظر گرفته شود. در محرمانگی جریان داده ها و موجودیتهای IoT را از شنود حفظ میکنیم در صحت مطمئن میشویم پیامهای رد وبدل شده بین دستگاههای IoT توسط فرآیندها یا افراد غیر مجاز دستکاری نشده و در قابلیت دسترسی اطمینان می یابیم که تجهیزات IoT از دسترس خارج نشده و دارای کارکرد صحیح هستند.

این سه مولفه میتواند در برقراری امنیت کلی IoT بکار رفته ولی بطور جزیی نیازمند نگاه صریح تر در اعتماد و حفظ حریم خصوصی هستیم. نیازمندیهای امنیتی کاربردهای مختلف ممکن است متفاوت باشد بنابراین باید آن نیازها و کاربردها سازگار بوده و نمیتوان برای همه تجهیزات IoT بطور یکسان قویترین استراتژیهای و سیاستهای امنیتی را در نظر گرفت. بعلاوه در برخی کاربردها استانداردهای حفظ حریم خصوصی تعریف شده سازمانها و نهادهای ناظر باید برآورده شود.

در بسیاری از موارد، یک اختلال عمده در مدل سنتی چالش های خاص خود را به وجود می آورد .در زیر مواردی از چالش های امنیتی و ملاحظات در طراحی و ساخت دستگاه ها یا سیستم های IoT ذکر شده است:

- به طور معمول دستگاه های کوچک و ارزان امنیت فیزیکی ندارند و یا از امنیت کمی برخوردارند.
- زیرساختهای محاسباتی، به منابع حافظه و محاسبه محدود است ،که ممکن است از الگوریتم های امنیتی پیچیده و تکامل یافته به دلیل عوامل زیر پشتیبانی نکند:
  - قابلیتهای محاسبات محدود امنیتی.
  - الگوریتم های رمزگذاری نیاز به قدرت پردازش بالاتر دارند.
  - چرخه پردازنده کم در مقایسه با رمزگذاری موثر.
- دستگاه ها یا سیستم های IoT طراحی شده برای کارکردن مستقل در حالت بدون اتصال جایگزین در صورتی که اتصال اولیه از بین رفته باشد میباشند.
- اغلب قبل از ایجاد دسترسی به شبکه نصب میشوند که زمان کل را افزایش می دهد
- نیازمند مدیریت ایمن از راه دور در طول و پس از شروع بکار اجزا است

Archive of SID
www.SID.ir

- مقیاس پذیری و مدیریت میلیاردها موجودیت در اکوسیستمIoT
- شناسایی نقاط پایانی با دیدگاه مقیاس پذیری
  - فردی - به عنوان مثال، کنتور هوشمند خانه
  - گروهی - به عنوان مثال، همه لامپ های داخل یک اتاق / خانه
  - چالش های مقیاس پذیری فرد در مقابل گروه
  - گاهی اوقات ممکن است موقعیت فرد از شناسه آن فرد (ID) مهم تر باشد
- مدیریت شبکه های چند تکه ای
  - به عنوان مثال، چراغ راهنمایی هوشمند که در آن چندین طرف موردنظر وجود دارد مانند خدمات اضطراری (کاربر)، شهرداری (مالک)، تولید کننده (فروشنده)
  - چه کسی دسترسی به منابع را فراهم می کند؟
  - مسئولیت پذیری در فرآیند امنیت
- انعطاف پذیری رمزنگاری
  - دستگاه های ادغام شده ممکن است از طول عمر الگوریتم بیشتر عمر کنند.
  - به عنوان مثال، کنتور هوشمند می تواند بیش از 40 سال دوام داشته باشد
  - الگوریتم های رمزنگاری عمری محدود تا زمان شکسته شدن آن الگوریتم ها دارند. [7]
- حفاظت فیزیکی
  - دستگاه های موبایل می توانند دزدیده شوند.
  - دستگاه های ثابت می توانند منتقل شوند.
- تکنیک های طراحی و تشخیص مداخله
  - همیشه روشن : نرخ نظرسنجی بالا، انرژی بیشتر، تشخیص سریع
  - نظرسنجی دوره ای: انرژی کمتر، تشخیص آهسته تر
  - فعال کردن روی رویداد: حداقل انرژی، بدون تشخیص

به طور کلی موجودیتهای IoT نمی توانند یک راه حل تک استفاده ای، تک مالکیتی باشند. دستگاه ها و پلت فرم کنترل که در آن داده ها ممکن است مصرف شده و به اشتراک گذاشته شوند، می توانند دامنه های مالکیت، سیاست، مدیریت و اتصال متفاوتی داشته باشند. در نتیجه، دستگاه ها باید دسترسی برابر و آزاد به تعدادی از مصرف کنندگان داده ها و کنترل کنندگان را بطور همزمان با حفظ حریم خصوصی و انحصار داده های مورد نیاز در بین آن مصرف کنندگان داشته باشند. در دسترس بودن اطلاعات در حین تدارک تفکیک داده بین مشتریان مشترک بسیار مهم است. ما باید کنترل هویت مناسب را ایجاد کنیم و روابط اعتماد بین اشخاص را برای به اشتراک گذاشتن اطلاعات مناسب ایجاد کنیم. به نظر می رسد که الزامات امنیتی پیچیده و رقابتی وجود دارد که در پلتفرم با منابع بالقوه محدود به کار گرفته می شود:

- تأیید اعتبار به چندین شبکه بصورت امن.

Archive of SID
www.SID.ir

- اطمینان ازاینکه که داده ها برای چندین گردآورنده در دسترس هستند.
- مدیریت تداخلات بین دسترسی داده ها.
- مدیریت نگرانی های امنیتی چندین مصرف کننده.
- ارائه احراز هویت قوی و حفاظت از داده ها (یکپارچگی و محرمانه بودن) که به راحتی به خطر نیوفتد.
- برقراری قابلیت دسترسی داده یا سرویس.
- ایجاد سیر تکامل در مواجهه با خطرات ناشناخته.

موارد بالا در جاییکه که دسترسی امن به داده ها از اهمیت حیاتی برخوردار است ارتباط خاصی به IoT دارد. به عنوان مثال، یک فرآیند صنعتی مهم می تواند به اندازه گیری دقیق و به موقع دما متکی باشد. اگر این نقطه پایانی در معرض حمله انکار سرویس (DoS)باشد، عامل جمع آوری فرآیند باید به نحوی آگاه شود. در چنین مواردی، سیستم باید بتواند اقدامات مناسب مانند یافتن اطلاعات از یک اتصال ثانویه، یا تاخیر انداختن انتقال اطلاعات را بصورت بلادرنگ انجام دهد. همچنین باید قادر به تشخیص بین داده های از دست رفته ناشی از وقوع حملات DoS و از دست دادن دستگاه به دلیل یک رویداد فاجعه بار در کارخانه باشد. ممکن است اینکار با استفاده از تکنیک های یادگیری ماشین (به عنوان مثال، مقایسه حالت عملیاتی نرمال با یک حالت حمله که قبلا آموخته) انجام می شود.

5- تهدیدات IoT

IPv6 بعنوان یک پایه و اساس برای IoT ، هدف همان تهدیدات و حملاتی است که بهIPv4 حمله میکرد، مانند smurfing یا همان حمله جلوگیری از سرویس بصورت توزیع شده، حملات شناسایی نقاط ضغف سیستم عامل و پورتهای شبکه برای بهره برداری بعدی در فرآیند حمله، جعل هویت، حملات تکه تکه شدن دیتاگرام IP ، sniffing و شنود ترافیک شبکه ، حملات کشف همسایه، دستگاه های مخرب (که فرآیند شناسایی امنیتی برای آنها انجام نشده) ، حملات مرد میانی و غیره. بنابراین، در هسته شبکه نیاز به همان راه حل های امنیتی مشابه IPv4 امروزی میباشد.

با این حال، IoT یک بعد کاملا جدید برای امنیت باز می کند. IoT جایی است که اینترنت با جهان فیزیکی مواجه میشود. این امر بعضی از پیامدهای جدی در امنیت دارد؛ چنانکه تهدید حمله از دستکاری اطلاعات به کنترل حرکت (به عبارت دیگر حرکت از دیجیتال به دنیای فیزیکی) تبدیل میشود. در نتیجه، به شدت سطح حمله را از تهدیدات و دستگاه های شناخته شده به تهدیدات امنیتی بیشتر در دستگاه ها، پروتکل ها و جریان های کاری جدید افزایش می دهد. بسیاری از سیستم های عملیاتی از سیستم های بسته (مانند SCADA ، Modbus، CIP) به سمت سیستم های مبتنی بر IP حرکت می کنند که سطح حمله را بیشتر گسترش می دهند. IoT می تواند تحت تأثیر گونه های مختلف تهدیدهای امنیتی از جمله موارد زیرقرار گیرد:

- کرم های معمولی که از ICT به IoT جهش کرده اند: طور کلی محدود به اشیایی است که در حال اجرا روی سیستم عامل مصرف کننده است : ویندوز، لینوکس، iOS، اندروید
- حملات با اسکریپتها و یا دیگر اهداف مقیم در IoT: وب کم های محافظت نشده، سرقت محتوا، شکستن سیستم های کنترل خانه
- جرایم سازمان یافته: دسترسی به مالکیت معنوی، خرابکاری و جاسوسی

Archive of SID
www.SID.ir

- تروریسم سایبری: نیروگاههای هسته ای (به عنوان مثال، ویروسStuxnet) ، نظارت بر ترافیک، راه آهن، زیرساخت های حیاتی

6- امنیت درIoT / M2M

IOT/M2M در کنترل صنعتی، حمل و نقل، شبکه هوشمند و بهداشت عمومی بر زندگی روزمره ما تاثیر می گذارد، بنابراین امنیت آن امری ضروری است. درگسترش شبکه های میتنی بر IP، برنامه هاو کاربردهای IoT / M2M با میزان و پیچیدگی فزاینده تر از قبل هدف حمله قرار میگیرند. مقیاس و زمینه IoT / M2M آن را تبدیل به هدفی موثر برای کسانی که قصد آسیب رساندن به شرکت ها، سازمان ها، ملل و مهمتر از همه مردم دارند می نماید. اهداف فراوان هستند و بسیاری از بخش های مختلف صنعت را پوشش می دهند. تأثیرات بالقوه می تواند از آسیبهای جزئی و یا جدی به زیرساخت ها شروع شده و نهایتا به از دست دادن زندگی برسد. اگر چه تهدیدات در محیط IoT ممکن است مشابه تهدیدات در محیط های سنتی فناوری اطلاعات باشد، تاثیر کلی می تواند به طور قابل توجهی متفاوت باشد. به همین دلیل است که در مجامع علمی برای تمرکز روی تجزیه و تحلیل تهدید [8] و همچنین برای ارزیابی های مخاطره برای اندازه گیری تاثیر یک حادثه امنیتی یا رخنه اتفاق افتاده تلاشهای زیادی شده است. یکی از عناصر اساسی در امن سازی زیرساخت های IoT در اعتبار سنجی دستگاهها با محوریت هویت و مکانیزم آنهاست. همانطور که قبلا ذکر شد، بسیاری از دستگاه های IOT ممکن است قدرت مورد نیاز برای محاسبه، ظرفیت حافظه یا ذخیره سازی برای حمایت از پروتکل های احراز هویت فعلی را نداشته باشند. طرح های رمزنگاری و تأیید هویت قوی امروزی مبتنی بر مجموعه های رمزنگاری مانند AES (Advanced Encryption Suite) برای انتقال اطلاعات محرمانه ، RSA (Rivest-Shamir-Adleman) برای امضاهای دیجیتالی و مبادله کلید و DH (Diffie-Hellman) برای مذاکرات و مدیریت کلید می باشند. این پروتکل ها قوی بوده و نیاز به منابع محاسباتی بالا دارند که ممکن است در تمام دستگاه های متصل به IoT موجود نباشد. در نتیجه، احراز هویت و صدور مجوز برای تطبیق با جهان جدید مرتبط با IoT ما نیاز به مهندسی مجدد مناسب دارد. همچنین، این پروتکل های احراز هویت وصدور مجوز، نیاز به درجه ای از مداخله کاربر از لحاظ پیکربندی و آماده سازی دارد. با این حال، بسیاری از دستگاه های IoT دسترسی محدودی دارند، بنابراین نیاز به پیکربندی اولیه برای محافظت از دستکاری، سرقت و سایر اشکال به خطر افتادن در طول عمر مفید آن، که در بسیاری موارد ممکن است سالها باشد، خواهند داشت.

برای غلبه بر این مشکلات، روشهای احراز هویت جدید که می توانند با استفاده از تجربه الگوریتم های رمزنگاری / اعتبار سنجی قوی امروزی ساخته شوند، مورد نیاز است. خبر خوب این است که بر روی فناوری ها و الگوریتم های جدیدکارهای زیادی در حال انجام است.

به عنوان مثال، اخیرا موسسه ملی استاندارد و فناوری (NIST) الگوریتم SHA-3 فشرده را به عنوان الگوریتم جدید برای دستگاههای به اصطلاح "ادغام شده" یا هوشمند که خودشان کامپیوتر کامل نبوده و به شبکه های الکترونیکی متصل میشوند را انتخاب کرده است. [9]

دیگر مولفه های امنیتی که می توانند مورد توجه قرار گیرند عبارتند از:

- بکارگیری موقعیت جغرافیایی و سطوح حریم خصوصی برای داده
- شناسه های قوی
- تقویت سایر روش های متمرکز شبکه مانند سیستم نام دامنه (DNS) با DNSSEC و DHCP برای جلوگیری از حملات
- اتخاذ پروتکل های دیگر که برای تأخیر یا اتصال گذرا (مثل شبکه های تاخیری) قابلیت تحمل بیشتری دارند[10]

Archive of SID
www.SID.ir

بسیاری از ملاحظات امنیتی برای پروتکل های IoT به رمزگذاری متکی هستند. همانطور که جریان های کاری جدید برای حسگرها و عناصر متصل به اینترنت تعریف می شوند، یک ناهمخوانی در افق های زمانی یک شکاف اضافی ایجاد می کند: در اینحالت دستگاه ها ممکن است اثربخشی رمزنگاری را ازبین ببرند. به عنوان مثال، یک کنتور برق در یک خانه می تواند پنجاه سال عمر کند، در حالیکه پروتکل رمزنگاری ممکن است نیمی از آن زمان تا وقتی که به خطر افتد، قابل استفاده باشد.

7- حریم خصوصی

حفاظت از حریم خصوصی از زمان آغاز اینترنت مورد توجه بوده است. IoT مشکل را تشدید می کند، زیرا بسیاری از کاربردها، امضاهای قابل ردیابی از موقعیت و رفتار افراد ایجاد می کنند. مسائل مربوط به حریم خصوصی بطور خاص در مراقبت های بهداشتی مطرح هستند، و بسیاری از برنامه های کاربردی جالب مراقبت های بهداشتی مثل ردیابی تجهیزات پزشکی در بیمارستان، نظارت بر آمار و اطلاعات حیاتی بیماران در خانه و یا در یک مرکز خدمات رسانی وجود دارد که در قلمرو IoT قرار دارند. در چنین محیطی، تأیید مالکیت دستگاه و هویت مالک هنگام جدا شدن دستگاه از صاحب مالکیت ضروری است. برای دستیابی به این هدف مکانیسم سایه سازی پیشنهاد شده است. اساسا، سایه های دیجیتال، اشیاء کاربر را برای انجام عمل از طرف وی و ذخیره تنها یک هویت مجازی که حاوی اطلاعات مربوط به ویژگی های آن است را فعال می کند.

ممکن است مدیریت هویت در IoT فرصت های جدیدی را با ترکیب روش های مختلف تأیید هویت، برای افزایش امنیت انسان ها و ماشین ها ارائه دهد. برای مثال، شناسایی زیستی در ترکیب با یک شی در شبکه شخصی می تواند برای باز کردن درب استفاده شود. باید تاکید کرد که حفظ حریم خصوصی و پیروی از آن، تحت نظارت قوانین کشوری قرار دارند.

8- مکانیزم امنیتی لایه ای

با استفاده ازیک رویکرد معماری لایه بندی میتوان تعریف بهتری از نیازمندیها ارائه داد: اینکه چه میزانی از امنیت نیاز است و همچنین اینکه چه وظایف امنیتی باید در مولفه های فیزیکی و منطقی کل سیستم IoT پیاده سازی شود.

بنابر این تعریف، معماری IoT علاوه بر تعربف مولفه های ارتباطی و واحد های مدیریت داده ها، باید مکانیزم های امنیتی و عملکرد آنها را نیز تعریف کند.

چندین مدل معماری امنیتی تا کنون پیشنهاد شده اند که هر کدام برخی از توابع و عملکردهای خاص را تعریف کرده و یا به انتزاع مفاهیم پرداخته است[11] .

- معماری باز IoT شامل :
- معماری مرجع اینترنت صنعتی (IIRA) ؛
- معماری اینترنت اشیاء (IOT-A) [5] ؛
- استاندارد برای یک چهارچوب معماری برای اینترنت اشیاء(IoT) ، توسعه یافته توسط IEEE P2413 WG؛
- معماری سطح بالای ETSI برای M2M ؛
- معماری مرجع اینترنت اشیاء (IoT RA -- ISO/IEC WD 30141)؛

بدلیل دامنه وسیع اینترنت اشیاء شاید یک معماری مرجع تکی برای همه کاربردها و محیط ها کافی نبوده و از اینرو طبیعی است که انتظار داشته باشیم تعدادی معماری مرجع جدید مورد نیاز باشد.

Archive of SID
www.SID.ir

برخی از این معماریهای پیشنهادی IoT ملاحظات امنیتی را مشابه روشهایی که تاکنون در امنیت مرسوم اینترنتی شاهد بودیم در نظر گرفته اند ولی در اغلب آنها قابلیتهایی مثل امنیت و مدیریت بصورت عمودی و به شکلی که از چند لایه عبور میکنند تعریف شده، و بدلیل اینکه هرروزه شاهد نقض امنیت در اینگونه معماریها هستیم، میتوان گفت که دارای ضعف هستند.

9- کارهای مرتبط

9-1- معماری امنیت اینترنت اشیاء با استفاده از OSiRM [12]:

این یک روشکلی در طراحی سیستم های IoT است که در آن به اهداف زیر توجه شده:

- امنیت هر دستگاه
- امنیت هر زیر شبکه
- امنیت هر شبکه انتقالی یا هر شبکه هسته (Core)
- امنیت خدمات ذخیره سازی یا تجزیه تحلیل آن

در این مدل بر ایجاد امنیت در هر فرآیندی در هر کدام از لایه ها تاکید شده است.

این روش بنام مدل مرجع اینترنت سیستم های باز اینترنت اشیاء(OSiRM) در [12] تعریف شده است.

OSiRM سه مکانیزم مربوط به امنیت را در بر می گیرد که می تواند به طور مؤثری در هر لایه به صورت مستقل وجود داشته باشد؛ احراز اصالت و صدور مجوز (A&A)؛ کدگذاری و مدیریت کلید (E&KM)؛ مدیریت شناسایی و اعتماد (T&IM) (مکانیزم های دیگر را می توان به لایه های مدل اضافه کرد).

لایه	وظیفه	مکانیزم امنیتی درون لایه ای
1- اشیاء	**این لایه تشکیل شده از دنیای اشیاء است.**	**L1 A&A; L1 A&KM; L1 T&IM**
2- اکتساب داده	**این لایه قابلیت های «اکتساب داده» را دربرمی گیرد.**	**L2 A&A; L2 A&KM; L2 T&IM**
3- شبکه بندی مه	**این لایه از «شبکه مه » و شبکه بندی محلی شده حمایت می کند.**	**L3 A&A; L3 A&KM; L3 T&IM**
4- متراکم کردن داده	**این لایه از تجمیع داده، جمع آوری داده ، خلاصه سازی داده و یا تبدیل پروتکل حمایت می کند.**	**L4 A&A; L4 A&KM; L4 T&IM**
5- متمرکز کردن داده	**این لایه از تابع متمرکز سازی داده حمایت می کند (شبکه هسته سنتی).**	**L5 A&A; L5 A&KM; L5 T&IM**
6- تحلیل و ذخیره سازی داده	**این لایه تحلیل داده و توابع ذخیره سازی را در بر می گیرد.**	**L6 A&A; L6A&KM; L6 T&IM**
7- کاربردها	**لایه کاربرد آرایهٔ گسترده ای از کاربردهای عمودی و/ یا افقی است.**	**L7 A&A; L7 A&KM; L7 T&IM**

جدول 1 : معماری OSiRM

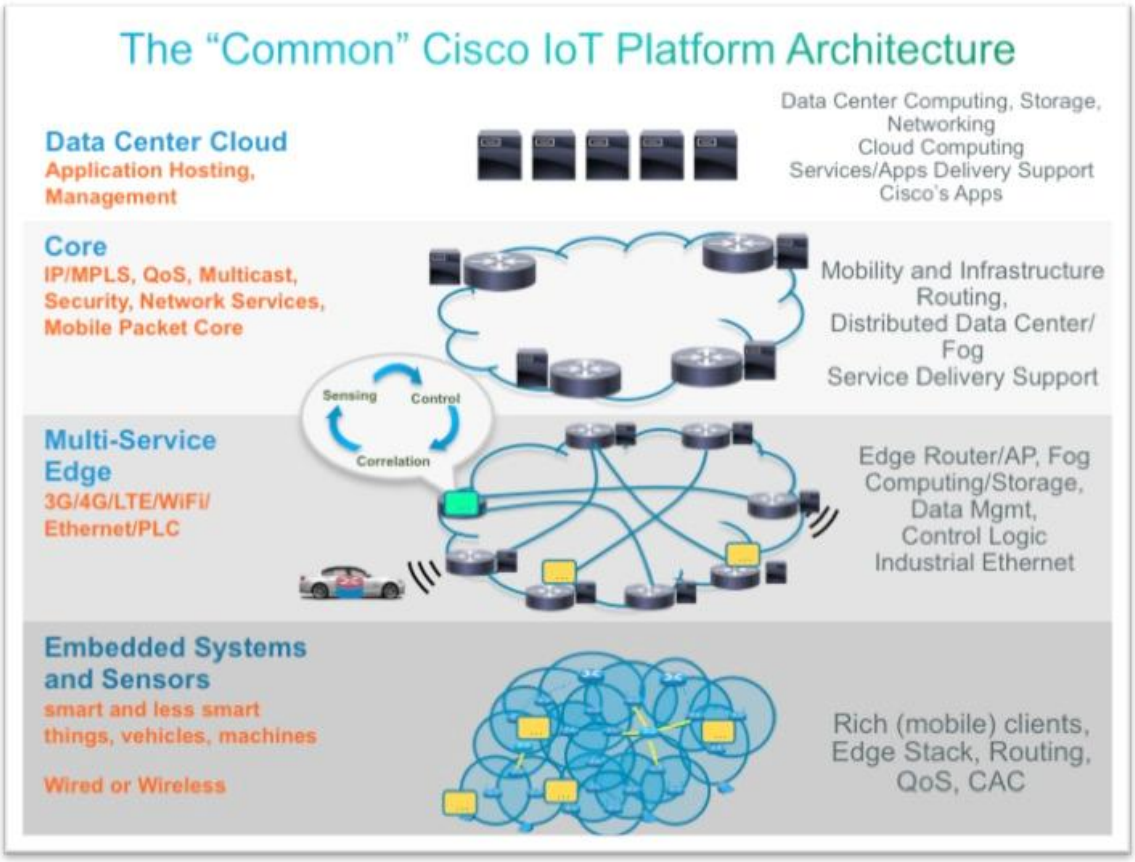
در مدل OSiRM تفاوت های بهینه شده ای برای یک تابع امنیت مورد نظر در لایه های مختلف وجود دارد، همچنین اتفاقات ویژه ای ممکن است با توجه به نوع شی و / یا نوع کاربرد رخ دهد. برای مثال در لایهٔ شبکه بندی مه ممکن است از یک الگوریتم رمزگذاری 64 بیتی استفاده شود در حالی که لایهٔ «تراکم سازی داده» یا «متمرکز سازی داده» ممکن است از الگوریتم رمزگذاری 256 بیتی استفاده شود.

Archive of SID

www.SID.ir

2-9- معماری سیسکو IoT/M2M

معماری سیسکو IoT/M2M از چهار لایه تشکیل شده است، برخی از آنها مشابه آنچه که در معماری های شبکه های معمولی سیسکو توصیف شده است میباشند.



شکل2: لایه های معماری شبکهIoT / M2M

الف - لایه سیستم های ادغام شده

اولین لایه معماری IoT / M2M از سیستم های ادغام شده، سنسورها و فعال کننده ها تشکیل شده است. به همین ترتیب، این دستگاه های کوچک، با سیستم عامل های مختلف، انواع CPU ها، حافظه و غیره هستند. انتظار می رود بسیاری از این موجودیت ها دستگاه های ارزان قیمت، دستگاه های تک وظیفه ای با اتصال شبکه اولیه، مانند سنسور دمای یا فشار باشند. علاوه بر این، این دستگاه ها می توانند در مکان های دور و یا غیر قابل دسترسی باشند که در آن مداخله یا پیکربندی توسط انسان تقریبا غیرممکن است. در کارکرد این لایه باید از صحت داده ها، مسیر از سنسور به جمع کننده و پارامترهای تأیید هویت اتصال بین نصب اولیه / پیکربندی دستگاه و البته اینکه حضور نهایی آن در زیرساخت های IoT نمی تواند مورد سوء استفاده قرار گیرد اطمینان حاصل شود.

www.SID.ir

ب - لایه لبه چند سرویسی

تنوع در قابلیت های دستگاه های نهایی و تعداد بالقوه عظیم آن اهمیت لبه چند سرویسی را در معماری IoT / M2M برجسته می کند. لبه چند سرویسی چند منظوره است و از اتصالات سیمی و بی سیم پشتیبانی می کند. حتی در داخل این دو دسته، این لایه باید از پروتکل های مختلف مانندZigbee ، IEEE 802.11، نسل سوم و چهارم موبایل پشتیبانی کند تا بتواند به چندین نقطه پایانی دست یابد. حتی در برخی موارد، ممکن است پروتکل های استفاده شده توسط دستگاه های پایه هیچ گونه قابلیت امنیتی ذاتی را نداشته باشند. خدمات امنیتی برای حفاظت از این نقاط پایانی ذاتا ناامن ضروری است. علاوه بر این، این لایه باید برای مقابله با مقیاس رشد نیازمندیها صورت پیمانه ای باشد. اجزاء و خدمات ارائه شده در یک پیمانه باید مشابه باشند تا پیمانه های اضافی را بتوان در یک زمان کوتاه اضافه کرد.

پ - لایه هسته شبکه

معماری لایه هسته شبکه شبیه به معماری است که در شبکه های متداول بکارگرفته شده است. عملکرد این لایه، فراهم کردن مسیرهایی برای انتقال و مبادله داده ها و اطلاعات شبکه بین چندین زیر شبکه است. تفاوت اصلی بین IoT و لایه های هسته مرسوم، مشخصات ترافیکی است. ترافیک IoT و داده ممکن است متفاوت باشد، به عنوان مثال، پروتکل های یکتا و اندازه متغیر بسته. خدمات امنیتی در هسته شبکه اطمینان میدهد که سیستم IoT / M2M به عنوان یک کل، برای محافظت در برابر تهدیدات زیر قوی شده است:

- مرد میانی (MITM): مهاجم می تواند با ایجاد ارتباط بین دو نقطه مکالمه، پیام های مبادله شده از یک طرف به طرف دیگر را استراق سمع وحتی ضبط کند.
- جعل هویت (spoofing): مهاجم یک هویت را به مخاطره می اندازد و بنابراین می تواند از طریق جعل هویت، ترافیک مخرب را به نقاط پایانی قربانی در شبکه ارسال کند.
- به خطر افتادن محرمانگی : داده های در حال انتقال، توسط یک مهاجم میتواند خوانده شده و تغییر داده شود.
- حمله تکرار : از طریق این حمله با جعل هویت ، داده های معتبر جلسه ای که قبلا ایجاد شده ، دوباره انتقال داده شده و یا به تأخیر انداخته میشوند.

ت - لایه ابر مرکز داده

معماری مرکز داده / لایه ابر شبکه شبیه به معماری است که در شبکه های معمولی بکار گرفته شده است. عملکرد این لایه، میزبانی برنامه هایی است که در ارائه خدمات و مدیریت معماری IoT مهم هستند. مجددا، خدمات امنیتی در مرکز داده / ابر شبکه در حصول اطمینان از اینکه سیستم IoT / M2M به طور کلی برای محافظت در برابر تهدیدات زیر قوی شده اند حیاتی هستند:

- حمله جلوگیری از خدمات (DoS) : تلاش یک مهاجم برای اینکه یک منبع را از دسترس خارج کند رسانه بیسیم. مثال خوبی از یک منبع آسیب پذیر برایDoS، است. در حالیکه امروزه بسیاری از فناوری ها برای تقویت پروتکل ها و امنیت

Archive of SID
www.SID.ir

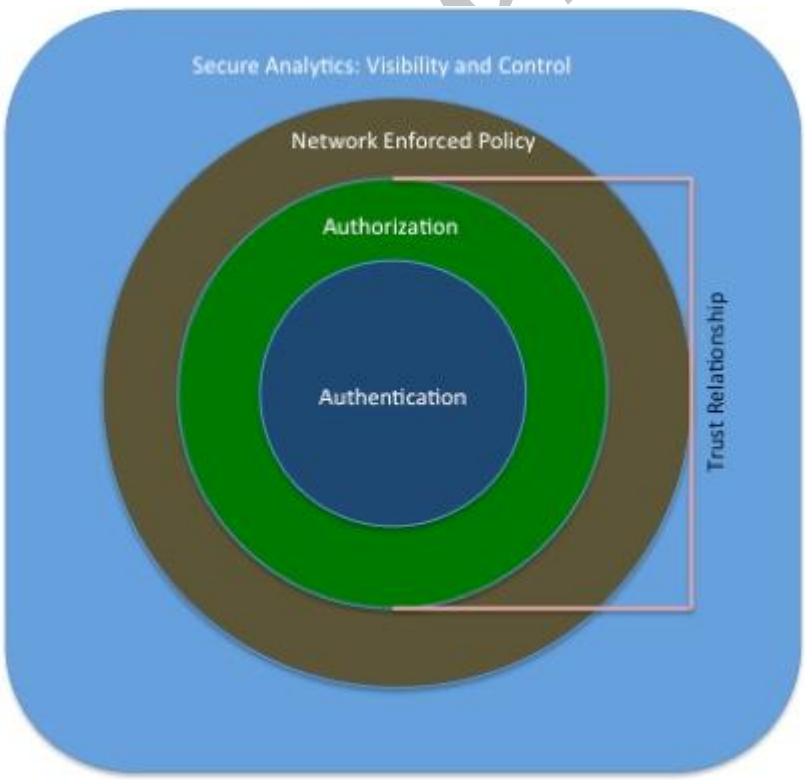
Wi-Fi، Long Term Evolution (LTE) وجود دارد ، یک پارایزیت انداز رادیویی ساده می تواند یک حمله DoS موثر در این رسانه های بی سیم باشد.

- بهره برداری از کامپوننت و نقطه پایانی بدین معنی که مهاجم می تواند به یک مولفه در سیستم IoT / M2M نفوذ کند (یا یک نقطه پایانی یا مولفه شبکه، برنامه یا ماژول) و از آن برای انجام سوء استفاده های بیشتر استفاده کند. این حملات تکامل یافته اند به طوری که به خطر افتادن یک عنصر تکی می تواند منجر به خطر افتادن بیشتر و یا نفوذ در سیستم شود. این موارد در حملات اخیر از قبیل استاکسنت [14] [13] و Duqu [15] نشان داده شده است. همچنین در صورتی که تقویت امنیت وبکارگیری بهترین شیوه ها دنبال نشود، سرورهای نرم افزاری و دستگاه های موجود در این لایه ممکن است در معرض سرریز بافر و حملات اجرای کد از راه دور قرار بگیرند.

تهدیدها در این لایه ها، از قبیل DoS ، تکرار تراکنش ها و یا سیستم های به خطر افتاده، معمولا می تواند از طریق مکانیزم های رمزنگاری شناخته شده، ارائه هویت های قوی با اعتبار به آنها در اجازه به اعتبار سنجی در شبکه و با سیاست های قوی برای کنترل دسترسی مناسب میتواند مورد رسیدگی و ملاحظه قرار گیرد.

10- چارچوب امنیت IoT / M2M پیشنهادی

برای رسیدگی به محیط بسیار متنوع IoT و چالش های امنیتی مربوطه، یک چارچوب امنیتی انعطاف پذیر مورد نیاز است.



شکل 3. چارچوب IoT ایمن

شکل 5 یک چارچوب برای امن سازی محیط IoT را نشان می دهد و شامل چهار جزء می شود:

www.SID.ir

- احراز هویت
- صدور مجوز
- سیاست اعمال شبکه
- تجزیه و تحلیل امن: قابلیت دید و کنترل

11- احراز هویت

در قلب این چارچوب، لایه احراز هویت، مورد استفاده برای ارائه و تأیید اطلاعات شناسایی موجودیت IoT است. هنگامی که دستگاه های متصل شده IoT / M2M (به عنوان مثال، سنسورهای ادغام شده و فعال کننده ها یا نقطه های پایانی) نیاز به دسترسی به زیرساخت های IoT دارند، روابط اعتماد بر اساس هویت دستگاه آغاز می شود. ممکن است روش های ذخیره و ارائه اطلاعات هویت به طور قابل توجهی برای دستگاه های IoT متفاوت باشد. ممکن است در شبکه های سازمانی معمول، نقاط پایانی توسط گواهی و اعتبار شخصی (مثلا نام کاربری و رمز عبور، توکن یا بیومتریک) شناسایی شوند. نقاط انتهایی IoT / M2M باید بوسیله ویژگیها و شناسه های منحصر بفردشان مثل: شناسه فرکانس رادیویی(RFID)، راز مشترک، گواهینامهX.509 ، آدرس MAC نقطه پایانی یا نوعی از ریشه اعتماد مبتنی بر سخت افزار غیرقابل تغییر، احراز هویت شوند تا دیگر نیازی به تعاملات انسانی نداشته باشند. ایجاد شناسه از طریق گواهی X.509 یک سیستم تأیید هویت قوی فراهم می کند. با این حال، در حوزهIoT، بسیاری از دستگاه ها ممکن است حافظه کافی برای ذخیره یک گواهی نداشته و یا حتی ممکن است قدرت CPU مورد نیاز برای اجرای عملیات رمزنگاری اعتبار سنجی(X.509 و یا هر نوع عملیات کلید عمومی) را نداشته باشند.
سبکها و روش های جدید، فرصتی برای تحقیق بیشتر در تعریف انواع اعتبارنامه کوچکتر و ساختارهای رمزنگاری و پروتکل های احراز هویت کمتر فشرده از دید محاسباتی ایجاد می کنند.

12- صدورمجوز

لایه دوم این چارچوب مجوزی است که دسترسی دستگاه را در سراسر شبکه کنترل می کند. این لایه با استفاده از اطلاعات هویت یک موجودیت بر لایه احراز هویت هسته ایجاد می شود. با مولفه های احراز هویت وصدور مجوز، یک ارتباط قابل اعتماد بین دستگاه های IoT برای تبادل اطلاعات ایجاد می شود. به عنوان مثال، یک خودرو ممکن است یک رابطه یا پیمان قابل اعتماد را با یک خودرو دیگر از همان فروشنده ایجاد کند. با این وجود، این رابطه اعتماد تنها می تواند به خودرو ها اجازه تبادل قابلیت های ایمنی خودشان را بدهد. هنگامی که یک پیمان معتبر بین خودروهای مشابه و شبکه فروشندگان آن برقرار می شود، ممکن است مجاز به اشتراک اطلاعات اضافی مانند خواندن کیلومتر شمار خودرو، آخرین سابقه تعمیر و نگهداری، و غیره باشد.

خوشبختانه، مکانیزم های سیاست های فعلی برای مدیریت و کنترل دسترسی به شبکه های مصرف کننده و سازمانی بسیار خوب به نیازهای IoT / M2M می پردازند. چالش بزرگ، ساخت یک معماری است که بتواند میلیاردها دستگاه IoT / M2M را با روابط متقابل اعتماد مقیاس پذیرو مدیریت کند. سیاست های ترافیکی و کنترل های مناسب در سراسر شبکه برای شکستن ترافیک داده ها و برقراری ارتباط انتها به انتها بکار گرفته خواهد شد.

Archive of SID

www.SID.ir

13- سیاست اجباری شبکه

این لایه دربرگیرنده تمام عناصری است که ترافیک نقطه پایانی چه داده کنترلی، مدیریتی ویا ترافیک داده واقعی را بطور امن ازطریق زیرساخت مسیریابی کرده و انتقال میدهد. شبیه لایه صدور مجوز، پروتکل ها و مکانیزم هایی از قبل برای تأمین امنیت زیرساخت شبکه وجود دارد که سیاست هایی را که مناسب استفاده در IoT / M2M هستند را تحت تاثیر قرار می دهد.

14- تجزیه و تحلیل امن: قابلیت دید و کنترل

این لایه تجزیه و تحلیل امن، خدماتی را تعریف می کند که تمام عناصر (نقطه پایانی و زیرساخت شبکه، شامل مراکز داده) می توانند برای تدارک سنجش از راه دور به منظور دستیابی به دید و در نهایت کنترل اکوسیستم IoT / M2M شرکت کنند. با بلوغ سیستم های اطلاعاتی بزرگ، ما می توانیم یک پلت فرم عظیم پایگاه داده موازی (MPP) که بتواند حجم زیادی از داده ها را بصورت بلادرنگ پردازش کند، را بکاربگیریم. وقتی ما این تکنولوژی را با تجزیه و تحلیل ترکیب می کنیم، می توانیم برخی از تجزیه و تحلیل های آماری واقعی را بر روی داده های امنیتی انجام دهیم تا ناهنجاری ها را بیابیم. بعلاوه این شامل تمام عناصری است که اطلاعات را جمع آوری و همبسته میکنند، از جمله سنجش از دور، برای تشخیص و شناسایی تهدید. مقابله با تهدید می تواند از سد کردن مهاجم از دسترسی به منابع بیشتر تا اجرای اسکریپت های اختصاصی برای شروع اصلاح مناسب باشد. داده های تولید شده توسط دستگاه های IoT تنها اگر الگوریتم های تجزیه و تحلیل یا سایر فرآیندهای هوشمند امنیتی برای شناسایی تهدید بدرستی تعریف شوند، ارزشمند هستند. ما می توانیم با جمع آوری داده ها از منابع مختلف و استفاده از پروفایل های امنیتی و مدل های آماری که بر لایه های مختلف الگوریتم های امنیتی ساخته شده است نتایج تحلیلی بهتری بدست آوریم.

همه ما می دانیم که زیرساخت های شبکه در حال پیچیده تر شدن هستند. توپولوژی ها را با هردو ابرهای عمومی و خصوصی تصور کنید؛ هوشمندی تهدیدات و توانایی های دفاع نیز باید مبتنی بر ابر باشد. تنظیم قابلیت دید، زمینه و کنترل لازم است تا هوشمندی دقیق را مدیریت کند.

اجزای درون این لایه عبارتند از:

- زیر ساخت واقعی IoT / M2M که داده های سنجش از راه دور و شناسایی آن به دست آمده و جمع آوری می شود.
- هسته مجموعه ای از توابع برای تلفیق، تجزیه و تحلیل داده ها برای اهداف ارائه قابلیت دید، و ارائه آگاهی زمینه ای و کنترل.
- پلت فرم تحویل برای تجزیه و تحلیل واقعی، ساخته شده از دو جزء اول، مورد بحث در بالا.

در حالی که ممکن است پیاده سازی واقعی IoT / M2M متفاوت باشد، این چارچوب را می توان به هر معماری اعمال کرد. این چارچوب به اندازه کافی ساده و انعطاف پذیر است تا حتی بتواند به دستگاههایی که کاربر انسانی دارند اگر در زیرساخت های IoT حضور دارند سرویس دهی داشته باشد (مثلا لپ تاپ ها، اسکنرهای دستی و ...).

آیا می توانید با استفاده از این چارچوب یک معماری داشته باشیم که 100٪ حفاظت از تهدیدها را فراهم کند؟ متأسفانه هنوز چنین موقعیتی وجود ندارد. با این حال، اعتقاد داریم که کلان داده و خط مشی های تحلیل نقش اصلی را بازی می کنند. تهدیدات امنیتی به طور مداوم در حال ظهور هستند و ما نیازمند توسعه یک معماری هستیم که بتواند از خود در برابر این تهدیدات دفاع کند. این چارچوب امنیتی پایه و اساسی را فراهم می کند که می توان از آن خدمات امنیتی مناسب را انتخاب کرد. شکاف ها نیز می تواند به عنوان زمینه های خاص شناسایی شده و مورد توجه قرار گیرد.

Archive of SID
www.SID.ir

15- نتیجه

در حالی که مفاهیم امنیتی برای ساختارهای IoT / M2M گسترده هستند، ساختن یک چارچوب امنیتی قابل دوام IoT / M2M می تواند پایه ای برای اجرای امنیت در محیط های مختلف از جمله تولید محصولات باشد. چارچوب پیشنهادی می تواند در توسعه پروتکل و محصول استفاده شده و علاوه بر آن در اجرای سیاستگذاریها در محیط های عملیاتی نیز مورد استفاده قرار گیرد.

همچنین نشان داده شد که میزان مشکل امن سازی در IoT بسیار بیشتر از امنیت IPv6 است. صنعت IoT هنوز در حال تحول است و پتانسیل زیادی برای حملات روز صفر وجود دارد. دراین شرایط می بایست امنیت در لایه مناسب ارائه شود. لایه نقطه پایانی ادغام شده، از دستگاه های بسیار محدود شده تشکیل شده است که این امر تا کنون رشد بدافزار را در این لایه را محدود کرده است. رشد سنسورهای مبتنی بر IP به رشد سطح حمله منجر شده است. این موضوع نشان دهنده این واقعیت است که پروتکل های امنیتی و تکنیک های شناسایی جدید مورد نیاز است و امنیت نقطه پایانی IoT نیاز به ارتباط با قابلیت های پیشرفته آن دارد. واضح است که IoT چالش های جدیدی را برای معماران شبکه و امنیت ایجاد می کند. سیستم های امن هوشمند تر که شامل تشخیص تهدید مدیریت شده، تشخیص ناهنجاری و تحلیل پیش گو هستند، نیاز به تکامل دارند. علاوه بر این، ما یک دیدگاه راجع به حریم خصوصی و پیامدهای آن در رابطه با امنیت و انطباق قانونی ارائه داده ایم.

مراجع

[1] International Workshop on Big Data and Data Mining Challenges on IoT and Pervasive Systems (BigD2M 2015)" *New Security Architecture for IoT Network*"

[2] D.Geneiatakis, I.Kounelis, R.Neisse , I.Nai-Fovino *" Security and Privacy Issues for an IoT based Smart Home*" 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) , Pages: 1292 - 1297 IEEE Conference Publications

[3] Journal of Computer and Communications, 2015, 3, 164-173 *Published Online May 2015 in SciRes.* http://www.scirp.org/journal/jcc http://dx.doi.org/10.4236/jcc.2015.35021

[4] Source: Cisco IBSG projections, UN Economic & Social Affairs http://www.un.org/esa/population/publications/longrange2/WorldPop2300final.pdf.

[5] C. Lai, R. Lu, D.Zheng, H.Li, and X.Shen, "*Toward Secure Large-Scale machine-to-Machine Communications in 3GPP Networks* ", IEEE Comm. Magazine Supplement, December 2015, pp12ff

[6] R. T. Tiburski, L. A. Amaral, E. de Matos, and F. Hessel, "*The Importance of a Standard Security Architecture for SOA - Based IoT Middleware*", IEEE Communications Magazine, December 2015

[7] Valerie Aurora, "*Lifetimes of cryptographic hash functions*", 2012, http://valerieaurora.org/hash.html

[8] ETSI TR103 167 v0.3.1 "*Machine to Machine Communications (M2M); Threat Analysis and Counter-*

Archive of SID
www.SID.ir

Measures to M2M Service Layer, 2011.

[9] "*NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition*", October 2, 2012, http://www.nist.gov/itl/csd/sha-100212.cfm.

[10] Delay Tolerant Networking Research Group: http://www.dtnrg.org/wiki.

[11] M. Weyrich and C. Ebert, "*Reference Architectures for the Internet of Thing*s", IEEE Software, IEEE Computer Society, Jan/Feb 2016, p.112 ff.

[12] D. Minoli, K. Sohraby, *et al*, "*IoT Considerations, Requirements, and Architectures for Insurance Applications*", in book *Internet of Things*, Q. Hassan Editor, CRC Press, 2017, ISBN 9781498778510

[13] Computerworld, "*Siemens: Stuxnet worm hit industrial systems*", September 16, 2010.

[14] Steven Cherry with Ralph Langner, "*How Stuxnet is Rewriting the Cyberterrorism Playbook*", October 2010, IEEE Spectrum.

[15] "*Duqu: A Stuxnet-like malware found in the wild, technical report*", October 14, 2011, Laboratory of Cryptography of Systems Security

Archive of SID

www.SID.ir