باسمه تعالی

عنوان مستند

امنیت فضای ابری برای IoT

فهرست مطالب

1 مقدمه

این گزارش چشم اندازی از سرویس های ابری و معماری های امنیتی را ارائه می کند که برای پشتیبانی از اینترنت اشیاء طراحی شده اند. با استفاده از سرویس های ابری و بهترین روش های امنیتی، سازمان ها می توانند تأسیسات IoT میان سازمانی و چند دامنه ای را در سرتاسر مرزهای مطمئن اداره و مدیریت کنند. پیشنهادات فضای ابری و امنیتی سرویس های وب آمازون (AWS)[1]، مؤلفه های پیشنهاد شده توسط Cisco (محاسبات مه مانند[2]) و همچنین Microsoft Azure بررسی می شوند.

تعهد بسیار به فضای ابری و امنیت فضای ابری، دو مورد از جنبه های اطلاعات حجیم IoT هستند که به امنیتی نیاز دارند. ذخیره سازی اطلاعات، تحلیل اطلاعات و سامانه های گزارش گیری IoT در کنار بهترین روش ها در زمینه چگونگی ایمن سازی این سرویس ها به طور مفصل بررسی خواهند شد. ایمن سازی انواع مختلف فضای ابری IoT به مدیریت این مسئله نیز نیاز دارد که کدام معیارهای امنیتی، وظایف مشتری و کدام وظایف ارائه دهنده سرویس هستند.

این گزارش، سرویس های فضای ابری و امنیت ابری IoT را از طریق بخش های زیر توضیح می دهد:

- **سرویس های ابری و IoT:** در این بخش، فضای ابری تعریف خواهد شد به دلیل اینکه به IoT ارتباط داشته و برای آن منفعت دارد. به علاوه، الزامات منحصر به فرد شناسایی خواهند شد که IoT در فضای ابری تحمیل می کند. در این بخش، قبل از بررسی عمیق کنترل های امنیتی مبتنی بر فضای ابری و دیگر پیشنهادات، تهدیدات امنیتی داخلی و خارجی مرتبط با IoT برای فضای ابری نیز شناسایی و بررسی خواهند شد.
- **کاوش پیشنهادات IoT ارائه دهنده سرویس فضای ابری (CSP)[3]:** چندین CSP و نرم افزار/ امنیت به عنوان یک سرویس آنها بررسی خواهد شد. محاسبات مه مانند Cisco[4]، Amazon AWS و Microsoft Azure توضیح داده می شوند.
- **کنترل های امنیتی IoT ابری:** عملکرد امنیتی مورد نیاز از طرف فضای ابری برای ساخت یک معماری تأثیرگذار امنیتی پروژه IoT بررسی می شود.
- **تشکیل یک معماری امنیت فضای ابری IoT سازمانی:** این بخش از پیشنهادات امنیت فضای ابری موجود برای ترکیب و تطبیق با یک معماری تأثیرگذار امنیت فضای ابری IoT استفاده می کند.

[1] Amazon Web Services

[2] توسعه محاسبات ابری تا مرز شبکه سازمان

[3] Cloud Service Provider

[4] Cisco's Fog Computing

- **دستورالعمل های جدید در محاسبات IoT دارای فضای ابری:** در این بخش از مبحث امنیت فضای ابری فاصله گرفته می شود تا اندکی درباره الگوهای جدید محاسباتی که فضای ابری آماده ارائه آنها است بحث شود.

2 سرویس های ابری و IoT

از نظر B2B، تأسیسات IoT مصرف کننده و صنعتی، هیچ چیزی بیشتر از سرویس های پشتیبانی کننده از IoT مبتنی بر فضای ابری، دستگاه ها، اطلاعات دستگاه، افراد و سازمان ها را به یکدیگر متصل نمی کند. درگاه ها، برنامه ها، رابط های پروتکل ها و تنوعی از تحلیل های اطلاعاتی و مؤلفه های اطلاعات تجاری، برای راحتی، هزینه و قیاس پذیری در فضای ابری قرار گرفته اند. در خصوص پشتیبانی از میلیاردها دستگاه IoT، سرویس های مبتنی بر فضای ابری، متقاعدکننده ترین محیط را برای شرکت های جدید یا وارث جهت بکارگیری این سرویس ها پیشنهاد می کنند. در پاسخ، CSPها خصوصیات بیشتری برای پشتیبانی ایمن از پیوستگی محصولات IoT پیشنهاد می کنند. کیت های راه انداز IoT که مبتنی بر فضای ابری و مورد پسند سازنده هستند، در حال ورود به عرصه هستند تا به شرکت های محصولات و سرویس های IoT در استقرار ابری محصولات با حداقل تلاش کمک کنند. سازمان هایی که مسیر استانداردسازی این راهکارهای پیوستگی ابری را طی می کنند، باید تضمین کنند که کنترل های امنیتی موجود در هر پیشنهاد را درک می کنند.

برای مثال، اخیراً ARM با Freescale و IBM برای ساخت کیت راه انداز IoT مبتنی بر فضای ابری همکاری کرده است[5]. این کیت دارای یک MCU است که به طور خودکار اطلاعات را به یک وب سایت روی اینترنت می فرستد. اگرچه این کیت برای آموزش سازندگان در زمینه چگونگی ساخت آسان فضای ابری در راهکارهای IoT تجهیز شده است، اما ضروری است که سازندگان درک کنند انجام این کارها در عمل بسیار متفاوت بوده و نیازمند یک فرآیند مهندسی امنیتی است.

این بخش مبحثی درباره برخی از سرویس های ابری ارائه می کند که از سامانه های IoT پیشتیبانی خواهند کرد. با بکارگیری میلیاردها محصولات IoT در سرتاسر سامانه های گوناگون توسط سازمان ها، فضای ابری مکانیزم بهینه ای برای ردیابی موقعیت و وضعیت این دستگاه ها است. سرویس های ابری دیگری وجود خواهند داشت که برای پشتیبانی از مهیاسازی، بروزرسانی های سفت افزار و کنترل پیکربندی دستگاه توسعه یافته اند. با توجه به امکان تأثیر مستقیم وضعیت عملیاتی و امنیتی دستگاه IoT، امنیت این سرویس ها اهمیت ویژه ای

[5] http://www.eetimes.com/document.asp?doc_id=1325828

دارد. احتمالاً مهاجمان این سرویس ها را هدف خواهند گرفت که در این صورت، قابلیت تغییرات گسترده در وضعیت بسیاری از دستگاه ها به طور یکجا را ارائه می کنند.

2–1 مدیریت دارایی/موجودی

یکی از مهمترین جنبه های یک IoT امن، قابلیت ردیابی دارایی ها و فهرست موجودی ها است. این قابلیت، خصوصیات دستگاه ها را نیز در برمی گیرد. فضای ابری راهکار فوق العاده ای برای اجرای مدیریت دارایی/موجودی سازمان است که چشم اندازی برای تمام دستگاه هایی که جهت اجرا در مرزهای سازمان ها ثبت و احراز شده اند فراهم می کند.

2–2 مدیریت مهیاسازی، صورت حساب و امتیاز سرویس

این مسئله یک مورد کاربردی قابل توجه است به دلیل اینکه بسیاری از فروشندگان دستگاه های IoT، دستگاه های خود را به عنوان یک سرویس به مشتری ارائه خواهند کرد. این کار به قابلیت ردیابی امتیازات، مجوزدهی به فعالیت های دستگاه (یا لغو مجوزها) و همچنین آماده سازی صورت حساب ها در واکنش به میزان استفاده نیاز دارد. نمونه هایی از این مورد، سرویس های اشتراک برای نظارت با دوربین و دیگر نظارت های مبتنی بر حسگر (برای مثال سرویس ثبت و ضبط ابری DropCam)، نظارت و ردیابی وسایل پوشیدنی (برای مثال سرویس های دستگاه FitBit) و بسیاری موارد دیگر را شامل می شود.

2–3 نظارت بلادرنگ

فعالیت های ابری استفاده شده در پشتیبانی از قابلیت های حیاتی عملیاتی مانند مدیریت اضطرار، کنترل صنعتی و تولید می توانند قابلیت های نظارت بلادرنگ را فراهم کنند. هر جایی که امکان پذیر باشد، بسیاری از سازمان ها سامانه کنترل، نظارت صنعتی و دیگر قابلیت ها را به فضای ابری منقل می کنند تا هزینه های عملیاتی را کاهش داده، اطلاعات را دسترس پذیرتر کرده و سرویس های B2B و B2C جدیدی راه اندازی کنند. با افزایش تعداد نقاط پایانی IoT، دستگاه هایی مانند کنترلرهای منطقی قابل برنامه ریزی (PLCها)[6] و واحدهای ترمینال راه دور (RTUها)[7] به طور مستقیم به فضای ابری متصل می شوند که از قابلیت نظارت کارآمدتر و مؤثرتر بر سامانه ها پشتیبانی می کنند.

[6] Programmable Logic Controllers
[7] Remote Terminal Units

2-4 هماهنگی حسگر

تراکنش های ماشین به ماشین، قابلیت های پیشرفته ای را برای هماهنگی و حتی اداره خودکار تبادلات سرویس ها ارائه می کنند. با گذشت زمان، جریان های کاری خودکارتر خواهند شد که به طور فزاینده انسان ها را از حلقه تراکنش خارج می کنند. فضای ابری نقش کلیدی در اجرای این جریان های کاری خودکار ایفا خواهد کرد. برای مثال، سرویس های ابری ظهور خواهند کرد که دستگاه های IoT می توانند آخرین اطلاعات، محدودیت ها یا دستورالعمل ها جمع آوری کنند. پروتکل های انتشار/اشتراک که بسیاری از اجرائیات IoT (برای مثال، MQTT) و همچنین ارتباطات RESTful را کنترل می کنند، برای اجرای این موارد کاربردی جدید ایده آل هستند.

2-5 اطلاعات و بازاریابی مشتری

یکی از خصوصیات قدرتمند IoT، قابلیت اصلاح بازاریابی برای مشتریان است. Salesforce[8] یک فضای ابری IoT ایجاد کرده که به شدت روی دیدگاه ها و دیگر دستگاه های هوشمند متمرکز است. فضای ابری حاوی Thunder است که موتور بلادرنگ و جدید حوادث را معرفی می کند. این سامانه قابلیت راه اندازی خودکار پیام رسانی یا ارسال هشدارهایی به پرسنل فروش را برای مشتریان فراهم می کند. یک مثال خوب، مفهوم تبلیغات محلی هوشمند است. برای مثال در این موارد، مشتریان به محض ورود به فروشگاه یا مرکز خرید، از طریق مکانیزمی شناسایی می شوند. پس از شناسایی، سابقه خرید، اولویت ها یا دیگر خصوصیات آنها بررسی شده و پیام رسانی اصلاح شده ارائه می شود. از دیگاه حریم خصوصی، تفکر درباره اینکه چگونه مکانیزم ردیابی یا سوابق جمع آوری شده توسط نهاد مخرب علیه مشتری قابل استفاده است، اهمیت دارد.

دیگر انواع اطلاعات مشتری IoT، بهبود کارایی انرژی را شامل می شود که برای محیط منعفت دارند. برای مثال، دستگاه های خانگی می توانند اطلاعات مصرف را با سامانه های Backend ابری به عنوان بخشی از راهکار شبکه هوشمند به اشتراک گذارند؛ استفاده از دستگاه می تواند براساس نیاز و قیمت تعدیل شده باشد. با جمع آوری اطلاعات دستگاه های IoT که شامل زمان و بازه مصرف، انرژی مصرف شده و قیمت گذاری کنونی بازار می شود، دستگاه ها و کاربران می توانند به منظور ذخیره هزینه های انرژی و کاهش تأثیر محیطی، با تغییر الگوهای مصرف واکنش نشان دهند.

[8] شرکت محاسبات ابری

2–6 اشتراک اطلاعات

یکی از مزایای اولیه IoT این است که می توان اطلاعات را با سهامداران زیادی به اشتراک گذاشت. برای مثال، دستگاه پزشکی قابل جاسازی می تواند اطلاعاتی را به مطب ارائه کند و آن مطب نیز می تواند آن اطلاعات را برای بیمه گذار فراهم نماید. این اطلاعات در کنار دیگر اطلاعات جمع آوری شده از بیمار نیز قابل نگهداری هستند.

سرویس های اشتراک اطلاعات تبادل پذیر فضای ابری، پیش نیازهای اجباری برای اجرای تجزیه و تحلیل قدرتمند IoT هستند. با توجه به تنوع پلتفرم های سخت افزاری، سرویس ها و ساختارهای IoT، ارائه دهندگانی مانند «wot.io» قصد دارند سرویس های تبادل اطلاعات لایه میان افزار را برای منابع و مخازن فروشندگان اطلاعات حجیم فراهم کنند. بسیاری از برنامه ها و پروتکل های پشتیبانی کننده IoT مبتنی بر انتشار/اشتراک هستند که به طور طبیعی خود را به چارچوب های میان افزاری قرض می دهند که می توانند زبان های اطلاعاتی گوناگونی را تفسیر کنند. چنین سرویس هایی برای اجرای پیشنهادات B2B، B2I و B2C حیاتی هستند.

2–7 انتقال/انتشار پیام

فضای ابری و قابلیت های متمرکز، تطبیق پذیر و انعطاف پذیر آن، محیط ایده آلی برای پیاده سازی سرویس های مقیاس بزرگ تراکنش پیام IoT است. بسیاری از سرویس های ابری از HTTP، MQTT و دیگر پروتکل ها پشتیبانی می کنند که در ترکیب های گوناگون می توانند اطلاعات را از طریق دیگر روش های ملزوم منتقل، صادر، منتشر یا ارسال کنند (به طور متمرکز یا در مرز شبکه). یکی از بزرگترین موانع در خصوص پردازش اطلاعات IoT، مدیریت مقیاس است. در گفتار ساده، IoT به قابلیت معماری فضای ابری برای قیاس انعطاف پذیری سرویس های اطلاعاتی خود (و بدین ترتیب سرویس های انتقال/انتشار پیام) جهت برآورده کردن تقاضاهای بی سابقه و فزاینده نیاز دارد.

8-2 بررسی تهدیدات IoT از دیدگاه فضای ابری

بسیاری از تهدیدات هدف دار برای زیرساخت های مبتنی بر فضای ابری، با تهدیدات علیه سامانه های IT غیرابری مشابه یا یکسان هستند. بایستی در کنار بسیاری موارد دیگر، نمایه تهدیدات زیر در نظر گرفته شود:

ناحیه تهدید	اهداف/حملات
مدیران و کاربران سامانه ابری	• استخراج و استفاده از رمزهای عبور، Tokenها و/یا کلیدهای SSH مدیر برای ورود و تخریب فضای ابری خصوصی و مجازی سازمان (به خطر افتادن حساب اصلی AWS سازمان در نظر گرفته شود). • اسکریپت نویسی میان سایتی مرورگر وب روی ماشین های میزبان کاربر/مدیر. • فایل های مخرب (برای مثال، مبتنی بر JavaScript) از طریق وب گردی یا پیوست های ایمیل (کامپیوترهای روت شده مدیر، روش حمله قابل توجهی برای آلوده کردن تشکیلات مبتنی بر فضای ابری یک سازمان ارائه می کنند).
نقاط پایانی مجازی (VMها، محفظه ها)	• آسیب پذیری های VM و دیگر محفظه ها • آسیب پذیری های برنامه تحت وب • درگاه های ناامن IoT • رابط های ناامن IoT • وب سرورهای دارای پیکربندی نامناسب • پایگاه داده های آسیب پذیر (برای مثال، تزریق SQL) یا پایگاه داده های دارای پیکربندی نامناسب برای کنترل های دسترسی
شبکه ها	• مؤلفه های شبکه بندی مجازی • حمله رد سرویس به هر نقطه پایانی
تهدیدات فیزیکی و منطقی برای دستگاه های IoT که به فضای ابری متصل می شوند	• درگاه های غیرمتمرکز و ناامن IoT • دستکاری و تخریب ترافیک یا دسترسی به اطلاعات • دستکاری و تزریق فایل های مخرب به ترافیک پروتکل ارتباطی IoT بین دستگاه ها، درگاه های غیرمتمرکز و درگاه های ابری • جاسوسی از نقطه پایانی دستگاه IoT (تغییر مسیرهای ارتباطی یا فقدان احراز هویت/مجوزدهی مناسب) • فقدان رمزگذاری/محرمانگی

	• بسته های رمزی ضعیف • فقدان حفاظت از رمزهای آتی[9] • ذخیره سازی ناامن پایگاه داده (متن ساده یا کنترل دسترسی ضعیف) روی دستگاه • سرقت دستگاه های IoT

لیست قبل، تنها نمونه کوچکی از موضوعات امنیتی است که باید آنها را در زمان انتقال یا استفاده از زیرساخت های IoT به فضای ابری مدیریت کرد. خوشبختانه، ارائه دهندگان بزرگ فضای ابری یا شرکای آنها برای اکثر تهدیدات بالا پاسخ هایی دارند، حداقل برای آنهایی که درون مرز مطمئن CPS وجود دارند. با این وجود، کنترل های امنیتی مبتنی بر فضای ابری نمی توانند جایگزین مسئولیت های فروشندگان دستگاه برای تقویت دستگاه های IoT و تضمین قدرتمند بودن برنامه های مجازی و اجزای داخلی ماشین مجازی شوند. اینها چالش هایی هستند که سازمان های بکارگیرنده باید با آنها مواجه شوند.

در خصوص مقیاس نسبی خطرات مبتنی بر فضای ابری، در اکثر موارد قابلیت های خودکار زیرساخت به عنوان یک سرویس (IaaS)[10] فضای ابری، به احتمال زیاد می توانند خطرات امنیتی را برای دستگاه ها و سامانه های عملیاتی IoT سازمان کاهش دهند. با چندین استثنای تقریبی، پیشنهادات امنیتی موجود برای زیرساخت و سرویس های فضای ابری میزبانی شده به متخصصان امنیت سایبری کمتری نیاز داشته و می توانند هزینه های پشتیبانی امنیت مکانی را کاهش دهند. سرویس های مهیا شده IaaS ابری به احتمال زیاد دارای پیکربندی های به طور پیش فرض ایمن و اعمال شده برای VMها و شبکه ها هستند که به سازمان های سرویس گیرنده از طریق مقیاس اقتصادی رویه امنیتی منفعت می رسانند. قبل از بررسی عمیق امنیت فضای ابری برای IoT، ابتدا برخی از پیشنهادات و مزایای تجاری IoT که امروزه در فضای ابری قابل دسترسی هستند بررسی خواهند شد.

3 کاوش پیشنهادات IoT ارائه دهنده سرویس ابری

پیشنهادات امنیتی مبتنی بر فضای ابری که امنیت به عنوان یک سرویس (SECaaS)[11] نیز نامیده می شوند، تجارت به سرعت در حال رشد و دارای فضای ابری را نشان می دهند و این پیشنهادات برای پشتیبانی از IoT

[9] خصوصیتی از پروتکل های ارتباط امن است که در صورت به خطر افتادن کلیدهای طولانی مدت، کلیدهای اتصال قبلی به خطر نمی افتند. این خصوصیت از اتصالات قبلی در مقابل به خطر افتادن آتی کلیدهای رمز یا رمزهای عبور محافظت می کند.

[10] Infrastructure-as-a-Service
[11] Security-as-a-Service

آماده هستند. نه تنها پیشنهادات SECaaS قیاس پذیر هستند، بلکه به سازمان ها در تأمین منابع محدود و دائماً در حال افول مهندسی امنیتی کمک می کند. اکثر سازمان های امروزی فاقد افراد و دانش مورد نیاز برای اجرای یکپارچگی امنیتی، بروز بودن با آخرین تهدیدات امنیتی، طراحی مراکز عملیاتی امنیتی و اجرای نظارت بر امنیت هستند. CPSها راهکارهایی ارائه می کنند.

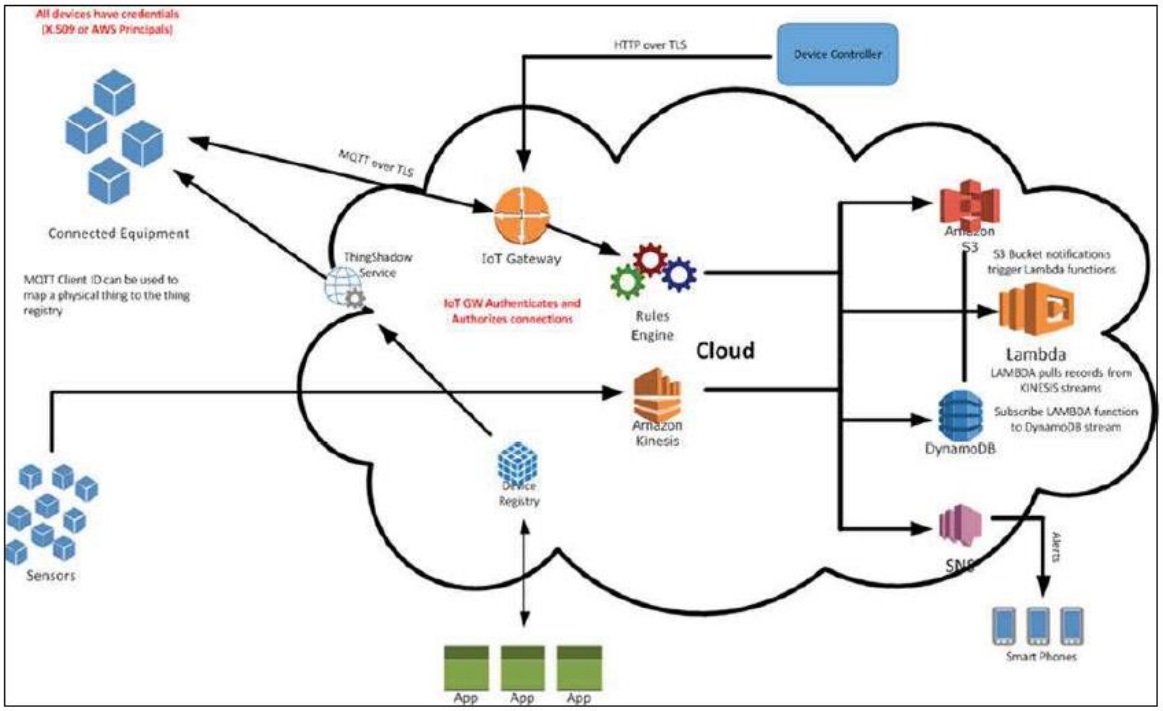
1–3 AWS IoT

Amazon اصلی ترین اجراکننده سرویس های IoT مبتنی بر فضای ابری است و در بسیاری موارد ارائه دهنده فضای ابری IoT خواهد بود. به گفته Amazon:

> AWS IoT یک پلتفرم ابری مدیریت شده است که به دستگاه های پیوسته اجازه می دهد به سادگی و به طور ایمن با برنامه های ابری و دیگر دستگاه ها ارتباط داشته باشند. AWS IoT می تواند از میلیاردها دستگاه و تریلیاردها پیام پشتیبانی کند و می تواند به طور مطمئن و ایمن آن پیام ها را پردازش و به نقاط پایانی AWS و دیگر دستگاه ها هدایت کند.[۱۲]

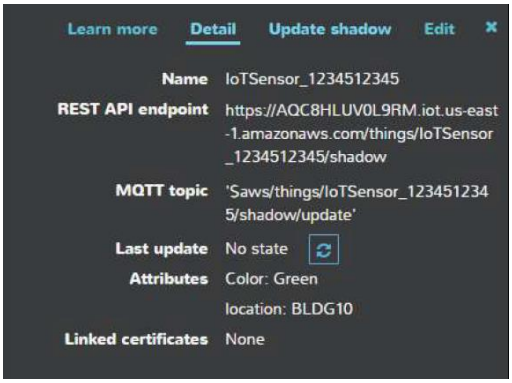
AWS IoT چارچوب Amazon است که به دستگاه های IoT اجازه می دهد با فضای ابری و با استفاده از مجموعه ای از پروتکل ها (HTTP، MQTT و غیره) ارتباط برقرار کند. زمانی که دستگاه های IoT در فضای ابری قرار گرفتند، می تواند با یکدیگر و دیگر سرویس ها از طریق رابط های برنامه ارتباط برقرار کنند. AWS IoT با تنوعی از دیگر سرویس های Amazon یکپارچه می شود. برای مثال، می توان از موتور انتشار و تحلیل بلادرنگ آن به نام «Kinesis» استفاده کرد. Kinesis Firehose به عنوان پلتفرم مصرف کننده و پذیرنده جریان های اطلاعاتی و بارگذاری آن در دیگر دامنه های Amazon از قبیل سرویس ساده ذخیره سازی (S3)[۱۳]، Redshift (ذخیره سازی اطلاعات) و جستجوی ارتجاعی Amazon (ES)[۱۴] عمل می کند. زمانی که در پلتفرم اطلاعاتی مناسب قرار گرفتند، مجموعه ای از تجزیه و تحلیل ها با استفاده از Kinesis Streams و Kinesis Analytics قابل اجرا هستند. Amazon Glacier[15] آرشیوبندی قیاس پذیر و بلند مدت اطلاعات و پشتیبانی برای اطلاعات با دسترسی کمتر ارائه می کند. در زمینه پشتیبانی از برنامه ها و تشکیلات IoT، AWS IoT به خوبی با Amazon Lambda، Kinesis، S3، CloudWatch، DynamoDB و مجموعه ای از دیگر سرویس های ابری مهیا شده توسط Amazon یکپارچه می شود:

[12] http://aws.amazon.com/iot/
[13] Simple Storage Service
[14] Elastic Search
[15] https://aws.amazon.com/glacier/



مجموعه ای از صنایع از جمله بهداشت شروع به بکارگیری پلتفرم Amazon IoT کرده اند. برای مثال، Philips برای استفاده از سرویس های AWS IoT به عنوان موتوری برای پلتفرم دیجیتالی HealthSuite خود شریک شده است. این پلتفرم به گونه ای طراحی شده تا به ارائه دهندگان سرویس پزشکی و بیماران اجازه تعامل به روش های جدید و تغییرپذیر و با استفاده از دستگاه های بهداشتی، منابع اطلاعاتی قدیمی، تجزیه و تحلیل ها و گزارش گیری را می دهد. بسیاری از دیگر شرکت های مرتبط با IoT شروع به استفاده یا شراکت با AWS در فعالیت های IoT خود کرده اند.

سرویس های CPS IoT مانند AWS IoT، قابلیت پیش تنظیم دستگاه های IoT و سپس بارگذاری پیکربندی ها در دستگاه های فیزیکی پس از اعلام آمادگی برای آنلاین شدن را پیشنهاد می کنند. زمانی که قابل استفاده شد، AWS IoT یک Thing Shadow مجازی ارائه می کند که می تواند وضعیت دستگاه IoT را در زمان آفلاین بودن حفظ کند. وضعیت پیکربندی در یک سند JSON که در فضای ابری ذخیره شده نگهداری می شود. بنابراین، برای مثال در صورتی که لامپ دارای MQTT آفلاین شد، یک دستور MQTT به انبار اشیای مجازی جهت تغییر رنگ آن قابل ارسال است. زمانی که لامپ دوباره آنلاین می شود، به طور صحیح رنگ خود را تغییر خواهد داد:



AWS Thing Shadow یک رابط بین برنامه کنترل کننده و دستگاه IoT است. Thing Shadow ها از پروتکل MQTT با موضوعات از پیش تعریف شده استفاده می کنند که برای تعامل با سرویس و دستگاه قابل استفاده هستند. پیام های MQTT که برای سرویس Thing Shadow ذخیره شده اند با «$aws/things/thingName/shadow» شروع می شوند. در زیر موضوعات ذخیره شده MQTT ذکر شده اند که برای تعامل با Shadow قابل استفاده هستند[۱۶]:

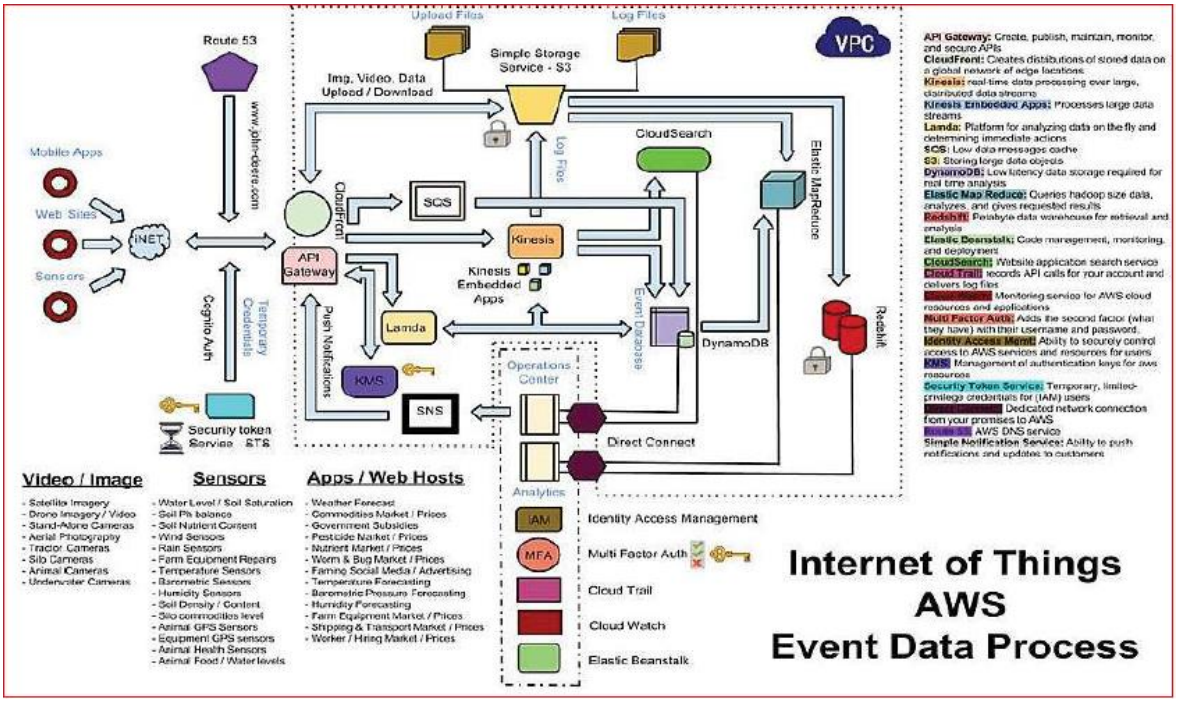
- /update
- /update/accepted
- /update/documents
- /update/rejected
- /update/delta
- /get
- /get/accepted
- /get/rejected
- /delete
- /delete/accepted
- /delete/rejected

اشیاء (Things) می تواند بروزرسانی شوند یا Thing Shadow دریافت کنند. AWS IoT یک مستند JSON برای هر بروزرسانی منتشر کرده و به هر درخواست دریافت بروزرسانی با وضعیت «/accepted» یا «rejected» پاسخ می دهد.

از دیدگاه امنیتی، ضروری است که فقط نقاط پایانی و برنامه های مجاز قادر به انتشار در این موضوعات باشند. همچنین ضروری است که کنسول مدیریتی به شکل صحیح قفل شده تا عاملان غیرمجاز نتوانند برای پیکربندی مستقیم دارایی های IoT به آن دسترسی پیدا کنند.

[16] http://docs.aws.amazon.com/iot/latest/developerguide/thing-shadow-mqtt.html

به منظور تشریح گردش کار پردازش اطلاعات AWS IoT، یک مورد کاربردی اضافی برای یک مزرعه بررسی می شود که از قابلیت های پردازش اطلاعات فضای ابری AWS استفاده می کند.

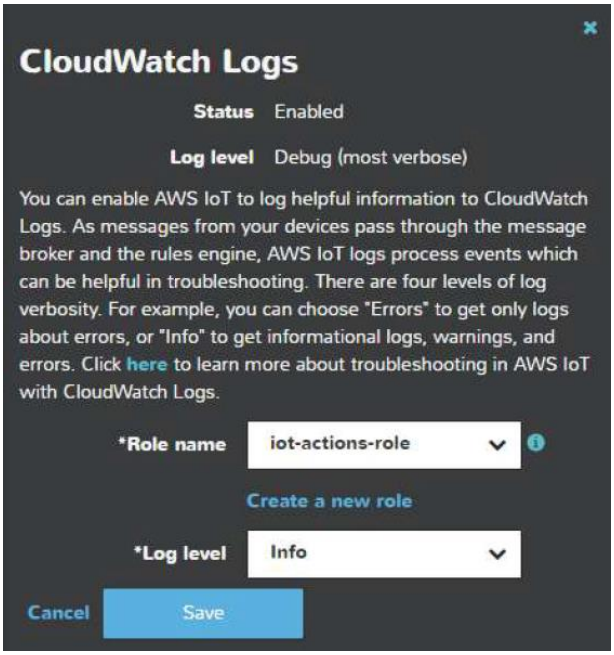


در این مورد کاربردی، چندین نقطه پایانی وجود دارد که اطلاعات را به فضای ابری AWS تزریق می کنند. اطلاعات از طریق چندین درب جلویی احتمالی وارد AWS می شود:

- Kinesis
- Kinesis Firehose
- MQTT broker

زمانی که اطلاعات وارد AWS شد، AWS IoT، قابلیت های موتور را به عنوان نقطه تصمیم گیری تعیین کرده تا مسیری که باید اطلاعات به آن فرستاده شود و هرگونه اقدام اضافی که باید روی اطلاعات صورت پذیرد مشخص گردد. در بسیاری از موارد، اطلاعات به پایگاه داده ارسال خواهد شد (برای مثال، S3 یا DynamoDB). Redshift نیز قابل اعمال بوده و باید برای حفظ سوابق در گذر زمان و همچنین برای ذخیره سازی بلند مدت اطلاعات استفاده شود.

در بسته AWS IoT، می توان از خصوصیات مدیریت یکپارچه گزارش از طریق CloudWatch استفاده کرد. به منظور گزارش گیری از حوادث فرآیندها روی جریان پیام های ارسالی دستگاه ها به زیرساخت AWS، CloudWatch در AWS IoT به طور مستقیم قابل تنظیم است. گزارش گیری از پیام می تواند برای پیام های خطا، هشدارها، پیام های اطلاعاتی یا پیام های عیب یابی تنظیم شود. اگرچه عیب یابی جامع ترین پیام ها را ارائه می کند، اما فضای ذخیره سازی بیشتری نیز دربرمی گیرد:



Amazon CloudTrail باید برای تشکیلات IoT مبتنی بر AWS نیز استفاده شود. CloudTrail از فراخوانی های AWS API سطح حساب برای اجرای تحلیل امنیتی، تجزیه و تحلیل و ردیابی سازگارپذیری پشتیبانی می کند. سامانه های مدیریت گزارش ثالث زیادی وجود دارد، مانند AlertLogic و SumoLogic که مستقیماً با CloudTrail یکپارچه می شوند.

2–3 بسته Microsoft Azure IoT

Microsoft نیز با Azure IoT Hub خود گام بزرگی در فضای ابری برداشته است. Azure خصوصیات قدرتمند مدیریت دستگاه IoT برای مجریان از جمله بروزرسانی و تنظیم نرم افزار/سفت افزار دستگاه دارد. فراتر از مدیریت دستگاه IoT، Azure خصوصیاتی ارائه می کند که به سازندگان اجازه می دهد دستگاه ها را در دامنه های عملیاتی خود سازماندهی و دسته بندی کنند. به عبارت دیگر، مدیریت توپولوژی سطح دستگاه IoT و همچنین پیکربندی به ازای هر دستگاه (پیش نیازی برای استقرار مدیریت سطح گروه، مجوزها و کنترل دسترسی) را ارائه می کند.

سرویس مدیریت گروه Azure از طریق API گروه دستگاه فراهم شده، در حالی که خصوصیات مدیریت، نسخه بندی نرم افزاری، مهیاسازی دستگاه و غیره از طریق API مدیریت رجیستری دستگاه آن ارائه شده اند[۱۷]. احراز هویت متمرکز با استفاده از چارچوب احراز هویت کنونی Azure Active Directory ارائه شده است.

[17] https://azure.microsoft.com/en-us/documentation/articles/iot-devguide/

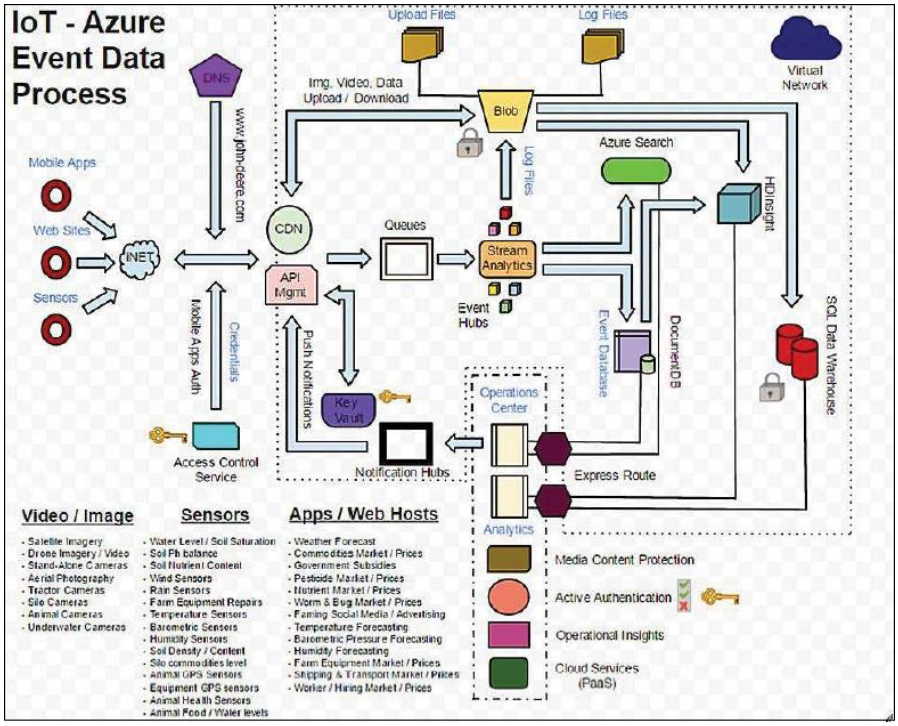
Azure IoT Hub از پروتکل های مرتبط با IoT مانند MQTT، HTTP و AMQP برای فعالسازی ارتباط دستگاه به فضای ابری و فضای ابری به دستگاه پشتیبانی می کند. با توجه تنوع اجتناب ناپذیر بودن استانداردهای ارتباطی، Azure قابلیت های ادغام میان پروتکلی را برای سازندگان از طریق قالب پیام عمومی IoT Hub فراهم می کند. قالب پیام از مجموعه ای از فیلدهای خصوصیت سامانه و برنامه تشکیل می شود. در صورت نیاز، ارتباطات دستگاه به فضای ابری می توانند از APIهای هاب فعلی حوادث Azure استفاده کنند، ولی در صورتی که احراز و کنترل دسترسی برای هر دستگاه مورد نیاز باشد، IoT Hub از آن پشتیبانی خواهد کرد.

احراز هویت و کنترل دسترسی برای هر دستگاه در Azure از طریق استفاده از Tokenهای امنیتی IoT Hub امکان پذیر است که هر سیاست و مجوز دسترسی دستگاه را نگاشت می کنند. احراز هویت مبتنی بر Token اجازه می دهد احراز هویت بدون انتقال پارامترهای امنیتی حساس از طریق سیم انجام شود. Tokenها بر کلید منحصر به فرد و تولید شده توسط Azure مبتنی هستند که با استفاده از ID دستگاه همراه سازنده یا ارائه شده توسط مجری تولید شده است.

به منظور تشریح گردش کار پردازش اطلاعات Azure IoT، به سامانه IoT مزرعه یکپارچه برگشته و پیکربندی Backend در Azure بررسی می شود. در خصوص AWS، نقاط ورودی گوناگونی در فضای ابری برای دستگاه های پیوسته وجود دارد. اطلاعات در Azure از طریق درگاه API یا از طریق سرویس های IoT که از REST و MQTT پشتیبانی می کنند، قابل تزریق هستند. سپس اطلاعات حافظه BLOB[18] یا DocumentDB قابل ارسال هستند. همچنین شایان ذکر است که شبکه ارسال محتویات Azure (CDN)[۱۹] ابزار مناسبی برای توزیع بروزرسانی های سفت افزار به موجودی دستگاه IoT است:

[18] مجموعه ای از اطلاعات باینری ذخیره شده

[19] Content Delivery Network



3–3 محاسبات مه مانند Cisco

استراتژی Cisco IoT برای فضای ابری این واقعیت را تشریح می کند که اکثریت دستگاه های IoT در مرز شبکه در تقابل با ناحیه نزدیک به پردازش متمرکز ابری فعالیت می کنند. بدین ترتیب، لغت «مه» (رطوبت قابل دید در سطح زمین (مرز) در مقابل ابر متمرکز (آسمان)) نشان دهنده بازاریابی Cisco از مفهوم شناخته شده محاسبات مرزی است. مقیاس خالص IoT، به منابع عملیاتی و امنیتی بسیار قدرتمند که در شبکه و پشته های کاربردی در مرزهای شبکه سازمان یکپارچه شده اند نیاز خواهد داشت. مزایای نگهداری اطلاعات و تا حد امکان پردازش به صورت مرکزی مرزی شامل موارد زیر می شود:

- **تأخیر کاهش یافته:** بسیاری از برنامه های مرزی متمرکز بر اطلاعات برای IoT بلادرنگ هستند به دلیل اینکه آنها مقادیر عظیمی از اطلاعات حسگر، تصمیم گیری محلی و واکنش را دربرمی گیرند.
- **بازده اطلاعاتی و شبکه:** مقادیر اطلاعاتی که IoT را تشکیل می دهند بسیار عظیم هستند و موارد بسیاری وجود دارد که مسدودسازی پورت شبکه ها فقط به منظور جابه جایی اطلاعات برای برنامه و حفظ امنیت منطقی به نظر نمی رسد.
- سیاست ها براساس شرایط مرز محلی، قابل مدیریت و کنترل محلی هستند.
- قابلیت اطمینان، دسترس پذیری و امنیت در مرز IoT براساس نیازهای محلی بهبود یافته اند.

شاید مزایای ذکر شده برای IoT صنعتی که فقط پردازش ابری مرکزی نیست، بسیار محسوس باشند. جریان حسگرهای حساس به زمان، کنترلرها و محرک ها، نظارت و گزارش گیری از برنامه ها و مجموعه اطلاعات حجیم که با IoT صنعتی مرتبط هستند، محاسبات مه مانند را به مدل جذابی تبدیل کرده اند.

با وجود اینکه محاسبات مه مانند Cisco در ابتدای چرخه حیات خود قرار دارد، از قبل در IOx[20] پیاده سازی شده است (چارچوب میان افزاری که بین سخت افزار و برنامه های مستقیماً اجراشونده روی تجهیزات مرزی قرار می گیرد). معماری پایه Iox از موارد زیر تشکیل می شود:

- **گره های Fog**: اینها نشان دهنده دستگاه هایی هستند (برای مثال، مسیریاب ها و سوییچ ها) که شبکه های مرزی را دربرمی گیرند و منابع میزبان را برای چارچوب Fog فراهم می کنند.
- **سیستم عامل میزبان:** روی گره های Fog، سیستم عامل میزبان قرار گرفته که از موارد زیر پشتیبانی می کند:
  - **چارچوب برنامه Cisco (CAF)**[21] برای مدیریت و کنترل برنامه محلی.
  - **برنامه ها** (از انواع گوناگون و امکان پذیر)
  - **سرویس های شبکه و میان افزار**
- **اداره کننده Fog**: پس از اتصال به APIهای شمالی CAF، اداره کننده Fog، مدیریت و مخازن متمرکز برنامه را برای برنامه های اجراشونده روی تمام گره های Fog فراهم می کند. مدیریت از طریق اداره کننده Fog و بواسطه درگاه Fog قابل دسترسی است.

توسعه محاسبات مه مانند IoT توسط کیت های توسعه نرم افزاری Cisco DevNet پشتیبانی شده است. سازمان های IoT می توانند از راهکارهای امنیت سایبری موجود مانند Cisco Netflow، TrustSec و موتور سرویس های هویتی (ISE)[22] نیز استفاده کنند.

[20] https://developer.cisco.com/site/iox/technical-overview/
[21] Cisco Application Framework
[22] Identity Services Engine

4–3 پلتفرم IBM Watson IoT

IBM Watson نیاز به معرفی ندارد. دنیا از سال 2010، زمانی که پلتفرم محاسبات شناختی Watson بهترین رقبا را در برنامه تلویزیونی معروف به نام «Jeopardy» شکست داد با قابلیت های آن آشنا است. قابلیت یادگیری و برطرف کردن مشکلات از مجموعه اطلاعات عظیم و تزریق شده در محاسبات شناختی Watson، در صنایع گوناگونی مانند بهداشت به خوبی مورد استفاده قرار گرفته است. امروزه، IBM از طریق اعمال دامنه پردازش Watson به اینترنت اشیاء در حال تقویت آن است. APIهای IoT عملیاتی IBM از طریق مرکز توسعه پلتفرم Watson IoT[23] قابل دسترسی هستند و شامل قابلیت های تعاملی مانند موارد زیر می شود:

- ایجاد لیست و بررسی دستگاه های IoT سازمان
- ثبت، بروزرسانی و بررسی دستگاه ها
- انجام عملیات روی مجموعه داده های تاریخی و تزریق شده

5–3 رابط های MQTT و REST

تراکنش ها و ارتباطات دستگاه IoT از طریق پشتیبانی پلتفرم از پروتکل های ارتباطی MQTT و REST تسهیل شده اند[۲۴] که به سازندگان IoT اجازه می دهند قابلیت های قدرتمند تزریق اطلاعات، تجزیه و تحلیل شناختی و خروجی اطلاعات را ایجاد کنند.

MQTT API پلتفرم Watson IoT، اتصالات رمزگذاری نشده روی درگاه 1883 و ارتباطات رمزگذاری شده روی درگاه های 8883 یا 443 را امکان پذیر می کند. شایان ذکر است که پلتفرم به TLS 1.2 نیاز دارد. بسته های رمزی پیشنهادی IBM عبارتند از:

- ECDHE-RSA-AES256-GCM-SHA384
- AES256-GCM-SHA385
- ECDHE-RSA-AES128-GCM-SHA256
- AES128-GCM-SHA256

ثبت دستگاه ها نیازمند استفاده از اتصال TLS است، به دلیل اینکه رمز عبور MQTT که توسط تونل TLS محافظت شده به مشتری برگردانده شده است.

زمانی که از MQTT برای اتصال دستگاه به فضای ابری استفاده شده، گزینه استفاده از یک Token بجای رمز عبور MQTT وجود دارد. در این مورد، مقدار «use-token-auth» بجای رمز عبور ارائه شده است.

---

[23] https://developer.ibm.com/iotfoundation/ and https://dveloper.ibm.com/iotfoundation/recipes/api-documentation/
[24] https://docs.internetofthings.ibmcloud.com/devices/mqtt.html

رابط REST نیز با TLS 1.2 ایمن شده است. درگاه مجاز 443 است و کلید API برنامه به عنوان نام کاربری عمل می کند، در حالی که Token احراز هویت به پشتیبانی از احراز هویت پایه HTTP به عنوان رمز عبور استفاده شده است.

4 کنترل های امنیتی IoT فضای ابری

با توجه به تنوع سرویس های مبتنی بر فضای ابری که از تشکیلات IoT پشتیبانی می کنند، هر نقطه پایانی ابری و ذینفع نقش حیاتی در ایمن سازی بسیاری از تراکنش ها ایفا می کند. این بخش لیست خلاصه ای از کنترل ها و سرویس های امنیتی پیشنهادی IoT ارائه می کند که سازمان باید در نظر بگیرد. کنترل های اصلی مانند احراز هویت و رمزگذاری در فضای ابری توسط تمام CSPها پشتیبانی شده اند، ولی باید CSP ها براساس پیشنهاداتشان در دیگر حوزه ها به دقت بررسی و در نظر گرفته شوند.

اکثر CSPها سرویس هایی را به روش های مختلف دسته بندی می کنند. سازمان می تواند به طور مستقیم یا غیرمستقیم این سرویس ها را براساس پیشنهادات بسته ی خاص، دریافت و از آنها منفعت ببرد. این سرویس ها به منظور ساخت ارتباطات ایمن انتقالی و قدرتمند در سرتاسر زیرساخت مجازی سازی شده به روش های مختلفی قابل ترکیب هستند.

4–1 احراز هویت (و مجوزدهی)

با در نظر گرفتن کنترل های امنیتی احراز هویت، سازمان باید اکثر موارد زیر را مدیریت کند:

1. اعتبار مدیر برای افراد دارای دسترسی به قابلیت ها و APIهای مدیریتی تأیید شود (در اینجا احراز هویت چند عاملی، با توجه به حساسیت زیاد کنترل های مدیریتی در زیرساخت مجازی ترجیح داده شده است).
2. کاربران نهایی برنامه های ابری احراز شوند.
3. برنامه های ابری از یکدیگر احراز شوند (از جمله درگاه ها و رابط های IoT).
4. دستگاه های IoT مستقیماً در درگاه ها و رابط ها احراز شوند (دستگاه هایی که دارای منابع عملیاتی و امنیتی ملزوم هستند).
5. کاربران نهایی از یک ارائه دهنده برنامه به ارائه دهنده دیگری احراز پراکسی شوند.

تنوعی از مکانیزم های احراز هویت توسط CSPها پشتیبانی شده اند. Amazon AWS و Microsoft Azure در بخش های زیر توصیف شده اند.

4-1-1 Amazon AWS IAM

سرویس احراز هویت AWS IAM که توسط فضای ابری Amazon پشتیبانی شده، پلتفرم احراز هویت چند خصوصیتی است که از هویت واحد، احراز هویت چند عاملی، مدیریت کاربر/نقش/مجوز و یکپارچگی کامل با دیگر سرویس های Amazon پشتیبانی می کند.

سرویس احراز هویت چند عاملی AWS IAM (برای مثال مبتنی بر Token) (MFA)[۲۵] از مجموعه ای از عوامل قالب MFA جهت تطبیق سازمان با چارچوب احراز هویت جدید یا چارچوب کنونی پشتیبانی می کند. Tokenهای سخت افزاری، حلقه کلیدها[۲۶]، کارت های دسترسی و دستگاه های MFA مجازی سازی شده (برای مثال، آنهایی که می توانند روی دستگاه موبایل اجرا شوند) توسط Amazon پشتیبانی شده اند. MFA توسط مدیران فضای ابری خصوصی و مجازی و همچنین کاربران نهایی قابل استفاده است.

احراز هویت ایمن انتقالی که بین چندین برنامه تحت وب جریان دارد (مخصوصاً مرورگرها)، توسط OAuth2.0 (RFC6749) قابل ارائه هستند (یک استاندارد باز برای احراز هویت که اجازه دسترسی ایمن و اختصاصی به وب سرویس های ثالث را می دهد). با این وجود، OAuth2 فقط دسترسی احراز هویت را فراهم می کند. قابلیت احراز هویت از طریق استفاده از سرویس OpenID Connect (OIDC)[۲۷] قابل ارائه بوده که براساس OAuth2 ساخت شده است. OIDC از Tokenهای شناسایی حاصل شده از طریق تراکنش OAuth2، به منظور پشتیبانی از احراز مجوزدهی برای کاربران استفاده می کند.

4-1-2 احراز هویت Azure

همانطور که قبلاً ذکر شد، Microsoft Azure احراز هویت متمرکز و واحد از طریق چارچوب احراز هویت Azure Active Directory (AD)[۲۸] خود ارائه می کند. Microsoft Azure «شناسایی به عنوان یک سرویس» OAuth2 و OpenID Connect را نیز در پیشنهاد Azure AD خود ارائه می کند. Amazon AWS این قابلیت و همچنین بخشی از پیشنهاد مدیریت هویت و دسترسی خود را ارائه می کند. در صورتی که ارائه دهنده فضای ابری انتخاب شده، OpenID Connect را پیشنهاد نکرده ولی OAuth2 را ارائه می کند، احتمالاً امکان یکپارچه کردن سرویس OAuth2 از ارائه دهنده یک با سرویس OpenID Connect (برای Tokenهای احراز هویت) از ارائه دهنده دو وجود دارد، هرچند که ارائه یک سرویس از طرف یک ارائه دهنده بعید به نظر می رسد.

[25] Multi-factor Authentication

[26] حلقه هایی که کلید را به دسته کلید وصل می کنند.

[27] OpenID Connect

[28] Active Directory

4-2 بروزرسانی های نرم افزاری/سفت افزاری

تعداد زیادی از آسیب پذیری های موجود در پشته های اجرای نرم افزار و سفت افزار از طریق چارچوب های وصله سریع، آسان و خودکار قابل پیشگیری هستند. به شدت پیشنهاد می شود یک قابلیت بروزرسانی خودکار و ایمن نرم افزار و سفت افزار برای دستگاه های نهایی پیاده سازی شود. فایل های اجرایی جدید یا بسته های اجرایی (وصله ها) باید به طور دیجیتالی در محیط DevOps و توسط سرویس امضای نرم افزاری قدرتمند امضا شده باشند. در خصوص دستگاه های نهایی، باید تضمین شود که بروزرسانی های نرم افزاری و سفت افزاری منتشرشونده به دستگاه های IoT نهایی، دارای قابلیت تصدیق از طریق آن دستگاه های نهایی هستند.

برخی CSPها از سرویس های نرم افزاری/سفت افزاری مانند Azure CDN و غیره پشتیبانی می کنند.

4-3 پیشنهادات امنیتی نقطه پایانی به نقطه پایانی

پیشنهادات امنیتی نقطه پایانی به نقطه پایانی زیر در تشکیلات ابری IoT در نظر گرفته شوند.

- تضمین شود که امنیت در درگاه از بین نرفته است. در حالت ایده آل، حفاظ های احراز هویت و یکپارچگی نقطه پایانی به نقطه پایانی باید از CSP تا دستگاه های IoT دارای درگاه های عمل کننده به عنوان گذرگاه ادامه داشته باشد. اگرچه این کار همیشه امکان پذیر نیست، ولی زمانی که گره های حسگر بکار گرفته شده جهت تصدیق اعتبار و یکپارچگی بروزرسانی ها و دستورات سفت افزار به درگاه تکیه می کنند باید اقدامات دفاعی جانبی اتخاذ شود.
- اعمال رویه های امن توسعه نرم افزار برای سرویس های وب و مجموعه اطلاعاتی که در خدمت دستگاه های IoT هستند.
- حفاظت کافی از برنامه های ابری که از جریان های تحلیل و گزارش گیری پشتیبانی می کنند.
- اعمال پیکربندی های امن برای مجموعه داده هایی که به برنامه های تحلیل و گزارش گیری تزریق می شوند.
- اعمال حفاظ های یکپارچگی برای اطلاعات دستگاه IoT. این کار نیازمند استفاده از حفاظ های یکپارچگی روی اطلاعات منتقل شده از دستگاه IoT به درگاه و همچنین درگاه به فضای ابری است.
- دستگاه های اجاره ای در محیط مشتری فعالیت خواهند کرد و ارائه دهندگان سرویس سهواً شبکه های مشتریان خود را با بدافزار آلوده نخواهند کرد (و برعکس). جداسازی این دستگاه ها روی شبکه های مشتریان باید در زمان ممکن انجام شود. این مورد کاربردی، قابلیت کلاهبرداری و/یا سرقت از سرویس های به سرقت رفته را امکان پذیر می کند و بدین ترتیب طراحی دستگاه ها به شکلی که از دستکاری جلوگیری کند، ضروری است. این کار با استفاده از حفاظ های ضد دستکاری یا واکنش گرا در برابر دستکاری قابل دستیابی است که در منابعی مانند NIST FIPS 140-2 توصیف شده اند.

- از تشکیلات ابری IoT به وسیله درگاه های قدرتمند و به طور صحیح تنظیم شده و تعدیل کننده بار، در مقابل حملات رد سرویس حفاظت شود (امروزه چندین راهکار صنعتی فوق العاده برای این مورد وجود دارد).
- ارائه تضمین هایی که نشان دهند اطلاعات منتقل شده به دستگاه های IoT (یا درگاه ها) توسط خود دستگاه ها احراز شده اند.
- رمزگذاری اطلاعات در صورت نیاز.
- تراکنش ها و پیام رسانی بین خود دستگاه ها (M2M) باید احراز شده باشد (از نظر یکپارچگی محافظت شده باشد).
- در تمام موارد، ارائه دهندگان سرویس باید بتوانند کنترل های امنیتی مرتبط با اطلاعات تولید شده توسط یک فرد یا یا دستگاه که می توان آن را به یک فرد ربط داد، ردیابی کنند. در مورد دستگاه پزشکی، آیا بیمار نه تنها از کاربرد اطلاعات تولید شده در مطب ها، بلکه برای هرگونه اطلاعاتی که توسط دستگاه های پیوسته در فضای ابری بارگذاری شده، مطلع شده و آن را احراز کرده است؟ اطلاعیه ها باید شامل هر سازمانی که ممکن است اطلاعات با آن به اشتراک گذاشته شود نیز شود.
- زمانی که ممکن است اطلاعات به سازمان های زیادی منتقل شده باشند، حفظ کنترل اطلاعات از طریق تخریب امکان پذیر نیست؛ هرچند، ارائه دهندگان سرویس باید تلاش کنند توافقات حریم خصوصی با سازمان های همتا را کسب کنند. به علاوه، کفایت کنترل های امنیتی پیاده سازی شده توسط آن سازمان ها ارزیابی شود.
- پیاده سازی کنترل های دسترسی انعطاف پذیر (استفاده از کنترل های دسترسی مبتنی بر صفت برای تصمیمات دسترسی دقیق تر).
- برچسب گذاری اطلاعات برای حفاظ های حریم خصوصی.
- ارائه اطلاعیه هایی در خصوص استفاده از اطلاعات.

4-4 حفظ یکپارگی اطلاعاتی

چگونه می توان یکپارچگی اطلاعاتی که برای مقاصد بیشمار و توسط ذینفع های بسیاری استفاده خواهند شد را تضمین کرد؟ در چارچوب سامانه IoT سازمانی، قابلیت اطمینان به اطلاعات جمع آوری شده حیاتی است. این کار نیاز به موارد زیر دارد:

- کنترل های احراز هویت و یکپارچگی اعمال شده برای دستگاه های IoT به منظور تضمین اینکه دستگاه های سرکش نتوانند اطلاعاتی به فضای ابری منتقل کنند.
- پیکربندی ایمن دستگاه های درگاه ها. ممکن است دستگاه های درگاه ها در مکان نصب شده باشند یا در فضای ابری فعالیت کنند، ولی این دستگاه های درگاه مقادیر عظیمی از اطلاعات را پردازش می کنند و بدین ترتیب باید از طریق موارد زیر ایمن سازی شوند:
  - گزارش گیری و تحلیل امنیت در یک SIEM.
  - پیکربندی های امن (سیستم عامل، پایگاه داده، برنامه).
  - حفاظت با دیوار آتشین
  - ارتباطات رمزگذاری شده روی هر رابط. این کار به استفاده از ارتباط رمزگذاری شده روی رابط مبتنی بر فضای ابری نیاز دارد. این کار معمولاً با امنیت لایه انتقال (TLS) و یک بسته رمزی مناسب حاصل می شود. روی رابط مبتنی بر حسگر، ارتباطات RF رمزگذاری شده به شدت توصیه می شوند.
  - احراز هویت قدرتمند با استفاده از مجوزهای PKI، در صورتی که امکان پذیر باشد.
- معیارهای امنیت نرم افزار برای وب سرویسی که با درگاه ها یا دستگاه ها ارتباط داشته و از آنها اطلاعات جمع آوری می کند.
- پیکربندی های ایمن زیرساخت (برای مثال، وب سرور) پشتیبانی کننده از وب سرویس IoT.

4-5 خود راه اندازی و ثبت امن دستگاه های IoT

به منظور اطمینان به مجوزهای استفاده شده جهت احراز هویت سرویس ها و درگاه ها توسط یک دستگاه خاص، بایستی حین مهیاسازی اولیه امنیتی برای دستگاه ها دقت شود. با توجه به اهمیت یک دستگاه خاص، خودراه انداز می تواند در سمت فروشنده یا شخصاً توسط یک عامل مطمئن رخ دهد. تکمیل خود راه انداز و ثبت، قابلیت مهیاسازی امن مجوزهای عملیاتی برای دستگاه ها (و روی شبکه) را در پی دارد.

4-6 نظارت امنیتی

درگاه ها/رابط های IoT باید به منظور جستجوی رفتار مشکوک نقاط پایانی پیکربندی شوند. برای مثال، رابط های MQTT باید پیام هایی از طرف ناشران و شرکایی دریافت کنند که ممکن است رفتار مخربی از خود نشان دهند. دستورالعمل های MQTT نسخه 3.1.1 نمونه هایی از رفتارهای گزارش شده را ارائه می کند:

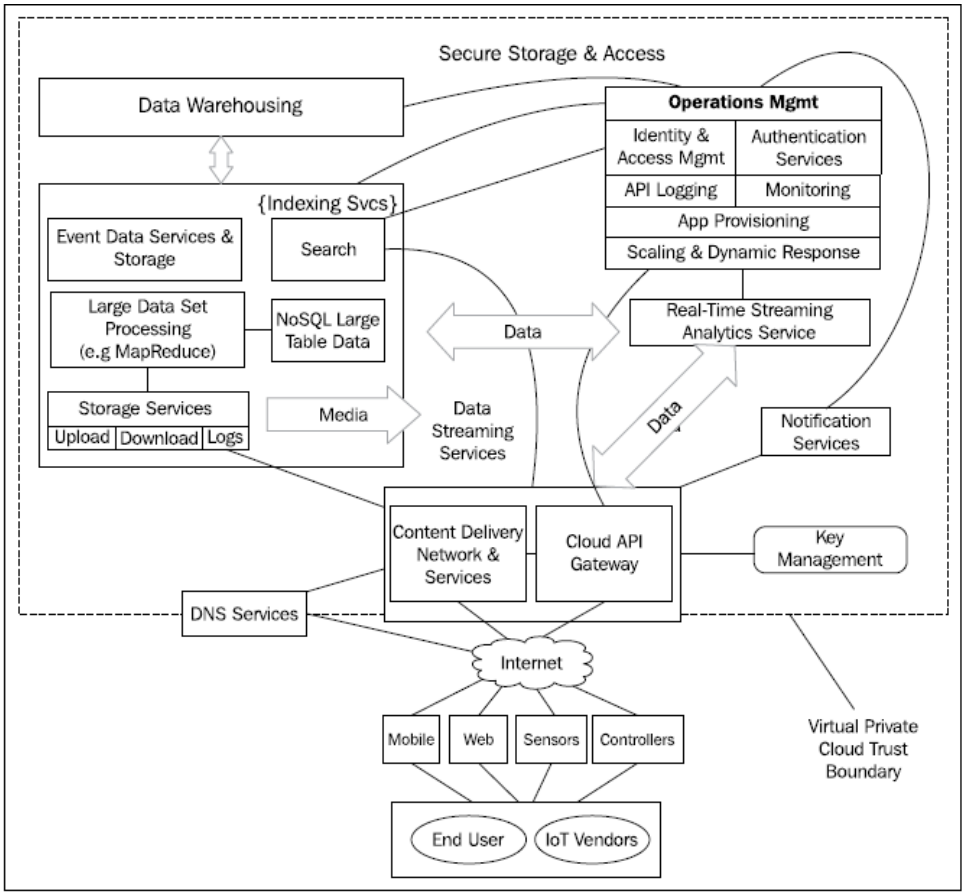
- تلاش های مکرر اتصال
- تلاش های مکرر احراز هویت
- خاتمه غیرعادی اتصالات
- بررسی موضوعی
- ارسال پیام های ارسال نشدنی
- سرویس گیرندگانی که متصل می شوند و اطلاعاتی ارسال نمی کنند.

شایان ذکر است که تنظیم یک SIEM برای شناسایی سوءاستفاده احتمالی از سامانه های IoT به تفکر نیاز دارد. درک اینکه چگونه رفتار یک دستگاه IoT خاص می تواند با حوادث رخ داده در دیگر بخش های کل سامانه مرتبط باشد، الزامی است.

5 ایجاد معماری امنیت ابری IoT سازمان

جنبه ها و گزینه های معماری زیادی برای سامانه IoT دارای فضای ابری وجود دارد. CSPها، ارائه دهندگان سرویس IoT و اتخاذکنندگان سازمانی باید قابلیت های ارائه شده را به منظور تمرکز بر کنترل های امنیتی مناسب در چارچوب پشتیبانی کننده بررسی کنند.

شکل زیر یک فضای ابری خصوصی مجازی و کلی از ارائه دهنده سرویس ابری است که سرویس های امنیتی و عملیاتی پایه را برای حفاظت از تراکنش های اطلاعاتی نقطه پایانی به نقطه پایانی ارائه می کند. این شکل سرویس های رایج و مجازی شده که برای IT عمومی و تشکیلات دارای IoT قابل دسترسی هستند، را نشان می دهد. تمام متقاضیان IoT نیازی به استفاده از قابلیت های ابری موجود نخواهند داشت، ولی اکثر آنها به یک سطح مقطع کمینه از سرویس های بالا نیاز خواهند داشت و لازم است به خوبی محافظت شده باشند:



در مواجهه با ایجاد معماری امنیتی در تقابل با سامانه ذکر شده در بالا، بایستی به خاطر سپرد که در حقیقت اصلاح معماری امنیت ابری IoT سازمان، بجای نوآوری و اتخاذ مجدد همه موارد، به گردآوری ساختارها و سرویس های اولیه معماری امنیت که از قبل در CSP وجود دارد دارند اشاره دارد. با این اوصاف، فعالیت های زیر که برخی از آنها به تفصیل در این کتاب بحث شده اند (بنابراین در اینجا با جزئیات ذکر نشده اند) به شدت توصیه می شوند:

1. سازماندهی یک مدل مشروح تهدید از طریق توصیف سامانه و نقطه شروع امنیتی:
   1) شناسایی تمام انواع پروتکل ها و پلتفرم های دستگاه IoT.
   2) شناسایی و طبقه بندی براساس حساسیت و حریم خصوصی تمام اطلاعات IoT حاصل از دستگاه های IoT در مرز شبکه.
   3) تعیین تهیه کنندگان و مصرف کنندگان نزدیک و دور اطلاعات حساس.
   4) شناسایی تمام نقاط پایانی سامانه، خصوصیات امنیت فیزیکی و منطقی آنها و اینکه چه کسی آنها را کنترل و مدیریت می کند.
   5) شناسایی تمام سازمان هایی که افراد آنها با سرویس ها و مجموعه داده های IoT تعامل داشته و/یا دستگاه ها را مدیریت، حفظ و پیکربندی می کنند. تضمین شود هر کدام چگونه در سامانه

ثبت شده اند، مجوز دریافت کرده اند و به سامانه دسترسی پیدا می کنند و (در صورت نیاز) چگونه ردیابی یا بازرسی شده اند.

6) تعیین ذخیره سازی، استفاده مجدد اطلاعات و حفاظ های مورد نیاز در صورت جداسازی یا در زمان انتقال.

7) براساس خطرات، تعیین نوع اطلاعاتی باید نقطه به نقطه حفاظت شوند (همچنین شناسایی آن نقاط) و اینکه کدام باید نقطه پایانی به نقطه پایانی محافظت شوند به طوری که بتوان برای مصرف کننده نهایی یا مخزن اطلاعاتی، صحت، یکپارچگی و در صورت نیاز محرمانگی اطلاعات را تضمین کرد.

8) در صورتی که یک درگاه میدانی مورد نیاز باشد، پروتکل های South و North مورد نیاز توسط آن پلتفرم به منظور ارتباط با دستگاه های میدانی (برای مثال ZigBee) و تلفیق و انتقال آن ارتباطات به درگاه ابری (برای مثال، HTTP در کنار TLS) بررسی شود.

9) ارزیابی خطر و حریم خصوصی در تقابل با اطلاعات نهایی شده تا کنترل های ملزوم که ممکن است در CSP وجود نداشته باشند، مشخص شود.

2. تنظیم معماری امنیتی از طریق موارد زیر: (مخصوص فضای ابری)

1) تدارکات امنیتی که مستقیماً از CSP قابل دسترسی هستند.

2) سرویس های امنیتی افزودنی مبتنی بر فضای ابری که از طرف شرکای CSP یا سرویس های سازگار و متقابل ثالث قابل دسترسی هستند.

3. توسعه و اتخاذ سیاست ها و رویه ها:

1) امنیت اطلاعات و رویه حریم خصوصی اطلاعات.

2) وظایف، سرویس ها و الزامات امنیتی کاربر و مدیر (برای مثال، شناسایی مکان هایی که احراز هویت چند عاملی در حفاظت از منابع خاص مورد نیاز است).

4. اتخاذ و پیاده سازی معماری امنیتی مخصوص به خود در چارچوب ها و APIهای پشتیبانی شده توسط CSP.

5. یکپارچه سازی رویه های امنیتی (چارچوب مدیریت خطر NIST این مورد را به خوبی توضیح می دهد).

6 دستورالعمل های جدید در محاسبات IoT دارای فضای ابری

قبل از اتمام این گزارش، لیست کردن برخی از خصوصیات دارای IoT در فضای ابری و همچنین برخی در دستورالعمل های آتی و جدید و موارد کاربردی IoT متصل به فضای ابری ارزشمند خواهند بود.

6–1 محرک های IoT فضای ابری

فضای ابری خصوصیات بسیاری دارد که آن را به پشته جذاب، تطبیق پذیر و اجراشدنی فناوری تبدیل کرده که از آن می توان سرویس های جدید IoT تجسم، ایجاد کرده و بکار گرفت. این بخش برخی از این موارد را ارائه می کند.

6–1–1 شبکه بندی تعریف شده نرم افزاری (SDN)

SDNها به عنوان قابلیت های نسل بعدی مدیریت شبکه ظهور کردند تا میزان فعالیت برای تنظیم مجدد شبکه ها و مدیریت مسیرهای مبتنی بر سیاست را ساده سازی و کاهش دهند. به عبارت دیگر، آنها برای برنامه پذیرتر و پویا کردن خود شبکه ساخته شدند (الزام قطعی برای مقیاس بزرگ و انعطاف پذیری مورد نیاز برای مدیریت ترافیک IoT دنیا). معماری های SDN از طریق جداسازی کنترل شبکه از قابلیت های ارسال کننده عمل می کنند. آنها از کنترلرهای SDN تشکیل شده اند که API شمالی یا پلی که به برنامه های شبکه متصل می شود و API جنوبی که کنترلرهای شبکه را به دستگاه های میدانی شبکه ارسال کننده ترافیک متصل می کنند، پیاده سازی می نمایند.

معماری های IoT که از سرویس های ابری بزرگ استفاده می کنند از قبل از SDN سود برده اند. سیستم های مجازی سازی بزرگ که سرورها، رابط ها و درگاه های مدیریتی را برای دستگاه های IoT میدانی و دیگر عناصر معماری IoT میزبانی می کنند، در Amazon، Google و دیگر ارائه دهندگان فضای ابری وجود دارند. با گذشت زمان، انتظار می رود قابلیت های دقیق تری در توانایی ساخت، تطبیق و سفارشی سازی پویای شبکه IoT ظهور کنند. SDNها امروزه از طریق فروشندگان امنیتی که چالش های حمله رد سرویس توزیع شده را هدف گرفته، استفاده شده اند و سازمان ها باید به دنبال اصلاح اجرائیات خود به منظور پشتیبانی از این قابلیت باشند.

6–1–2 سرویس های اطلاعاتی

با توجه به مقادیر عظیم اطلاعات، منابع اطلاعاتی و مخازن اطلاعاتی در IoT، محیط ابری ابزارهای قدرتمندی برای مدیریت و سازماندهی این اطلاعات ارائه می کند. برای مثال، Amazon DynamoDB قابلیت های بسیار قیاس پذیر، دارای تأخیر کم، پایگاه داده NoSQL برای توانمندسازی سرویس های ذخیره سازی، اشتراک و تجزیه و تحلیل اطلاعات IoT ارائه می کند. از طریق Frontend وب ساده، سازندگان خصوصیات جداول، گزارش

ها، دسترسی و غیره را ایجاد و مدیریت می کنند. یک مزیت برای سازمان های IoT این است که مدل های قیمت گذاری متناسب با مقدار اطلاعاتی است که در واقع استفاده می شود.

امنیت اطلاعات، احراز هویت و کنترل دسترسی براساس هر جدول در DynamoDB قابل پیاده سازی است که از سامانه مدیریت هویت و دسترسی AWS استفاده می کند. بدین معنی که یک سازمان واحد می تواند مجموعه ای از تحلیل ها را انجام داده، اطلاعات مشتق جمع آوری شده در جدول مجزا را تولید کرده و سپس آن اطلاعات را از طریق برنامه ای برای بسیاری از مشتریان منحصر به فرد خود در دسترس قرار دهد.

6-1-3 پشتیبانی از محفظه برای محیط های توسعه امن

یکی از چالش هایی که محیط های توسعه IoT با آن مواجه شدند، ماهیت متنوع پلتفرم های سخت افزاری IoT است. مجموعه ای از پلتفرم ها دارای کیت های توسعه نرم افزاری، APIها و درایورها هستند. زبان های برنامه نویسی استفاده شده در سخت افزارهای گوناگون نیز متغیر است (از C تا C جاسازی شده تا Python و بسیاری دیگر). یک محیط توسعه قابل استفاده مجدد که میان کل تیم توسعه قابل اشتراک است بایستی به منظور پشتیبانی از این سناریوها به اندازه کافی انعطاف پذیر باشد.

یک راهکار برای پشتیبانی از محیط توسعه IoT بسیار انعطاف پذیر، استفاده از فناوری محفظه است. با استفاده از این فناوری، محفظه ها با کتابخانه ها و بسته های مورد نیاز برای توسعه نوع دستگاه کنونی قابل ساخت هستند. این محفظه ها میان تیم توسعه به عنوان پایه توسعه قابل تکثیر و اشتراک گذاری هستند. از آنجایی که انواع جدیدی از دستگاه های IoT توسط تیم توسعه داده شده اند، پایه های جدیدی که پشته های کتابخانه نرم افزاری جدید را اضافه می کنند، برای مصرف قابل ایجاد هستند.

6-1-4 محفظه ها برای پشتیبانی از تشکیلات

استفاده از Docker به عنوان ابزار توسعه، مزیت ارزشمندی برای ذخیره سازی، استقرار و مدیریت گردش کار نسخه های پشتیبان دستگاه IoT ارائه می کند. Docker با قابلیتی طراحی شده که سازندگان و مدیران سیستم را قادر می سازد نسخه پشتیبان نرم افزاری/سفت افزاری را مستقیماً در سخت افزار IoT مستقر کنند. این راهکار دو مزیت دیگر نیز دارد:

- نسخه های پشتیبان دستگاه از طریق Docker قابل بروزرسانی هستند (نه فقط استقرار اولیه).
- Docker با یک سامانه آزمایش مانند Ravello برای آزمایش کامل سامانه قابل ادغام است. Ravello Systems چارچوب قدرتمندی برای استقرار و آزمایش مجازی برنامه های VMWare/KVM در کپسول های ابری خودمختار و اجرا شونده در AWS یا Google Cloud ارائه می کند.

در حالی که Docker قابلیت قدرتمند بکارگیری محفظه ها را ارائه می کند، فناوری دیگر به نام Kubernetes منبع باز گوگل از Docker استفاده کرده تا به سازمان ها اجازه دهد مجموعه محفظه های بزرگ را مدیریت

کنند. قابلیت محاسبات توزیع شده مجموعه های بزرگ و به سادگی مدیریت شده محفظه ها، یک محرک عظیم IoT است.

6-1-5 میکروسرویس ها

میکروسرویس ها، مفهوم تجدید شده تعدیل برنامه های بزرگ و یکپارچه سازمانی (وب UI و APIهای REST، پایگاه داده، منطق اصلی تجاری و غیره) در سرویس های کوچک و بایتی مانند معماری سرویس محور (SOA)[۲۹] هستند. این فناوری یک راهکار برای ساده سازی و پیشگیری از پیچیدگی برنامه های سازمانی ارائه می کند که در واکنش به تغییر الزامات رشد کرده و به سرعت افزایش می یابند. با وجود شباهت مفهومی با SOA، معماری های میکروسرویس، الزامات سامانه بزرگ را به VMهای کاربردی خودمختار و مجازی تقسیم می کنند. معمولاً هر کدام دارای منطق تجاری، Backend اطلاعاتی و APIهای متصل شونده به دیگر میکروسرویس ها هستند. در معماری میکروسرویس، هر میکروسرویس یکتا در نوع محفظه انتخابی به طور مجازی کشف شده است (برای مثال، Docker یا VMWare).

معماری های میکروسرویس نه تنها می توانند توسعه و پشتیبانی بلند مدت برنامه های ابری بزرگ و کوچک را ساده سازی کنند، بلکه خود را به طور طبیعی به قابلیت ارتجاعی ابری قرض می دهند. در صورتی که سازمان از چندین میکروسرویس تشکیل شده و دو تای آنها (شاید ثبت حساب یا سرویس اعلان) مورد تقاضا هستند، معماری ابری می تواند محفظه های میکروسرویس جدید را فقط برای سرویس های تحت تأثیر بچرخاند.

مشاغل می توانند برنامه های سازمانی جدید IoT را تصور کنند که از محیط اطلاعاتی قدرتمند IoT استفاده می کند؛ با استفاده از میکروسرویس ها، آنها می توانند به سرعت سرویس های جدید تشکیل داده و آنها را در واکنش به اطلاعات و فراز و فرودهای پردازش، به طور پویا اندازه گیری کنند. به علاوه، حفظ فرآیندهای توسعه سریع آسان تر است به دلیل اینکه هر تیم سریعی می تواند به دقت بر یک یا دو میکروسرویس یکتا تمرکز کند.

[29] Service Oriented Architecture

6-1-6 پیش به سوی اتصال 5G

در حالی که ایالات متحده، اروپا و آسیا اختلافات خود را در ساخت استاندارد 5G کنار گذاشته اند، تعدادی از خصوصیات برجسته آن وعده منقلب کردن و افزایش تعداد اشیاء، موارد کاربرد و برنامه هایی را می دهد که از اینترنت استفاده می کنند. شبکه بندی فراگیر از طریق 5G یک محرک کلیدی اینترنت اشیاء در قابلیت پشتیبانی از دستگاه های بیشتر با نرخ های بسیار بالاتر نسبت به شبکه های LTE خواهد بود (تقریباً 10 برابر). تاکنون، بررسی های رقابتی از دستورالعمل 5G روی موارد زیر توافق کرده اند[30]:

- نرخ های اطلاعاتی باید از 1 GB/s شروع شده و تا چندین GB/s افزایش یابد.
- تأخیر باید به کمتر از یک میلی ثانیه برسد.
- تجهیزات 5G باید نسبت به تجهیزات قبلی، در انرژی کم مصرف تر باشند.

با توجه به فضای IP آدرس IPv6 و اتصال 5G در آینده نزدیک (و فراتر از آن)، جای هیچ شگفتی نیست که بسیاری از شرکت های آینده نگر سرمایه گذاری کلانی کرده و در حال آماده سازی برای رشد غیر قابل باور در IoT هستند.

6-2 دستورالعمل های مبتنی بر فضای ابری

این بخش فقط چندین مثال براساس محرک های ابری بالا و مواردی ارائه می کند که با استفاده از پردازش ابری متمرکز و توزیع شده، برای هدایت IoT در مسیرهای جدید امکان پذیر هستند.

6-2-1 محاسبات سریع و IoT (منابع محاسبات پویا)

اقتصاد به اصطلاح اشتراکی در سرویس هایی مانند Uber، Lyft، Airbnb، توزیع مجدد انرژی خورشیدی منزل محور به شبکه برق و دیگر الگوهای تجاری ارائه شده که به مالکان منابع (خودروها، آپارتمان ها، پنل های خورشیدی و غیره) اجازه می دهد چرخه های اضافی به ازای چیزی ارائه کنند. محاسبات سریع (ODC)[31] همچنان به طور نسبی جدید و در حال رشد است، ولی به طور چشمگیری در معماری های ارتجاعی مبتنی بر فضای ابری استفاده شده اند. منابع محاسباتی سریع و تغییر پویای تقاضای سرویس گیرنده، برنامه ریزی، ارسال و ساخته شده اند.

مزایای زیاد فضای ابری IoT می تواند به طور معکوس از خود پیشی بگیرد. IoT دارای 5G در تعداد خالص دستگاه های مرزی و منابع محاسباتی موجود خود می تواند به برنامه های مبتنی بر فضای ابری در قابلیت

[30] http://www.techrepublic.com/article/does-the-world-need-5g/
[31] On-Demand Computing

دسترس پذیر کردن منابع محاسباتی پنهان برای برنامه های مرزی گوناگون منفعت برساند. یک برنامه مرزی محاسباتی متمرکز در نظر گرفته شود که احتمالاً نمی تواند روی یک دستگاه واحد پردازش کند. اکنون تصور شود که دستگاه قادر است از ظرفیت پردازش دستگاه های مرزی اطراف خود که متعلق به دیگر کاربران است استفاده کند. فضای ابری پویا و محلی مورد نیاز که توسط اشیا برای اشیا پشتیبانی شده اند به شبکه های 5G و برنامه های تصور شده نیاز خواهند داشت. به علاوه پشتیبانی از شبکه، ODC تسهیل شده برای IoT به تکامل در معماری های برنامه های جدید مانند میکروسرویس ها و واحد اجرای دقیق که قبلاً بحث شد نیاز خواهد داشت.

از دیدگاه امنیتی، دامنه های محاسباتی ایمن و مطمئن در دستگاه های IoT، یک الزام پایه برای ODC مهیا شده برای IoT خواهد بود. منعفت از طریق امکان فراهم سازی چرخه های محاسباتی توسط خودرو برای یک شغل نزدیک، فرآیند یا فرد راه دور یا حتی یک ارائه دهنده فضای ابری در نظر گرفته شود. بارگذاری های اجرایی سریع و پردازش کد نامطمئن روی خودرو باید دارای دامنه مجزا و درجه بالایی از تضمین باشد، در غیر این صورت شاید برنامه ها و اطلاعات شخصی به سادگی توسط فرآیند های موقتی و مهمان به خطر بیفتند. ARM، TrustZone و دیگر فناوری های امروزی فقط نقطه شروعی برای این نوع از محاسبات میان دامنه را برای IoT ارائه می کنند.

6-2-2 مدل های توزیع شده مطمئن و جدید برای فضای ابری

در گزارش های قبلی بحث شد، مجوزهای دیجیتالی و PKI به طور گسترده برای ایمن سازی نقاط پایانی سرویس گیرنده و سرویس مبتنی بر فضای ابری استفاده شده اند. امروزه حفظ اطمینان واحد میان دامنه های گوناگون و مطمئن یک اقدام ساده یا لزوماً کارآمدی نیست. با همین هدف در ماه می سال 2016، Apache Foundation پروژه جدید به نام Milagro در برنامه توسعه خود ایجاد کرد[۳۲]. Milagro به این دلیل قابل توجه است که از رمزنگاری مبتنی بر جفت شدن و چندین نهاد مطمئن و توزیع شده (DTAها)[۳۳] جهت تولید مستقل چندین اشتراک کلید خصوصی با سرویس گیرندگان و سرورها استفاده می کند. نقاط پایانی مصرف کننده، مقادیر نهایی رمزنگاری را برای اجرای احراز هویت متقابل و توافق کلیدی در سرتاسر هر چیزی که محیط ابری نیاز داشته باشد ایجاد می کنند. ایده اصلی این است که DTAها توسط هر تعداد سازمان مستقل که هر کدام یک راهکار SECaaS برای نهادهای پایانی ارائه می کنند، قابل اجرا باشند. ماهیت توزیع شده این مدل توسط سلسله مراتب های مطمئن و یکپارچه امروزی و از طریق الزام مهاجمان در آلوده کردن تمام DTAهای موجود در تولید محتویات یک کلید کاربر نهایی بهبود می بخشد. در صورتی که Milagro از دوران نهفتگی با موفقیت

[32] http://milagro.apache.org/
[33] Distributed Trust Authorities

خارج شود، ممکن است برخی مدل های مطمئن و توزیع شده منبع باز جدید برای فضای ابری و تشکیلات وابسته IoT ظهور کنند.

6-2-3 IoT شناختی

IBM Watson و رابط های جدید IoT آن تنها شروعی از پردازش اطلاعات شناختی برای اینترنت اشیاء هستند. در کل، IoT برای گروه بندی تمام موارد کاربردی احتمالی پردازش شناختی به مجموعه های کوچکتر، بسیار بزرگ است؛ هرچند، لیست زیر تنها بخش کوچکی از موارد حول سامانه های IoT و اطلاعات همراه با تحلیل های شناختی را نشان می دهد:

- **نظارت پیشگویانه سلامتی:** مجموعه داده های حجیم نظارت بر سلامت در کنار ابرداده های گوناگون بیمار به سامانه های شناختی اجازه خواهد داد با شفافیت و احتمال بیشتری شرایط بیماری یا دیگر امراض را قبل از ظهور پیش بینی کنند. اکثر تحقیقات چشمگیر، عوامل خطر را براساس اطلاعات بسیار محدود ارزیابی می کنند. با نظارت سلامت، وسایل پوشیدنی، سرویس های ادغام اطلاعات IoT و دیگر منابع اطلاعاتی عمومی و خصوصی، سامانه های شناختی وضوح و دقت بسیار بیشتری برای فعالیت و شناسایی خطرات سلامتی خواهند داشت. سامانه های IoT، ستون این قابلیت ها خواهند بود.
- **روش های مسیریابی مبتنی بر همکاری:** تحریک گروه های UAS کوچک که در محیط های رد شده GPS به منظور درک کلی از محیط خود برای مسیریابی کارآمدتر فعالیت می کنند.

7 چکیده

در این گزارش، فضای ابری، پیشنهادات ارائه دهنده سرویس ابری، فعالسازی IoT توسط فضای ابری، معماری های امنیتی و اینکه فضای ابری چگونه دستورالعمل های جدید و قدرتمندی برای اتصال و پشتیبانی از اینترنت اشیاء تولید می کند بحث شدند.