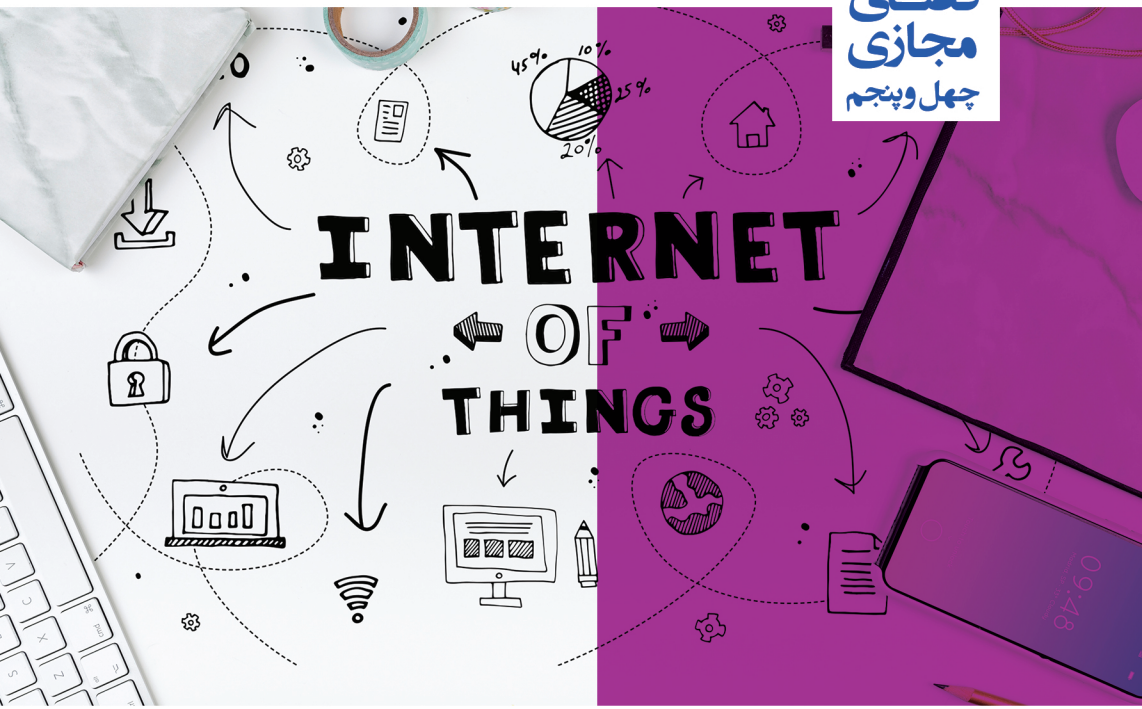
مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

عصر فضای مجازی
چهل و پنجم



گامی بسوی همگرایی امن زیرساخت ابری و اینترنت اشیا

To wards secure convergence of cloud and IOT

بسم الله الرحمن الرحیم

عصر فضای مجازی

گزارش شماره ۴۵
آبان ۱۳۹۹

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

گامی بسوی همگرایی امن زیرساخت ابری و اینترنت اشیا

محتوای انتشار یافته در این اثر
الزاماً بیانگر دیدگاه مرکز ملی فضای مجازی نیست

تهیه شده در پژوهشگاه فضای مجازی
(گروه علوم و فناوری‌های نوین)

تهیه کنندگان: مهندس نیلوفر کریمی‌آذر (کارشناس ارشد امنیت اطلاعات)، مهندس سید محمد اسماعیلی (کارشناس ارشد امنیت اطلاعات)،
مهندس وحید بهمنی(کارشناس ارشد امنیت اطلاعات)
ناظر علمی: مهندس محمدمهدی رضاپور

نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش خیابان ۱۶غربی، پلاک ۲۰
تلفن: ۸۶۱۵۱۰۶۱-۰۲۱
کد پستی: ۱۵۱۵۶۷۴۳۱۱

فهرست

سخن نخست ۵
چکیده ۹
مقدمه ۱۳

بخش اول (رایانش ابری و اکوسیستم اینترنت اشیا)

رایانش ابری و اکوسیستم اینترنت اشیا ۱۹

بخش دوم (چالش‌های امنیتی)

چالش‌های امنیتی ۲۷

۲-۱- اتصال ۲۹
پروتکل‌های ناهمگن برای ارتباطات ۲۹
جریان داده‌ی ناامن از Edge به Cloud ۳۰

۲-۲- تحلیل ۳۱
تأثیر ابر غیر متمرکز بر امنیت ۳۲

۲-۳- یکپارچگی ۳۲
وابستگی امنیت به خدمات کسب و کارهای عمودی ۳۲
وابستگی معیارهای امنیت IOT به توسعه دهندگان در این حوزه ۳۳
دستگاه‌های منسوخ شده ۳۳

بخش سوم (سناریوهای حمله)

سناریوهای حمله ۳۷

۳-۱- میزبانی دشمن ۳۷
۳-۲- مسیرهای پرخطر ۳۹
۳-۳- درو و برداشت محصول ۴۲
۳-۴- Open House ۴۵

بخش چهارم (پیشـــگیری های امنیتی)

پیشگیري های امنیتی ۵۱

۴-۱- اتصال ۵۱

مجازی سازی دستگاه برای ایجاد همگنی ۵۱

ارتباطات امن، تحلیل جریان امنیتی و امنیت داده‌ها در حالت rest ۵۲

۴-۲- تحلیل ۵۳

امنیت فیزیکی و سایبری در دستگاه‌های لبه ۵۳

۴-۳- یکپارچگی ۵۴

اضافه شدن پارامترهای اندازه گیری امنیت ۵۵

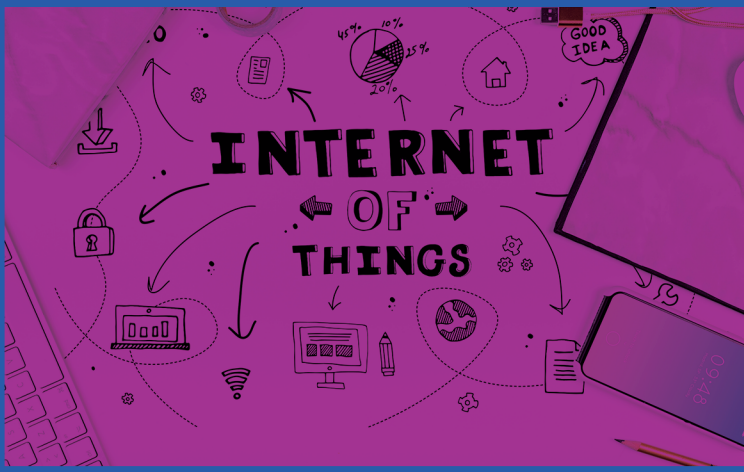
بروز رسانی خودکار و امن نرم افزار ۵۶

امنیت نقاط پایانی از طریق همه محیط ها ۵۷

جمع‌بندی ۵۹

منابع ۶۳

سخن نخست



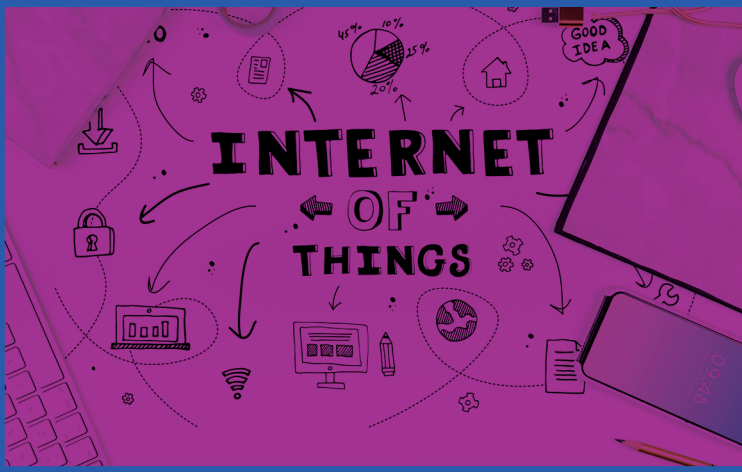
سخن نخست

فضای مجازی با شتاب شگرف و رو به تزایدی که در حال بسط و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را درنوردیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می‌دهد. لذا به نظر می‌رسد دو نگاه کلان به فضای مجازی وجود دارد: نگاه اول که بالاخص در ابتدای رشد و تکوین فضای مجازی مسلط شده بود، آن را همچون ابزاری کنار سایر ابزارهای بشری تصویر می‌کرد که تنها طریقیت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره کننده فضای مجازی و سایه گستری آن در حوزه ها و شئون بشر در یک دهه اخیر آن را چون سکویی می‌داند که بسیار فراتر از شأن ابزاری حیات انسان‌ها را سامان جدیدی داده و ادعای تمدن نوینی را دارد. رویکردی که از قضا از چشمان بصیر رهبر انقلاب نیز دور نمانده و انتظاری تمدنی از فضای مجازی در ایران را مطالبه داشته اند.

در همین راستا گزارش‌های عصرفضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه‌ی فضای مجازی را ارتقاء بخشیده و آن‌ها را برای مواجهه فعال و خردمندانه با تحولات این عرصه مهیا سازد.

سید ابوالحسن فیروزآبادی
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

چکیده

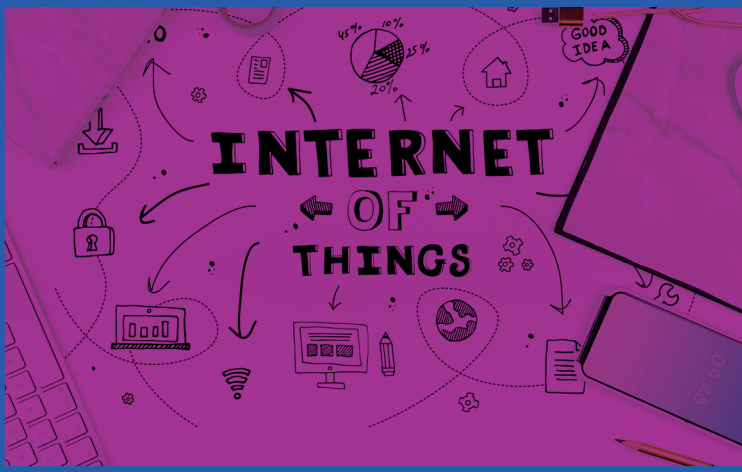


چکیده

هـدف از انتشـار ایـن سـند ارائـه یـک دیـد سـطح بـالا در مـورد مسـائل امنیتـی بـه توسـعه دهنـدگان اینترنـت اشـیا و ارائـه دهنـدگان راهکارهـای یکپارچـه اینترنـت اشـیا می‌باشـد کـه ازخدمـات ابـری اسـتفاده می‌کننـد و همچنیـن ارائـه دهنـدگان سـرویس ابـری (CSP هـا) کـه راهکارهـای ابـری بـرای اینترنـت اشـیا ارائـه می‌دهنـد.

واژگان کلیـدی: اینترنـت اشـیا، رایانـش ابـری، پیشـگیری‌های امنیتی، اکوسیسـتم، چالش‌هـای امنیتـی، محاسـبات لبـه، توسـعه، امنیـت فیزیکـی و سایبری

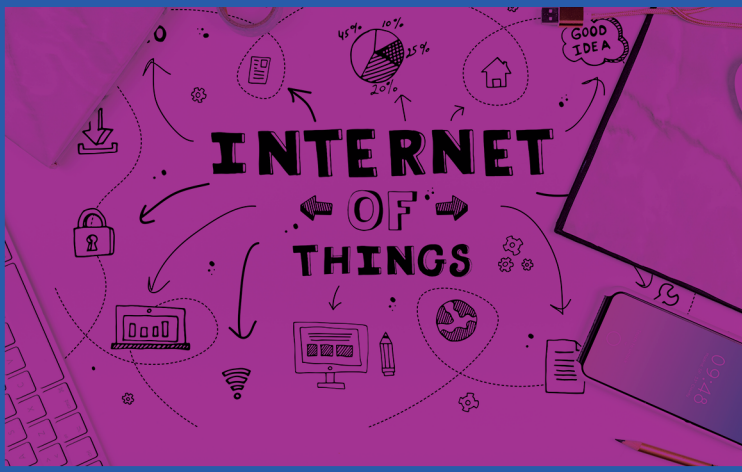
مقدمه



مقدمه

این گزارش، ترجمه سند با عنوان "Towards secure convergence of Cloud and IoT" است که در ۱۷ ام سپتامبر سال ۲۰۱۸ میلادی توسط آژانس امنیت سایبری اتحادیه اروپا (ENISA) منتشر شده است.

بخش اول



بخش اول

رایانش ابری و اکوسیستم اینترنت اشیا

در طول چند سال گذشته ما شاهد رشد بالای محصولات اینترنت اشیاء (IoT) هستیم. با رشد بازار IoT هر ساله میلیاردها دستگاه جدید بصورت آنلاین توسعه داده می‌شوند. گارتنر پیش بینی می‌کند تا سال ۲۰۲۰ اشیا متصل به ۲۰,۴ میلیارد خواهد رسید.[1] این چیزها (یا دستگاه‌ها)، به شبکه متصل می‌شوند تا اطلاعاتی را که از طریق کلیه داده‌های سنسورهای محیطی جمع‌آوری‌شده‌اند را تولید کند و یا به سیستم‌های دیگر اجازه می‌دهد تا از طریق عملگرها به دنیای بیرونی دسترسی پیدا کنند. اتحادیه بین المللی اروپا اینترنت اشیا را به عنوان "اکوسیستم سایبر فیزیکی سنسورها و محرک‌های بهم پیوسته، که امکان تصمیم گیری هوشمند را فراهم می‌کنند" تعریف می‌کند.[2] در قلب اینترنت اشیا، اطلاعات قرار دارد که در چرخه مستمر سنجش، تصمیم گیری و اقدامات قرار می‌گیرد.

دستگاه‌های IoT داده‌های زیادی را تولید می‌کنند. ابر به عنوان بخشی از اکوسیستم اینترنت اشیا، جریان، فرآیند، تحلیل و

1 https://www.gartner.com/newsroom/id/3598917
2 https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

ذخیره سازی این داده‌ها را مدیریت می‌کند.خصوصا وقتی اینترنت اشیا با سرویس‌های مبتنی بر ابر یکپارچه شود می‌تواند سریعتر و به صرفه‌تر در محیط‌های سازمانی توسعه یابد.

با گسترش اینترنت اشیا، رایانش ابری به گونه ای محقق می‌شود تا نیازهای اکوسیستم اینترنت اشیا را برطرف کند و بسیاری از ویژگی‌های جدید برای جمع آوری، ذخیره و پردازش داده‌های تولید شده توسط اینترنت اشیا را فراهم کند. از جمله این ویژگیها می‌توان به مجازی سازی دستگاه، ابزارهای هوش تجاری، یادگیری ماشین، فرمان و کنترل (C&C)، پردازش برای انجام تجزیه و تحلیل‌های پیچیده و رابط‌های برنامه نویسی نرم افزار (API) اشاره کرد.[1]

در حالی که این همگرایی Cloud Computing و IoT فرصت‌هایی را به همراه می‌آورد، خطرات و چالش‌های جدیدی را نیز به وجود می‌آورد. به طور خلاصه، در این مقاله سعی شده است:

- شناسایی و بحث در مورد چالش‌های امنیتی ناشی از همگرایی اینترنت اشیا و ابر
- اهمیت مسائل امنیتی با طرح چهار سناریوی حمله
- ترسیم چالش‌های شناسایی شده برای پیش گیری‌های امنیتی

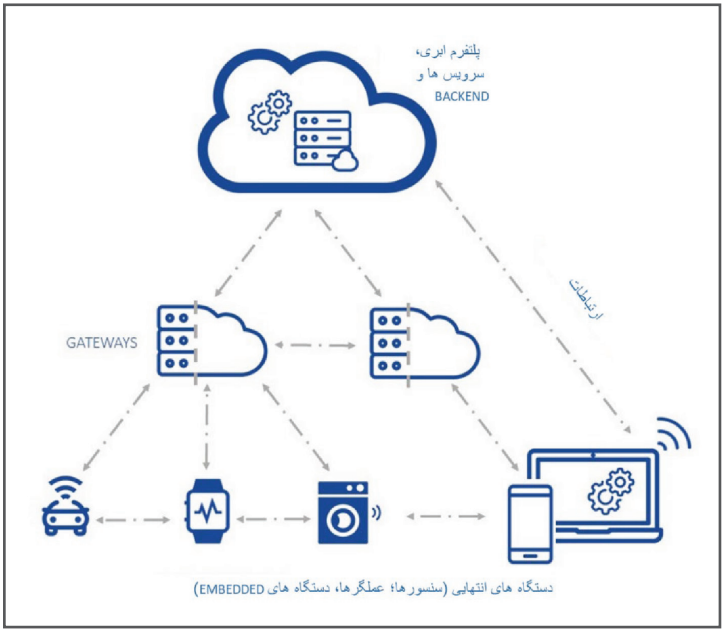
هدف از این کار، ارائه یک بررسی سطح بالا در مورد مسائل امنیتی به مخاطبان زیر است:

- توسعه دهندگان و یکپارچه کنندگان اینترنت اشیا که از سرویس هاس ابری برای توسعه اینترنت اشیا استفاده می‌کنند.

1.https://www.postscapes.com/internet-of-things-platforms/

• ارائه دهندگان خدمات ابری (CSPها) با راهکارهای زیرساخت ابر برای اینترنت اشیا

طبق توصیه‌های امنیتی پایه ایی اتحادیه اروپا، اکوسیستم اینترنت اشیا از سه مؤلفه اساسی، دستگاه‌ها (یا چیزها)، ارتباطات و پلتفرم ابری، backend، خدمات تشکیل شده است. این مؤلفه‌ها و تعامل آنها در شکل زیر نشان داده شده است.



شکل ۱. معماری اکوسیستم اینترنت اشیا با IoT Cloud

قبل از رشد اینترنت اشیا، رایانش ابری به صورت سنتی میزبان کارهایی

بـود کـه بـه ویژگی‌هایـی از قبیـل کشسـانی، چنـد مسـتاجری، مقیـاس پذیـری یـا سـازگاری نیـاز داشـت. بـا ظهـور اینترنـت اشـیا، ابـر ویژگی‌هـای خـود را بـرای مدیریـت و پاسـخ دادن بـه رخدادهـا از هـر جایـی و در هـر زمانـی، بهبـود داد و یـک مـدل جدیـد بـه نـام "IoT Cloud" ایجـاد کـرد[1]. IoT Cloud، قابلیـت دریافـت ویژگی‌هـای جدیـدی ماننـد پاسـخ سـریع، بـه موقـع و انعطـاف پذیـر را دارد. امـروزه ارائـه دهنـدگان خدمـات ابـری از زبان‌هـای برنامـه نویسـی تابعـی بـا معماری‌هـای میکروسرویسـی پشـتیبانی می‌کننـد. ایـن ویژگی‌هـا باعـث پاسـخ سـریع بـه سـرویس‌های درخواسـتی می‌شـود[2] و سـطح برنامه‌هـای کاربـردی محـور در ابـر را افزایـش می‌دهـد.

بـه طـور خلاصـه، بـا اسـتفاده از ایـن مـدل جدیـد توسـعه دهنـدگان اینترنـت اشـیا می‌تواننـد بـا کنتـرل از راه دور، روی دسـتگاه‌های اینترنـت اشـیا کار کننـد. بـه عنـوان مثـال، ارزیابـی وضعیـت دارایـی هـا، بررسـی مشـخصات آنهـا، پیکربنـدی یـا پیکربنـدی دوبـاره آنهـا، اصلاح و بروزرسـانی آنهـا و گـزارش گیـری از انـواع وضعیـت و تنظیمـات. ایـن مـوارد، بـرای دسـتگاه‌های اینترنـت اشـیا کـه توسـط IoT Cloud مدیریـت می‌شـوند، در صـورت بـروز خطـا و از بیـن رفتـن، ریسـک‌های جدیـدی را ایجـاد می‌کنـد. پیـاده سـازی امنیـت در ابـر، آن هـم در حالتـی کـه مدیریـت آن بـا IoT Cloud میباشـد و دسـتگاه‌های بیشـماری تحـت نظـارت و مدیریـت قـرار میگیرنـد بسـیار حیاتـی می‌شـود.

امنیت ابر همچنان موضوعی اسـت که اتحادیه اروپا در مسـتندات منتشرشـده

1. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/making-sense-of-internet-of- things-platforms
2.http://searchcloudcomputing.techtarget.com/opinion/Event-driven-applications-drive-next-wave-of-IaaS-evolution

قبلی[۳۲۱]، آنرا ترسیم و تجزیه و تحلیل کرده است. در این مقاله به اختصار، ما بر چالش‌های امنیتی ناشی از این مدل جدید IoT Cloud و همگرایی آن با اکوسیستم اینترنت اشیا و تعامل دو سویه آنها تمرکز می‌کنیم. براساس استاندارد بین المللی امنیت نرم افزارهای تحت وب (OWASP)، هر دو جنبه امنیتی در این همگرایی با چالش‌هایی روبرو هستند.

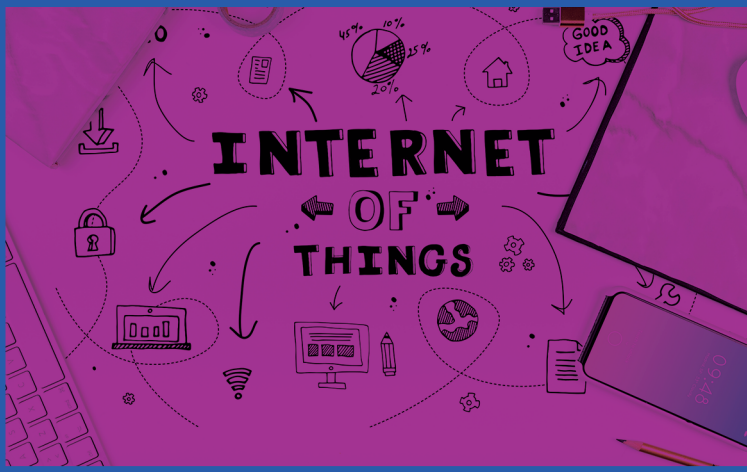
رابط کاربری ابر به عنوان یکی از سطوح حمله در اینترنت اشیا بیان شده است. [۴] در حالی که در گزارش 10Cloud Top [۵] Security Risks که شامل خدمات و یکپارچه سازی داده است، محدود به امنیت دستگاه‌های اینترنت اشیا شده است.

بر اساس مدل مرجع اینترنت اشیا اتحادیه اروپا و تعامل مولفه‌ها مانند شکل ۱، ما جنبه‌های امنیتی همگرایی IoT و Cloud را در سه دسته اصلی طبقه بندی می‌کنیم:

- اتصال: تعامل و ارتباطات بین endpoints[۶]، Gateway[۷]ها و ابر
- تجزیه و تحلیل: پردازش، جمع آوری داده‌های تولید شده از دستگاه‌های اینترنت اشیا و فیلتر آن در سطوح مختلف اکوسیستم اینترنت اشیا
- یکپارچه سازی: ویژگی‌هایی که جریان دو طرفه داده را به موقع ایجاد می‌کند به عنوان مثال رابط‌های کاربری ابر و کنترل و فرمان از راه دور دستگاه‌های اینترنت اشیا از طریق رایانش ابری

1.https://www.enisa.europa.eu/publications/exploring-cloud-incidents
2. https://www.enisa.europa.eu/publications/security-aspects-of-virtualization
3. https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment
4. https://www.owasp.org/index.php/IoT_Attack_Surface_Areas
5.https://www.owasp.org/index.php/Category:OWASP_Cloud_%E10_90%80%2_Project
۶. نقاط پایانی
۷. گذرگاه ،دروازه / سیستمی که اتصال میان دو شبکه ارتباطی متفاوت و مجزا به هم را فراهم میسازد

بخش دوم



بخش دوم

چالش‌های امنیتی

جـدا از سنسـورها و عملگرهـا، IoT اغلـب میـان افزارهـای قدیمـی و سیسـتم‌های جدیـد را بـه هـم متصـل می‌کنـد تـا بتواننـد تعامـل برقـرار کننـد. ایـن سیسـتم‌ها از طریـق Gateway بـه ابـر وصـل می‌شـوند و از پـردازش داده‌هـای سنسـورها تصمیـم گیـری می‌شـود. گاهـی اوقـات، مسـئله قابلیـت همـکاری کـه در محیط‌هـای حسـاس عملیاتـی ماننـد سـلامت، انـرژی، حمـل و نقـل هوایـی بـکار میـرود، نگرانـی در مـورد امنیـت اکوسیسـتم اینترنـت اشـیا را افزایـش می‌دهـد.

دغدغه‌هـای زیـادی در امنیـت پروسـه‌های کاری IoT و فرآیندهـای مرتبـط بـا آن وجـود دارد. حمـلات مختلـف روی دسـتگاه‌های IoT می‌تواند حمـلات بـر روی دسترسـی بـه منابـع شـبکه یـا Cloud و بالعکـس را برای مهاجمـان آسـان‌تر کنـد. بـا ذکـر ایـن نکتـه می‌تـوان درک بهتـری از سـطوح حمـلات بـر روی Cloud و دسـتگاه‌های انتهایـی IoT داشـت. امنیـت ضعیـف در دسـتگاه‌های IoT یـا 12Gateway‌هـای آن می‌توانـد بـه طـور بالقـوه منجـر بـه اتصـال ناامـن و ورود جریـان داده‌هـا بـه سـمت

Cloud با پیامدهای مخاطره آمیز در امنیت این اکوسیستم شود.

اتحادیه اروپا چالش‌های امنیتی زیر را که در سه دسته اصلی مدل مرجع اینترنت اشیا اتحادیه اروپا قرار دارد، شناسایی کرده است. تحلیلی از این چالش‌ها در این بخش توضیح داده شده است.

اتصال	• پروتکل‌های ناهمگن برای ارتباطات
تجزیه و تحلیل	• پردازش به موقع در لبه، امنیت را تحت الشعاع قرار می‌دهد • تأثیر غیر متمرکز بودن ابر روی امنیت
یکپارچه سازی	• وابستگی امنیت به خدمات کسب و کارهای عمودی • وابستگی معیارهای امنیت IOT به توسعه دهندگان در این حوزه • دستگاه‌های منسوخ شده

لازم به ذکر است که علاوه بر تحلیل چالش‌ها، اتحادیه اروپا سناریوهای حمله‌ی خاص را توسعه می‌دهد. این سناریوها را با استفاده از مصاحبه‌هایی که با متخصصان خاص هر موضوع توسعه می‌دهد تا بتواند اهمیت چالش‌های امنیتی را مشخص کند . این سناریوها در بخش سناریوی حمله با هدف تکمیل و متناسب سازی چالش‌های امنیتی ارایه‌شده در این فصل، ارائه شده است.

۲-۱- اتصال

پروتکل‌های ناهمگن برای ارتباطات [1]

گستردگی اپلیکیشن‌های IoT از خانه‌های هوشمند گرفته تا صنعت هوشمند می‌باشد که می‌توان با این تفاسیر نتیجه گرفت مواردی همچون دامنه، سخت افزار، سیستم عامل، پروتکل و روش‌های اتصال شبکه در حوزه IoT بسیار متنوع است. در بین راهکارهای ارائه شده در حوزه اینترنت اشیا، سیستم‌های قدیمی‌تر معمولا به فناوری‌های اختصاصی خاصی متکی می‌باشند در حالی که دیگر استانداردهای جدیدتر IoT دامنه گسترده تری مانند MQTT[2] و یا پشته پروتکل IETF[3] را برای دستگاه‌های IoT (به صورت محدود) به کار می‌گیرند. [4] این تنوع غالبا باعث ایجاد محیطی از تفاوت‌های فردی و متفاوت در یک سازمان می‌شود که مانع از توسعه سرویس‌های value-added (سود حاصل از تفاوت بین قیمت فروش و هزینه تولید یک محصول) با استفاده از دستگاه‌های IoT منبع پایین و همچنین تفاوت سطح امنیتی در هر پیاده سازی می‌شود. با ذکر این نکته، می‌توان برآورد کرد که توسعه دهندگان به دنبال اضافه کردن فرآیندهای بیشتری در سیستم‌های IoT فعلی نسبت به دستگاه‌های قدیمی‌تر هستند. در این بروز رسانی‌ها طیف گسترده ای از گزینه‌های اتصال به شبکه، پروتکل‌ها و روش‌های ارتباطی پیاده سازی می‌شود. معمولاً در تلفیق دستگاه‌های جدید با دستگاه‌های قدیمی‌تر تأثیر آن بر امنیت محاسبه نمیشود. در

1. http://journals.sagepub.com/doi/full/683425/2015/10.1155
2. http://mqtt.org/
3. Internet Engineering Task Force
4. https://tools.ietf.org/pdf/draft-moore-iot-security-bcp00-.pdf

یک استاندارد IoT، غالبا دستگاه مورد نظر معمولا دارای گزینه‌های مختلفی برای برقراری ارتباط با دیگران است و قطعا سطوح امنیتی که در هر فرآیندی اجرا می‌شود، متفاوت خواهد بود.

جریان داده‌ی ناامن از Edge به Cloud

بخش جذاب دیگر مدل اینترنت اشیا، پردازش داده‌ها است. پردازش داده‌ها می‌تواند با در لبه موسوم به Edge Computing[1] یا در Cloud انجام شود. محاسبات لبه روشی را برای استفاده برنامه‌ها با جمع آوری یا پردازش داده‌ها به دستگاه‌های پردازشی داخلی، به دور از گره‌های متمرکز، تحلیل و ایجاد دانش منطقی شبکه را فراهم می‌کند.

اگرچه محاسبات لبه باعث افزایش پاسخ سریع و تصمیم گیری آن می‌شود. (به عنوان مثال استفاده از یادگیری ماشین برای تصمیم گیری‌های خودمختار)، اما منجر به یک توزیع ناامن و غیرقابل کنترل از داده‌ها می‌شود که با در نظر گرفتن میزان و حساسیت داده هایی که منتقل میشود می‌توانند حیاتی شوند. پردازش و قابلیت ذخیره سازی محدود برخی از نقاط انتهایی ممکن است ویژگی‌های امنیتی مانند احراز هویت، رمزگذاری و روش های حفظ یکپارچگی وجامعیت داده را محدود کرده و کنترل دسترسی و همچنین محرمانه بودن یا یکپارچگی داده‌های منتقل شده به ابر را به خطر اندازد.[2] حتی وقتی ویژگی‌های امنیتی فعال هستند، پیاده سازیاشتباه، میتواند تأثیر زیادی بر امنیت کل مدل داشته باشد.

1.https://www.forbes.com/sites/jonmarkman/03/04/2018/this-is-why-you-need-to-learn-about-edge-computing/
2. https://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php

۲-۲- تحلیل

پردازش به موقع در لبه، امنیت را تحت الشعاع قرار می‌دهد.

طبق پیش بینی IDC[1]، ۴۳ درصد محاسبات IoT تا سال ۲۰۲۱ در لبه اتفاق خواهد داد.[2] به خصوص در IoT، محاسبات در لبه می‌توانند مزایای عملکردی مانند محاسبات به موقع و کاهش وابستگی اتصال شبکه به ابر را فراهم سازند. با این وجود، لبه از نظر فیزیکی در مقایسه با Cloud دارای دسترس پذیری بالاتری است و امن سازی آن نسبت به ابر، سخت‌تر است، بنابراین بیشتر مستعد حملاتی هستند که نیاز به حضور فیزیکی مهاجمان دارند .با توجه به ماهیت IoT، محاسبه لبه در دستگاه‌هایی که می‌توانند در هر مکانی واقع شوند، از محیط‌های بسیار امن تا محیط‌های با امنیت کمتر انجام می‌شود. در بسیاری از موارد جداکردن شبکه امکان پذیر نیست و دسترسی فیزیکی به دستگاه‌های واقعی محدود نمی‌شود. به خطر انداختن امنیت دستگاه در لبه و دسترسی به داده‌های رمزنگاری شده برای پردازش به موقع روی آن می‌تواند پیوند مورد اطمینان دستگاه IoT و Cloud را خراب کند و اطلاعاتی که قرار بود رمزگذاری شود را باقی بگذارد. همچنین اقدامات امنیتی منظم در ابر مانند نظارت، که می‌تواند از چنین حملاتی علیه دستگاه‌ها جلوگیری کند، سخت‌تر و کم‌تر قابل‌کنترل است.[3]

1. International Data Corporation
2.http://techblog.comsoc.org/04/03/2017/idc-directions-2017-iot-forecast-related-sessions/
3.https://www.sciencedirect.com/science/article/pii/S0167739X15003015

تأثیر ابر غیر متمرکز بر امنیت

همانطور که قبلاً ذکر شد، نه تنها دستگاه‌های اینترنت اشیا، پراکنده هستند، بلکه با محاسبات لبه، بخش‌ها و قابلیت‌های ابر نیز در محیط پیرامون پراکنده می‌شوند.علیرغم برخورداری از جنبه‌های مثبت امنیت (به عنوان مثال اشیا کمتر به صورت مستقیم و از راه دور با سرویس‌های ابری که بیانگر کاهش حملات DDOS[1] است.) ابر غیر متمرکز چالش‌هایی را به همراه دارد. به عنوان مثال، محدودیت از نظر ویژگی کشسانی در مقایسه با ابر باعث می‌شود که لبه IoT در برابر حملات DoS[2] آسیب پذیرتر شود، و پیچیدگی هماهنگی استفاده از روش‌های امنیتی (مانند بروزرسانی‌ها / بروز رسانی firmware[3] ها / وصله کردن) را افزایش می‌دهد.[4]

۲-۳- یکپارچگی

وابستگی امنیت به خدمات کسب و کارهای عمودی

استفاده مورد نظر از اینترنت اشیا نقش مهمی ایفا می‌کند. هنوز هم موارد بسیاری وجود دارد که امنیت کلی موجود می‌تواند بر امنیت اکوسیستم اینترنت اشیا از جمله ابر تاثیر گزار باشد. به خصوص هنگامی که در زیرساخت‌هایی که عملیات حیاتی انجام می‌شود (به عنوان مثال، بیمارستان هوشمند) از اینترنت اشیا استفاده می‌شود، امنیت سایبری می‌تواند پتانسیل ایمنی را داشته باشد. اگرچه امنیت IoT باید به اندازه کافی قوی باشد تا مناسب استقرار

۱.حمله منع سرویس (Denial Of Service)
۲. حمله منع سرویس توزیع شده (Distributed Denial of Service)
۳. یک ترکیب سخت افزار و نرم افزاری کامل که نیازمند هیچ رابطی نیست و با استفاده از بخش‌های نرم افزاری می توان بصورت مستقیم و بدون واسطه با بخش‌های سخت افزاری آن ارتباط برقرار کرد.
4. https://ieeexplore.ieee.org/document/7165580/

در همه محیط‌ها باشد، اما مسائل بسیاری به دلیل پیچیدگی زیاد پلتفرم‌های بهم پیوسته و مدیریت آنها، هنوز وجود دارد.

وابستگی معیارهای امنیت IOT به توسعه دهندگان در این حوزه

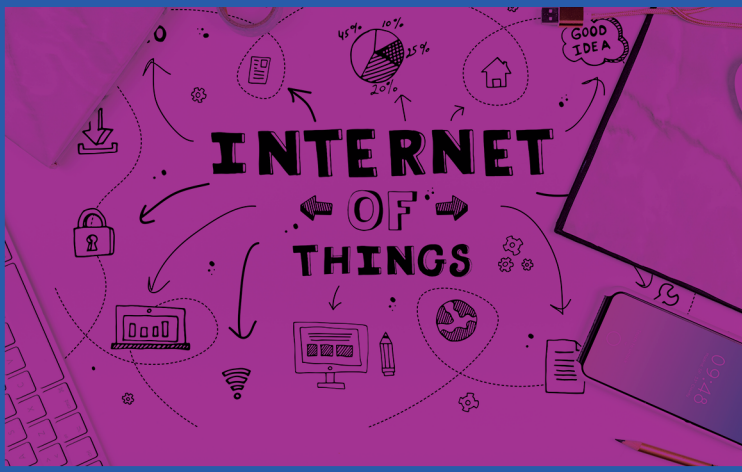
دانش امنیتی توسعه دهندگان IOT جهت هوشمند سازی اشیاء در سطح پایینی قرار دارد. پارامترهای اصلی امنیت در دستگاه‌های هوشمند که شامل راه اندازی امن، احراز هویت اشیاء، رمزگذاری و جامعیت پیام و همچنین برنامه مدیریت و ذخیره کلیدها می‌باشد معمولا به درستی پیاده سازی نمی‌شوند. تعریف دستورالعمل چرخه توسعه امن نرم افزار و سخت افزار می‌تواند بسیار چالش برانگیز باشد چرا که این فرآیندها شامل الزاماتی از قبیل سخت افزارهای مختلف، پروتکل‌ها و روش‌های اتصال به شبکه در توسعه IoT می‌باشد و می‌تواند تعریف این چرخه را پیچیده‌تر کند.

دستگاه‌های منسوخ شده

ممکن است بسیاری از دستگاه‌ها هرگز نرم افزارهای خود را بروز رسانی نکرده باشند، برای اینکه ممکن است یا تولید کننده دستگاه، بروز رسانی آن را ارئه ندهد یا ممکن است مشتریان بروزرسانی‌هایی را که قبلاً در دسترس قرار داده شده بودند را استفاده و اعمال نکنند. از طرفی دستگاه اینترنت اشیا حتی از رابط کاربری

جهت امکان بروز رسانی دستی نرم افزار خود پشتیبانی نمی‌کند.

بخش سوم



بخش سوم

سناریوهای حمله

خارج از چالش ها، برخی از تهدیدهای مهم وجود دارد که به انطباق Cloud و IoT اشاره دارد. برخی از این تهدیدها با حملههایی مانند DDoS، دستکاری دادههای سنسورها، تزریق کد یا همان SQL injection و یا مخاطرات بروز رسانی FOTA) Frimware). [1] در این بخش، ما بعضی از سناریوهای حمله که این نگرانیهای اصلی در مورد انطباق زیرساخت ابر و IoT را نشان میدهد را ارائه میدهیم.

۳-۱- میزبانی دشمن

در همین زمان، خانم Darkhat که آخرین وصله امنیتی موجود در این به روزرسانی را در اختیار دارد و تصمیم دارد از حفرههای امنیتی موجود در کلیه دستگاههای منسوخ که دارای آن نرم افزار هستند، استفاده کند. او آنها را به عنوان botnet دستگاههای IoT اضافه می کند چند روز بعد، آقای Soulful هنگامی که برخی از قابلیتهای کاربردی با دستگاههای جدید، آشپزی را تجربه می کند، بسیار

1. https://tools.ietf.org/pdf/draft-moore-iot-security-bcp00-.pdf
Firmware-Over-The-Air

تحریک می‌شود: و به آرامی به آنها پاسخ می‌دهد، و گاهی اوقات حتی وظایفی را که تبلت او فرمان می‌دهد را انجام نمی‌دهد. هنوز هم درباره اینکه چگونه این دستگاه‌ها باید زندگی او را آسان‌تر کرده و سخت‌تر نکنند، در حال فکر کردن است، اما توجه او به اخبار تلویزیون جلب می‌شود. ظاهراً یک بیمارستان در یک بحران قرار گرفته است، زیرا سرویس‌های ابری آنها دچار اختلال شده است و داده‌هایی روی هاست در حال حاضر در دسترس نیستند، انکار سرویس‌هایی عادی سرویس دهندگان. نه تنها آنها نمی‌توانند به داده‌های حیاتی برای بیماران خود دسترسی پیدا کنند، بلکه دستگاه‌های پزشکی هوشمند در حال استفاده نیز نمی‌توانند بروز شوند و به همین جهت به درستی کار نمی‌کنند. آقای Soulful با خود میگوید "دقیقاً همان چیزی که می‌گفتم، این اشیا باهوش فقط مشکل را ایجاد می‌کنند" چیزی که او حتی نمی‌تواند تصور کند این است که، مردم عادی درست مثل او میزبان زامبی‌هایی بودند که این حمله را انجام دادند، بدون اینکه حتی آنها بدانند.

گزینه ای را برای استفاده در اختیار کاربران قرار می‌دهد که تصمیم بگیرند یک بروزرسانی مهم نصب شود یا نه، که این پاسخ آن ریسک بالایی دارد. در این حمله، یک مهاجم وصله ای را که برای کاربران منتشر شده است، پیگیری می‌کند تا آنها بتوانند دستگاه‌های خود را بروز کنند، مهندسی معکوس را در برابر آن انجام دهند و آسیب پذیری این وصله و سعی در رفع آن را پیدا می‌کنند. مهاجم برای

استفاده از این آسیب‌پذیری، کدمخربی را برای استفاده ایجاد می‌کند و آن را منتشر می‌کند، بنابراین تمام دستگاه‌های منسوخ شده، آلوده میشوند و بخشی از یک بات نت اینترنت اشیا می‌شوند. پس از آن، مهاجم این بات نت‌ها را فرمان دهی و کنترل می‌کند تا یک حمله DDoS را علیه یک زیرساخت حیاتی انجام دهد، و این باعث ایجاد اختلال در سرویس‌ها و دسترسی داده‌ها و در نتیجه ایجاد تأثیر بالایی در جامعه خواهد شد که اگر سیستمی برای بروزرسانی خودکار و امن نرم افزار وجود داشت، می‌توانست از این موضوع جلوگیری شود.

تاثیر	دامنه کاربرد
بالا : تاثیر هدف قرار دادن بات نت CII بر جامعه	مشتریان، خانه‌های هوشمند
مخاطرات و چالش‌های امنیتی	**پیشگیری‌های امنیتی**
• دستگاه‌های منسوخ شده IoT • پروتکل‌های ناهمگون برای ارتباطات • جریان داده‌های ناامن از Edge به Cloud	• ارتباطات امن، تحلیل جریان امنیتی و امنیت داده‌ها در حالت rest • افزودن الزامات امنیتی به محیط IoT

۳-۲- مسیرهای پرخطر

John Prompt از آمبولانس هوشمند جدیدی که چند ماه پیش بیمارستان برای آنها فراهم کرده بود، بسیار خوشحال بود. با وجود بسیاری از پیشرفت ها، ویژگی محاسبه مسیر یابی بیشتر مورد علاقه او بود. با در نظر گرفتن اطلاعات ترافیک در زمان واقعی که مستقیماً

از سنسورهایی که در اطراف منطقه تعبیه شده‌اند جمع آوری شده است، سیستم به صورت خودکار مسیر بهینه را در سریعترین زمان ممکن برای رسیدن به بیمارستان نشان می‌دهد، که در صورت بحرانی بودن وضعیت سلامتی بیمار می‌تواند تغییراتی را ایجاد کند. این ویژگی‌ها با فعال سازی و پشتیبانی فرآیندهای یادگیری ماشینی با میزبانی ابر در بیمارستان، انجام می‌شود.[1] اطلاعات جمع آوری شده توسط سنسورهای مستقر در سطح شهر، تحلیل و پردازش می‌شوند تا بتوانند بهترین مسیر را محاسبه کنند، اشتباهات و خطاهای آن را یاد بگیرند و با آموزش مستمر، روند آن را اصلاح کنند.

با این وجود، اکنون چند روزی است که John با چند مشکل در سیستم جدید روبرو می‌شود. نه تنها او بیش از هر زمان دیگری در ترافیک گیر کرده است، بلکه یک روز یک بیمار در آمبولانس درگذشت در حالی که آنها در تلاش بودند تا بفهمند که چرا محاسبه مسیریابی باعث شده تا آنها از خیابان بدون خروجی بگذرند. وی گمان می‌کند که سرویس مسیریابی به درستی کار نمی‌کند، اما وقتی نگرانی‌های خود را برای تیم مسئول در بیمارستان مطرح می‌کند، آن‌ها هیچگونه بی‌نظمی را در سیستم‌ها پیدا نمی‌کنند، نه در دستگاه‌های هوشمند که در اطراف منطقه وجود دارند و ترافیک را کنترل می‌کنند، و نه در پردازش داده‌هایی که توسط این دستگاه‌ها به ابر فرستاده می‌شوند.

و در واقع، سیستم مسیریابی مشکلی ندارد. آقای Sly چند هفته پیش

1.https://www.infoworld.com/article/3140545/artificial-intelligence/how-to-approach-machine-learning-in-the- cloud.html

به بعضی از دستگاه‌های هوشمند که با سیستم نظارت، محدوده خود را کنترل می‌کنند، دسترسی فیزیکی پیدا کرد و مدارک و گواهینامه‌های دیجیتال آنها را به سرقت برد. با استفاده از آنها، او توانست موفق به احراز هویت در ابر، بشود و به تعداد زیادی از دستگاه‌ها دسترسی پیدا کند. به این ترتیب، او توانست بعضی از پارامترها و اندازه آستانه آنها را تغییر دهد، بنابراین داده‌های ارسال شده به ابر را دستکاری می‌کند. از آنجا که تعداد زیادی از دستگاهها تحت تأثیر قرار گرفتند، این امر در اقدامات یادگیری ماشینی در ابر، تاثیر زیادی ایجاد کرد و در نتیجه در مسیرهای اشتباه قرار گرفتند .

امروزه دستگاه‌های اینترنت اشیا در حیات وحش هم قرار داده می‌شوند، بدون اینکه صاحبان، کنترل صحیحی از آنها داشته باشند. در این سناریو، یک مهاجم به صورت فیزیکی به چند دستگاه اینترنت اشیا که در مکان‌هایی از جاده‌ها قرار داده شده است دسترسی پیدا می‌کند و مجوزها / گواهینامه دیجیتالی آنها را به سرقت می‌برد. پس از آن، مهاجم با استفاده از آنها موفق به احراز هویت در ابری که آنها استفاده می‌کنند می‌شود و به تعداد زیادی دستگاه‌ها دسترسی پیدا می‌کند.

او سپس به این دستگاه‌ها فرمان می‌دهد که داده‌های مخرب و دستکاری شده را که در فرآیندهای یادگیری ماشین تأثیر داشت، به ابر ارسال کنند بنابراین بر یادگیری دستگاه‌ها (که معمولاً به عنوان حمله poison شناخته می‌شوند) تأثیر می‌گذارد.

در نتیجه، کل فرایند بی ثبات شده است و باعث می‌شود هنگام محاسبه مسیرها، نتایج اشتباهی ایجاد شود که این موضوع با توجه به اینکه مسئله مرگ و زندگی به کارایی این مسیریابی‌ها بستگی دارد، بسیار حساس است. اگر این دستگاه‌ها از حفاظت فیزیکی بیشتری برخوردار بودند و از دسترسی فیزیکی به دستگاه جلوگیری می‌شد، از ابتدا گواهی‌ها به سرقت نمی‌رفت.

تاثیر	دامنه کاربرد
بالا : از دست رفتن پتانسیل زندگی	زیرساخت‌های حیاتی اطلاعات
چالش‌ها و مخاطرات امنیتی	**پیشگیری‌های امنیتی**
• مجازی سازی دستگاه برای ایجاد همگنی • ارتباطات امن، تحلیل جریان امنیتی و امنیت داده‌ها در حالت rest	• جریان داده‌ی نامن از Edge به Cloud • پردازش به موقع در لبه، امنیت را تحت الشعاع قرار می‌دهد

۳-۳- درو و برداشت محصول

برداشت محصول به عنوان یک شغل خانوادگی به واسطه پروژه Greenheart با سرعتی شگفت انگیزی در حال رشد است، چراکه آنها دستگاه‌ها و سامانه‌های هوشمند را در مزرعه خود بکار میبردند و به اولین مزرعه هوشمند منطقه تبدیل شده اند.[1] تراکتورهای خود ران آنها به خاطر اینکه امکان کنترل از راه دور دارند و می‌توان از دور کارکرد آنها را کنترل و بررسی کرد باعث صرفه جویی زیادی در

1. https://www.link-labs.com/blog/iot-agricultur

زمـان و انـرژی می‌شـوند و عـلاوه بـر ایـن، بـا ایـن سـامانه سنسـورهای برداشـت و تحلیـل شـرایط خـاک، داده‌هـای سـامانه یـاد شـده را بهینـه می‌کننـد و در نتیجـه آبیـاری براسـاس آن داده‌هـا تنظیـم می‌شـود کـه آب کافـی در دسـترس محصـول باشـد و همچنیـن آب هـدر نـرود و در صـورت تشـخیص شـرایط نامسـاعد، داشـبورد مدیریتـی هوشـمند، هشـدار مربـوط بـه آن مسـئله خـاص را بـرای کاربـر ارسـال می‌کنـد.

بـه خاطـر موفقیـت پـروژه Greenhearts اعضـای خانـواده Brownsoul، صاحبـان مـزارع مجـاور را کـه تـلاش می‌کردنـد بـا راه حل‌هـای مـدرن و نوآورانـه‌ی همسـایگان رقابـت کننـد و بالاتـر بـودن کیفیـت راه حل‌هـای سـنتی را بـه اثبـات برسـانند عصبانـی می‌کنـد. بنابرایـن جوانتریـن پسـر همسـایه کـه در رشـته کامپیوتـر تحصیـل کـرده اسـت، تصمیـم بـه دشـمنی دارد و در ایـن راسـتا تـلاش می‌کنـد تـا یکـی از همکارانـش کـه تجربـه هـک دارد بـرای پیشـبرد اهدافـش بـه او کمـک کند. در ابتـدا خوشـبختانه بـرای آنهـا فـرم احرازهویـت بـرای دسترسـی بـه پنـل اصلـی Cloud در مزرعـه هوشـمند Greenhearts بـه درسـتی تأمیـن نشـد و بنابرایـن ورود نیـز بـه درسـتی تأییـد نشـد کـه در نتیجـه نتوانسـتند بـه پنـل اصلـی دسترسـی پیـدا کننـد. ولـی متأسـفانه در ادامـه تلاش‌هـا مشـخص می‌شـود کـه توسـعه دهنـدگان بـر روی فـرم ورود بـه سیسـتم، آزمون‌هـای امنیتـی (تسـت نفـوذ) انجـام نداده‌انـد کـه یـک تزریـق کـد SQL یـا همـان Sql Injection بـه آنهـا اجـازه داد کـه بـدون داشـتن هویـت معتبـر بـه کنتـرل اپلیکیشـن تحـت وب مبتنـی بـر ابـر، دسترسـی

غیر مجاز پیدا کنند. آنها سپس به داشبورد دسترسی پیدا کردند که آن داشبورد تمام دستگاه‌های هوشمند را به صورت مرکزی اداره می‌کند و آنها پارامترهایی که منجر به رفتار سنسورهای خاک میشد را به صورت بدون صدای زنگ خطر یا عدم ارسال هشدار به کاربر، تغییر دادند و سامانه را خراب کردند.

چند هفته بعد، هنگامی که برداشت محصول صورت گرفت، آنها متوجه نشدند که چرا کل محصولات خراب شده است و مهمتر از همه، چرا سیستم هوشمند به آنها هشدار نداده است که مشکلی وجود دارد. Cloud در اکثر موارد امکان کنترل و فرمان دستگاه‌های IoT را به راحتی برای کاربران فراهم می‌کند، بنابراین یکی از عناصر اصلی برای تأمین امنیت هم می‌تواند باشد. در این سناریو، مهاجم از یک فرم احراز هویت که تست امنیتی نشده بود، استفاده کرد و با استفاده از تزریق کد SQL، به پنل اصلی Cloud دسترسی پیدا کرد. نتیجه این امر این است که مهاجمان به ویژگی‌های کنترل و فرمان دستگاه‌های IoT دسترسی پیدا کرده و پارامترهای تصمیم گیری سنسورهای خاک را بدون ارسال هر گونه هشدار، دچار خطا کرد. اگر فرم احراز هویت به درستی انجام شود می‌توان از این امر جلوگیری کرد. تست نفوذ و رفع باگ های امنیتی تجهیزات ابری و IoT به صورت جدی لازم است و بسته به کارهایی که کاربران می‌خواهند انجام دهند، میبایست لایه‌های مختلف امنیتی و مکانیزم کنترل دسترسی وجود داشته باشد.

تاثیر	دامنه کاربرد
متوسط: زیان‌های مالی زیاد	شرکت‌های کوچک و متوسط رو به بالا
مخاطرات و چالش‌های امنیتی	**پیشگیری‌های امنیتی**
• وابستگی امنیت به خدمات کسب و کارهای عمودی • وابستگی معیارهای امنیت IOT به توسعه دهندگان در این حوزه	• اضافه شدن پارامترهای اندازه گیری امنیت • امنیت نقاط پایانی از طریق همه محیط ها

۳-۴- Open House

این دوره فعالیت شلوغی در SharpLocks Inc است و کارمندان برای حفظ شغل خود، سخت در محل کار تلاش می‌کنند. آنها از قبل سیستم‌های قفل‌های هوشمند مسکونی را تهیه کردند و موفقیت آنها باعث شد تا بازار هدف خود را گسترش دهند تا محیط‌های کاری را نیز تحت پوشش قرار دهند.

خانم گلد قصد دارد از شیوه مزاحمت استفاده کند و وانمود کند که وظایف منظم نظارت و تنظیمات را روی قفل‌های هوشمند انجام می‌دهد، وی قصد دارد از مکانیزم بروزرسانی FOTA[1] که این برند پیروی می‌کند سوءاستفاده کند. "حامیان" او یک سیستم عامل مخرب را برای قفل‌های هوشمند، فراهم کردند، که به کارت‌های RFID[2] آنها دسترسی می‌دهد تا به هر قفل هوشمند SharpLock دسترسی داشته باشند و قابلیت دستیابی به هرگونه فرضیاتی توسط آنها در نظر گرفته شده است را ایجاد کند، و یک کارت "Master"[3] را برای آنها فراهم کند. با توجه به اینکه پس از دو روز قرار هست یک بروزرسانی جدید سیستم عامل برنامه ریزی شود

1. Firmware Over The Air
2.Radio-frequency identification
3. https://en.wikipedia.org/wiki/Mastercard

کـه بـه طـور خـودکار بـه دسـتگاه‌ها اجبـاری شـود، وی قصـد دارد تـا بروزرسـانی مخـرب سـریع‌تر اثـر کنـد. رابـط کاربـری Gateway، از طریـق Cloud بـه اپلیکیشـن‌ها و دسـتگاه‌های بیرونـی، نقـش هـای مدیریتـی و امنیتـی ماننـد کنتـرل دسترسـی، تعـادل بـار ترافیـک یـا بروزرسـانی‌ها را ارائـه می‌دهـد. خانـم Gold از ایـن مزیـت اسـتفاده می‌کنـد، بـه کنسـول مدیریتـی رابـط کاربـری Gateway دسترسـی پیـدا می‌کنـد و بـا سیسـتم عامـل مخـرب، آن را مجبـور بـه بروزرسـانی قدیمـی می‌کنـد.

در ایـن دوره، حامیـان مرمـوز بـا اسـتفاده از کارت Master موقـت خـود، می‌تواننـد بـه صـورت فیزیکـی بـه یـک موسسـه حقوقـی کـه مـدت طولانـی هـدف آنهـا قـرار گرفتـه بـود، دسترسـی پیـدا کننـد. بـا توجـه بـه وسـعت زیـاد ایـن بنـگاه خـاص و تعـداد بسـیار زیـادی از افـراد کـه در آنجـا کار می‌کننـد، از حضـور آنهـا غافـل میماننـد. آنهـا مجموعـه ای از اسـناد بسـیار محرمانـه را کـه مدت‌هـا پـس از آن‌هـا آنجـا بـوده اسـت را سـرقت می‌کننـد و بـدون هیـچ گونـه اشـتباهی از سـاختمان خـارج می‌شـوند.

تهدیـدات خـودی بـه عنـوان یکـی از نگـران کننـده تریـن تهدیدهـا در بیـن CSP[1] هـا شـناخته شـدند. در ایـن حالـت، یـک مهاجـم خـودی بـه داشـبورد مدیریتـی رابـط کاربـری Gateway دسترسـی پیـدا می‌کنـد تـا یـک بروزرسـانی اجبـاری مخـرب را بـه دسـتگاه‌های IoT وارد کنـد (در اینجـا قفل‌هـای هوشـمند). رابـط Gateway، از رابـط کاربـری Gateway، از طریـق Cloud بـه اپلیکیشـن‌ها و دسـتگاه‌های بیرونـی، نقـش هـای مدیریتـی و امنیتـی ماننـد کنتـرل دسترسـی، تعـادل بـار

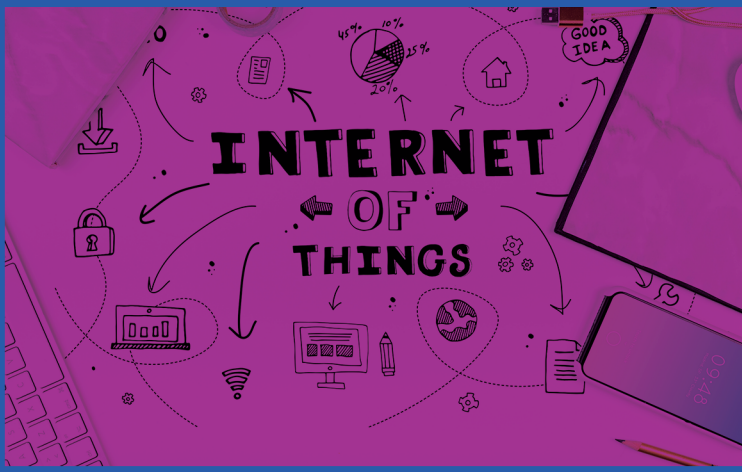
۱. ارائه دهندگان سرویس ابری

ترافیک یا بروزرسانی‌ها را ارائه می‌دهد. دسترسی به معنی آن است که او می‌تواند از مکانیسم FOTA سوءاستفاده کند و تمام دستگاه‌های مدیریت شده توسط رابط کاربری Gateway را ناامن بگذارد.تا زمانی که برنامه بروزرسانی شده انجام نشود قفل‌ها برای دسترسی به مراکز محافظت شده توسط مهاجمان باز می‌شود و باعث می‌شود در این حالت سرقت اسناد بسیار محرمانه، بر شرکت و مشتری‌های آن تأثیر بگذارد. اگر یک سیستم نظارت فعال، در مورد این بروزرسانی ناخواسته، هشدار می‌داد، می‌توانست از این امر جلوگیری شود، و اگر این شرکت خط مشی توسعه canary را رعایت میکرد، همه دستگاه‌ها تا زمانی که مطمئن شوند بروز رسانی به درستی کار می‌کند، بروز نمیشدند.

تاثیر	دامنه کاربرد
بالا : نقض محرمانگی ,سرقت اطلاعات مشتری	شرکت‌های بزرگ
مخاطرات و چالش‌های امنیتی	**پیشگیری‌های امنیتی**
• وابستگی معیارهای امنیت IOT به توسعه دهندگان در این حوزه • خودی[۳۳]	• ارتباطات امن، تحلیل جریان امنیتی و امنیت داده‌ها در حالت rest • امنیت نقاط پایانی از طریق همه محیط ها

۳۳ اگرچه در چالش‌های امنیتی این مقاله به عنوان تهدیدی خاص برای مساله همگرایی اینترنت اشیا و رایانش ابری تحلیل نشده است، اما این یک تهدید قابل‌توجه است که در بسیاری از موارد از جمله این مورد، استفاده می‌شود.

بخش چهارم



بخش چهارم

پیشـــگیری های امنیتی

مباحـث مطـرح شـده می‌توانـد امنیـت اکوسیسـتم Cloud یـا IoT را بـه طـور کلـی بـه خطـر بیاندازد.بـه همیـن دلیـل، می‌تـوان از چندیـن تجربـه، فنـاوری و محصـولات و روش‌هایـی اسـتفاده کـرد کـه در ادامـه، لیسـتی از دسـتورالعمل‌های عمومـی کـه نشـان می‌دهـد چگونـه می‌تـوان بـه راهکارهـای امـن رسـید را ارائـه می‌دهیـم.

۴-۱- اتصال

مجازی سازی دستگاه برای ایجاد همگنی

روش‌هـای مجـازی سـازی، صـرف نظـر از آنچـه کـه بـه ابـر مشـهور اسـت، بـرای نهـان سـازی پیچیدگی‌هـا درپشـت یـک لایـه سـازگار مفیـد اسـت. بنابرایـن، در چنیـن محیـط ناهمگـن، مفهـوم یکنواختی یک دسـتگاه هـم از نظـر ارتباطـی و هـم از نظـر امنیتـی، را می‌تـوان درک کـرد[1] مجـازی سـازی دسـتگاه‌ها می‌توانـد در چندیـن سـطح در محیـط اعمـال شـود: ماننـد اسـتفاده از کانتینـر کردن[2] سیسـتم عامـل دسـتگاه‌های IoT بـرای

1. http://journals.sagepub.com/doi/full/683425/2015/10.1155
2.https://www.scribd.com/document/360971818/Exploring-Container-Virtualization-in-IoT-Clouds

ایزوله و یکپارچگی برنامه ها، برای اینکه تمام دستگاه‌های IoT در زیرساخت ابری، سریعاً یک معادل مجازی در آنجا داشته باشند. این شیوه‌ها امکان جدا کردن نقاط انتهایی ناهمگن IoT و ابر را فراهم می‌آورد، و امنیت را در قالب یک لایه مدیریتی فراهم می‌کند، و این باعث می‌شود امنیت دستگاه از سوی Cloud بررسی شود.

همانطور که قبلاً گفته شد، نقاط انتهایی از پروتکل‌های ناهمگن که با سطوح مختلف امنیتی به روش‌های ارتباطی مختلفی، ارتباط برقرار می‌کنند، استفاده می‌کنند، بنابراین راه طبیعی برای بهبود اشیا، همگن سازی میباشد.. الزامات ناهمگنی دستگاه‌ها مانند پهنای باند، تأخیر، دسترسی باید در این فرآیند در نظر گرفته شود.

ارتباطات امن، تحلیل جریان امنیتی و امنیت داده‌ها در حالت rest

به عنوان اولین گام برای تأمین امنیت بین Cloud و Edge، نیاز به درک و طبقه بندی داده‌های منتقل شده (مثلاً عمومی یا محرمانه) و اطمینان از محرمانه بودن و جامعیت داده‌ها میباشد. برای این کار، باید از رمزنگاری در زمان انتقال استفاده شود به عنوان مثال با استفاده از یک شبکه خصوصی مجازی (VPN) برای اتصال به ابر خصوصی مجازی (VPC) و پروتکل TLS[1] در ارتباطات و به عنوان مثال در حالت Rest، با استفاده از توکن‌های امنیتی یا جداسازی پایگاه داده‌ها از امنیت داخلی.[2] حتی زمانی که بدرستی کنترل و مدیریت شود، امنیت تعداد

1. Transport Layer Security
2. https://www.slideshare.net/AmazonWebServices/deep-dive-aws-security-by-design

زیادی از داده‌های تولید شده توسط تعداد زیادی نقاط انتهایی باید تامین شود، که از طریق همان روش‌های فیلتر کردن و جمع آوری برای مدیریت داده‌ها در لبه استفاده می‌شود، می‌توان برای افزودن امنیت در این سطح استفاده کرد. ما می‌توانیم از این اقدامات اولیه جهت پردازش داده استفاده کنیم تا از این طریق جریان‌های مخرب، احراز هویت و مجوزهای دسترسی دستگاه ها، تشخیص ناهنجاری‌ها یا احتمال data flooding[2] که به ابر هدایت می‌شوند را از قبل بررسی و امن سازی شوند.

۴-۲- تحلیل

امنیت فیزیکی و سایبری در دستگاه‌های لبه

یکی از مراحل آتی برای تأمین امنیت محیطی، امنیت فیزیکی نقاط پایانی است که مستقیما باید به آن پرداخت شود. از آنجا که پراکندگی دستگاه‌های لبه، دسترسی فیزیکی به آنها را آسان‌تر می‌کند، برای مقابله با این خطر، باید سخت افزار مورد نیاز با الزامات پیاده سازی امنیتی، توسعه داده شود.[3]ویژگی‌هایی از قبیل امنیت تجدید پذیر (جایگزینی تنها بخشی به جای جایگزینی کامل سیستم هک شده)، گزارش خرابی به ابر یا هدایت پردازش‌ها به یک دستگاه هوشمند در لبه،[4] که باعث می‌شود یک مهاجم حتی در هنگام دسترسی فیزیکی از مزایای آن استفاده کند. علاوه بر این، وقتی امنیت به فرآیندهای محاسبات لبه اضافه

1.https://journalofcloudcomputing.springeropen.com/articles/10.1186/s-017-13677 2-0090
3.https://azure.microsoft.com/en-us/blog/securing-the-intelligent-edge/
4.https://www.microsoft.com/en-us/research/wp content/uploads/03/2017/SevenProp ertiesofHighlySecureDevices.pdf

می‌شود بدلیل قابلیت‌های محدود دستگاه‌های لبه، با چالش‌هایی روبرو هستند که می‌توان از رویکرد متوسطFog Computing استفاده کرد. همانطور که در استانداردNIST[1] که اخیرا منتشر شد، توضیح داده شده است،Fog Computing (محاسبات مه) می‌تواند قابلیت‌های مقیاس پذیری ابر را نزدیک به دستگاه‌های لبه با هدف افزایش کارایی، عملکرد و امنیت در لبه، فراهم کند.

۴-۳- یکپارچگی

اضافه کردن مولفه‌های امنیت به محیط‌های اینترنت اشیا

بمنظور کاهش بار برخی از مشکلات توسعه دهندگان و تولید کنندگان، با وارد کردن مولفه‌های جدید محیطی، که منحصراً روی تأمین امنیت تمرکز دارند، می‌توان امنیت را تقویت کرد. وسایل امنیتی، روترها و gateway ها راهی برای اضافه شدن امنیت در سطح لبه، تقویت کنترل در حوزه‌هایی هستند از نظر ناهمگنی و تعداد داده و دستگاه‌ها دارای مشکلات بیشتری هستند. به عنوان نمونه، یک gateway امنیتی که در یک محیط خانه هوشمند قرار می‌گیرد، نه تنها عملکرد داده‌ها و فعالیت‌های ارتباطی را کنترل و نظارت می‌کند، بلکه می‌تواند بخشی از شبکه ناامن و آسیب پذیر را از بقیه محیط جدا کند.[2] بنابراین امنیت در محدوده شبکه خانگی علاوه بر امنیت نسبت به ابر قابل استفاده است. با مهاجرت به ابر، یک مولفه وجود دارد که با استفاده از آن، یک

1. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.325-500.pdf
2.https://www.rcrwireless.com/20170320/opinion/reality-check-csps-need-to-take-a-leadership-role-in- securing-iot-tag10

لایه کنترلی در شبکه اضافه می‌کند و از نظر امنیتی این تفکیک را بین لبه و backend فراهم می‌کند. ما به رابط کاربری gateway مراجعه می‌کنیم، که مربوط به یک مولفه واسطه با پتانسیل انجام فرآیندهای امنیتی از قبیل تست canary [۲۱]، بررسی مجوز عبور بسته ها، تأیید هویت / مجوز و کنترل دسترسی [۳] یا محافظت در برابر حملات مانند حملات DDOS و فرایندهای FOTA.

اضافه شدن پارامترهای اندازه گیری امنیت

تلاش‌های زیادی برای تامین امنیت، در سازمانها، شرکتها، بخشها و صنایع عمودی انجام شده است که بسته به حیاتی بودن آنها، بودجه و اولویت‌های آنها متفاوت است. داشتن مجموعه ای ازمعیارهای اندازه گیری امنیت برای اینترنت اشیا عنوان راهکار این مشکل، باعث هماهنگی و افزایش سطح امنیت در کل اینترنت اشیا می‌شود. با توجه به این موضوع، اتحادیه اروپا در این راستا تلاش کرده است و دستورالعمل‌ها و توصیه‌هایی را در زمینه زیرساخت‌های حیاتی اطلاعات ارائه کرده است.[۴] که صرف نظراز صنایع عمودی، یک سطح امنیتی پایه را در تمام محیط‌ها تضمین خواهد کرد.

1.https://aws.amazon.com/about-aws/whats-new/11/2017/amazon-api-gateway-supports-canary-release-deployments/
2.https://docs.aws.amazon.com/apigateway/latest/developerguide/canary-release.html
3.https://azure.microsoft.com/en-us/blog/securing-the-intelligent-edge/
4. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

بروز رسانی خودکار و امن نرم افزار

از یک طرف، خود دستگاه‌های اینترنت اشیا ناهمگن هستند و از طرف دیگر، محاسبات لبه مدل غیر متمرکز را تشدید و کنترل آنها را سخت‌تر می‌کند. ابر به امنیت دستگاه‌هایی که با مدل غیر متمرکز سازگار هستند و کنترل آنها را سخت‌تر می‌کند می‌تواند کمک کند. این امر با در نظر گرفتن برخی پارامترهای امنیتی سطح بالا می‌تواند انجام شود. ساز و کارهای بروزرسانی امن نرم افزار، مانند فرآیندهای FOTA [1]، به ابر (با توجه به دید متمرکز شده از کل محیط) اجازه می‌دهد امنیت را به صورت سریع و مؤثر توزیع کند و به این روش از حمله جلوگیری کرده و اختلال را به حداقل برساند. [2]

به عنوان مثال، بازیابی یک دستگاه پس از حمله سایبری می‌تواند با بازیابی بروزرسانی OTA، که در آن بروزرسانی‌های امنیتی از طریق اینترنت به دستگاه اعمال می‌شوند، به صورت مؤثرتری حاصل شود.

یک نمونه امن شیء که در آن بروزرسانی‌های نرم افزاری به صورت خودکار رمزنگاری، مدیریت و توسعه داده می‌شوند و از طریق کل پشته امنیتی دستگاه می‌تواند پیچیدگی و زمان پشتیبانی برای حفظ امنیت را کاهش دهد.

1.https://ieeexplore.ieee.org/document/8110218/
2.https://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php

امنیت نقاط پایانی از طریق همه محیط ها

امن سازی کل محیط اینترنت اشیا موضوعی چالش برانگیز است، که حتی با در نظر گرفتن نیاز امنیت انتها به انتها از طریق کل زنجیره ارزش برای دستیابی به امنیت توزیع شده این چالش بیشتر می‌شود. بعضی از اقدامات لازم برای حفظ امنیت سطح بالا، به عنوان مثال، با استفاده از یک طرح کنترل دسترسی کامل و کارآمد، که باید در کل محیط اعمال شود [1]، از زیرساخت ابری تا ریزترین سنسور استفاده می شود.این امر با استفاده از یک مجموعه قوی بر اساس هویت (تعیین کاربران، گروه ها، خدمات و نقش ها) بدست می‌آید تا به عنوان پایه ای برای احراز هویت قبل از هرگونه ارتباط بین مولفه ها، باشد و پس از آن با استفاده از ریزدانگی مجوزها (با نقش‌ها و طراحی صحیح خط مشی ها) بکار گرفته شود. برای اینکه این طرح به درستی کار کند، رمزنگاری و مدیریت کلید از اصول اولیه و ضروری جهت پیاده سازی آن است. مدیریت کلید در تامین امنیت دستگاه نقش اساسی دارد زیرا شامل ایجاد، تجدید، انتقال و محاسبه موارد رمزنگاری شده (یعنی کلیدها و گواهی ها) می‌شود. از این نظر، لازم است دستگاه‌های اینترنت اشیا بتوانند کلیدهای خصوصی را در ماژول‌های امنیتی سخت افزاری (**HSM**) [2] ذخیره کنند و از کلیدها و گواهی‌های تولید شده پشتیبانی کنند تا مستقیماً در دستگاه‌های **IoT** به صورت پیش فرض توزیع شوند . علاوه بر این، وجود دستورالعمل‌های عمومی و ملاحظات مربوط به مدیریت

1.https://www.slideshare.net/jsoldat/-05internetofthingsio-tcloudcomputing
2. https://safenet.gemalto.com/data-encryption/hardware-security-modules-hsms

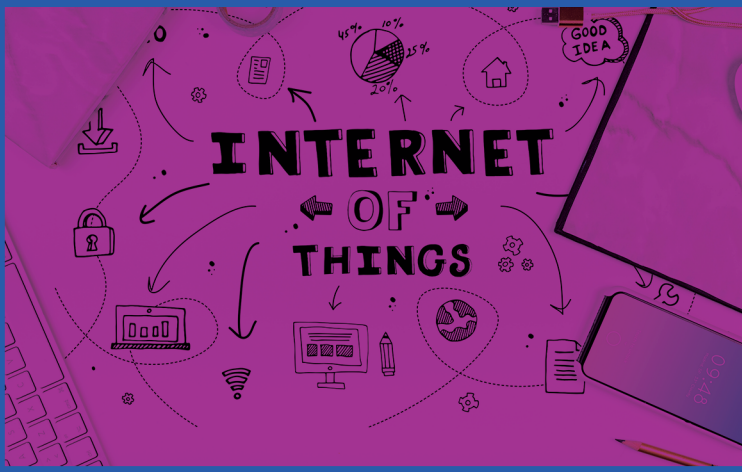
کلید می‌تواند راهنمایی هایی[1] را برای پیاده سازی مدیریت کلید رمزنگاری شده در یک برنامه با روشی امن، برای توسعه مدیریت اینترنت اشیا فراهم کند.

جنبه بعدی برای مقابله، مربوط به انجام اقدامات امنیتی در هر لایه از محیط است، که به موانع امنیتی آنها اشاره کردیم. از امنیت فیزیکی دستگاه ها، اقدامات و مکانیزم‌های امنیتی شبکه (ابرهای خصوصی مجازی، رابط‌های کاربری gateways ها) و امنیت سیستم با استفاده از FOTA ، تا حفاظت از داده‌ها با دسته بندی و رمزنگاری داده‌ها.

آخرین جنبه مهم، یکپارچگی امنیت در شبکه‌ها و سیستم‌های توسعه داده شده است. برای این کار، اولین پارامتر معرفی چرخه عمر توسعه نرم افزار به عنوان بهترین تجربه در فعالیت‌های عادی محیط اینترنت اشیا است. فرآیندی مانند سیستم‌های کنترل نسخه یا یکپارچگی و تحویل مستمر می‌تواند به شیوه ای یکپارچه به استفاده از امنیت در کل محیط کمک کند. به عنوان نمونه، اصول توسعه canary امکان استفاده امن از ویژگی‌ها یا کدهای جدید در برخی از سیستم‌ها را برای یک دوره کوتاه فراهم می‌کند تا آنها را به صورت live آزمایش کنند. [2] این امکان را برای ارزیابی در سناریوی واقعی جدید توسعه فراهم می‌کند تا مسائل را شناسایی کند و در صورت بروز اشتباه، تاثیرات آن را کاهش دهد.

1. https://www.owasp.org/index.php/Key_Management_Cheat_Sheet
2.https://searchaws.techtarget.com/tip/Enable-canary-deployments-with-Lambda-API-Gateway

جمع بندی



جمع‌بندی

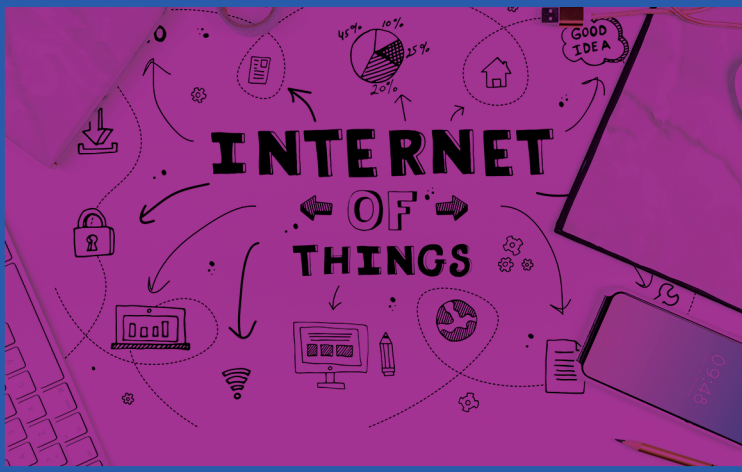
در پایان این مقاله، ما چالش‌های امنیتی همگرایی زیرساخت ابری و اینترنت اشیا و همچنین راه رسیدن به راه حل‌های امنیتی احتمالی آنها را ارائه دادیم.

با توجه به توصیه‌های امنیتی پایه ایی اتحادیه اروپا برای اینترنت اشیا و به طور خاص تعریف معماری اکوسیستم اینترنت اشیا و مدل مرجع اتحادیه اروپا برای IoT، ما سه دسته اصلی را برای چالش‌های امنیتی و توصیه‌های امنیتی این مقاله تعریف کردیم. بر اساس این سه دسته، ما لیستی از چالش‌های امنیتی را طبق لیست زیر طبقه بندی و مشخص کرده ایم:

دسته بندی	چالش‌های امنیتی	پیشگیری‌های امنیتی
اتصال	• پروتکل‌های ناهمگن برای ارتباطات • جریان داده‌ی ناامن از Edge به Cloud	• مجازی سازی دستگاه برای ایجاد همگنی • ارتباطات امن، تحلیل جریان امنیتی و امنیت داده‌ها در حالت rest
تحلیل	• پردازش به موقع در لبه، امنیت را تحت الشعاع قرار دهد. • تأثیر غیر متمرکز بودن ابر روی امنیت	• امنیت فیزیکی و سایبری در دستگاه‌های لبه

یکپارچگی	• وابستگی امنیت به خدمات کسب و کارهای عمودی • وابستگی معیارهای امنیت IOT به توسعه دهندگان در این حوزه • دستگاه‌های منسوخ شده	• اضافه کردن مولفه‌های امنیت به محیط‌های اینترنت اشیا • اضافه شدن پارامترهای اندازه گیری امنیت • بروز رستانی خودکار و امن نرم افزار • امنیت نقاط پایانی از طریق همه محیط ها

منابع



1. Document: Towards secure convergence of Cloud and IoT

| TLP GREEN | SEPTEMBER 2018

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

csri.majazi.ir

حـوزه فضـای مجـازی بـه انـدازه انقـلاب اسـلامی اهمیـت دارد. ایـن فضـا مثـل یـک رودخانـه پـر از آب و خروشـان اسـت کـه مـی آیـد و دائمـاً هـم بـر آب آن افـزوده و خروشـان تـر مـی شـود. اگـر مـا بـر ایـن رودخانـه تدبیـر کنیـم و برنامـه داشـته باشـیم، زه‌کشـی کنیـم و هدایـت کنیـم ایـن رودخانـه را تـا بـه سـد بریـزد، می‌شـود فرصـت. اگـر رهایـش کنیـم و برنامـه‌ای بـرای آن نداشـته باشـیم می‌شـود یـک تهدید.

csri.majazi.ir