بسم الله الرحمن الرحیم

گزارش سند

گزارش شماره ۳
آبان ۱۳۹۹

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

توصیه‌های امنیتی پایه برای اینترنت اشیا در حوزه زیرساخت‌های اطلاعاتی حیاتی

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

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

تهیه‌کنندگان: مهندس نیلوفر کریمی آذر-
کارشناس ارشد امنیت اطلاعات / بنیان گذار رسانه مرجع مطالعات موردی اینترنت اشیاء
مهندس زهرا کرمانی- کارشناس فناوری اطلاعات و ارتباطات / مدیرعامل شبکه هوشمند پیچک

ناظر علمی: محمد مهدی رضاپور

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

فهرست

بخش چهارم (معیارهای امنیتی و تجربه‌ها)

بخش پنجم (تحلیل GAP)

بخش ششم (توصیه‌های بسیار مهم برای بهبود امنیت سایبری IoT)

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 خیره‌کننده فضای مجازی و سایه گستری آن در حوزه‌ها 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 داشته‌اند.

در همین راستا گزارش‌های عصرفضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه 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

اینترنت اشیاء (IoT) یک الگوی مهم و رو به رشد با ابعاد فنی، اجتماعی و اقتصادی است. از نظر اتحادیه اروپا، IoT یک مفهوم نوظهور است که شامل یک اکوسیستم از خدمات گسترده و دستگاه‌های متصل است. این فناوری‌ها به منظور همگرایی پویا با داده‌ها، داده‌ها را جمع آوری، تبادل و پردازش می‌کنند. IoT چالش‌های امنیتی مهمی را دارد که باید برطرف شوند. پیاده سازی‌ها با چالش‌های امنیتی جدیدی همراه است که، تهدیدات و خطرات زیادی را به دنبال دارد. حفاظت از توسعه اینترنت اشیا به محافظت از تمام سیستم‌های وابسته (دستگاه ها) از جمله، بسترهای ابری و خدمات، برنامه‌های کاربردی ابزارهای پشتیبانی و ... بستگی دارد. بررسی چالش‌ها و اطمینان از امنیت محصولات و خدمات IoT یک اولویت اساسی است. یکی از نگرانی‌های اصلی تأثیراتی است که حمله از زمان توسعه اینترنت اشیا صورت گرفته باشد که ممکن است تهدیدهای مختلفی داشته باشد و می‌تواند امنیت، حریم خصوصی و امنیت

مردم را به خطر بیاندازد. علاوه بر این از IoT به عنوان یک عامل حمله در برابر سایر زیرساخت‌های حیاتی می‌توان استفاده کرد. فراتر از اقدامات امنیتی فنی، لازم است خط مشی‌های جدید و تصویب قوانین جدید برای اینترنت اشیا مطرح شود. همچنین چالش‌های نظارتی، گستردگی و پیچیدگی‌های اینترنت اشیا رو به افزایش است و عدم وجود ساختارهای قانونی و نظارتی و عدم وجود چهارچوب‌های امنیتی مشخص، باعث شده است تا بیشتر شرکت‌ها و تولیدکنندگان در هنگام طراحی دستگاه‌های IoT، از رویکرد خاص خود استفاده کنند. که خود مشکلات قابلیت همکاری بین دستگاه‌های سازندگان مختلف و دستگاه‌های IoT و سیستم‌های سنتی را ایجاد می‌کند. به همین دلایل، اتحادیه اروپا مجموعه ای از توصیه‌های امنیتی پایه را برای IoT تعریف می‌کند که هدف آن ارائه آگاهی در مورد الزامات امنیتی اینترنت اشیا، مشخص کردن دارایی‌های حیاتی و تهدیدات مربوطه، ارزیابی حملات احتمالی و شناسایی اقدامات امنیتی متناسب، بمنظور محافظت از سیستم‌های اینترنت اشیا می‌باشد.

واژگان کلیدی: اینترنت اشیا، ملاحظات امنیتی، معیارهای امنیتی، توصیه‌ها، تجربه‌ها، تهدید، سناریو حمله

مقدمه

مقدمه

ایـــن گـــزارش، خلاصـــه ای از مباحـــث ســـند بـــا عنـــوان « Baseline Security Recommendations for IoT » اســـت کـــه در ۲۰ ام نوامبـر سـال ۲۰۱۷ میـلادی توسـط آژانـس امنیـت سـایبری اتحادیـه اروپـا (ENISA) منتشـر شـده اسـت.

بخش اول

معرفی

بخش اول

معرفی

تعـدادی از توصیه‌هـای تهیـه شـده بـا بهـره منـدی از نظـرات کارشناسـان بـه شـرح زیـر اسـت.

•هماهنگی اقدامات و مقررات امنیت IoT

برای صنعت IoT، ارائه دهندگان، تولید کنندگان، انجمن ها

•افزایش آگاهی از نیاز به امنیت سایبری IoT

بـرای صنعـت IoT، ارائـه دهنـدگان، تولیـد کننـدگان، انجمن‌هـا، دانشـگاه‌ها، گروه‌هـای مصـرف کننـده، نهادهـای رگولاتـوری

•تعریـف دسـتورالعمل‌های چرخـه عمـر توسـعه امـن نـرم افـزار و سـخت افـزار بـرای IoT

برای توسعه دهندگان IoT، اپراتورهای پلتفرم، صنعت، تولید کنندگان

•دسـتیابی بـه اجمـاع نظـر بـرای قابلیـت همـکاری در کل اکوسیسـتم اینترنـت اشـیا

برای صنعت IoT، ارائه دهندگان، تولید کنندگان، انجمن‌ها، رگولاتورها

• **ایجاد انگیزه‌های اقتصادی و اجرایی برای امنیت IoT**
در نظر گرفته شده برای صنعت IoT، انجمن‌ها، آکادمی‌ها، گروه‌های مصرف کننده، رگولاتورها
• **ایجاد مدیریت چرخه عمر امن محصول و خدمات اینترنت اشیا**
برای توسعه دهندگان IoT، اپراتورهای پلتفرم، صنعت، تولید کنندگان
• **شفاف سازی مسئولیت بین ذینفعان اینترنت اشیا**
برای صنعت IoT، رگولاتورها

اینترنت اشیا میلیاردها سیستم هوشمند و میلیون‌ها برنامه کاربردی، مشتریان و کسب و کارهای جدید را راهبری می‌کند. رفتارهایی که به دنبال راهکارهای افزایش هوشمندی هستند. پیش بینی می‌شود تا سال ۲۰۲۰ تقریباً ۳ تریلیون دلار در فرصت‌های کسب و کاری جدید برای فروشندگان مختلف و شرکت‌هایی که روی اینترنت اشیا سرمایه گذاری می‌کنند.

نمونه‌هایی از این فرصت‌ها شامل:
• **مدل‌های جدید کسب و کار:** روندهای جدید با ارزش برای مشتریان، با بازدهی سریعتر
• **تنوع بخشیدن به جریان درآمدی:** کسب درآمد از خدمات اضافه شده به خدمات کسب و کارهای سنتی

•**اطلاعات به موقع:** جمع آوری سریع اطلاعات محصولات و فرآیندهای سریعتر، بهبود بازار، چابکی و اجازه تصمیم گیری سریع
• **دید جهانی:** ایجاد ردیابی آسان از یک زنجیره تأمین به دیگری

هدف از این گزارش تشریح توصیه‌های اولیه امنیت سایبری برای IoT با محوریت زیرساخت‌های اطلاعاتی و حیاتی است که شامل امکانات، شبکه‌ها، خدمات وتجهیزات فناوری می‌باشد که این زیرساخت‌ها به دلیل امکان خرابی یا مختل شدن بسیار مهم هستند که میتواند عواقب شدیدی برای سلامتی، ایمنی و رفاه اقتصادی شهروندان به همراه داشته باشد. در این راستا، اقدامات امنیتی اولیه برای IoT در این گزارش ارائه شده است.

یک چالش اساسی در تعیین اقدامات امنیتی پایه برای IoT پیچیدگی ناشی از آن و تنوع در زمینه‌های کاربردی اینترنت اشیاو تعادل بین ویژگی‌های هر دامنه است.
بر این اساس، این گزارش مبتنی بر دانش واطلاعات تخصصی قبلی اتحادیه اروپا است.

تعدادی از صنایع عمودی اینترنت اشیا شامل:
• **خانه‌های هوشمند**
• **شهرهای هوشمند و حمل و نقل عمومی هوشمند**

- **شبکه هوشمند**
- **اتومبیل‌های هوشمند**
- **فرودگاه‌های هوشمند**
- **بیمارستان‌های هوشمند**

این گزارش با هدف بیان انواع مخاطرات اینترنت اشیاء شامل زیرساخت‌های اطلاعاتی حیاتی (CII) و همچنین جزئیات اقدامات امنیتی برای مقابله با تهدیدات شناسایی شده، انجام شده است. همچنین مجموعه ای از توصیه‌ها را برای شکل دادن به تلاش‌ها و ایده‌های آتی آینده و همراستا با یک رویکرد جامع برای تأمین امنیت اینترنت اشیاء ارائه می‌دهد.

ENISA (اتحادیه اروپا) شیوه‌های امنیتی IoT موجود، دستورالعمل‌های امنیتی، استانداردهای مربوط به صنعت را شناسایی و تحلیل کرد. و با بررسی و تحلیل فعالیت‌های موجود و در حال انجام شامل ایده‌های تحقیقاتی در زمینه امنیت IoT برای زیرساخت‌های اطلاعاتی حیاتی (به عنوان مثال صنعت ۴,۰، ارتباطات ماشین به ماشین (M2M)، به روز رسانی IoT) و مقایسه شیوه‌ها و استانداردها، اقدامات امنیتی پایه را توسعه داده است، اقدامات امنیتی که باید توسط ذینفعان مربوطه اعمال شود.

در سال ۲۰۱۷، ENISA گروه کارشناسان امنیت اینترنت اشیا (IoTSEC) را راه اندازی کرد. گروه ENISA IoTSEC یک بستر

تبادل اطلاعات است که متخصصان را برای اطمینان از امنیت اکوسیستم اینترنت اشیا گرآوردی می‌کند. کارشناسان گروه IoTSEC دارای یک یا چند مورد از تخصص‌های زیر هستند.

- **اینترنت اشیا با تمرکز بر امنیت سایبری.**
- **تهیه کنندگان و توسعه دهندگان سخت افزار و نرم افزار اینترنت اشیا با تمرکز بر امنیت سایبری.**
- **انجمن‌ها و سازمان‌های غیر انتفاعی حوزه امنیت اینترنت اشیاء.**
- **نهادهای رگولاتور، آکادمی‌ها، نهادهای استاندارد و سیاست گذاران.**

۱-۱-زمینه سیاست اتحادیه اروپا و بین المللی

در سال‌های گذشته، کمیسیون اروپا تلاش کرده است تا پذیرش IoT را در این کشور تسهیل کند. اروپا با اتخاذ مجموعه ای از اقدامات حمایت از سیاست و راه اندازی یک سری از طرح‌های مربوطه، از پتانسیل‌های خود استفاده می‌کند. در مارس ۲۰۱۵، کمیسیون اروپا، اتحادیه نوآوری اینترنت اشیاء را با هدف ایجاد یک اکوسیستم نوآورانه و صنعتی محور IoT اروپا ایجاد کرد که تا امروز بزرگترین انجمن IoT اروپا شناخته شده است. و همکاری‌هایی با کلیه ذینفعان IoT در بازار رقابتی IoT و مدل‌های کسب و کاری جدید که

بـه نفـع شـهروندان و کسـب و کارهـای اروپایـی اسـت، ایجـاد کـرده اسـت. اسـتراتژیDSM[1]، کـه دو مـاه بعـد آن در مـاه May سـال ۲۰۱۵ تصویـب شـد، تأکیـد می‌کنـد.

از تکـه تکـه شـدن قابلیـت همـکاری اینترنـت اشـیا بـرای دسـتیابی بـه پتانسـیل‌های خـود، جلوگیـری کـرده و اروپـا را از نظـر توسـعه، یـک قـدم جلوتـر بـرده اسـت. از اینترنـت اشـیا بمنظـور پاسـخگویی بـه نیازهـای DSM و آگاهـی از سیاسـت‌های آتـی آن، اسـتفاده می‌شـود کـه کمیسـون اروپـا در April سـال ۲۰۱۶، چشـم انـداز IoT اتحادیـه اروپـا را در سـند «Advancing the Internet of Things in Europe» مشـخص کـرد.

این چشم اندازها بر اساس سه رکن مختلف زیر هستند.

- **پیشرفت اکوسیستم IoT**
- **رویکرد IoT با محوریت انسانی**
- **یک بازار واحد برای اینترنت اشیا**

ایـن کمیسـیون در نقشـه راه خود برای استانداردسـازی فنـاوری اطلاعات و ارتباطـات بـرای اسـتراتژی DSM پنـج اولویـت را مشـخص کـرد. بـه عنـوان مثـال نسـل پنجـم ارتباطـات سـیار سـلولی (5G)، امنیـت سـایبری، رایانـش ابـری و کلان داده یکـی از ۵ اولویت‌هاسـت، اولویـت دیگـر ترویـج

1.Digital Single Market

یک بازار واحد اروپایی برای اینترنت اشیا هست که در در ژانویه سال ۲۰۱۷ « اقتصاد داده اروپا « آغاز شد. این برنامه، خط مشی‌ها و راهکارهای قانونی درباره جریان آزاد داده‌ها در سراسر کشور را ارائه می‌دهد.علاوه بر تمام این ابتکارها، اتحادیه اروپا اهداف ویژه IoT را در برنامه تحقیق و نوآوری، افق ۲۰۲۰ تعیین کرده است. علاوه بر این، کارگروه محافظت از داده‌ها، خطرات اصلی محافظت از داده‌های موجود در اینترنت اشیا را مشخص می‌کند تازه ترین اقدام اتحادیه اروپا در سپتامبر ۲۰۱۷ انجام شد، گواهینامه امنیت سایبری در مورد قانون سایبری فناوری اطلاعات و ارتباطات منتشر شد. که توصیف استراتژی کلی امنیت سایبری اتحادیه اروپا است. هدف آن ایجاد انعطاف پذیری بیشتر اتحادیه اروپا نسبت به حملات سایبری، بهبود شیوه‌های شناسایی و تقویت همکاری‌های بین المللی است که این سند مجموعه ای از اقدامات را ارائه می‌دهد، که برخی از آن‌ها به طور خاص به IoT جهت دهی می‌شوند، مانند تشویق «security by design»[1] که در کل چرخه عمر دستگاه‌هایی که اینترنت اشیا را تشکیل می‌دهند و تولید محصولات با معیارها و پارامترهای این چارچوب صورت بگیرد. پیشرفته ترین روش‌های توسعه امن، که تحت آزمون‌های امنیتی کافی قرار گرفته‌اند و فروشندگان متعهد شده‌اند در صورت بروز آسیب پذیری‌های جدید، نرم افزار خود را به روز کنند. با افزایش تهدیدات، و مهم شدن قانون سال ۲۰۱۷ اتحادیه اروپا

۱. تامین امنیت با طراحی محصول

در بهبود امنیت سایبری در اینترنت اشیا، این قانون در تاریخ اول August سال ۲۰۱۷ توسط چهار سناتور آمریکا معرفی شد. که به یک سری حملات سایبری مربوط به IoT که در سال ۲۰۱۶ رخ داده است پاسخ داده است. که این قانون حداقل الزامات امنیت سایبری برای دستگاه‌های متصل خریداری شده توسط دولت ایالات متحده، را به شرح ذیل اعلام می‌کند.

• فروشندگان را ملزم می‌کند که از امکان وصله‌های امنیتی دستگاه‌های خود اطمینان داشته باشد. و دارای پروتکل‌های استاندارد صنعت باشند، و عدم استفاده ازرمزهای عبور هک شده و بدون آسیب پذیری‌های امنیتی شناخته شده باشند.

• فروشندگان ملزوم به فروش آن دسته از دستگاه‌های اینترنت اشیا هستند که گواهینامه‌هایی ارائه شده ای داشته باشند که در زمان ارائه محصول، از لحاظ سخت افزاری و یا نرم افزاری یا مولفه‌های firmware[1] آن، بدون هر گونه آسیب پذیری و نقص امنیتی شناخته شده باشد. واگر یک فروشنده آسیب پذیری‌ها را شناسایی کند، باید افشا کند و آن‌ها را به موقع وصله امنیتی کند.

• هر یک از نهادهای اجرایی ملزم هستند تا تمامی دستگاه‌های متصل در حال استفاده توسط آژانس امنیت

۱.یک ترکیب سخت افزار و نرم افزاری کامل که نیازمند هیچ رابطی نیست و با استفاده از بخش های نرم افزاری می‌توان بصورت مستقیم و بدون واسطه با بخش های سخت افزاری آن ارتباط برقرار کرد.

سایبری را ثبت کنند.

• همراهی با NIST، و مشخص کردن معیارهای خاص، به عنوان مثال تقسیم بندی شبکه، برای استفاده آژانس‌های امنیت سایبری

• راهبری وزارت امنیت داخلی ایالات متحده آمریکا (DHS) برای مدیریت برنامه‌های حفاظت ملی (NPPD)، تا دستورالعمل‌های توسعه راهکارهای آشکارسازی آسیب پذیری را تهیه کند تا پژوهشگران اجازه کشف آسیب‌پذیری‌ها را داشته باشند. تا آن‌ها را با فروشندگان به اشتراک بگذارند.

• الزام ارائه گزارش موثر، به همراه توصیه‌هایی برای بروز رسانی‌ها، که پس از ۵ سال به کنگره ارسال خواهد شد.

۱-۲-مخاطبان گزارش

این گزارش مجموعه ای از اقدامات خاص امنیتی و پایه ای را ارائه می‌دهد که می‌تواند برای محافظت از سیستم‌ها و محیط‌های اینترنت اشیا مورد استفاده قرار گیرد. مخاطب اصلی گزارش، سازمان‌هایی هستند که میخواهند راهکارهای اینترنت اشیا را بکار گیرند و همچنین تولید کنندگان و اپراتورهای ارائه محصولات،

راهکارهـا و خدمـات IoT. ایـن گـزارش همچنیـن مربـوط بـه مسـئول IT اسـت.

شامل:

- کارشناسان IoT، تولید کنندگان و توسعه دهندگان نرم افزار
- کارشناسان امنیت اطلاعات
- معمارهای راهکارهای امنیت و فناوری اطلاعات
- مدیران ارشد امنیت اطلاعات (CISO)
- کارشناسان حفاظت از زیرساخت اطلاعاتی حیاتی (CIIP)

لازم بـه ذکـر اسـت کـه توصیه‌هـای ایـن گـزارش می‌توانـد بـرای حمایـت از طرح‌هـای ایجـاد خطـی مشـی در رابطـه بـا امنیـت اینترنـت اشـیا مفیـد باشـد و از ایـن رو رگولاتورهـا نیـز جـزو مخاطب‌هـای گـزارش قـرار دارنـد. توصیه‌هـای ایـن گـزارش می‌توانـد بـرای حمایـت از سیاسـت گذاری‌هـا مـورد توجـه و اسـتفاده قـرار بگیـرد و مـوارد مربـوط بـه امنیـت IoT و از ایـن رو بـه رگولاتورهـای مربوطـه نیـز مربـوط می‌شـوند.

۱-۳-متدولوژی

ایـن مطالعـه بـا اسـتفاده ازروش پنـج مرحلـه ای انجـام شـده اسـت کـه در در شـکل زیـر نشـان داده شـده اسـت و بـا تعریـف دامنـه شـروع می‌شـود و بـا جمـع آوری اطلاعـات اولیـه از منابـع رسـمی و کارشناسـان ایـن حـوزه انجـام و بـا تهیـه گـزارش خلاصـه یافته‌هـا و توصیه‌هـا بـه مخاطبـان

پایان می‌یابد.

شکل ۱-۱- متدولوژی استفاده شده دراین مطالعه

۱-۴-ساختار

ادامه گزارش به شرح زیر است:

- **فصل ۱:** معرفی گزارش و تعریف هدف رسیدن به متدولوژی استفاده شده
- **فصل ۲:** تعریف و مستندسازی مولفه‌های کلیدی و محیطی اینترنت ا شیا
- **فصل ۳:** تحلیل تهدیدات اصلی، آسیب پذیری‌ها، مخاطرات و توسعه سناریوهای حمله
- **فصل ۴:** توسعه و دسته بندی معیارهای امنیتی مشخص و قراردادن آن‌ها درحوزه گزارش
- **فصل ۵:** گپ‌ها و چالش‌های آتی که در حوزه پروژه وجود خواهد داشت.
- **فصل ۶:** توصیه‌های امنیتی بر اساس اقدامات امنیتی توسعه یافته و گپ‌ها وچالش‌های مشخص شده در فصل‌های قبلی.

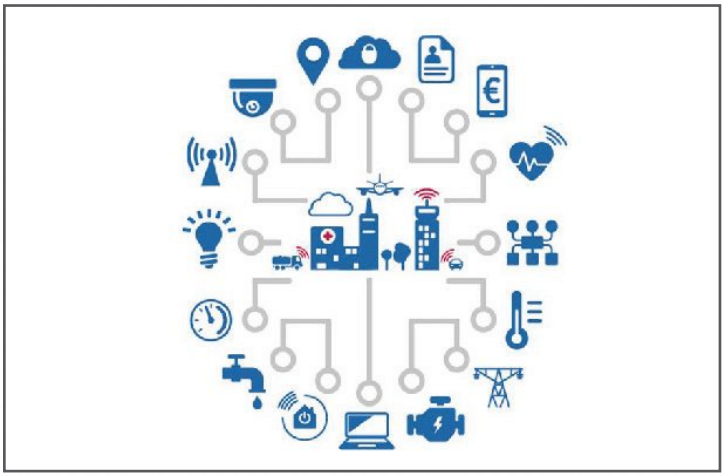
بخش دوم

الگوی IoT

بخش دوم

الگوی IoT

اتحادیه اروپا IoT را به عنوان اکوسیستم سایبر- فیزیکی سنسورها و عملگرهای متصل تعریف می‌کند که توانایی ایجاد تصمیم گیری هوشمندانه را دارد.



شکل ۱-۱- متدولوژی استفاده شده دراین مطالعه

۲-۱-مولفه‌های اینترنت اشیا

۲-۱-۱- چیزها در اینترنت چیزها

در محیط‌های IoT، یک چیز، شیء ایی فیزیکی یا مجازی است که قابل شناسایی و یکپارچه شدن با شبکه‌های ارتباطی باشد.

۲-۱-۲- تصمیم گیری هوشمند

تعداد دستگاه‌های متصل به «سیستم‌های هوشمند» که می‌توانند داده‌ها را ذخیره، پردازش، تحلیل و به اشتراک بگذارند، به شدت رو به افزایش است که باعث می‌شود میلیاردها چیز یا (همان کلمه شیء رایج درایران) و ماشین به شبکه متصل شوند و داده‌های زیادی تولید بشود. از این رو، نیاز است تحلیل داده‌ها و روش‌های مدیریتی داده هوشمند، توسعه یابد. تصمیم گیری هوشمند قبل از هر چیز به اطلاعات موجود برای تصمیم گیری بستگی دارد و این اطلاعات به صورت داخلی قابل تحلیل هستند و برخی از «چیزها» می‌توانند داده‌های جمع آوری شده خود را پردازش کنند یا به مولفه دیگری از اکوسیستم IoT، مانند سرویس زیرساخت ابری، Gateway[1] ها «Thing»[2]دیگری و غیره سپرده شود.

۲-۱-۳- سنسورها و عملگرها

سنسورها یکی از اصلی ترین ساختارهای ایجاد اینترنت

۱.گذرگاه ،دروازه / سیستمی که اتصال میان دو شبکه ارتباطی متفاوت و مجزا به هم را فراهم میسازد.

۲.چیز / Internet Of Things (اینترنت چیزها)

اشـیا هسـتند، زیـرا آن‌هـا یـک مولفـه مکمـل هسـتند کـه امـکان نظـارت محیطـی را می‌دهنـد. آن‌هـا میتواننـد بـه انـدازه میلـی متـر هـم کوچـک باشـند و بـه راحتـی در اشـیا فیزیکـی جـای گیرنـد. در سـطح فیزیکـی، سنسـورها می‌تواننـد شـاخص‌های فیزیکـی، شـیمیایی یـا بیولوژیکـی تعریـف شـده، را انـدازه گیـری و اطلاعـات مربـوط به شـبکه و اپلیکیشـن‌ها را جمع آوری کنند و سـپس داده‌های مرتبط را تولید می‌کنند کـه می‌تـوان آن‌هـا را بـه موقـع پـردازش و یـا بـرای بازیابی‌هـای بعـدی ذخیـره می‌شـود و میتوانـد تـا صدهـا کیلومتـر دورتـر آن را دریافـت کنـد. برخـی از نمونه‌هایـی از سنسـورها، سنسـورهای شـتاب سـنج، سنسـورهای دمـا، حسـگرهای فشـار، سنسـورهای روشـنایی، و ... می‌باشـد.

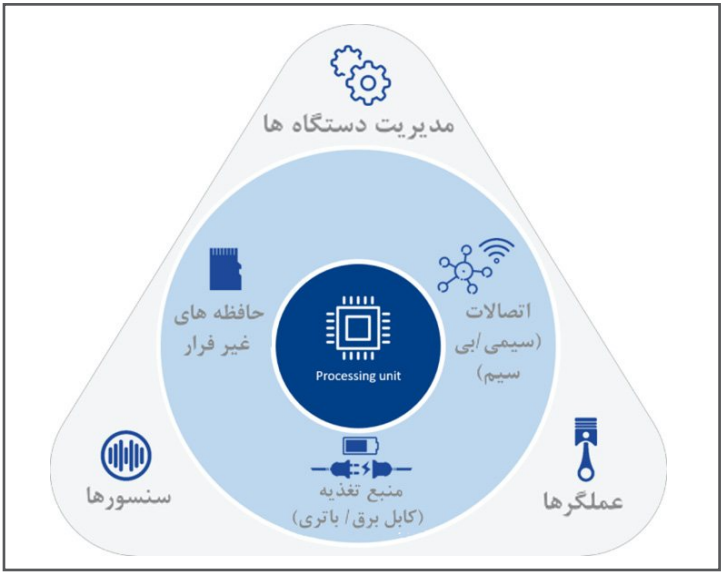
عملگـر را می‌تـوان بعنـوان نهـاد مسـئول بـرای حرکـت یـا کنتـرل سیسـتم در نظـر گرفـت. بـه زبـان سـاده، یـک عملگـر عکـس یـک سنسـور کار می‌کنـد. ورودی الکتریکـی را می‌گیـرد و آن را بـه اقـدام فیزیکـی تبدیـل می‌کنـد. بـا اسـتفاده از نمونـه لامپ‌هـای هوشـمند و ترموسـتات هوشـمند، عملگرهـای آن‌هـا می‌تواننـد بـرای تنظیـم روشـنایی و سـیگنال ناشـی از یـک سـیگنال نـور، از یـک سنسـور نـور اسـتفاده کننـد. سنسـور دمـا نیـز بـرای تنظیـم دمـا، بـه همیـن ترتیـب از عملگرهـای رایـج اسـتفاده می‌کند.

۲-۱-۴- سیستم‌های Embedded[1]

سنسـورها و عملگرهـا مولفه‌هـای اساسـی IoT هسـتند. آن‌هـا ممکـن

۱.سـامانه‌های نهفتـه/ شـامل سـاختار هـای دیجیتـال هسـتند کـه اجـزای بسـیار گوناگونـی شـامل انـواع نـرم افزار،سـخت افـزار و سیسـتم عامـل در آن هـا جاسـازی شـده اسـت.

است به زیرساخت‌های ابری متصل شوند و از طریق Gateway داده‌های جمع آوری شده از سنسورها، پردازش می‌شوند. دستگاه‌های IoT که تن‌ها دارای شبکه‌های حسگر و عملگرها هستند، می‌توانند به عنوان سیستم‌های Embedded نیز شناخته شوند.



شکل ۲-۱- ساختار یک IoT embedded system

۲-۱-۵- ارتباطات

نیازهای ارتباطی بسته به نوع آنها، در بین انواع مختلف شبکه IoT بسیار متفاوت است پروتکل‌های مورد استفاده درتوسعه

IoT محدود به انتخاب و بسته به نوع استفاده است. ترکیب پروتکل‌های مختلف در IoT یک روش متداول است که برای اطمینان از قابلیت همکاری از Gateway استفاده می‌کند.

SESSION		AMQP, CoAP, DDS, MQTT, XMPP
NETWORK	ENCAPSULATION	6LowPAN, Thread
	ROUTING	CARP, RPL
DATALINK		Bluetooth / BLE, Wi-Fi / Wi-Fi HaLow, LoRaWAN, Neul, SigFox, Z-Wave, ZigBee, USB

۲-۲-ملاحظات امنیتی

زندگی ما همواره وابسته به دستگاه‌های هوشمند و متصل است، و این مساله میتواند حریم خصوصی افراد را به خطر بیاندازد و امنیت عمومی را تهدید کند. بنابراین امنیت یکی از نگرانی‌های اصلی مربوط به اینترنت اشیا است که باید الزامات آن در کنار الزامات ایمنی مورد توجه قرار بگیرد. زیرا هر دو موضوع کاملا جدی هستند. موضوع مهم دیگر با توجه به ناهمگونی و پیچیدگی‌های ذاتی اکوسیستم اینترنت اشیا و همچنین دغدغه‌های عدم مقیاس پذیری، نقش حاکمیت اینترنت اشیا است.

موارد زیر موضوعاتی است که مانع ادغام امنیت و اکوسیستم اینترنت اشیا می‌شود.

حمله‌هایی در سطح گسترده: تهدیدات و مخاطرات مربوط به اینترنت

اشیا بسیار زیاد و در حال گسترش است. و با توجه به تاثیری که بر سلامت، ایمنی و حریم خصوصی شهروندان دارد و با توجه به رویکرد اینترنت اشیا که بر اساس جمع آوری، ارسال و پردازش داده‌های مختلف از منابع مختلف از جمله داده‌های حساس است، دورنمایی از گسترش تهدیدهای مربوط به اینترنت اشیا را می‌دهد.

منابع محدود دستگاه: بکارگیری شیوه‌های امنیتی رایج در اینترنت اشیا به دلیل محدودیت‌های فنی دستگاه‌ها، شامل حافظه، پردازشگر و باتری مصرفی، نیاز به مهندسی‌های دوباره دارد، به همین جهت کنترل‌های پیشرفته امنیتی نمیتوانند کاملا آن‌ها را پوشش دهند.

اکوسیستم پیچیده: اینترنت اشیا مجموعه ای از دستگاه‌های مستقل نیست، بلکه یک اکوسیستم غنی، متنوع و گسترده از دستگاه‌ها، ارتباطات و رابطها (Interfaces ها) و افراد تشکیل شده است، که نگرانی امنیتی را تشدید می‌کند .

تدوین استانداردها و مقررات: تدوین و پذیرش استانداردها و مقررات برای تصمیم گیری‌ها، تدابیر و بهترین تجربه‌های امنیتی برای اینترنت اشیا، به کندی و در حالی صورت میگیرد که روند فناوری‌های نو ظهور ادامه دارند و این موضوع نگرانی‌های مربوطه را پیچیده‌تر می‌کند.

توسعه گسترده: بجز کاربردهای تجاری اینترنت اشیا، در روندهای اخیر مشاهده شده است که افراد شروع به هوشمند کردن زیرساخت‌های حیاتی (CIs) با بکارگیری اینترنت اشیا بر روی زیرساخت سنتی، کرده‌اند.

یکپارچگی امنیت: دیدگاه‌ها و نظرات متفاوت و مختلف از طرف ذینفعان، یکپارچگی امنیت را سخت و دچار چالش کرده است. مثلا برای هر دستگاه یا سیستم اینترنت اشیا راهکارهای متفاوتی برای احراز هویت وجود دارد که لازم است یکپارچه باشد.

جنبه‌های ایمنی: به دلیل وجود عملگرها در دنیای فیزیکی، تهدیدات امنیتی میتواند منجر به تهدیدات ایمنی شود، به عنوان مثال، حملات اخیر به خودروهای متصل باعث تهدیدهای ایمنی می‌شود.

هزینه کم: با گسترش نفوذ اینترنت اشیا و عملکردهای پیشرفته ای که در چندین بخش حیاتی ارائه شد، با بهره گیری از ویژگی‌هایی مانند جریان داده‌ها، نظارت پیشرفته و یکپارچه سازی، پتانسیل صرفه جویی زیادی را در هزینه نشان می‌دهد. برعکس، اغلب این مورد اتفاق می‌افتد که دستگاه‌ها و سیستم‌های IoT معمولا با کاهش هزینه در ارتباط است که از لحاظ امنیتی پیامدهایی خواهد داشت. تولید کنندگان ممکن است برای

اطمینـــان از کاهـــش هزینه‌هـــا ترجیـــح دهنـــد کـــه ویژگی‌هـــای امنیتـــی را محـــدود کننـــد، بنابرایـــن ممکـــن اســـت امنیـــت محصـــول قـــادر بـــه محافظـــت در در برابـــر انـــواع خاصـــی از حمـــلات اینترنـــت اشـــیا نباشـــد.

فقـــدان تخصص: این یک حوزه نسـبتا جدید اسـت و بنابراین فقـدان افراد با توانایی و تخصص مناسـب درزمینه امنیت سـایبری اینترنت اشـیا وجود دارد.

بـــروز رســـانی‌های امنیتـــی: اعمـــال بـــروز رســـانی‌های امنیتـــی در اینترنـــت اشـــیا چالش‌هـــای زیـــادی دارد، چـــرا کـــه خصوصیـــات رابط‌هـــای کاربـــری قابـــل دســـترس کاربـــران، اجـــازه روش‌هـــای متـــداول بروزرســـانی ســـنتی را نمی‌دهـــد. تامیـــن امنیـــت ایـــن روش‌هـــا و تضمیـــن امـــن بـــودن ایـــن بروزرســـانی‌ها دارای ریســـک اســـت. بـــه ویـــژه در بـــروز رســـانی‌های OTA[1]

برنامه‌نویســـی ناامـــن: از آنجایـــی کـــه فشـــارهای «time to market» (زمـــان کوتـــاه ورود بـــه بـــازار) بـــرای محصـــولات اینترنـــت اشـــیا بیشـــتر از ســـایر مـــوارد اســـت، ایـــن موضـــوع محدودیت‌هایـــی جهـــت تـــلاش بـــرای توســـعه امنیـــت و حریـــم خصوصـــی را در طراحـــی محصـــول ایجـــاد می‌کنـــد. بـــه همیـــن دلیـــل، و گاهـــی بـــه دلیـــل مســـائل مربـــوط بـــه بودجـــه، شـــرکت‌ها و توســـعه دهنـــدگان محصـــولاتIoT ، بیشـــتر روی عملکـــرد و قابلیت‌هـــای اســـتفاده از محصـــول تاکیـــد دارنـــد تـــا الزامـــات امنیتـــی آن.

1. Over-the-air

تعهـدات نامشـخص: بـه دلیـل عـدم شـفافیت تعهـدات، در صـورت بـروز یـک حادثـه امنیتـی در یـک مقیـاس بـزرگ، مشـکلات و ابهاماتـی پیـش می‌آیـد عـلاوه بـر ایـن مسـئله چگونگـی مدیریـت امنیـت اسـت و بـه ایـن سـوال هنـوز پاسـخی داده نشـده اسـت. کـه وقتـی یـک بخـش، زیـر نظـر چنـد ذینفـع اسـت چگونـه می‌تـوان امنیـت را تامیـن کـرد یـا در بیـن ایـن ذینفعـان مسـئولیت بـا کـدام اسـت. کـه اجبـاری کـردن مسـئولیت یـک مسـئله مهـم دیگـر اسـت.

۲-۳-چالـــش تعییـــن معیارهـــای امنیتـــی پایـــه در صنعـــت افقـــی

اکثـر کارشناسـان در مـورد پیچیدگـی مطالعـه امنیـت IoT از طریـق یـک صنعـت افقـی، بـه دلیـل اقدامـات امنیتـی و تاثیـر تهدیـدات تعییـن شـده بـا آن‌هـا موافقـت کردنـد. بـا توجـه بـه اهمیـت دارایی‌هـای مختلـف، کـه بسـته بـه مـورد اسـتفاده، کاربـرد و سـناریوی مـورد اسـتفاده متفـاوت اسـت.

بـرای هـر محیـط IoT لازم اسـت کـه یـک ارزیابـی ریسـک انجـام شـود تـا از طریـق تهدیدهایـی کـه می‌توانـد بـر دارایی‌هـای مختلـف تاثیـر بگـذارد، سـناریوهای احتمالـی حملـه را در خدمـات اینترنـت اشـیا تعریـف کنـد، و آن‌هـا را در خدمـات اینترنـت اشـیا تعریـف کنـد، و از ایـن طریـق مشـخص کنـد کـه کـدام مخاطـرات حیاتـی هسـتند و یـا کدامیـک را میتـوان بـی اهمیـت عنـوان کـرد، اثـر کدامیـک را میتـوان کاهـش داد. پیچیدگـی مربـوط بـه صنعـت افقـی بـه ایـن دلیـل اسـت کـه بجـای پرداختـن بـه یـک صنعـت عمـودی اینترنـت اشـیا ماننـد ماشـین‌های هوشـمند، فرودگاه‌هـای هوشـمند، خانه‌هـای هوشـمند، حمـل و نقـل

عمومی هوشمند،ICS / SCADA [1] و غیره. استفاده می‌شود. با این وجود، این گزارش جنبه‌های صنعت افقی اینترنت اشیا را همانطور که در بخش‌های صنعت عمودی دیده می‌شود، در نظر می‌گیرد و بنابراین هدف از آن برآورده کردن نیاز اولویت دار تعریف معیارهای امنیت پایه اینترنت اشیا در برابر زیرساخت‌های اطلاعاتی حیاتی است. در این رابطه، این گزارش تلاش‌های قبلی ذکر شده در بخش‌های عمودی را تکمیل کرده و در نتیجه یک رویکرد جامع نسبت به امنیت IoT را ترویج می‌کند.

۲-۴-معماری

راهکارهای اینترنت اشیا روی اپلیکیشن‌های خاص متمرکز شده که فاقد استاندارسازی است و باعث معماری پراکنده و ناهمگن می‌شود، اتحادیه اروپا چند معماری موجود اینترنت اشیا را بررسی کرده و بر اساس آن یک معماری ارائه داده است تا با مولفه‌های اصلی معماری، قابلیت‌های همکاری را در بین دارایی‌های مختلف و محیط پلتفرمی و ...افزایش یابد تا شاید گامی در جهت ایجاد یک معماری مشترک برای اینترنت اشیا شود، مواردی که بررسی کرده است، عبارتند از:

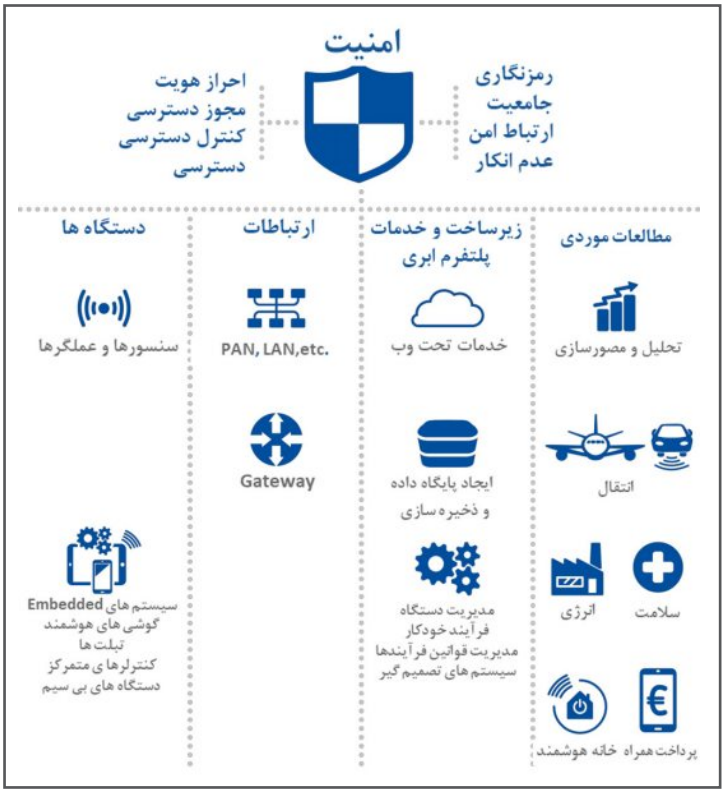
- AIOTI High Level Architecture functional model[2]
- FP-7ICT – IoT-A Architectural reference model[3]
- NIST Network of Things (NoT)[4]
- ITU-T IoT reference model[5]
- ISO/IEC CD 30141 Internet of Things Reference Architecture (IoT RA)[6]

1.Industrial control systems (ICS) /Supervisory Control and Data Acquisition (SCADA)/ https://www.enisa.europa.eu/publications/ics-scada-dependencies
2.https://aioti-space.org/wp-content/uploads/03/2017/AIOTI-WG-3IoT-High-Level-Architecture-Release_1_2.pdf
3.http://www.meet-iot.eu/deliverables-IOTA/D5_1.pdf
4.http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.183-800.pdf
5.https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures
6.https://www.w3.org/WoT/IG/wiki/images/9/9a/10N0536_CD_text_of_ISO_IEC_30141.pdf

•ISACA Conceptual IoT Architecture[7]

•oneM2M Architecture Model[8]

•IEEE P2413 - Standard for an Architectural Framework[9]



شکل ۱- ۲- مدل مرجع و سطح بالا اینترنت اشیا

7.https://www.isaca.org/Journal/archives/2017/Volume3-/Pages/default.aspx
8.http://www.onem2m.org/images/files/deliverables/Release2/TS20%-0001-Functional_Architecture-V0_10_2.pdf
9.https://standards.ieee.org/develop/project/2413.html

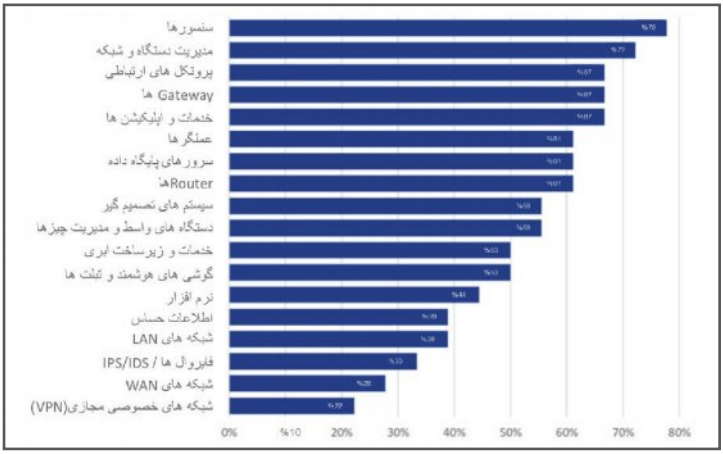
۲-۵-دسته بندی دارایی

گروه دارایی	دارایی ها	توضیحات
دستگاه های اینترنت اشیا	سخت افزار	اجزای مختلف فیزیکی (بجز سنسورها و عملگر ها) که دستگاه های IoT در آنها ساخته می شود. این ها شامل میکروکنترلرها ، ریزپردازنده ها ، درگاه های فیزیکی دستگاه ، Motherboard و غیره است.
	نرم افزار	این نرم افزار شامل سیستم عامل دستگاه IoT ، frimware آن و برنامه ها و اپلیکیشن نصب شده یا در حال اجرا است.
	سنسورها	این زیر سیستمهایی هستند که هدف آنها شناسایی و یا اندازه گیری وقایع و رخداد ها در محیط آن و ارسال اطلاعات به سایر دستگاه های الکترونیکی جهت پردازش است. سنسورهای زیادی برای اهداف متفاوت وجود دارد ، مانند سنسوراندازه گیری دما ، سنسور حرکت و غیره.
	عملگرها	واحد های خروجی دستگاه IoT هستند که تصمیمات را بر اساس اطلاعات قبلی پردازش شده، اجرا می کنند.
سایر دستگاه های اکوسیستم IoT	دستگاه های واسط اینترنت اشیا	اینها دستگاه هایی هستند که هدف آنها خدمت به عنوان واسط یا به عنوان جمع کننده بین سایر دستگاه های IoT یک اکوسیستم اینترنت اشیا است. علاوه بر این ، دستگاه هایی که توسط کاربران برای واسطه و تعامل با دستگاه های IoT مورد استفاده قرار می گیرد.
	دستگاه های مدیریت چیزها	اینها دستگاه هایی هستند که بطور خاص برای مدیریت سایر دستگاه های IoT ، شبکه ها و غیره طراحی شده اند.

	سیستم های Embedded	آنها در یک واحد پردازش قرار دارند که به آنها امکان می دهد داده ها را به تنهایی پردازش کنند. آنها شامل سنسورهای تعبیه شده و یا عملگرها ، قابلیت های شبکه برای اتصال مستقیم به ابر ، جمع آوری اطلاعات حافظه و امکان اجرای نرم افزار هستند.
ارتباطات	شبکه ها	آنها به نودهای مختلف اکوسیستم IoT اجازه می دهند تا داده ها و اطلاعات را با یکدیگر از طریق یک Data link تبادل کنند. شبکه های مختلفی با توجه به پوشش مکانی آنها وجود دارد که از جمله آنها می توان به LAN (W)، PAN (W) ها ، PAN ها و WAN (W) ها اشاره کرد.
	پروتکل ها	مجموعه ای از قوانین را در مورد چگونگی ارتباط بین دو یا چند دستگاه IoT از طریق یک کانال معین تعریف می کنند. پروتکل های ارتباطی زیادی وجود دارد ، که می تواند بی سیم یا سیمی باشد. نمونه هایی از پروتکل های ارتباطی IoT عبارتند از: ZigBee، MQTT، CoAP، BLE و غیره.
زیرساخت	Router ها	مؤلفه های شبکه هستند که بسته های داده را بین شبکه های مختلف اکوسیستم IoT هدایت می کنند.
	Gateway ها	Node های شبکه ای هستند که برای ارتباط با شبکه دیگری از محیط IoT استفاده می شوند که از پروتکل های مختلفی استفاده می کنند. Gateway ممکن است ترجمه پروتکل، ایزوله کردن و غیره را فراهم کند تا قابلیت همکاری سیستم را فراهم کند.

	منبع تغذیه	انرژی الکتریکی را به یک دستگاه IoT و به اجزای داخلی آن تأمین می کند. منبع تغذیه می تواند اکسترنال و سیمی باشد و یا به بصورت باتری درون خود دستگاه باشد.
	دارایی ها امنیت	این گروه شامل دارایی هایی است که به طور خاص روی امنیت دستگاه ها ، شبکه ها و اطلاعات IoT متمرکز شده اند. برجسته ترین اینها شامل فایروال ها ، فایروال های تحت وب (WAF)، CASB ها برای محافظت از ابر ، IDS ها ، IPS ها و سیستم های احراز هویت با مجوز دسترسی است.
بسترها و پلتفرم	خدمات تحت وب	اینها خدماتی در شبکه جهانی وب هستند که رابط مبتنی بر وب را برای کاربران وب یا برنامه های متصل به وب فراهم می کنند. این بدان معنی است که فناوری های وب می توانند در IoT برای ارتباطات انسان به ماشین (H۲M) و ارتباطات M۲M استفاده شوند.
	خدمات و زیرساخت های ابری	در IoT می توان از بسترهای ابری برای جمع آوری و پردازش داده های دستگاههای پراکنده استفاده کرد و همچنین قابلیت پردازشی ، ذخیره سازی ، اپلیکیشن ها ، خدمات و غیره را نیز فراهم می کند.
سیستم های تصمیم گیر	داده کاوی	به الگوریتم ها و خدمات مربوط به پردازش داده های جمع آوری شده و تبدیل آن به یک ساختار تعریف شده برای استفاده بیشتر ، با استفاده از فناوری های کلان داده برای کشف الگوهای موجود در data sets های مقیاس بزرگ اشاره دارد.

	پردازش داده ها و خدمات پردازشی	خدمات ابزارهای پردازش داده های جمع آوری شده بمنظور به دست آوردن اطلاعات مفید ، که می تواند برای اعمال قوانین، تصمیم گیری ها و خودکار سازی فرایندها استفاده شود. برای یادگیری استفاده از اطلاعات موجود در طول زمان می توان از یادگیری ماشین استفاده کرد.
خدمات و اپلیکیشن ها	تحلیل داده و مصورسازی	پس از جمع آوری و پردازش داده ها ، بمنظور شناسایی الگوهای جدید ، بهبود کارایی عملیاتی و غیره میتوان اطلاعات حاصل را تحلیل کرد.
	مدیریت دستگاه و شبکه	مدیریت دستگاه ها و شبکه های اکوسیستم IoT شامل بروزرسانی های نرم افزاری سیستم عامل ، سیستم عامل و اپلیکیشن ها است. یادگیری ماشین می‌تواند برای یادگیری از اطلاعات بدست آمده در طول زمان استفاده کند.
	میزان مصرف دستگاه ها	زمینه سازی دستگاه ها و شبکه های اکوسیستم IoT ، به منظور درک وضعیت فعلی، الگوهای استفاده، عملکرد و غیره.
اطلاعات	حالت rest	اطلاعات ذخیره شده در یک پایگاه داده در بسترهای ابری یا در خود دستگاه ها.
	هنگام انتقال	اطلاعات ارسال شده از طریق شبکه بین دو یا چند مولفه اینترنت اشیا تبادل میشود.
	هنگام استفاده	اطلاعاتی که بطور کلی توسط یک برنامه ، سرویس یا مولفه اینترنت اشیا مورد استفاده قرار می گیرد.



شکل ۲-۲- میزان حیاتی بودن دارایی

بخش سوم

تهدیدات وتحلیل ریسک

بخش سوم

تهدیدات و تحلیل ریسک

هدف اصلی این فصل تعیین و لیست تهدیدات اصلی امنیتی، آسیب پذیری، و مخاطرات است. عوامل و سناریوهای حمله ای که بر روی دستگاه‌ها و شبکه‌های IoT تأثیر می‌گذارد و اهمیت آن را درسطوح مختلفی بیان می‌کند. سه سناریوی حیاتی حمله، به همراه جزئیات و پیچیدگی‌ها به همراه توصیه‌های امنیتی برای مقابله با تأثیرات و عوارض جانبی آن‌ها بیان شده است.

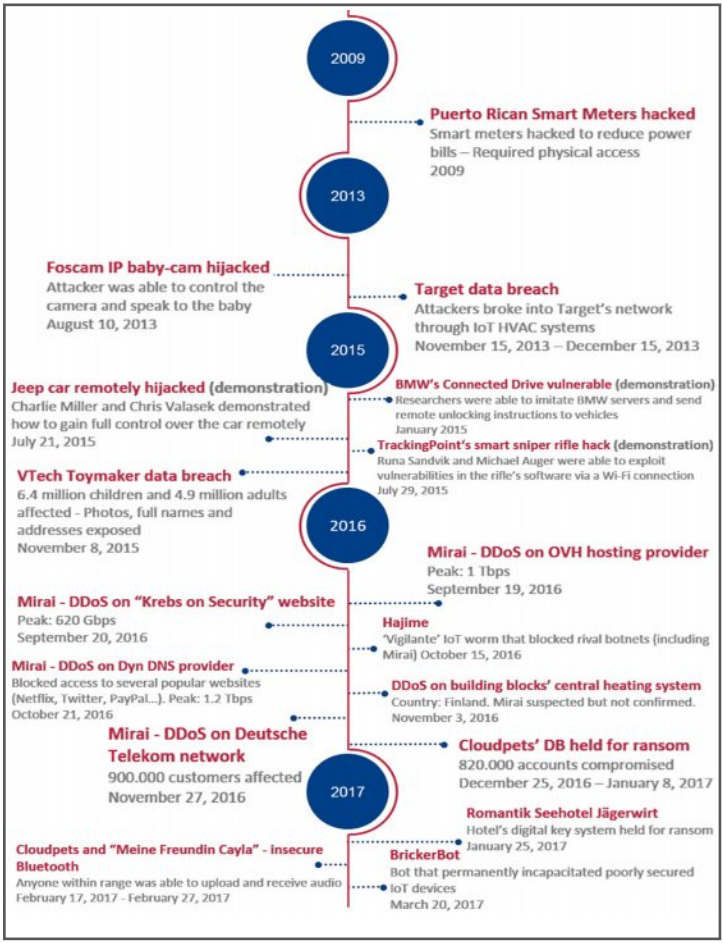
۳-۱-حوادث امنیتی

در سال‌های گذشته، کمیسیون اروپا تلاش کرده است تا پذیرش IoT را در این کشور تسهیل کند اروپا و با اتخاذ مجموعه ای از اقدامات حمایت از سیاست و راه اندازی یک سری از طرح‌های مربوطه، از پتانسیل‌های خود استفاده می‌کند. در مارس ۲۰۱۵، کمیسیون اروپا اتحاد نوآوری اینترنت اشیاء را با هدف ایجاد یک اکوسیستم نوآورانه و صنعتی محور IoT اروپا ایجاد کرد که تا امروز

بزرگترین انجمن IoT اروپا شناخته شده است. و همکاری‌هایی با کلیه ذینفعان IoT در بازار رقابتی IoT و مدل‌های کسب و کاری جدید که به نفع شهروندان و مشاغل اروپایی است، ایجاد کرده است. و دو ماه بعد از آن در ماه May سال ۲۰۱۵ میلادی استراتژی DSM[1]«Digital Single Market»، تصویب شد.

تعداد تهدیدات امنیتی که دستگاه‌های IoT را هدف قرار داده، طی سال‌های گذشته افزایش یافته است شکل زیر نشانگر برخی از حوادث اصلی امنیت IoT که از سال ۲۰۰۹ کشف و یا اتفاق افتاده اند، می‌باشد. و نشان می‌دهد که چگونه تعداد حملات به IoT افزایش یافته است. لازم به ذکر است که این لیست جامع نیست و فقط نمونه‌های اصلی را شامل می‌شود.

1.https://ec.europa.eu/commission/priorities/digital-single-market/



شکل ۱-۳- نمودار زمانی حوادث امنیتی اینترنت اشیا

۳-۲-دسته بندی تهدید

همانطور که در بخش قبلی مشاهده شد، تعداد حملات مستقیم با IoT اخیرا افزایش یافته است و در سال ۲۰۱۶ حمله ای تحت عنوان بات نت Mirai مطرح شد.

در جدول ۳، تهدیدهای طبقه بندی شده و دارایی‌های تحت تأثیر آن‌ها بطور خلاصه شرح داده شده است.

۳-۳-نمونه‌هایی از سناریوهای حمله امنیت سایبری اینترنت اشیا

نمونه‌هایی از سناریوهای حمله سایبری به اینترنت اشیا تهدیدها و ریسک‌هایی که پیش از این در بخش ۳.۲ ذکر شده‌اند را میتوان توسط مهاجمان برای تاثیر cascade و آسیب‌های بیشتر در زیر ساخت‌های مختلف مورد استفاده قرار داد. سناریوهای حمله مختلف و سطح اهمیت هر حمله از تحقیقات و مطالعات موردی و همچنین اطلاعات ارائه‌شده توسط متخصصانی که در این گزارش نقش داشتند، جمع‌آوری شده‌است.

شایان‌ذکر است که حملات ممکن است در کل فرآیند رخ دهند و

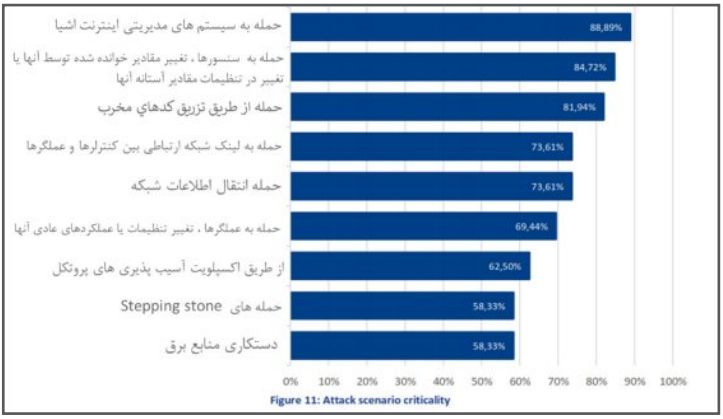
تاثیراتی که ممکن است در هر بخش خاص از فرآیند داشته باشد مورد تحلیل قرار گرفته‌است.

سناریوهای حمله	سطح اهمیت
۱. حمله به لینک شبکه ارتباطی بین کنترلرها و عملگرها	بالا– حیاتی
۲. حمله به سنسورها ، تغییر مقادیر خوانده شده توسط آنها یا تغییر در تنظیمات مقادیر آستانه آنها	بالا– حیاتی
۳. حمله به عملگرها ، تغییر تنظیمات یا عملکردهای عادی آنها	بالا– حیاتی
٤. حمله به سیستم های مدیریتی اینترنت اشیا	بالا– حیاتی
٥. از طریق اکسپلویت آسیب پذیری های پروتکل	بالا
٦. تزریق کدهای مخرب به داشبورد سیستم ها	بالا– حیاتی
۷. حمله های Stepping stone	متوسط رو به بالا
۸. DDoS با استفاده از بات نت های اینترنت اشیا	حیاتی
۹. دستکاری منابع برق و بهره برداری از آسیب پذیری های خواندن	متوسط رو به بالا
۱۰. باج افزار	متوسط رو به حیاتی

برای این سناریوها، بازخورد مرتبط دیگری در زمینه این گزارش دریافت شده است شامل شرح مختصری از حمله و تاثیرهای بالقوه تهدیدات در نسخه کامل این گزارش مطرح شده است.

۳-۴-سناریوهای حمله حیاتی

در طی مصاحبه با کارشناسان و ذینفعان ذیربط، سناریوهای حمله یادشده در مورد محیط IoT که شرح آن داده شد و به تفصیل توضیح داده شد. از کارشناسان خواسته شد تا ۱۰ نمونه سناریو را رتبه بندی کنند .



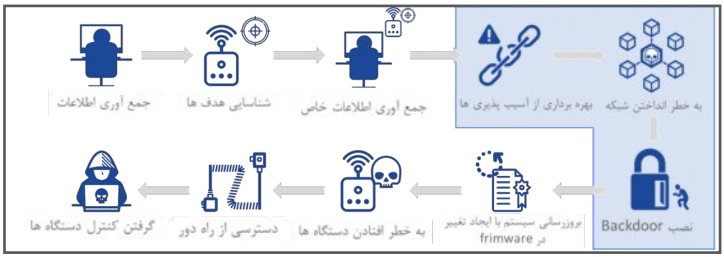
شکل ۳-۲- حیاتی بودن سناریو حمله

سه سناریوی حمله حیاتی:

- سناریوی حمله ۱: حمله به سیستم های مدیریتی IoT
- سناریوی حمله ۲: دستکاری مقادیر در دستگاه‌های IoT
- سناریوی حمله ۳: بات نت و تزریق کد مخرب

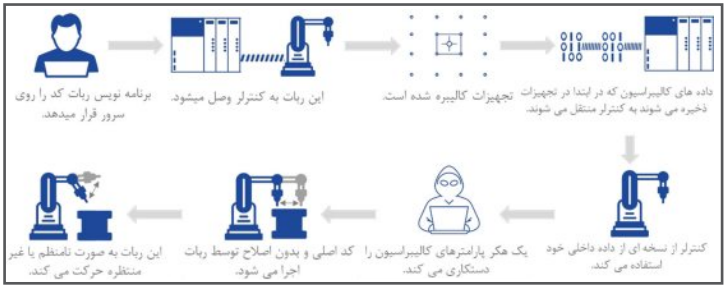
در بخش‌های بعدی نسخه کامل فایل به توضیح هر یک از این سناریوها از جمله تاثیر آنها، ذینفعان، ریسک‌ها و اقدامات متقابل برای محافظت در برابر آن‌ها و سایر مشخصات فنی اشاره شده است.

۳-۴-۱- سناریوی حمله ۱: حمله به سیستم های مدیریتی IoT



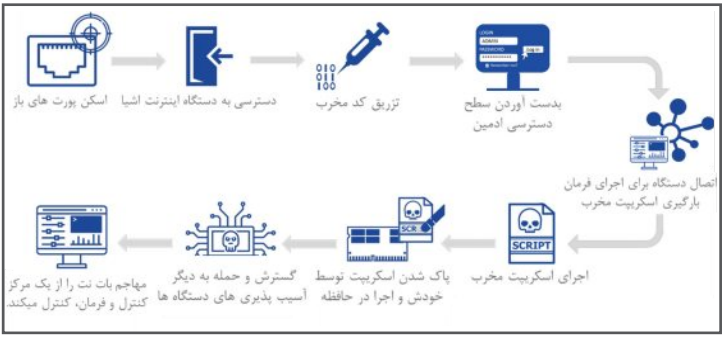
شکل ۳-۳- به خطر افتادن سیستم های مدیریتی اینترنت اشیا

۳-۴-۲- سناریوی حمله ۲: دستکاری مقادیر در دستگاههای IoT



شکل۴-۳- دستکاری مقادیر در دستگاه های اینترنت اشیا

۳-۴-۳-سناریوی حمله ۳: بات نت و تزریق کد مخرب



شکل ۵-۳- بات نت و تزریق کد مخرب

بخش چهارم

معیارهای امنیتی و تجربه ها

بخش چهارم

معیارهای امنیتی و تجربه ها

در فصل چهارم لیست مفصلی از اقدامات امنیتی و تجربه‌ها ارائه شده است، که هدف آن‌ها کاهش تهدیدات، آسیب پذیری‌ها و مخاطرات یاد شده است که بر دستگاه‌ها و محیط‌های اینترنت اشیا تأثیر می‌گذارد. این اقدامات امنیتی و تجربه‌ها با هدف اعمال در سطوح مختلف اینترنت اشیا تعریف شده است. به جای تامین امنیت صنایع عمودی اینترنت اشیا، برای توسعه آن در صنایع افقی تعریف شده است. بنابراین، اقدامات امنیتی تعریف شده طیف گسترده ای از ملاحظات امنیتی، مانند امنیت طراحی، محافظت از داده‌ها، تحلیل ریسک و غیره مجموعه اقدامات امنیتی و تجربه‌ها در این گزارش بر اساس موارد زیادی تعیین شده است شامل تحقیقات و مطالعات موردی، که دستورالعمل‌های مختلف امنیتی، استانداردها و غیره را در نظر گرفته است. لیستی از این منابع را می‌توانید در پیوست گزارش نسخه اصلی تحت عنوان (Security standards and references reviewed) پیدا کنید.

اقدامات امنیتی مختلف و تجربه های خوبی (و نه بهترین تجربه ها) مشخص شده که در چند حوزه امنیتی در این گزارش ارائه شده است. هدف، پوشش دهی هر محیط IoT به صورت صنعت افقی است، تا طبقه بندی و تعریف بنحوی باشد که اقدامات امنیتی برای کدام سطح اکوسیستم IoT اعمال شود. حوزه‌های امنیتی پیشنهادی به شرح زیر تعریف شدند:

• مدیریت امنیت سیستم مدیریت و مدیریت ریسک: شامل اقدامات امنیتی در مورد تحلیل ریسک امنیتی سیستم اطلاعاتی، خط مشی، اعتباربخشی، شاخص‌ها و ممیزی، و منابع انسانی امنیت.

• مدیریت اکوسیستم: شامل معیارها و اقدامات امنیتی و نگاشت آن‌ها در اکوسیستم و ارتباط آن‌ها

• معماری امنیت فناوری اطلاعات: شامل اقدامات امنیتی در رابطه با پیکربندی سیستم‌ها، مدیریت دارایی، تفکیک سیستم، فیلتر کردن ترافیک و رمزنگاری.

• مدیریت امنیت فناوری اطلاعات: شامل اقدامات امنیتی در مورد حساب‌های مدیریتی و سیستم‌های اطلاعاتی دولت.

• شناسایی و مدیریت دسترسی: شامل اقدامات امنیتی در مورد احراز هویت، شناسایی و حق دسترسی

• پشتیبانی امنیت فناوری اطلاعات: شامل اقدامات امنیتی در مورد روش‌های پشتیبانی و نگهداری و دسترسی از راه دور

• امنیت فیزیکی و محیطی

• آشکارسازی: شامل اقدامات امنیتی در مورد کشف، لاگین و تحلیل log ها می‌باشد.

• مدیریت حوادث امنیت رایانه ای: شامل اقدامات امنیتی در مورد سیستم اطلاعات و تحلیل و رویارویی با حوادث امنیتی و اقدام مناسب و گزارش حادثه.

• استمرار عملیات: شامل اقدامات امنیتی در مورد مدیریت استمرار کسب و کار و مدیریت بازیابی از فاجعه

• مدیریت بحران: شامل اقدامات امنیتی آن سازمان و فرآیند مدیریت بحران می‌باشد.

این حوزه‌های امنیتی هنگام تدوین اقدامات مختلف امنیتی و تجربیات مورد توجه قرار گرفته است. روش‌هایی برای IoT، را میتوانید در بخش ۱-۴ تا ۳-۴ نسخه کامل گزارش مشاهده کنید. شرح دقیق هر یک از معیارهای امنیتی و اقدام مناسب آن و حوزه امنیتی آن، به همراه اسناد و منابع موجود است.

همانطور که قبلاً ذکر شد، این حوزه‌های امنیتی، معیارهای امنیتی را بر اساس صنعت افقی و سطوح اکوسیستم IoT طبقه بندی می‌کنند و در اکوسیستم آن مورد استفاده قرار می‌گیرند. جدا از حوزه کاربرد آنها، هر اقدام امنیتی می‌تواند با توجه به ماهیت آن انجام شود.

این اقدامات می‌توانند خط مشی هایی باشند که هنگام توسعه دستگاه باید در نظر گرفته شوند، اقدامات سازمانی نیز با تمرکز بر کسب و کارها و کارکنان سازمان خود مورد نیاز است و در آخر، معیارهای فنی با هدف کاهش مخاطرات احتمالی دستگاه‌های IoTو سایر مولفه های اکوسیستم IoT ممکن است مورد استفاده قرار گیرند. بر این اساس، معیارهای امنیتی پایه IoT شناسایی و مشخص شده است. که از این پس به عنوان تجربه های خوب GP :(Good Practice)در سه دسته اصلی ذکر شده است.

- **خط مشی‌ها (PS)**
- **معیارهای سازمانی، معیارهای فرآیندی و مردم (OP)**
- **معیارهای فنی (TM)**

۴-۱-خط مشی ها

اولین مجموعه از اقدامات امنیتی به سیاست‌ها و خط مشی هایی اشاره دارد که به صورت کلی امنیت اطلاعات را هدف قرار می‌دهند و هدفشان ایجاد ثبات و استحکام بیشتر است. که باید برای فعالیت‌های سازمان کافی و حاوی اطلاعات مستند باشد. در این زمینه، اقدامات امنیتی و تجربیات زیر تعریف شده‌اند.

لازم به ذکر است که با اشاره به معیارهای امنیتی شامل امنیت و حریم خصوصی در هنگام طراحی، لازم است ویژگی‌های خاص در معیارهای امنیتی مورد استفاده قرار گیرد (برای مثال، امنیت در طراحی به خصوصیات متفاوتی هنگام توسعه بستگی دارد به عنوان مثال هنگامی که یک سیستم یا دستگاه اینترنت اشیا در یک محیط خانگی در نظر گرفته می‌شود، در مقایسه با یک دستگاه اینترنت اشیا در یک زیرساخت حیاتی، متفاوت است و با توجه به ریسک سایبری که در سناریوها مطرح شد، لازم است ملاحظات امنیتی در این خصوص در نظر گرفته شود.

۴-۱-۱- امنیت در طراحی و توسعه محصول

• **GP-PS-01** امنیت کل سیستم IoT بایستی رویکردی سازگار و جامع در طول چرخه عمر محصول و در تمامی سطوح طراحی و توسعه دستگاه داشته باشد و برنامه و یکپارچه سازی امنیت در کل ساخت و توسعه آن را درنظر بگیرد.

- **GP-PS-02** امکان یکپارچه سازی خط مشی های امنیت با فناوری های مختلف را تضمین کند.
- **GP-PS-03** امنیت باید ریسک های ناشی از ایمنی انسان‌ها را در نظر بگیرد.
- **GP-PS-04** طراحی برای حفاظت از منبع برق نباید امنیت را به خطر بیاندازد.
- **GP-PS-05** معماری را به گونه ای طراحی کنید تا مولفه‌ها در صورت حملات به صورت محافظت شده مانند کپسوله کردن باشند.
- **GP-PS-06** برای تولید کنندگان سخت افزار IoT و توسعه دهندگان نرم افزار IoT اجرای برنامه های آزمون لازم است تا بررسی کند که آیا محصول مطابق آنچه انتظار می‌رود عمل کند. تست نفوذ به شناسایی رفتارهای دورزدن ورود پس از احراز هویت و وضعیت کلی امنیت کمک میکند.
- **GP-PS-07** برای توسعه دهندگان نرم افزار IoT، بررسی کد های در حال اجرا بسیار مهم است. این به کاهش خطاها در نسخه نهایی محصول کمک می‌کند.

۴-۱-۲- حریم خصوصی در طراحی محصول

حریم خصوصی را به عنوان بخشی جدایی ناپذیر از سیستم تبدیل کنید.

• **GP-PS-09** ارزیابی‌های تأثیر حریم خصوصی را قبل از انتشار اپلیکیشن های جدید انجام دهید.

۴-۱-۳- مدیریت دارایی

• **GP-PS-10** برای روش های مدیریت دارایی و کنترل‌های پیکربندی را برای شبکه های کلیدی و سیستم‌های اطلاعاتی ایجاد و نگهداری کنید.

۴-۱-۴- شناسایی و ارزیابی ریسک و مخاطرات

• **GP-PS-11** شناسایی ریسک های قابل توجه با استفاده از یک رویکرد دفاع در عمق

• **GP-PS-12** شناسایی محیط و موارد استفاده از دستگاه اینترنت اشیا

۴-۲- معیارهای سازمانی، معیارهای فرآیندی و مردم

همه کسب و کارها باید معیارهای سازمانی برای امنیت اطلاعات داشته باشند. تجربیات و اقدامات پرسنل آن‌ها باید امنیت را افزایش دهد، مدیریت فرآیندها را تضمین کند و با اطمینان خاطر از اطلاعات، فعالیت سازمان انجام شود. همچنین سازمان‌ها باید اطمینان حاصل کنند که پیمانکاران و تامین کنندگان مسئول وظایف مورد نظر

هستند. در صورت بروز حادثه‌های در امنیت سازمان، سازمان باید آماده (مسئولیت، ارزیابی و پاسخ) باشد.

۴-۲-۱- پشتیبانی مادام العمر

- **GP-OP-01** تدوین استراتژی مادام العمر محصولات اینترنت اشیا
- **GP-PS-02** مدت زمان امنیت و پشتیبانی وصله های امنیتی (فراتر از ضمانت محصول) را مشخص کنید.
- **GP-PS-03** عملکرد و آسیب پذیری‌های شناخته شده را تا پایان مدت پشتیبانی چرخه عمر محصول برطرف کنید.

۴-۲-۲- راهکارهای اثبات شده

- **GP-PS-04** از راهکار های اثبات شده، یعنی پروتکل‌های ارتباطی و الگوریتم های رمزنگاری شناخته شده توسط انجمن های علمی و غیره استفاده کنید. و از راهکارهای اختصاصی خاص مانند الگوریتم های رمزنگاری ویرایش شده و سفارشی، جلوگیری شود.

۴-۲-۳- مدیریت آسیب پذیری‌های امنیتی و یا حوادث

- **GP-PS-05** روش‌هایی را برای تحلیل و رسیدگی به حوادث امنیتی تنظیم کنید.
- **GP-PS-06** افشای هماهنگ آسیب پذیری.

• **GP-PS-07** در بسترهای به اشتراک گذاری اطلاعات شرکت کنید تا آسیب‌پذیری‌ها را گزارش کرده و اطلاعات به موقع و حیاتی را در مورد تهدیدات سایبری فعلی و آسیب پذیری هایی که از سوی شرکای عمومی و خصوصی دریافت کنید.

• **GP-OP-08** یک مکانیسم افشای عمومی برای گزارش‌های آسیب پذیری ایجاد کنید، به عنوان مثال برنامه‌های Bug Bounty

۴-۲-۴- آگاهی رسانی و آموزش های امنیت برای منابع انسانی

• **GP-OP-09** اطمینان حاصل کنید که تجربه های پرسنل باعث افزایش حفظ حریم خصوصی میشود و کارکنان آموزش را در حفظ حریم خصوصی و اقدامات امنیتی ترویج می‌کنند.

• **GP-OP-10** فعالیت‌های آموزش حریم خصوصی و امنیت را نظارت و مستندسازی کنید.

• **GP-OP-11** اطمینان حاصل کنید که نقش‌ها و مسئولیت‌های امنیت سایبری برای همه نیروهای کاری مشخص شده است و وظایف پرسنل را متناسب با مشخصات پروژه‌ها و مهندسان امنیت مورد نیاز، تخصیص داده شده است.

۴-۲-۵- روابط شخص ثالث

• **GP-OP-12**داده‌های پردازش شده توسط شخص ثالث باید با توافقنامه حفاظت از پردازش داده‌ها منطبق باشد.

• **GP-OP-13**فقط داده های شخصی مشتریان با رضایت صریح از مشتریان را با طرفین ثالث به اشتراک بگذارید، بجز مواردی که برای استفاده از ویژگی های محصول و یا محدود به سرویس های عملیاتی مورد نیاز شود.

• **GP-OP-14**برای تولیدکنندگان سخت‌افزار IoT و توسعه دهندگان نرم‌افزار IoT، داشتن خط مشی های مدیریت ریسک سایبری، در زنجیره تامین و برقراری ارتباط با الزامات امنیتی سایبری برای تامین کنندگان و شرکای خود، ضروری است.

۴-۳-معیارهای فنی

بدیهی است که معیارهای امنیتی و تجربیات باید ابعاد فنی را هم لحاظ کند تا آسیب‌پذیری‌های اینترنت اشیا را کاهش دهند.

در زیر ما یک مرور کلی از معیارهای فنی لازم برای نگهداری و حفاظت از امنیت اطلاعات در اینترنت اشیا ارائه می‌کنیم. از آنجا که این معیارها در صنعت افقی در کل بخش‌های صنایع عمودی هم هستند، و با توجه به ویژگی‌های خاص هر صنعت عمودی، معیارهای بیشتری را می‌توان برای هر بخش عمودی معرفی کرد.

بکارگیری این معیارهای فنی باید ویژگی‌های اکوسیستم IoT مانند مقیاس پذیری را در نظر داشته باشد، یعنی با توجه به تعداد بسیار زیادی از دستگاه های درگیر، ممکن است اقدامات خاصی لازم باشد در سطح اجزای معماری تخصصی به عنوان مثال Gatewayها انجام شود .

امنیت سخت افزار، مدیریت یکپارچه و مطمئن، امنیت و حریم خصوصی، حفاظت از داده، ایمنی و قابلیت اطمینان، به روز رسانی امن نرم افزار وFirmware، احراز هویت، مجوز دسترسی، کنترل دسترسی- امنیت فیزیکی و محیطی، رمزنگاری، ارتباطات امن و مطمئن، امن سازی اینترفیس‌ها و خدمات شبکه، استفاده از ورودی و خروجی امن، ثبت لاگ‌ها، نظارت و حسابرسی، مواردی هستند که جزو معیارهای فنی میباشد. که شرح اقدامات این بخش در نسخه کامل گزارش موجود است.

بخش پنجم

تحلیل GAP

بخش پنجم

تحلیل GAP[1]

در این فصل تحلیلی در مورد گپ اصلی در رابطه با امنیت سایبری در اینترنت اشیا ارائه شده است. بخش مهمی از موضوع پرداختن به امنیت سایبری در اینترنت اشیا و تعریف گپ‌ها - فضای بین وضعیت کنونی و دولت است. از سوی دیگر دستیابی به این گپ‌ها، یعنی حرکت به سمت بلوغ و تعیین اقداماتی است که باید انجام شود. در مصاحبه‌هایی که با متخصصان اینترنت اشیا انجام شد، یک موضوع مشترک وجود داشت. بلوغ امنیت در اینترنت اشیا در مرحله اولیه توسعه قرار دارد. گپ‌های زیر به عنوان مهم‌ترین دسته از شکاف‌هایی است که توسط متخصصانی که در این مطالعه شرکت کردند شناسایی شدند و تحلیل مقایس‌های از منابع امنیتی اینترنت اشیا موجود همانطور که در پیوست گزارش در نسخه کامل تحت عنوان» (Security standards and references reviewed)» ذکر شده است، انجام دادند.

۱. تحلیل شکاف/ فاصله بین پیش بینی و واقعیت

مـا شـکاف‌ها را بـا در نظـر گرفتـن دو بعـد بررسـی می‌کنیـم یعنـی در ابتـدا بـا تحلیـل موانـع و در پایـان تغییراتـی کـه بایـد بـرای بهبـود و تضمیـن امنیـت در اینترنـت اشـیا در نظـر گرفتـه شـوند. مـا همچنیـن چالش‌هـای مربوطـه را کـه بعنـوان عامـل مانـع در تامیـن امنیـت پایـدار IoT عمـل می‌کننـد، را تشـریح می‌کنیـم.

هـدف ن‌هایـی از پرداختـن بـه امنیـت اینترنـت اشـیا و گپ‌هـای ایمنـی، تضمیـن دسترسـی بـه همـه دارایی‌هـا، حفـظ سـطح مـورد نیـاز بـرای حفـظ حریـم خصوصـی، و نیـز دسـتیابی و انعطـاف پذیـری بـالا در برابـر حمـلات سـایبری اسـت، بنابرایـن ایمنـی فیزیکـی را در کنـار امنیـت سـایبری تضمیـن می‌کنـد.

گپ‌هـای زیـر بـه عنـوان مهم‌تریـن دسـته از شـکاف‌ها توسـط متخصصـان شناسـایی شـده اسـت. کـه شـرح کامـل آن‌هـا در نسـخه کامـل گـزارش موجـود اسـت.

گپ ۱: تدوین مقررات و رویکردهای امنیتی موجود
گپ ۲: فقدان آگاهی و دانش
گپ ۳: طراحی و یا توسعه ناامن
گـپ ۴: عـدم قابلیـت همـکاری در دسـتگاه‌های مختلـف IoT، پلتفرم‌هـا و3framework‌هـا
گپ ۵: عدم انگیزه‌های اقتصادی

گپ ۶: فقدان مدیریت مناسب چرخه عمر محصول

بخش ششم

توصیه های بسیار مهم برای بهبود امنیت سایبری IoT

بخش ششم

توصیه های بسیار مهم برای بهبود امنیت سایبری IoT

این فصل شامل فهرستی از توصیه‌های high-level (سطح بالا) برای توسعه دهندگان، اپراتورها و متخصصان امنیتی است که به آن‌ها کمک خواهند کرد تا سطح امنیتی دستگاه های اینترنت اشیا و ارتباطات میان آن‌ها را بهبود بخشند. توصیه‌هایی که در اینجا مورد بحث قرار گرفته است، مربوط به ذینفعانی است که کل طیف اینترنت اشیا را در بر می‌گیرند و هدفشان رفع شکاف های موجود تعریف شده در فصل ۵ است.

۶-۱-توصیه ها

توصیه‌های پیشنهادی در جدول زیر ذکر شده است.

ردیف	شرح
۱	افزایش هماهنگی اقدامات و مقررات امنیت اینترنت اشیا
۲	افزایش آگاهی برای نیاز به امنیت سایبری IoT
۳	تعریف دستورالعمل‌های چرخه عمر توسعه امن نرم‌افزار و سخت‌افزار برای IoT

۴	رسیدن به اجماع برای قابلیت همکاری در کل اکوسیستم اینترنت اشیا
۵	ایجاد و تقویت انگیزه‌های اقتصادی و اجرایی برای امنیت اینترنت اشیا
۶	ایجاد مدیریت چرخه امن محصول و خدمات اینترنت اشیا
۷	شفاف سازی مسئولیت در بین ذینفعان IoT

۶-۲-جزئیات توصیه ها

۶-۲-۱- افزایش هماهنگی اقدامات و مقررات امنیت اینترنت ا شیا

توصیه در نظر گرفته شده برای: صنعت IoT، ارائه دهندگان، تولید کنندگان، انجمن ها

تدوین دستورالعمل‌های امنیتی IoT، استانداردها و برنامه‌های دیگر باید مورد توجه قرار گیرد. اولین گام در جهت تعیین لیستی از بهترین تجربه‌ها و دستورالعمل‌ها برای امنیت و حفظ حریم خصوصی IoT است که می‌تواند به عنوان مبنایی برای توسعه و استقرار سیستم‌های IoT در بازار، استفاده شود (به عنوان مثال گزارش‌های مشاوره ای از AIOTI و ECSO). گزارش فعلی ENISA چنین لیستی را ارائه می‌دهد و با طبقه بندی کلیه اقدامات امنیتی بر اساس مجموعه ای تعریف شده و ساختار یافته از حوزه‌های امنیتی، یک گام جلوتر می‌رود. از نظر هماهنگ سازی استانداردها، جالب است بدانیم که مفهوم استاندارد توسط صنعت مورد استقبال و پشتیبانی قرار می‌گیرد، اما گروه‌های ذینفعان زنجیره‌های تحقیق و توسعه مختلف

دارنـد و ایـن بـه صـورت ذاتی باعث تکه تکه شـدن می‌شـود. توصیه می‌شـود بـرای مقابلـه با ایـن پراکنده بـودن، مجموعـه ای از تجربیات، دسـتورالعمل‌ها و الزامـات امنیتـی در IoT، کـه در سراسـر اروپـا رایـج اسـت، ایجـاد شـود.

کمیسـیون اتحادیـه اروپا باید تسـهیل کننده ایـن فرآیند باشـد و این گزارش ENISA می‌توانـد بـه عنـوان سـکوی پـرش بـرای تلاش‌هـای مرتبط باشـد. هـر بخـش می‌توانـد براسـاس زمینـه خـاص و عوامـل ریسـک ذاتـی در هـر بخـش متعاقبـا بـر تعییـن مجموعه‌هـای خاصـی از تجربیـات، دسـتورالعمل‌ها و الزامـات مـورد نیـاز خـود، تمرکـز کنـد. کمیسـیون اروپـا و دولت‌هـای عضـو می‌تواننـد هماهنگـی و همـکاری سـهامداران و ذینفعـان (صنعـت، کاربـران) را هدایـت کننـد و ENISA می‌توانـد یـک تسـهیل کننـده مهـم در ایـن فرآینـد باشـد.

فرآینـد تـدارکات، موضـوع دیگـری برای اعمـال هماهنگـی با اسـتانداردهای پایـه و الزامـات سیسـتم IoT اسـت. در هماهنگـی بایـد در نظـر گرفتـه شـود کـه بخش‌هـای مختلـف زیـادی ماننـد انـرژی، حمـل و نقـل، وجـود دارد. بنابرایـن بایـد در ابتـدا هماهنگـی در هـر بخـش انجـام شـود.

۶-۲-۲- افزایش آگاهی برای نیاز به امنیت سایبری IoT

توصیه‌هـای در نظـر گرفتـه شـده بـرای: صنعـت IoT، ارائـه دهنـدگان،

تولید کنندگان، انجمن‌ها، آکادمی‌ها، گروه‌های مشتریان، رگولاتورها

امنیت سایبری یک مسئولیت مشترک بین همه ذینفعان درگیر است. بنابراین ضروری است که ذینفعان درک کاملی از خطرات و تهدیدهای مرتبط با آن و همچنین راهکارهای تامین امنیت و محافظت در برابر آن‌ها را داشته باشند. بنابراین افزایش آگاهی از اهمیت ویژه ای برخوردار است و برای انجام این کار به شدت توصیه می‌شود.

همانطور که در چشم انداز، تهدید روزافزون و حوادث امنیتی بیشمار در مورد IoT قابل مشاهده است، در حال حاضر، فقدان دانش در توسعه دهندگان IoT و صنایع به عنوان کاربران نهایی و مشتریان وجود دارد. برای رفع این کمبود، توصیه‌های هدفمند برای هر سه دسته ذینفعان، عبارتند از:

•آموزش و آموزش امنیت باید در صنایع ایجاد شود، از جمله دانشی از جدیدترین روشها، بهترین تجربه‌ها، معماری‌های مرجع و در دسترس بودن بلاک‌های سازنده، روش‌ها و ابزارهای امن سازی سیستم‌های IoT

•کاربران نهایی و مشتریان باید آموزش ببینند تا بتوانند هنگام خرید سیستم‌ها و دستگاه‌های IoT آگاهانه تصمیم بگیرند.

ترویج آگاهی از امنیت اینترنت اشیا به شدت مهم هستند، همچنین بمنظور حفظ سطح پایه امنیت سایبری برای امنیت« Things هایی»که آن‌ها خریداری کرده یا در حال کار با آن‌ها هستند.

• در میان جامعه توسعه دهنده، آگاهی برای اتخاذ اصول اساسی امنیت باید افزایش یابد بجای اینکه وابسته به هر صنعت عمودی باشد. آموزش‌های ارائه شده توسط شرکت‌هایی که بر امنیت IoT متمرکز شده‌اند نیز سودمند هستند و باید دنبال و پیگیری شوند. به صورت مشابه، اقداماتی مانند کافه علمی امنیت سایبری می‌توانند موثر واقع شوند. در نهایت، آموزش‌ها و دوره‌های مدارس و دانشگاه‌ها (با در نظر گرفتن موضعی برای رسیدن به مخاطبان بیشتر) درک بهتری از امنیت اینترنت اشیا را در بین نسل جوان ترویج خواهد داد و در نتیجه در بلندمدت به افزایش آگاهی کمک کردند.

۶-۲-۳- تعریف دستورالعمل‌های چرخه عمر توسعه امن نرم‌افزار و سخت‌افزار برای IoT

توصیه در نظر گرفته شده برای: توسعه دهندگان IoT، اپراتورهای پلتفرم، صنعت، تولید کنندگان

توسعه دهندگان، تولید کنندگان و ارائه دهندگان محصولات و راهکارهای IOT باید یک چرخه عمر توسعه امن نرم افزار (SSDLC)[1] را برای ارائه‌های IoT خود اتخاذ و فرآیندهای مربوط

1.secure software development lifecycle

را در عملیات خود ادغام کنند. امنیت باید به طور کلی، در سطح برنامه و در هر یک از مراحل SDLC[1] اجرا شود. بنابراین مهم است که شرکت‌های بیشتری را تشویق کنیم که مولفه‌های امن را ارائه دهند که برای توسعه دهندگان و مشتریان نهایی نیز استفاده شود.

مفاهیم امنیت و حریم خصوصی به صورت پیش‌فرض و امنیت و حریم خصوصی به وسیله طراحی معمولا به عنوان سنگ بنای امنیت اینترنت اشیا مطرح می‌شوند. بدیهی است که بکار بردن این مفاهیم در چندین محیط مختلف که ویژگی‌های خاصی دارند، چالش برانگیز است. در IoT ریسک سایبری وابسته به سناریوهای کاربردی است و از این نظر باید اصول امنیت و حفظ حریم خصوصی در طراحی محصول در نظر گرفته شود. علاوه بر اقدامات مربوطه، از سوی دیگر بخش‌های فناوری اطلاعات نیز می‌توانند در بلوغ اتخاذ چنین اصولی برای اکوسیستم IoT سودمند باشند.

۶-۲-۴- رسیدن به اجماع برای قابلیت همکاری در کل اکوسیستم اینترنت اشیا

توصیه در نظر گرفته شده برای: صنعت IoT، ارائه دهندگان، تولید کنندگان، انجمن‌ها، رگولاتور ها

مسئله قابلیت همکاری با توجه به مقیاس بسیار زیاد و نفوذ

1.software development lifecycle

اکوسیستم اینترنت اشیا و زنجیره‌های تامین پیچیده و تعدد ذینفعان درگیر، به اکوسیستم IoT وابسته است. تضمین و ترویج قابلیت همکاری دستگاه‌های بسته‌بندی، پلت فرم‌ها و چارچوب ها و همچنین شیوه‌های امنیتی یک مولفه اساسی از امنیت اینترنت اشیا است و بنابراین باید مورد تشویق و ترغیب قرار گیرد.

توصیه‌هایی که بدون شک در این راستا کمک خواهند کرد عبارتند از:

- تشویق استفاده چارچوب قابلیت همکاری باز که امنیت را پوشش بدهد.
- ارائه شفافیت در زمینه امنیت چارچوب قابلیت همکاری
- توسعه آزمایشگاه‌های قابلیت هم‌کاری به صورت آزاد و قابل‌دسترس برای امنیت

۶-۲-۵- ایجاد و تقویت انگیزه‌های اقتصادی و اجرایی برای امنیت اینترنت اشیا

توصیه‌های در نظر گرفته شده برای: صنعت IoT، انجمن‌ها، دانشگاه‌ها، گروه‌های مشتریان، رگولاتورها

واضح است که عدم وجود امنیت بر تداوم کسب وکار تاثیر

می‌گذارد و این برای اینترنت اشیا نیز صادق است که توسط اقدامات واحد R & D (تحقیق و توسعه) هدایت می‌شود و برای انتشار محصولات و خدمات در بازار عجله دارند. در این رابطه، تداوم کسب‌وکار می‌تواند به عنوان یک محرک برای توجیه هزینه‌ها در راهکارهای امنیت سایبری عمل کند. علاوه بر این، تقاضای بازار در مورد امنیت سایبری به دلیل عدم درک مشتریان از امنیت سایبری به عنوان ارزش افزوده، تا حدی پایین است. مشارکت مشتریان بسیار مهم است و باید بیشتر مورد حمایت قرار گیرد. و مستلزم تصمیم گیری مکانیزم‌های بیشتری برای ترویج امنیت سایبری اینترنت اشیا می‌باشد.

در حال حاضر مزیت رقابتی برای اینرنت اشیا با تمرکز بر روی time to market انجام می‌شود تا secure to market. این تعادل باید تغییر داده شود که سطح خاصی از امنیت و حریم خصوصی قبل از استقرار در بازار، تشویق شود تعریف چارچوب‌های امنیتی که توسط معیارهای امنیتی پایه پشتیبانی می‌شوند می‌تواند راهی به سمت جلو در این مسیر باشد.

استفاده از طرح‌های دیگر مانند صدور گواهینامه و برچسب زدن نیز می‌تواند درک بهتر و شفافی را از نظر امنیت IoT ترغیب کند و بنابراین باید مورد توجه قرار گیرد (همچنین میتواند به نفع کاربران

نهایی و مشتریان و افزایش آگاهی آن‌ها از امنیت IoT بشود.)

۶-۲-۶- ایجاد مدیریت چرخه امن محصول و خدمات اینترنت اشیا

توصیه در نظر گرفته شده برای: توسعه دهندگان IoT، اپراتورهای پلتفرم، صنعت، تولید کنندگان

امنیت نقش مهمی در تمام مراحل چرخه عمر یک محصول اینترنت اشیا ایفا می‌کند. این مراحل شامل طراحی، توسعه، آزمایش، تولید، استقرار، نگهداری، پشتیبانی، و پایان عمر (به عنوان مثال decommissioning[1]) است. بدیهی است که فرایندهای امنیتی متمرکز وهدفمند برای تمام این مراحل تعریف می‌شوند.

علاوه بر این، فرآیندهای امنیتی. بمنظور برآورده کردن این نیاز، باید به درستی اجرا شوند. الزامات امنیتی پایه و بلاک‌های سازنده باید در هر مرحله در دسترس باشند.

جنبه دیگر قابل‌توجه شامل بروز رسانی‌های امنیتی است که یک موضوع مهم را در زمینه اینترنت اشیا ایجاد می‌کنند. پس از توسعه، بروز رسانی‌های امنیتی باید فراهم شود که در آن عملا الزامات دانشی خاص و یا تعهدات مالی در مورد مشتریان در یک مدت و شرایط مشخص تا «پایان زمان پشتیبانی» ارائه شود. جنبه دوم باید به صورت واضح توسط تولیدکننده / ارایه‌دهنده محصول IoT تعریف

۱.یک اصطلاح کلی در فرآیند رسمی برای خارج کردن چیزی از وضعیت فعال

شود و به صورت واضح برای مشتریان نهایی ارسال شود.

۶-۲-۷- شفاف سازی مسئولیت در بین ذینفعان IoT

توصیه در نظر گرفته شده برای:، صنعت IoT، رگولاتورها

همانطور که در مصاحبه با کارشناسان مشخص شده است یک مسئله بسیار مهم در زمان بررسی اینترنت اشیا، مربوط به مسئولیت است. این امر در حوزه IoT از اهمیت ویژه ای برخوردار است، زیرا ماهیت فیزیکی سایبری IoT به امنیت مربوط می‌شود.
موضوع مسئولیت، باید مورد توجه قرار گیرد. این سؤال وجود دارد که مسئولیت در کجا ممکن است بین ذینفعان مختلف و متنوع اکوسیستم IoT مانند توسعه دهندگان، تولید کنندگان، ارائه دهندگان، فروشندگان، اپراتورهای پشتیبانی پس از فروش، ارائه دهندگان شخص ثالث و کاربران نهایی قرار گیرد. موضوعات مربوط به مسئولیت باید در چارچوب قوانین و مقررات ملی اروپا مورد بررسی قرار گیرد. در مواردی که در این قانون به عنوان گپ مشخص شده‌اند، باید موارد مرتبط با مسئولیت توجه شود.

جمع بندی

توصیه هـــای امنیتی پایه برای IoT
درحوزه زیرســـاخت های اطلاعاتی حیاتی

جمع‌بندی

هـدف از ایـن گـزارش تشـریح توصیه‌هـای اولیـه امنیت سـایبری بـرای IoT بـا محوریـت زیرسـاخت‌های اطلاعاتـی حیاتـی بـود کـه شـامل امکانـات، شـبکه‌ها، خدمـات وتجهیـزات فنـاوری می‌باشـد ایـن زیرسـاخت‌ها بـه دلیـل امـکان خرابـی یـا مختـل شـدن بسـیار مهـم هسـتند کـه میتوانـد عواقـب شـدیدی بـرای سـلامتی، ایمنـی و رفـاه اقتصـادی شـهروندان بـه همـراه داشـته باشـد.

در ایـن راسـتا، اقدامـات امنیتـی اولیـه بـرای IoT در ایـن گـزارش ارائه شـد کـه بـرای تلاش‌هـای بیشـتر در خصـوص یـک رویکـرد هماهنـگ اتحادیـه اروپـا، بـه عنـوان نمونـه مطالعاتـی، زمینـه را بـرای تصویـب ضمنـی اینگونـه اقدامـات و معیارهایـی ماننـد صـدور گواهینامـه بـرای کشـور فراهـم شـود.

منابع

1. Document: Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures | NOVEMBER 2017


مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی