مروری بر چالش ها و تهدیدات امنیت و حریم خصوصی اینترنت اشیاء در سازمان های فرهنگی

الهام طریق الاسلامی* [۱]، دکتر علی اکبر رضایی [۲]

چکیده

اینترنت اشیاء[۳]، به عنوان یکی از برجسته ترین تحولات فناوری در دهه های اخیر، زیرساختی فراهم کرده است که اشیاء فیزیکی از طریق حسگرها و اتصال به اینترنت، قادر به جمع آوری، پردازش و تبادل داده شوند. این فناوری با وجود کاربردهای گسترده در حوزه های مختلف، به ویژه در سازمان های فرهنگی (مانند موزه ها، کتابخانه ها و مراکز تاریخی)، چالش های جدی در زمینه ی امنیت و حریم خصوصی ایجاد کرده است. هدف این مقاله ی مروری، بررسی و تحلیل چالش ها و تهدیدات امنیتی شامل حملات سایبری، انتقال داده های رمزگذاری نشده و استقرار غیرمجاز دستگاه ها و نقص در به روز رسانی است. همچنین چالش های حریم خصوصی مانند جمع آوری بدون رضایت اطلاعات شخصی و استفاده از آنها، از موانع اصلی پذیرش گسترده ی این فناوری محسوب می شود. در این میان، فناوری زنجیره ی بلوک به عنوان یکی از راهکارها برای افزایش امنیت، حفظ محرمانگی و مدیریت دسترسی در اینترنت اشیاء معرفی شده است. این پژوهش در پایان، بر ضرورت تدوین استانداردها، قوانین بازدارنده و فرهنگ سازی پیش از ورود فناوری های نوین تأکید کرده و پیشنهادهایی برای تحقیقات آینده در زمینه ی امنیت و حریم خصوصی اینترنت اشیاء در سازمان های فرهنگی ارائه می دهد.

واژگان کلیدی: امنیت، حریم خصوصی، اینترنت اشیاء، روش های حفاظتی، زنجیره ی بلوک، سازمان های فرهنگی

۱. مقدمه

با توجه به رشد روز افزون استفاده از فناوری های نوین در عرصه های مختلف، اینترنت اشیاء به عنوان یکی از برجسته ترین تحولات تکنولوژیک در دنیای امروز شناخته شده است. این فناوری به سازمان ها این امکان را می دهد که تجهیزات و اشیاء مختلف را به شبکه های اینترنت متصل کرده و به طور هوشمندانه و خودکار، اطلاعات را جمع آوری و پردازش کنند. در این میان، سازمان های فرهنگی شامل موزه ها، گالری ها، کتابخانه ها و مراکز تحقیقاتی، به طور فزاینده ای از اینترنت اشیاء برای ارتقای خدمات، حفاظت از اشیاء تاریخی و بهبود مدیریت استفاده می کنند. با این حال، همین فناوری، آن ها را با تهدیدات امنیتی و چالش های حریم خصوصی مواجه ساخته است که می تواند اطلاعات حساس فرهنگی، منابع تاریخی و حریم شخصی کاربران را به خطر اندازد.

---

[۱] نویسنده ی مسئول: دانشجوی دکتری رشته ی مدیریت و برنامه ریزی فرهنگی، دانشکده ی مدیریت و اقتصاد، دانشگاه علوم و تحقیقات تهران، دانشگاه آزاد اسلامی، ایران، آدرس الکترونیکی: elham.tarigholeslami@iau.ir

[۲] استادیار رشته ی مدیریت و برنامه ریزی فرهنگی، دانشکده ی مدیریت و اقتصاد، دانشگاه علوم و تحقیقات تهران، دانشگاه آزاد اسلامی، ایران

[۳] (IoT)

اهمیت و ضرورت پرداختن به این موضوع از آنجا ناشی می شود که اینترنت اشیاء به دلیل تنوع دستگاه ها، محدودیت های محاسباتی، اتصال گسترده و ماهیت توزیع شده، آسیب پذیری متعددی دارد. عدم توجه به این چالش ها می تواند منجر به نقض محرمانگی، از دست رفتگی یکپارچگی داده ها و اختلال در دسترسی به خدمات شود. از این رو، هدف این تحقیق مروری، شناسایی و تحلیل ابعاد مختلف امنیت و حریم خصوصی اینترنت اشیاء در سازمان های فرهنگی، بررسی تهدیدات موجود و ارائه ی روش های حفاظتی مبتنی بر فناوری های نوین مانند «زنجیره ی بلوک» است تا بتوان زمینه را برای بهبود سیستم های امنیتی و حفظ حریم خصوصی در این سازمان ها فراهم آورد.

۲. هدف تحقیق

هدف این تحقیق مروری، بررسی و تحلیل ابعاد مختلف امنیت و حریم خصوصی اینترنت اشیاء در سازمان های فرهنگی است. این تحقیق میتواند به شناسایی چالش ها و تهدیدات امنیتی موجود در این حوزه کمک کند و پیشنهادهایی برای بهبود سیستم های امنیتی موجود و حفظ حریم خصوصی در سازمان های فرهنگی ارائه دهد.

۳. پرسش های تحقیق

۱-۳. تهدیدات و چالش های امنیتی و حریم خصوصی اینترنت اشیاء در سازمان های فرهنگی کدام اند؟

۲-۳. روش های حفاظتی پیشنهاد شده برای مقابله با این تهدیدات و چالش ها کدام اند؟

۴. روش شناسی تحقیق

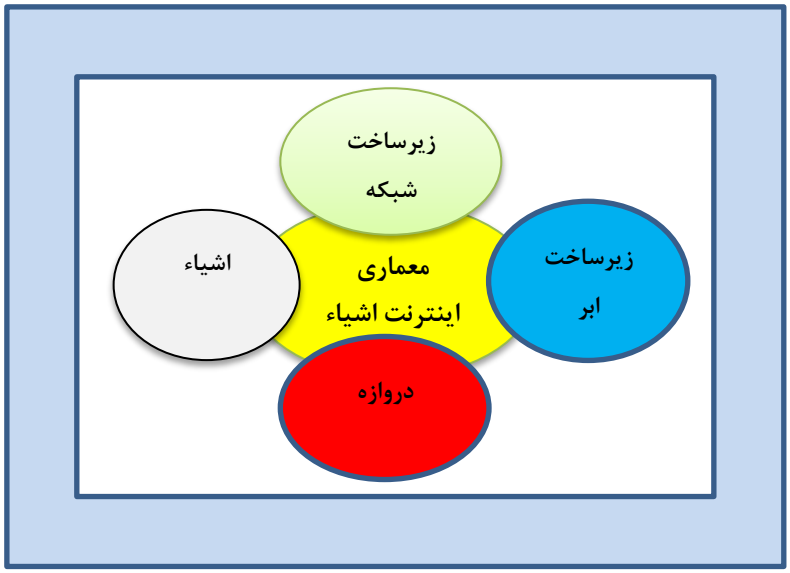
پژوهش حاضر از نوع مطالعات مروری روایتی است که با هدف شناسایی، دسته بندی و تشریح چالش های امنیت و حریم خصوصی اینترنت اشیاء در سازمان های فرهنگی انجام شده است. انتخاب رویکرد مروری روایتی به دلیل ماهیت اکتشافی موضوع و گستردگی ابعاد آن (فنی، حقوقی، مدیریتی و فرهنگی) صورت گرفته است. جستجوی منابع به دو زبان فارسی و انگلیسی در بازه ی زمانی سال های ۲۰۱۶ تا ۲۰۲۵ (میلادی) و ۱۳۹۶ تا ۱۴۰۴ (هجری شمسی) انجام شد. استراتژی جستجو، استفاده از مقالات منتشر شده در مجلات علمی- پژوهشی، کتاب ها و گزارش های فنی معتبر و اسناد بالادستی و مطالعات موردی مرتبط با کاربرد اینترنت اشیاء در سازمان های فرهنگی است.

اطلاعات منابع انتخابی با استفاده از روش تحلیل محتوای جهت دار استخراج شد، بدین معنا که ابتدا چارچوب اولیه ای از مفاهیم اصلی (شامل تعاریف، ویژگی ها، اجزا، انواع اینترنت اشیاء، مزایا، تهدیدات امنیتی، چالش های حریم خصوصی، محرمانگی، اعتماد، و راهکارهای حفاظتی مانند زنجیره ی بلوک) تعیین گردید. سپس هر منبع بر اساس این چارچوب بررسی شد و مفاهیم مرتبط استخراج و دسته بندی گردید. در پایان، یافته ها به صورت توصیفی و ساختار یافته ارائه شده است. محدودیت های روش شناختی پژوهش شامل کمبود مطالعات تخصصی در حوزه ی اینترنت اشیاء در سازمان های فرهنگی، دسترسی محدود به برخی مقالات بین المللی و تغییرات سریع فناوری بوده است که ممکن است برخی از یافته های مقالات قدیمی تر (پیش از سال ۲۰۱۸)، تا حدی منسوخ شده باشد. با این وجود، سعی شده است با جستجوی جامع و استفاده از منابع معتبر، تصویر نسبتاً کاملی از وضعیت موجود ارائه گردد. قلمرو مکانی تحقیق به طور خاص بر سازمان های فرهنگی در ایران و سایر کشورهای جهان تمرکز دارد.

۵. تعاریف و پیشینه ی اینترنت اشیاء

۵-۱. تعریف اینترنت اشیاء

ماده ی ۲۹ اعلامیه ی مرکز نظارت بر داده ی پیام های اتحادیه اروپا (مصوب ۲۰۱۰ با الحاقات و اصلاحات ۲۰۱۵)، در تعریف اینترنت اشیاء بیان می دارد: «اینترنت اشیاء» زیرساخت هایی هستند که در آن، میلیاردها حسگر تعبیه شده در دستگاه های کاربردی روزمره؛ برای ضبط، پردازش، ذخیره و انتقال داده ها طراحی شده است و همانطور که از قابلیت ارتباط با عامل انسانی برخوردار هستند، با بهره مندی از شناسه های منحصر به فرد، با دستگاه ها یا سیستم های دیگر با استفاده از قابلیت های شبکه، تعامل برقرار می کنند. (آقایی طوق و ناصر، ۱۳۹۹)



شکل ۱. معماری اینترنت اشیاء (نوروزی، ۱۴۰۳)

اینترنت اشیاء، یکی از جدیدترین تکنولوژی های پیشرفته است و یک پارادایم ارتباطی انقلابی است که هدف آن ایجاد یک چارچوب نامرئی و نوآورانه برای اتصال بسیاری از دستگاه های دیجیتال با اینترنت است. بدین ترتیب، در نظر دارد اینترنت را جذابتر و فراگیرتر کند. اینترنت اشیاء؛ روش تعامل تمام کسب و کارها، دولت ها و مصرف کنندگان را با دنیای فیزیکی تغییر خواهد داد و به طور کلی، شامل تجهیزات و ابزارهایی شامل اشیاء و وسایل محیط پیرامون ما هستند که به شبکه ی اینترنت متصل شده و به آن ها «شیء» گفته می شود. اشیاء، دارنده ی قابلیتهای محاسباتی و شبکه بندی لازم برای انجام کارهای محول شده به آنها می باشند که میتوان آنها را توسط برنامه های کاربردی موجود در تلفن های هوشمند، رایانک[۴] و سایر سیستم های هوشمند، کنترل و مدیریت کرد. اینترنت اشیاء، ترکیبی از سیستم های جاسازی شده ی متصل به ابر است که برای دسترسی به سرویس های مرتبط با تکنولوژی اطلاعات که از ترکیبی از اشیای

[۴] Tablet

الکترونیکی و پروتکل اینترنت استفاده می کند و توسط سرویس گیرنده به کار گرفته میشود. (سلمانی و خسروی، ۱۴۰۰)، (مرکز اینترنت اشیاء ایران، ۱۳۹۹)

اینترنت اشیاء، اتصال اشیاء متحرک فیزیکی[۵] از طریق اینترنت است که با تراشه ی الکترونیکی، حسگرها و سایر اشکال سخت افزاری تعبیه شده است. هر دستگاه با برچسب های شناسه ی فرکانس رادیویی (RFID) در سطح جهانی به طور منحصر به فرد شناسایی می شود. (زندیار و همکاران، ۱۴۰۰)، (آزادی و همکاران، ۱۳۹۷)، (نوروزی، ۱۴۰۳) اینترنت اشیاء شبکه ی جهان شمولی از اشیاء است که از هر مکانی توسط پروتکل های ارتباطی، قابل آدرس دهی و دسترسی هستند. دلیل بوجود آمدن اینترنت اشیاء این است که هر شیء ای که در سراسر دنیا پخش شده است، قابلیت اندازه گیری، درک و فهم، پیش بینی و حتی تغییر در دنیای پیرامون خود را داشته باشد. (صفری و همکاران، ۱۴۰۰)

با توسعه ی اینترنت اشیاء، تعداد تجهیزات شبکه ای در حال افزایش است و بار مراکز داده ی ابری نیز افزایش میابد، برخی سرویس های حساس به تأخیر نمی توانند به موقع پاسخ دهند که منجر به کاهش کیفیت سرویس دهی می شود. (سلمانی و خسروی، ۱۴۰۰)

۲-۵. پیشینه ی اینترنت اشیاء

اصطلاح «اینترنت چیزها»، توسط «کوین اشتون» در سال ۱۹۹۹ در طول کار خود در (Procter & Gamble) ساخته شد. اشتون که در زمینه ی بهینه سازی «زنجیره ی تأمین» مشغول به کار بود، خواستار توجه رهبر ارشد به فناوری جدید هیجان انگیزی به نام سامانه ی بازشناسی با امواج رادیویی[۶] شد. «اینترنت اشیاء» دیدگاهی بود که در آن تمام اشیاء فیزیکی با استفاده از فرستنده های (RFID) یا گیرندگان، شناسایی و ردیابی می شوند. امروزه (IOT)، این دیدگاه را به اتصال چیزها به هر چیزی، هرکسی، هرکجا و هر زمان، گسترش داده است. (زندیار و همکاران، ۱۴۰۰)، (آزادی و کرباسی، ۱۳۹۷).

۳-۵. کاربرد اینترنت اشیاء در سازمان های فرهنگی

«اینترنت اشیاء» راه جدیدی برای حفاظت «اشیاء» و «مکان‌های تاریخی» ایجاد کرده است و با گرد هم آوردن حسگرهای پیشرفته، اتصال و تجزیه و تحلیل سریع، نظارت بر آن ها در زمان واقعی را برای انجام اقدامات اصلاحی جهت حفظ و مدیریت این گنجینه‌ها ممکن می‌سازد.

«بناهای تاریخی» و «گنجینه های فرهنگی» توسط نیروهای بسیاری از جمله آلودگی، تخریب، تغییرات آب و هوایی و عوامل دیگر در معرض خطر قرار دارند. حفاظت به طور سنتی، با استفاده از بازرسی های دستی مکرر انجام می شود که «تغییرات آهسته» را از دست می دهد یا «اطلاعات ناقصی» برای مداخلات ارائه می دهد.

اینترنت اشیاء با ارائه ی نظارت خودکار ۲۴ ساعته و تعمیر و نگهداری پیش بینی شده، این مشکلات را برطرف می کند. (Dabrowska,۲۰۲۴) در اوایل دهه ی ۲۰۰۰، بسیاری از سیستم های چندرسانه ای، استفاده از مدل‌های (IoT) را در سامانه های میراث فرهنگی بررسی کردند که به عنوان «اینترنت اشیاء فرهنگی»[۷] شناخته می شود. از سال ۲۰۱۰ برخی

---

[۵] Things

[۶] RFID or Radio frequency identification

[۷] IoCT or Internet of cultural things

کشورها مانند ایالات متحده، چین، کره و ژاپن، تحقیقاتی راجع به اینترنت اشیاء را تأمین مالی می کنند و کشورهای عربی مانند مصر باید پتانسیل (IoCT) برای حفاظت از میراث فرهنگی را بررسی کنند. (Mohamed, ۲۰۲۴)

«سایت های میراث فرهنگی حفاظت شده» می توانند به «رشد جوامع محلی اقتصاد» کمک کنند، اگرچه مستلزم آن است که سیاست هایی برای حفظ آن ها اعمال شود، اما فن آوری های اینترنت اشیاء ذاتاً منطقی ترین جایگزین هستند. پارادایم اینترنت اشیاء باعث می شود هنگامی که یک شیء با محیط اطراف تعامل داشته باشد، او را «باهوش» سازد.

همراه با فن آوری های سنجش، شبکه های حسگر بی سیم، امکان نظارت و مدیریت را به شیوه ای کارآمد فراهم می کند. به عنوان مثال، برای ردیابی شرایط محیطی در فضاها، شناسایی تغییرات ساختاری در مواد، یا هشدار از حضور غیرعادی در مناطق ممنوعه مناسب هستند. چنین برنامه های اینترنت اشیایی می توانند حفظ، ارزیابی و به ثمر رساندن میراث فرهنگی را بهبود بخشند. (Astorga González & Co., ۲۰۲۰)

۴-۵. اینترنت اشیاء در ایران

«سند ملی اینترنت اشیاء» در شورای عالی فضای مجازی در ایران در سال ۱۳۹۷ تدوین شده است و وزارتخانه ها و نهادهای مختلف، مسئولیت های مختلفی را برای تحقق آن بر عهده دارند، اما برای عملیاتی کردن آن اقدامی نشده است و این خلأ احساس می شود. در این خصوص، دولت ها باید قبل از ورود یک فناوری یا تکنولوژی، «فرهنگ سازی» را شروع کنند و به صورت قانونمند آن را اجرا کنند ولی معمولاً در ایران، ابتدا تکنولوژی و یا ابزار نوین توسط وارد کننده در داخل عرضه میشود و مردم نیز از آن استفاده می کنند، آنگاه دولت به فکر فرهنگ سازی می افتد که همیشه این راه ناموفق بوده است. این تکنولوژی باید با پیوست فرهنگی بومی وارد کشور شود تا به زیرساخت های فرهنگی کشور ضربه ای وارد نشود. (دانشجویان ایران، ۱۳۹۷)

۶. ویژگی های اینترنت اشیاء

۱-۶. نامتجانس بودن: نامتجانس بودن اشیاء این فناوری، یکی از مهم ترین ویژگی های فناوری اینترنت اشیاء است. این «تنوع» وسایل و ابزارهای موجود در بستر این فناوری باعث می شود که نوع برخورد و تعامل آنها با یکدیگر چالش برانگیز باشد. با توجه به اینکه این فناوری میتواند بسیاری از اشیاء و هویت های فیزیکی و مجازی پیرامون ما را با یکدیگر درگیر و متصل کند، در نتیجه، حجم زیادی از داده و اطلاعات را تولید خواهد کرد که پیامد آن پردازش حجم زیادی از ترافیک تبادلی بین اشیاء و پردازش سنگین این داده ها خواهد بود. (شعبانی پور و همکاران، ۱۳۹۷)

۲-۶. درک جامع: با استفاده از (RFID)، سنسورها و بارکد دو بعدی، اطلاعات جسم در هر زمان و هرکجا، بدست می آید و اطلاعات و سیستم های ارتباطی میتوانند به طور نامتناهی در محیط اطراف ما جاسازی شود. شبکه ی سنسور، مردم را قادر میسازد تا از راه دور با دنیای واقعی ارتباط برقرار کنند.

فناوری های شناسایی، شامل اشیاء و شناسایی مکان ها می باشند. شناسایی و به رسمیت شناختن جهان فیزیکی، پایه و اساس اجرای ادراک کلی است.

۳-۶. انتقال قابل اطمینان: از طریق انواع شبکه های رادیویی در دسترس، شبکه های مخابراتی و اینترنت، اطلاعات مربوط به اشیاء در هر زمان میتواند در دسترس باشد. فناوری ارتباطی در اینجا شامل انواع تکنولوژی های انتقال سیم و بیسیم، فناوری های سوئیچینگ[۸]، فناوری های شبکه و فناوری های دروازه می باشد. اینترنت اشیاء علاوه بر ایجاد تعامل بین جهان فیزیکی و دنیای مجازی، جامعه و دنیای دیجیتال را هم، به هم متصل می کند.

۳-۶. پردازش هوشمند: با جمع آوری داده های (IoT) به پایگاه داده ها، فناوری های محاسباتی هوشمند مختلف از جمله ابررایانه، قادر به پشتیبانی از برنامه های داده (IoT) می باشند. ارائه دهندگان خدمات شبکه، میتوانند دهها میلیون یا حتی میلیارد تکه پیام را فوراً را از طریق پردازش ابری پردازش کنند؛ بنابراین فناوری ابررایانه، ترویج کننده ی (IoT) خواهد بود. (مرکز اینترنت اشیاء ایران، ۱۴۰۴)

۷. اجزای اینترنت اشیاء

اینترنت اشیاء شامل شبکه ها، دستگاه ها و داده های به هم پیوسته در فواصل طولانی است. یک «سیستم کامل اینترنت اشیاء» شامل چند جزء است:

۷-۱. دستگاه های حسگر

«حسگرها» اولین لایه ی اکوسیستم اینترنت اشیاء هستند که برای جمع آوری داده های دقیق و قابل اعتماد، ضروری هستند. آنها از آشکارسازها و محرک ها تشکیل شده اند.

۷-۱-۱. حسگرها / پروب ها (آشکارسازها)

حسگرها که به نام آشکارسازها نیز شناخته می‌شوند، داده‌های لحظه‌ای دقیق را از محیط اطراف جمع‌آوری می‌کنند. اندازه گیری عوامل مختلف مانند دما، رطوبت، نور، شاخص فرابنفش[۹] و گاز.

۷-۱-۲. موتورها/ عملگرها

«عملگرها» با انجام اقداماتی به نشانک[۱۰] یا دستورات پاسخ می دهند. به عنوان مثال، آنها می توانند گرمایش و سرمایش را کنترل کنند، مانند یک تهویه ی مطبوع هوشمند که هنگامیکه حسگرها کسی را در اتاق تشخیص نمی دهند، متوقف می شود.

۷-۲. ارتباطات

«ارتباطات» یک جزء حیاتی از اینترنت اشیاء است که اتصال شبکه بین دستگاه ها، حسگرها، محرک ها و ابر را تسهیل می‌کند. این ارتباط، رمزگشایی داده ها و اقدامات بعدی در (IoT) را امکان پذیر می کند.

۷-۳. برنامه ای برای پردازش و تحلیل داده ها

[۸] Switching
[۹] Ultraviolet index or UV
[۱۰] Signal

اینترنت اشیاء «تجزیه و تحلیل» داده های گسترده را پردازش می کند، شاخص های کلیدی عملکرد[۱۱] و ناهنجاری ها را بیدرنگ شناسایی می کند و امکان اقدام فوری برای جلوگیری از مشکلات را فراهم می کند.

۷-۴. رابط کاربری

«رابط کاربری» (IoT)، کنترل و تنظیمات برگزیده ی دستگاه را فعال می‌کند که از طریق دستگاه‌ها یا از راه دور قابل دسترسی است.

فناوری هایی مانند شبکه های حسگر بی سیم[۱۲]، ارتباطات میدان نزدیک[۱۳]، بلوتوث کم مصرف[۱۴]، سامانه ی بازشناسی با امواج رادیویی (RFID)، موزه ها را برای مدیریت موجودی بهبود می بخشد. پیشرفت در فناوری اطلاعات و ارتباطات (Wi-Fi)، دستگاه های موبایل، حسگرها و برنامه های مقرون به صرفه، در حال تغییر عملیات و خدمات هستند. گزینه های ارتباطی مختلف توسط شبکه ی گسترده ی کم مصرف[۱۵]، شبکه ی محلی بی سیم[۱۶]، و شبکه ی محدوده ی شخصی بی سیم[۱۷] ارائه شده است. (Mohamed, ۲۰۲۴)

۷-۵. دروازه های اینترنت اشیاء[۱۸]

«داده های خام» حسگرها باید از «دروازه ها» عبور کنند تا به «ابر» برسد. بنابراین، دروازه ها نقش مهمی در اینترنت اشیاء دارند. پروتکل های شبکه، ارتباط یکپارچه بین دستگاه ها را تفسیر می کند و از ترافیک مدیریت و امنیت داده ها اطمینان حاصل می کند. آنها به عنوان یک لایه ی امنیتی محافظ عمل می کنند و از فناوری رمزگذاری پیشرفته برای حفاظت از داده ها در برابر دسترسی غیرمجاز و حملات مخرب استفاده می کنند.

۷-۶. ابر در اینترنت اشیاء [۱۹]

«ابر»، داده های جمع آوری شده ی (IoT) را به سرعت پردازش می کند، با تمام اجزاء متصل می شود و تصمیمات بلادرنگ می گیرد. «سرعت» بسیار حیاتی است، به ویژه برای موقعیت های بحرانی مانند سلامت و ایمنی. هدف اصلی (IoT) ارائه ی اطلاعات به سرعت است و آن را به چارچوبی چابک و امن برای اتصال سامانه ها، افراد و برنامه ها تبدیل میکند. (Mohamed,۲۰۲۴)

۷-۷. استانداردها و پروتکل های اینترنت اشیاء (IoT Protocols)

[۱۱] KPIs or Key Performance Indicators
[۱۲] WSN or Wireless Sensor Network
[۱۳] NFC or Near field communication
[۱۴] Bluetooth Low Energy or BLE
[۱۵] LPWAN or Low-power wide area network
[۱۶] WLAN or Wireless local Area Network
[۱۷] WPAN or Wireless Personal Area Network
[۱۸] IoT Gate ways
[۱۹] IoT Cloud

«پروتکل‌های اینترنت اشیاء»، بخشی جدایی ناپذیر از معماری آن هستند. بدون استانداردها و پروتکل‌های اینترنت اشیاء، سخت افزار بی فایده تلقی می‌شود، زیرا به دلیل وجود آن‌ها است که تبادل داده توسط سخت افزار امکان‌پذیر می‌گردد و از بین این داده‌های منتقل شده، اطلاعات مفید می‌تواند توسط کاربر نهایی استخراج شود.

در اینترنت اشیاء، پروتکل‌ها به دو دسته ی ارتباطی و داده ای تقسیم می‌شوند:

۷-۷-۱. پروتکل های ارتباطی

هر شبکه یا بستر ارتباطی اینترنت اشیاء، نیاز به پروتکل یا پروتکل‌های خاص خود را دارد و با استفاده از آن‌ها می‌توان انتقال داده را انجام داد و شامل بلوتوث، وای فای، زیگبی[۲۰]، شبکه های سلولی موبایل، LoRaWAN، Z-Wave، Sigfox، RFID، NB-IoT، RPL است.

۷-۷-۲. پروتکل های داده ای اینترنت اشیاء

داده ها بین دستگاه ها و سیستم های دیگر مانند سکوی اینترنت اشیاء[۲۱] انتقال می یابند. برخی از دستگاه ها دارای سنسورهایی هستند که داده ها را با فاصله ی زمانی منظم فشار می دهند. سنسورهای دیگر با یک مدل کشش، در جایی که شما باید اطلاعات را درخواست کنید کار می کنند. چندین پروتکل داده وجود دارد که می توانیم در (IoT) استفاده کنیم.

چهار پروتکل محبوب این دسته شامل MQTT، CoAp، DDS، AMQP است. (مرکز اینترنت اشیاء، ۱۴۰۴) یکی از پروتکل های ارتباطی در اینترنت اشیاء و شبکه های کم توان و پراتلاف که به آن اشاره شد، پروتکل (RPL) است. تاکنون در طرح های مربوط به دفاع در برابر تهاجم به این پروتکل، از ایده های مختلفی مانند سیستم های کشف نفوذ، توابع درهم ساز و امضای دیجیتال و یا ترکیبی از آنها استفاده شده است. (شعبانی پور و همکاران، ۱۳۹۷)

۸. مزایای اینترنت اشیاء

اینترنت اشیاء با اتصال دستگاه‌ها و اشیاء به اینترنت و فراهم کردن امکان تبادل اطلاعات بین آنها، مزایای قابل توجهی در زمینه‌های مختلف ایجاد کرده است؛ برخی از این وظایف عبارت‌اند از:

۸-۱. افزایش کارایی و بهره وری

اینترنت اشیاء با خودکارسازی و بهینه‌سازی فرایندها به شرکت‌ها و سازمان‌ها کمک می‌کند تا بهره وری خود را افزایش دهند. در محیط‌های صنعتی، دستگاه‌های متصل به اینترنت می‌توانند داده‌های لحظه‌ای را از وضعیت خود ارسال کنند و از بروز خرابی‌های ناگهانی جلوگیری کنند. این نظارت لحظه‌ای موجب کاهش زمان خاموشی و هزینه‌های نگهداری می‌شود.

۸-۲. صرفه‌جویی در هزینه‌ها

[۲۰] Zigbee

[۲۱] IoT Platform

اینترنت اشیاء با بهبود فرایندها و همچنین کاهش نیاز به نیروی انسانی در بسیاری از وظایف، باعث کاهش هزینه‌ها می‌شود. به عنوان مثال، در خانه‌های هوشمند، دستگاه‌های متصل می‌توانند مصرف انرژی را بهینه کنند و مثلاً چراغ‌ها و سیستم‌های گرمایشی یا سرمایشی تنها در مواقع نیاز روشن شوند که این امر درنهایت به کاهش مصرف انرژی و هزینه‌های مربوط به آن منجر خواهد شد.

۸-۳. بهبود تجربه ی کاربری

اینترنت اشیاء می‌تواند نیازهای خاص کاربران را شناسایی کرده و تجربه‌ای سفارشی سازی شده را ارائه دهند. به عنوان مثال، خودروهای هوشمند با توجه به الگوی رانندگی کاربر، پیشنهاداتی برای مسیرهای بهتر ارائه می‌دهند، یا دستگاه‌های هوشمند به کاربران اطلاعات دقیقی از وضعیت سلامتی آنها ارائه می‌کنند.

۸-۴. افزایش امنیت و ایمنی

در بحث امنیت و ایمنی نیز اینترنت اشیاء نقش مهمی ایفا می‌کند. دستگاه‌های متصل به اینترنت اشیاء مانند دوربین‌های امنیتی، حسگرهای دود و سیستم‌های هشدار به کاربران اجازه می‌دهند تا از وضعیت خانه یا محیط کار خود آگاه باشند و در صورت بروز مشکل، سریعاً اقدام کنند. این سیستم‌ها می‌توانند به صورت خودکار هشدارهایی به موبایل ارسال کنند و حتی اقدامات خودکاری مثل قفل کردن درب‌ها را انجام دهند.

۸-۵. تصمیم‌گیری بهتر و مبتنی بر داده‌ها

یکی از بزرگ ترین مزایای (IoT) این است که با جمع‌آوری داده‌های دقیق و تحلیلی، به سازمان‌ها و افراد کمک می‌کند تا «تصمیمات بهتری» را اتخاذ کنند. دسترسی به اطلاعات گسترده و لحظه‌ای از دستگاه‌ها، امکان تحلیل داده‌ها و پیش‌بینی روندها را فراهم کرده و به بهبود عملکرد و کاهش خطرات کمک می‌کند.

۸-۶. بهبود مدیریت منابع

اینترنت اشیاء نقش بسزایی در زمینه ی«استفاده ی بهینه از منابع» ایفا می‌کند. به عنوان مثال، در کشاورزی، سنسورهای متصل به اینترنت، اطلاعات دقیق در مورد وضعیت خاک، میزان رطوبت و نیاز به آب را فراهم می‌کنند که به کشاورزان در مدیریت بهینه ی منابع آب و مواد مغذی کمک می‌کند یا در شهرهای هوشمند، (IoT) با نظارت بر مصرف انرژی و مدیریت بهینه ی ترافیک، به بهبود زندگی شهری کمک می‌کند. (مرکز اینترنت اشیاء ایران، ۱۴۰۴)

۹. انواع اینترنت اشیاء

به طور کلی، اینترنت اشیاء با توجه به نحوه ی عملکرد خود در دسته بندی‌های مختلفی قرار می‌گیرند و هر یک از آنها ویژگی‌های منحصر به فرد خود را دارند. برخی از رایج ترین انواع اینترنت اشیاء به شرح زیر است:

۹-۱. اینترنت اشیاء مصرف کننده[۲۲]

[۲۲] Consumer Internet of Things

در این نوع از اینترنت اشیاء، تمرکز اصلی روی راحتی «مشتریان فردی» است و تلاش می‌شود تا خدماتی ارائه شود که مشتریان هدف بتوانند با استفاده از اینترنت اشیاء، فعالیت‌های روزمره ی خود را به شکل راحت تری دنبال کنند. لوازم خانگی، لوازم صوتی- تصویری، وسایل روشنایی و ... ، تنها برخی از شناخته شده ترین انواع آن به شمار می‌روند.

۹-۲. اینترنت اشیاء تجاری[۲۳]

«اینترنت اشیاء تجاری»، به دستگاه‌ها و سیستم‌هایی اشاره دارد که به صورت «تجاری» و «سازمانی» مورد استفاده قرار می‌گیرند. «ضربان سازهای هوشمند» و «سیستم‌های پایش»[۲۴] دو نمونه از پرکاربردترین نمونه‌های استفاده از اینترنت اشیاء در صنایع تجاری مثل بهداشتی و حمل و نقل هستند.

۹-۳. اینترنت اشیاء صنعتی[۲۵]

«اینترنت اشیاء صنعتی» را می‌توان جا افتاده‌ترین و بالغ‌ترین نوع اینترنت اشیاء دانست. در اینترنت اشیاء صنعتی، تمرکز روی بخش صنعت، سازمان‌ها و کارخانه‌های فعال در این حوزه است و تلاش می‌شود تا میزان کارایی، بهره وری، امنیت و خروجی عملیات‌ها به شکلی بهبود پیدا کند که در نهایت، منجر به بازگشت سرمایه برای مجموعه شود.

۹-۴. اینترنت اشیاء نظامی[۲۶]

همانطور که از نام این نوع از اینترنت مشخص است، از فناوری‌های اینترنت اشیاء در زمینه ی «نظامی» استفاده می‌شود. به عنوان مثال، ربات‌های نظامی که امروزه نقش مهمی در بحث‌های نظامی ایفا می‌کنند، با به کارگیری فناوری‌های اینترنت اشیاء ساخته شده‌اند.

۹-۵. اینترنت اشیاء فرهنگی (IOCT)

«اشیاء و موجودیت های فرهنگی» نیز مانند سایر اشیاء و موجودیت ها، میتوانند از طریق اینترنت و بدون مداخله ی انسان با یکدیگر و با تولیدکننده و متصدی[۲۷]، به تبادل اطلاعات بپردازند. همانطورکه شهر، خانه و سایر محیط ها و اکوسیستم ها[۲۸]، میتوانند هوشمند شده و به اینترنت متصل شوند و خدمت ارائه کنند، محیط های فرهنگی و مذهبی مانند سینما، تئاتر و تماشاخانه ها، حوزه های علمیه، دانشگاه ها و مدارس، قطب های گردشگری، مساجد، موزه ها و ... هم هوشمند شده و در ارتباط با یکدیگر یا در ارتباط با محیط های غیرفرهنگی، می توانند به جامعه خدمت رسانی فرهنگی و غیرفرهنگی کنند.

---

[۲۳] Commercial Internet of Things or CIoT

[۲۴] Monitoring

[۲۵] IIoT or Industrial Internet of Things

[۲۶] Military Things

[۲۷] Operator

[۲۸] Ecosystem

اشیاء فرهنگی، فکری، هنری و رسانه ای همچون بازی های رایانه ای، فیلم های سینمایی، مطبوعات، صنایع دستی، پویانمایی[۲۹]، کتب و ... نیز، در صورت داشتن «هویت رقومی»، میتوانند به برقراری ارتباط از طریق شبکه های اینترنتی با یکدیگر و سایر اشیاء تولیدکننده و متصدی پرداخته و خدمات فرهنگی و غیرفرهنگی متمایزی ارائه کنند.

«شناسنامه دارکردن اشیاء فرهنگی» کمک می کند که حقوق مؤلف به ویژه در صنایع فرهنگی حفظ شود. همچنین با توجه به پرداخت «یارانه های کلان» در صنعت فرهنگ، امکان ارزیابی صنایع فرهنگی و جلوگیری از رانت و فساد ایجاد می شود. رونق آثار هنری و رسانه ای مانند صنایع دستی و فیلم سینمایی؛ تجاری کردن فرهنگ و کسب درآمد از صنایع فرهنگی؛ و ایجاد نقشه ی پراکنش سلایق فرهنگی، هنری، فکری و رسانه ای افراد در کشور از طریق شناسنامه دارکردن آثار و محصولات فرهنگی، از مزایای اینترنت اشیاء فرهنگی است که می تواند درخط مشی گذاری تولید و توزیع آثار هنری و همچنین اصلاح جامعه از طریق آثار فرهنگی به کار آید. (Nasrollahi, & Zaroodi, ۲۰۲۰)

تأثیرات فرهنگی اینترنت اشیاء در این حوزه ها است و در حال تغییر این دامنه ها است:

۱. باورها، ارزش‌ها و آیین‌های مذهبی؛

۲. نظام باورها و ارزش‌های فرهنگی؛

۳. نظام رفتار و سبک‌های رفتاری؛

۴. عبارات شفاهی؛

۵. عبارات رفتاری؛

۶. ارتباطات انسانی؛

۷. نهاد خانواده؛

۸. میراث فرهنگی، ساختار و شکل‌های رسانه‌ای فرهنگی؛

۹. میراث فرهنگی، ساختار و سازمان‌های فرهنگی؛

۱۰. نظام آموزشی؛

۱۱. ساختارهای تصمیم‌گیری؛

۱۲. ساختار و اشکال سازمان‌دهی و حکمرانی سیاسی؛

۱۳. نظام‌های بهره برداری از منابع؛

۱۴. نظام‌های دانش، خرد، مهارت‌ها و ظرفیت‌های بومی (Nasrollahi, & Zaroodi,۲۰۲۰)

۱۰. بررسی چالش ها و تهدیدات در اینترنت اشیاء

بعضی از چالش های اساسی در بحث اینترنت اشیاء شامل نقص حریم خصوصی؛ امنیت؛ اعتماد بیش از اندازه بر فناوری؛ محرمانگی؛ قابلیت همکاری و استانداردها؛ قانون، نظارت و حقوق؛ و اقتصادهای نوظهور حجم دادها، تفسیر داده ها، پیچیدگی نرم افزاری، تحمل گسیختگی، منبع تغذیه و ارتباطات بیسیم می باشد که مهم ترین آنها مورد بررسی قرار

[۲۹] Animation

می گیرد. اینترنت اشیاء در حال حاضر اتفاق می افتد و نیاز به رسیدگی به چالش های آن و به حداکثر رساندن مزایای آن در حین کاهش خطرات آن وجود دارد. (ساکت، ۱۳۹۸)

مهم ترین چالش حال حاضر در اینترنت اشیاء، مسأله ی «امنیت» است. امنیت در گره؛ امنیت در زیرساخت و ارتباطات لایه ی فیزیکی؛ امنیت در پروتکل های لایه ی شبکه و پروتکل ارتباطی؛ امنیت در لایه ی برنامه های کاربردی و نقل و انتقال داده ها و اطلاعات؛ و امنیت در انتقال اطلاعات به ابر داده؛ چند مورد از مواردی است که به لزوم توجه به ایمنی در این فناوری اشاره دارد. (شعبانی پور و همکاران، ۱۳۹۷)

۱-۱۰. چالش های امنیتی اینترنت اشیاء

برنامه های اینترنت اشیاء به طور گسترده در بسیاری از زمینه های زندگی اجتماعی مانند مراقبت های بهداشتی و درمانی، مدیریت انرژی و خودکارسازی[۳۰] صنعتی و خانگی، نظارت بر محیط زیست، حمل و نقل و ... ، کاربرد دارد. اینترنت اشیاء که به سرعت در حال رشد است، می تواند تأثیرات فرهنگی بسیاری در جامعه داشته باشد، بنابراین به گونه ای باید سیاست گذاری شود تا در صورت تکامل، نه تنها به فرهنگ آسیب نرساند، بلکه در خدمت فرهنگ باشد. (زرودی و همکاران، ۱۳۹۶)

معماری های اینترنت اشیاء قرار است با جمعیتی حدود میلیاردها اشیاء سر و کار داشته باشد، که با یکدیگر و با دیگر نهادها، مانند انسان ها و یا نهادهای مجازی تعامل خواهند داشت. همه ی این تعاملات باید به نحوی محافظت شود، از جمله حفاظت از اطلاعات و تأمین خدمات تمام بازیگران مربوطه و نیز محدود کردن تعداد حوادثی که بر کل اینترنت اشیاء تأثیر می گذارد. با این حال، «حفاظت اینترنت اشیاء» یک کار پیچیده و دشوار است. تعداد حمله های در دسترس حمله کننده های مخرب با توجه به اتصال جهانی (دسترسی هر کسی) و دسترس پذیری (دسترسی به هر مکان، در هر زمان)، به عنوان روندهای اصلی اینترنت اشیاء ممکن است گیج کننده باشند.

«تهدیداتی» که میتواند بر نهادهای اینترنت اشیاء تأثیر گذارد، متعدد هستند. مانند حملات با هدف کانال های ارتباطی مختلف، تهدیدات فیزیکی، محرومیت از خدمات، ساخت هویت، و غیره. در نهایت، پیچیدگی ذاتی اینترنت اشیاء که در آن نهادهای ناهمگن متعدد واقع در زمینه های مختلف می توانند اطلاعات را با یکدیگر مبادله کنند، پیچیدگی های بیشتر طراحی و به کارگیری مکانیزم های امنیتی کارآمد، سازگار و مقیاس پذیر را می طلبد. (ساکت، ۱۳۹۸)

با وجود تمام مزایای بیان شده، به دلیل اینکه اشیاء، متصل به اینترنت هستند همانند کامپیوتر و موبایل های هوشمند، آنها نیز در معرض «نفوذ غیرمجاز» و «هک شدن» می باشند. به علت گستردگی افرادی که با مجموعه ی اینترنت اشیاء در ارتباط خواهند بود، در صورت هک شدن آنها، اثرات زیانبار و گسترده ای خواهد داشت. به دلیل عدم دقت و رعایت نکردن نکات ایمنی، موارد متعددی از هک کردن دوربین های مداربسته و امنیتی به منظور جاسوسی و یا وارد شدن به آن محیط و یا مشاهده ی فعالیتهای حریم خصوصی افراد و منتشر کردن آن در اینترنت برای مشاهده ی همگان وجود دارد.

امنیت و محرمانه بودن، مسائل مهمی برای کاربردهای اینترنت اشیاء بوده و همچنان با چالش های بزرگی مواجه است. مهمترین مشکل مرتبط با امنیت در اینترنت اشیاء، بحث «احراز هویت» و «جامعیت داده ها» است. از آنجایی که

[۳۰] Automation

احراز هویت معمولاً نیازمند وجود سرورها و زیرساخت های مناسب برای تبادل پیام میان اجزاء مختلف است، تأمین آن در اینترنت اشیاء، کار دشواری است. (ساکت، ۱۳۹۸)

در حال حاضر، دزدی نرم افزار و حملات مخرب، خطرات زیادی برای امنیت (IoT) بوجود آورده است. این تهدیدها ممکن است اطلاعات مهمی را که منجر به خسارت های اقتصادی و اعتبار میشود، به سرقت ببرند. (زندیار و همکاران، ۱۴۰۰) بعضی از پژوهش های صورت گرفته با اولویت بندی فناوری هایی که «قابلیت ارتقاءبخش حفاظت از امنیت سایبری» را دارند، سعی در حل مسائل امنیتی و افزایش امنیت ساختارهای اینترنت اشیاء دارند، و بعضی پژوهش های دیگر مانند «زنجیره ی بلوک» (بلاک چین)، با دسته بندی کاربری های اینترنت اشیاء، استانداردها و پروتکل های مشترک و پیاده سازی یک چرخه و مدیریت آن در لایه های مختلف اینترنت اشیاء، سعی در حل چالش های امنیت دارند. (سلمانی و خسروی، ۱۴۰۰)

این فناوری نوپا، با توجه به گسترش کاربری آن، دارای آسیب پذیری‌ها و چالش‌هایی در ارتباط با امنیت است، به طوریکه می‌توان از امنیت، تحت عنوان «پاشنه آشیل اینترنت اشیاء» یاد کرد. این آسیب‌پذیری‌ها باعث ایجاد نگرانی‌های جدی از توسعه ی این فناوری شده است. نگرانی‌های مربوط به امنیت اینترنت اشیاء و آسیب‌پذیری‌های آن شامل این موارد است:

۱. افزایش کاربردها و خدمات مبتنی بر اینترنت اشیاء در صنایع مختلف؛

۲. فراهم آوردن امنیت و حریم خصوصی و دسترسی راحت و گسترده به اینترنت که معضلات امنیتی فضای سایبری[۳۱] را گریبانگیر این فناوری کرده است؛

۳. افزایش انگیزه‌ها برای انجام فعالیت‌های مخرب امنیتی در حوزه ی اینترنت اشیاء؛

۴. نقش کارکردی و انکارناپذیر آسیب‌پذیری‌های امنیتی در بروز و ظهور فعالیت‌های مخرب در حوزه ی اینترنت اشیاء؛

۵. توسعه ی تکنیک‌ها و مفاهیم برای بهینه سازی امنیت و کاهش آسیب‌پذیری‌ها؛

۶. تعریف قوانین جدید در زمینه ی گسترش کاربری و توسعه ی کسب وکارها با ممانعت از ایجاد آسیب پذیری‌ها و حفظ حریم خصوصی.

با توجه به موارد فوق و همچنین محدود بودن منابع مالی و انسانی، هزینه و زمانی که باید برای جبران خسارت ناشی از حفره‌های امنیتی موجود در فناوری اینترنت اشیاء صرف کرد و حتی صدمات جانی‌ای که ممکن است عدم توجه و شناخت موضوعات امنیتی در این حوزه به بار آورد، ضرورت شناسایی و پرداختن به مسائل و چالش‌های امنیتی آن احساس می‌شود. (مرکز اینترنت اشیاء ایران، ۱۴۰۴)

مهم ترین چالش های امنیتی اینترنت اشیاء

سه عامل اصلی برای امنیت اینترنت اشیاء وجود دارد:

۱. محرمانه بودن اطلاعات، ۲.حفظ حریم خصوصی، و ۳. اعتماد

[۳۱] Cyber

۱. محرمانه بودن اطلاعات: این چالش تضمین می کند تنها کاربران مجاز، قادر به دسترسی و تغییر داده باشند، و آن شامل دو جنبه است: اول؛ مکانیزم کنترل دسترسی، و دوم، یک فرایند احراز هویت اشیاء.

۲. حفظ حریم خصوصی: حریم به عنوان یک کنترل دسترسی به اطلاعات شخصی تعریف شده است و نگهداری اطلاعات خاص و اطلاعات محرمانه را مقدور می سازد؛ ویژگی های حفظ حریم خصوصی، سری بودن، گمنامی و خلوتی آن است. بیشتر محققان در حال حاضر به دنبال افزایش و توسعه ی حریم خصوصی در برنامه های کاربردی هستند، فناوری های بهبود حریم خصوصی می تواند به موضوع اشیاء، تراکنش یا سیستم متمایل گردد و آن برای محافظت از هویت در اینترنت استفاده می شود. در محیط اینترنت اشیاء، امنیت و حریم خصوصی برای تضمین یک تعامل قابل اعتماد بین دنیای فیزیکی و دنیای مجازی مهم هستند. (مرکز اینترنت اشیاء ایران، ۱۴۰۴)

۳. اعتماد: اعتماد جهت اعمال قوانین امنیتی در سیستم تضمین شده است و نمونه ی رایج اعتماد، گواهینامه های دیجیتال[۳۲] هستند. (مرکز اینترنت اشیاء ایران، ۱۴۰۴)

۲-۱۰. تهدیدات امنیتی اینترنت اشیاء

اکثر محققان براین باورند که دستگاه های مورد استفاده در اینترنت اشیاء؛ به دلیل محدودیتهای فنی، آسیب پذیرتر از فناوری های اینترنتی هستند و این امر منجر به ایجاد تهدیدهای بیشتری می شود. تهدید بیانگر فعالیتی است که از شکاف های امنیتی سیستم برای دستیابی به منافع مشخص استفاده می کند.

تهدیدات امنیتی شامل موارد زیر می باشد:

۱. کنترل نشده: عمدتاً شامل «مبتدیانی» است که از نرم افزارهای رخنه گر[۳۳] در دسترس استفاده می کنند.

۲. سازمان یافته: توسط افرادی که از نقاط آسیب پذیر سیستم آگاه هستند و میتوانند با نوشتن و دستکاری کدها و پردازه نویسی[۳۴] از آنها سوءاستفاده کنند، رقم میخورد.

۳. پایدار پیشرفته: یک حمله ی هماهنگ و شبکه ای پیچیده است که به دنبال سرقت داده ها از اطلاعات با ارزش بالا در صنایعی مانند تولید، بانکداری و دفاع ملی است. (نوروزی، ۱۴۰۳) مبادله ی اطلاعات مهم و خصوصی در برنامه هایی مانند خانه ی هوشمند یا مراقبت های بهداشتی هوشمند از راه دور، زمینه را برای سوءاستفاده ی مهاجمان و نقض حریم خصوصی افراد فراهم می کند. افزون بر این، اطلاعات مربوط به مکان یابی عناصر خاص شبکه، میتواند توسط «شنودگران» برای طراحی حملات به عناصر یا رویدادهای خاص، مورد سوءاستفاده قرار گیرد. تهدیدها و خطرات همچنان درحال توسعه هستند، زیرا هکرها راههای جدیدی برای نفوذ به سیستم های ناامن ابداع میکنند که تهدیدی برای خود اکوسیستم[۳۵] است.

شش حمله و خطر امنیتی سایبری اینترنت اشیاء

---

[۳۲] Digital
[۳۳] Hack
[۳۴] Script
[۳۵] Ecosystem

«حملات سایبری» از متداولترین و مهمترین حملات اینترنت اشیاء بوده و شامل برخی «تهدیدات خارجی» نیز می باشد:

۱. وسعت اینترنت اشیاء: میتوان گفت تعداد کل نقاط ورود و دسترسی غیرمجاز به سیستم، اولین گام حملات سایبری محسوب شده و شامل تمام نقاط آسیب پذیر امنیتی دستگاه های اینترنت اشیاء، نرم افزارهای مورد استفاده و اتصالات شبکه است. اندازه و وسعت اینترنت اشیاء و توانایی ایمن سازی آن، یکی از بزرگترین تهدیدهای یک سازمان محسوب می شود. تعداد واقعی دستگاه های اینترنت اشیاء در جهان در حال افزایش است و در سال ۲۰۲۳ با ۱۶ درصد رشد، به ۱۶.۷ میلیارد نقطه ی پایانی فعال رسیده است. در گزارشی مطرح شده است که سازمان به طور متوسط نزدیک به ۱۳۵۰۰۰ نقطه ی پایانی را مدیریت می کند. علاوه بر این، دستگاه های اینترنت اشیاء، معمولاً به صورت شبانه روزی، هفت روز در هفته و به تعداد نامحدودی متصل هستند.

۲. دستگاه های ناامن: دستگاه های افراد، می توانند یک خطر امنیتی برای کل اکوسیستم اینترنت اشیاء باشند. دیوارهای آتش[۳۶]، رمزگذاری و نامرئی کردن دستگاه ها در شبکه برای جلوگیری از اتصال نقاط پایانی به دستگاه های اینترنت اشیاء قبل از اینکه مهاجمان فرصت دسترسی اولیه را داشته باشند، ضروری است. دستگاه ها به دلیل محدودیت هایشان، یعنی ظرفیت محاسباتی کم و طراحی کم مصرف، اغلب فاقد کنترل های امنیتی داخلی هستند. در نتیجه، بسیاری از دستگاه ها نمی توانند از ویژگی های امنیتی مانند احراز هویت، رمزگذاری و کنترل دسترسی پشتیبانی کنند. حتی زمانی که نقاط پایانی دارای برخی از گزینه های امنیتی مانند رمزهای عبور هستند، برخی سازمان ها همچنان آنها را بدون استفاده یا فعال کردن اجرا می کنند.

۳. نگهداری و به روز رسانی: مسائل مربوط به تعمیر و نگهداری مناسب دستگاه های جانبی و به روز رسانی نرم افزار، چالش زیادی برای اینترنت اشیاء ایجاد میکند. محدودیت های اتصال و همچنین قابلیت های محدود دستگاه و منابع تغذیه ممکن است به روز رسانی های دستگاه ها را با مشکل مواجه کند.

بسیاری از سازمان ها از «دستگاه های قدیمی» برای ذخیره سازی داده ها استفاده می کنند که حاوی آخرین «استانداردهای امنیتی» نیستند. هنگامی که سازمان هایی با دستگاه های قدیمی، با اینترنت اشیاء ادغام شوند، می توانند شبکه را در معرض خطرات امنیتی قرار دهند. همچنین فقدان پایش و مشاهده ی نقاط پایانی، مهمترین مانع برای دستیابی به یک وضعیت امنیتی قوی است.

۴. استقرار غیرمجاز دستگاه ها به معنای استقرار نقاط پایانی اینترنت اشیاء «بدون پشتیبانی رسمی» یا «مجوز» از بخش فناوری اطلاعات یا بخش امنیتی است. این نقاط پایانی ممکن است «دستگاه های شخصی غیرمجاز» که دارای آدرس آیپی[۳۷] هستند، مانند ردیاب های تناسب اندام یا دستیارهای دیجیتال[۳۸]، یا فناوری های مخصوص کسب و کارها و سازمان ها، مانند چاپگرهای بیسیم باشند. درهرصورت، آنها خطراتی را برای سازمان ایجاد می کنند، زیرا ممکن است استانداردهای امنیتی سازمان را برآورده نکنند، و حتی اگر چنین باشد، ممکن است به روش هایی پیکربندی و مستقر

[۳۶] Firewall
[۳۷] Internet Protocol
[۳۸] Digital

شده باشند که از بهترین شیوه های امنیتی پیروی نکنند. علاوه براین، «مدیران فناوری اطلاعات» و «تیم های امنیتی» عموماً از این استقرارها اطلاعی ندارند و بنابراین ممکن است آنها را رصد یا بر ترافیک آنها نظارت نکنند و به هکرها شانس بیشتری برای هک کردن موفقیت آمیز و ناشناخته ی آنها بدهند. همچنین هکرها می توانند با تزریق گره های جعلی به شبکه، به گره های قانونی متصل به اکوسیستم اینترنت اشیاء حمله کرده و در نتیجه داده های جاری بین گره های جعلی و قانونی را تغییر داده یا کنترل کنند.

۵. انتقال داده های رمزگذاری نشده: دستگاه های اینترنت اشیاء بسته هایی از داده ها را که همه چیز را از خوانش دما گرفته تا سرعت شیء اندازه گیری و ضبط می کنند، جمع آوری می کنند. آنها بسیاری از این داده ها را برای پردازش، تجزیه و تحلیل و ذخیره سازی به مکان های مرکزی معمولاً در فضای ابری ارسال می کنند. آنها همچنین اطلاعاتی را دریافت می کنند که اغلب دستگاه ها را از اقداماتی که باید انجام دهند مطلع می کنند.

مطالعات نشان داده اند که بسیاری از داده های ارسال شده، رمزگذاری نشده اند، بنابراین داده های شخصی و محرمانه را در شبکه افشا می کنند و به مهاجمان این امکان را می دهند تا به ترافیک رمزگذاری نشده ی شبکه گوش دهند، اطلاعات شخصی یا محرمانه را جمع آوری کنند و سپس از آن برای سوءاستفاده بهره ببرند. با دسترسی به شبکه از طریق یک دستگاه اینترنت اشیاء، مهاجمان می توانند داده های ابری را بدزدند و سپس تهدید کنند که داده ها را نگه می دارند یا حذف می کنند یا آنها را عمومی می کنند مگر اینکه باج بگیرند (باج افزار).

۶. تهدیدات خارج از شبکه: یک شبکه ی اینترنت اشیاء علاوه بر «آسیب پذیری های داخلی»، دارای «تهدیدهایی از خارج محیط» اینترنت اشیاء می باشد. یکی از این تهدیدات «ربات ها» هستند. در این نوع حملات، مهاجم، یک دستگاه اینترنت اشیاء را از طریق پورت[۳۹] محافظت نشده یا کلاهبرداری فیشینگ[۴۰] با بدافزار آلوده می کند و سپس آن را به یک شبکه ی ربات[۴۱] اینترنت اشیاء تبدیل می کند که برای انجام «حملات سایبری گسترده» استفاده می شود.

بوت مسترها[۴۲]، دستگاه های اینترنت اشیاء را به دلیل پیکربندی های ضعیف امنیتی و تعداد دستگاه هایی که می توانند به شبکه ی ربات تبدیل شوند، هدف جذابی می دانند. غالباً حملات انکار سرویس توزیع شده از شبکه های اینترنت اشیاء استفاده می کنند تا ترافیک شبکه ی هدف را مختل کنند. شرکت نوکیا در سال ۲۰۲۳ گزارشی را منتشر کرد که نشان داد تعداد ربات های اینترنت اشیاء درگیر در حملات انکار سرویس توزیع شده مبتنی بر ربات، به حدود یک میلیون دستگاه افزایش یافته است. (نوروزی، ۱۴۰۳)

۳-۱۰. چالش حریم خصوصی اینترنت اشیاء

«گیبس»[۴۳] (۲۰۰۸) حریم خصوصی را به عنوان «محدودیت دسترسی دیگران به یک شخص» تعریف می کند و اشاره می کند که این محدودیت بر اساس سه عنصر قرار گرفته است:

[۳۹] Port
[۴۰] Phishing
[۴۱] Botnet
[۴۲] Master Boot
[۴۳] Gibbs

۱. پنهان کاری (کنترل اطلاعات)

۲. ناشناسی (اقدام بدون توجه دیگران)

۳. تنهایی (محدود کردن دسترسی فیزیکی به یک فرد)

علاوه بر این، او اشاره به اهمیت تعادل حریم خصوصی شخصی در برابر دیگر حقوق فردی و در برابر کالای اجتماعی جمعی دارد. (مرکز اینترنت اشیاء ایران، ۱۴۰۴)

اینترنت اشیاء، نوید بخش یک عصر جدید از محاسبات است که به موجب آن هر شیء قابل تصور «مجهز» میشود، و یا به یک دستگاه هوشمند متصل می شود که اجازه ی جمع آوری داده ها و ارتباطات از طریق اینترنت را می دهد. اینترنت اشیاء، حریم خصوصی افراد را از نظر «جمع آوری» و «استفاده از اطلاعات شخصی افراد» به چالش می کشد.

به دلیل آنکه داده های بیشتری از منابع مختلف با استفاده از این دستگاه ها جمع آوری می شوند، اینترنت اشیاء می تواند تأثیر قابل توجهی بر حریم خصوصی اشخاص با پتانسیل اضافی برای نظارت گسترده ی افراد بدون اطلاع یا رضایت آنها داشته باشد. به عبارتی، حفظ حریم خصوصی، قوانینی که تحت آن هر فرد کاربر باید به چه اطلاعاتی دسترسی پیدا کند را تعریف می نماید. دلیل اصلی که حفظ حریم خصوصی در اینترنت اشیاء از ضروریات محسوب می شود، به حوزه ی کاربری و فناوری های مورد استفاده در اینترنت اشیاء برمی گردد. برنامه های کاربردی در بخش مراقبت های بهداشتی، بیانگر برجسته ترین حوزه ی کاربری هستند که در آن اطمینان یافتن از وجود امنیت در حوزه ی اطلاعات در فناوری اینترنت اشیاء ضروری می نماید.

به علاوه، در چشم انداز اینترنت اشیاء، نقش تکنولوژی های ارتباطی برجسته تر خواهد شد. انطباق گسترده در رسانه های بی سیم برای تبادل اطلاعات، موجب نشر و نمو مباحث جدید در حوزه ی نقض حریم خصوصی می گردد. در واقع، شبکه های بی سیم، به دلیل قابلیت دسترسی از راه دور، خطر نقض حریم خصوصی را افزایش می دهند، چون باعث می شوند که سیستم در معرض خطر بالقوه استراق سمع و حملات پوششی قرار بگیرد. از این رو، حفظ حریم خصوصی، نشانگر یک مسأله ی واقعی است که ممکن است توسعه ی اینترنت اشیاء را با محدودیت مواجه سازد.

به طور کلی، نیازمندی های حریم خصوصی در اینترنت اشیاء را می‌توان به این صورت دسته بندی کرد:

۱. حفاظت از اطلاعات شخصی (اطلاعات اکتسابی و ذاتی) و جلوگیری از نشت آن‌ها؛

۲. تنظیم رضایت نامه برای استفاده از اطلاعات شخصی افراد (صدور مجوز حریم خصوصی: چونکه شخص باید روی نحوه ی افشای اطلاعات خود کنترل کامل داشته باشد)؛

۳. اطمینان از پاک شدن اطلاعات خصوصی افراد پس از استفاده (فراموشی دیجیتالی)؛

۴. حفظ حریم خصوصی و گمنامی (اجازه ی استفاده از نام مستعار در شرایط خاص) برای مجموعه های ناهمگون از دستگاه‌ها که توسط مدیریت هویت دیجیتال مهیا می‌شود؛

۵. ارائه ی سیاست ها و چارچوب لازم برای حفظ حریم خصوصی و ثبت قوانین مربوط به آن؛

۶. بررسی شرایط استفاده از پل شبکه[۴۴] در صورت نیاز برای حفظ حریم خصوصی؛

۷. سازگاری حریم خصوصی سیستم های مختلف؛

[۴۴] Bridge

۸. حفظ حریم خصوصی هنگام جستجو یا کشف سرویس ها و دستگاه‌های اینترنت اشیاء؛

۹. بررسی اثر استفاده از هویت یکتا در سطح جهانی در حریم خصوصی و راهکارهای مقابله با خطرات احتمالی آن (استفاده از مشتقات هویت ها)؛

۱۰. اطمینان از عدم افشای مالکیت داده، دستگاه و اشیاء برای افراد غیرمجاز؛

۱۱. تنها شخص مجاز برای خواندن برچسب های[۴۵] مرتبط با حریم خصوصی، مالک آن باشد؛

۱۲. عدم امکان ردیابی فعالیت های یک شیء توسط شیء دیگر؛

۱۳. اطلاعات انتقال مرتبط با حریم خصوصی، تنها باید برای طرفین ارتباط قابل فهم باشد؛

۱۴. ایجاد پروتکل ها و الگوریتم های مخفی کننده ی اطلاعات خصوصی افراد مثل چهره یا مکان، به طوری که تنها اشخاص مجاز، قابلیت باز کردن آن را داشته باشند؛

۱۵. پیشنهاد پروتکل برای توافق روی سطح حریم خصوصی لازم برای اطلاعات منتشر شده. (مرکز اینترنت اشیاء ایران، ۱۴۰۴)

۴-۱۰. چالش های موجود در راستای حفاظت از داده های خصوصی

۱-۴-۱۰. چالش انعقاد قراردادهای تولید و مصرف کننده

هنگام به کارگیری ابزارهای اینترنت اشیاء، «اطلاعات مصرف کنندگان این ابزارها» به همراه افرادی که مصرف کنندگان با آنها در ارتباط هستند و حتی اطلاعات محیط پیرامون آنها، قابل دریافت توسط این ابزارها است؛ از این رو، در صورتیکه در اطلاعات دریافت شده، سوءاستفاده ای صورت پذیرد؛ میتواند اثرهای غیرقابل جبرانی برجای بگذارد. از طرف دیگر، خرید چنین ابزارهایی از تولیدکنندگان آنها، در قالب قراردادهای الحاقی صورت میپذیرد؛ از اینرو، مصرف کنندگان ملزم خواهند بود، تمام شرایط از پیش تعیین شده را بدون برخورداری از حق شرط یا قدرت چانه زنی قبول و قرارداد را منعقد نمایند. این امر، نه تنها اختیار مصرف کنندگان در انعقاد قراردادها را تحت الشعاع قرار میدهد، بلکه گاه منجر به پیش بینی شروطی غیرمنصفانه میشود. در مواردی، مفاد قرارداد به نحوی گنجانده می شود که به جهت برخورداری عبارات از بار حقوقی، بسیاری از مصرف کنندگان از درک مفهوم عبارات نوشته شده عاجز بوده، بدون آگاهی به مفاد آن شروط، نسبت به انعقاد قرارداد اقدام می کنند.

چالش دیگر، مسأله ی «تهدید مالکیت دارندگان ابزارها» توسط تولیدکنندگان آنها است که به صورت ضمنی یا جداگانه، نسبت به قرارداد فروش صورت می پذیرد. در دنیای حاضر، استفاده ی مالکان از ابزارهای اینترنت اشیاء به دلیل مسأله ی حق انحصاری تولیدکننده از بهره برداری از فناوری ابداعی خود، به شکلی بروز نموده است که در صورت خرابی یا نقص ابزار، دارنده از تعمیر شخصی آن محروم بوده و باید طبق قرارداد، به نمایندگی های تعیین شده توسط تولیدکننده مراجعه نماید. این امر در مواردی می تواند منجر به ایجاد مشکل گردد. در این خصوص می توان به پرونده ی «شرکت صنایع سنگین جان دیر»[۴۶]، تولیدکننده ی «تراکتورهای هوشمند» اشاره کرد. هنگامی که تراکتور دارنده، با نقص فنی

[۴۵] Tag
[۴۶] John Deere

هنگام برداشت محصول مواجه گردید، به جهت ضرورت، دارنده، شخصاً مبادرت به «تعمیر» آن کرد. شرکت مزبور از طریق فن آوری «کنترل از راه دور»، مبادرت به از کارانداختن تراکتور نمود که این امر منجر به صدمات مالی بسیار زیادی به دارنده ی زمین کشاورزی گردید.

۲-۴-۱۰. چالش تعامل میان پردازنده و کنترل کننده

به دلیل آنکه ابزارهای اینترنت اشیاء برای انجام وظایف از پیش تعیین شده مبادرت به جمع آوری انبوهی از اطلاعات می نمایند؛ در موارد لزوم، «پردازش» آنها توسط یک پردازنده باید با سرعت و دقت بالا صورت پذیرد تا خللی در راستای عملکرد این ابزار ایجاد نشود. (آقایی طوق و ناصر، ۱۳۹۹)

۳-۴-۱۰. چالش محرمانگی اینترنت اشیاء

«محرمانگی اطلاعات» بیانگر یک مسأله ی اساسی در اینترنت اشیاء می باشد و تضمین آن مستلزم این است که تنها «اشخاص مجاز» بتوانند به داده ها دسترسی داشته باشند و آن را اصلاح نمایند. در زمینه ی کسب و کار، این امر کاملاً تحقق پیدا کرده است که به موجب آن، اطلاعات به عنوان یک دارایی که باید مورد حفاظت قرار بگیرد و دارای ارزش بازار رقابتی است، نشان داده می شود.

با توجه به اینکه برنامه های کاربردی اینترنت اشیاء، مربوط به قلمرو فیزیکی می باشد، حصول اطمینان از محرمانه بودن اطلاعات، یکی از محدودیت های اصلی برای بسیاری از استفاده کنندگان است. این اطلاعات به طور حتم محرمانه هستند، چون گسترش و توزیع کنترل نشده ی آنها می تواند به «اعتبار» و «مزیت رقابتی شرکت ها» در میان سایر شرکت ها آسیب وارد نماید. به عنوان مثال، میتوان به هشدارهای ظهور سونامی یا زلزله توسط حسگرهای محیطی اشاره نمود. در چنین شرایطی اطلاعات باید از طریق اعضای مورد اطمینان در دسترس قرار گیرند. بنابراین، اطلاعات باید با توجه به استراتژی های «مدیریت ریسک» در محیط قرار داده شوند. نشت چنین اطلاعاتی در حوزه ی عمومی ممکن است باعث افزایش هرج و مرج و بروز وحشت و در معرض خطر قرار دادن امنیت گروه های زیادی از مردم شود.

در این زمینه، تکنیک های مختلف کنترل دسترسی، برای اطمینان از محرمانه بودن در سیستم های مدیریت دانش، پیشنهاد شده اند. همچنین روش استانداردی که با ویژگی های محیط اینترنت اشیاء تناسب داشته باشد، ارائه گردیده است. این شیوه، «کنترل دسترسی بر مبنای وظیفه» نام دارد. کنترل دسترسی بر مبنای وظیفه، به عنوان یک گزینه ی موفق که به طور گسترده و سطح بالایی برای کنترل دسترسی اختیاری و اجباری مورد استفاده قرار گرفته، در دو دهه ی گذشته ظهور یافته است و در آن دسترسی ها و کاربری ها به نقش ها اختصاص داده شده است. کاربران از طریق تعیین نقش، به طور غیرمستقیم مجوز لازم را کسب می کنند. در رویکرد اینترنت اشیاء، مزیت عمده ی کنترل دسترسی بر مبنای وظیفه این است که امتیاز دسترسی از طریق تکالیف نقش، به صورت پویایی قابل اصلاح است. به طور ویژه، داده های اینترنت اشیاء بیشتر نشان دهنده ی جریان اطلاعاتی است که در زمان واقعی در دسترس قرار می گیرند تا اینکه بیانگر یک پایگاه داده استاتیک[۴۷] باشد.

[۴۷] Statics

سیستم های مدیریت جریان داده، به طور فزاینده ای برای حمایت از برنامه های کاربردی در زمان واقعی، در یک گستره ی وسیع مورد استفاده قرار می گیرند، مانند نظارت بر شبکه، شبکه های حسگر و ... ، و راه حل های مناسبی را برای اینترنت اشیاء ارائه می دهند.

در اینترنت اشیاء، تکنیک های کنترل دسترسی باید با سیستم های مدیریت جریان داده ها ادغام شوند. یکی از جنبه هایی که باید در زمان بروز مشکل محرمانه بودن در نظر گرفته شود، مدیریت شناسایی (هویت) است. در حقیقت این موضوع در فناوری اینترنت اشیاء بسیار مهم است که در آن تلفیقی از دنیای فیزیکی و دیجیتالی وجود دارد و مشکلی که مشاهده می گردد، مربوط به پیدا کردن راه حل ها به شیوه ای امن برای شناسایی اشیاء و فرایندهای مربوط به صدور مجوز است. (مرکز اینترنت اشیاء ایران، ۱۴۰۴)

۴-۴-۱۰. چالش اعتماد به اینترنت اشیاء

یکی از چالش برانگیزترین مشکلات فناوری اینترنت اشیاء، «قابلیت اعتماد» آن (قابلیت اطمینان و در دسترس بودن) است. مفهوم اعتماد در زمینه های متعدد و با معانی گوناگونی مورد استفاده قرار می گیرد. اعتماد یک مفهوم پیچیده در ادبیات علوم اطلاعاتی و علوم کامپیوتر محسوب می گردد که هیچ اجتماع نظری در موردش وجود ندارد و با توجه به دیدگاه های مختلف، تعاریف متنوعی نیز در مورد اعتماد وجود دارد. مشکل اصلی در خصوص شیوه های تعریف از اعتماد، وجود عدم وابستگی بین تعاریف و شیوه های ارزیابی و ارائه ی معیار می باشد. به عنوان تعریفی که به طور گسترده مورد استفاده قرار می گیرد، «اعتماد» این گونه تعریف می شود: اعتماد، سیاست های امنیتی تنظیم شده ی مربوط به دسترسی به منابع و اختیاراتی است که برای تحقق چنین سیاست هایی مورد نیاز می باشد.

علاوه بر این، ضروری است تا زبان مذاکره ی مؤثر و قابل اطمینانی را ابداع نماییم که قادر باشد ویژگی های اختیاری را ساده نموده و به گونه ای منعطف، نیازمندی های حفاظتی را از طریق تعریف سیاست های افشاگرانه، به طورگسترده ای ارائه نماید. تعریفی جامع از مدل مؤثر اعتماد، باید هر دو بعد اینترنت اشیاء را پوشش دهد: ماهیت توزیعی سطح بالای اینترنت اشیاء و نیاز بسیاری از برنامه های آن از حیث زمان پاسخگویی و یا پیچیدگی محاسباتی. به عبارت دیگر؛ ما نیاز داریم تا از رویکردهای تمرکزی و ایستا که از راه حل های مدیریت اعتماد به طور گسترده استفاده می نمایند، به سمت اتخاذ یک رویکرد پویا و توزیع شده حرکت نماییم که بر این فرض استوار است که هیچ نوع رابطه ی اعتمادی از قبل میان اعضای سیستم تعریف نشده است. علاوه بر این، باید یک چارچوب منعطف برای مدیریت اعتماد معرفی شود، به گونه ای که نیازهای مقیاس پذیری را به خوبی تأمین نماید. (مرکز اینترنت اشیاء ایران، ۱۴۰۴)

۱۱. محافظت در برابر خطرات امنیتی اینترنت اشیاء

۱-۱۱. رویکرد چند لایه ای برای کاهش خطرات امنیتی اینترنت اشیاء

تیم های فناوری اطلاعات باید «رویکردی چند لایه ای» برای کاهش خطرات امنیتی اینترنت اشیاء داشته باشند. شیوه ها و استراتژی های گسترده ای وجود دارد که سازمان ها می توانند آنها را به کار گیرند، اما مدیران نیز باید راهکارهای خاص متناسب با انواع مختلف حملات اینترنت اشیاء داشته باشند.

امنیت اینترنت اشیاء، ترکیبی از سیاست و نرم افزار کاربردی برای شناسایی و مقابله با هرگونه تهدید است. تیم های فناوری اطلاعات که بر دستگاه های اینترنت اشیاء نظارت می کنند، باید خط مشی هایی مانند «گذرواژه های قوی» برای دستگاه های موجود در شبکه داشته باشند و از نرم افزار تشخیص تهدید برای پیش بینی هرگونه حمله ی احتمالی استفاده کنند. آنها همچنین باید دارای «نرم افزار جامع تشخیص و مدیریت دارایی» باشند. هرچه تیم های فناوری اطلاعات نقاط پایانی مستقر شده ی سازمان خود و داده های دستگاه های اینترنت اشیاء خود را بیشتر ببینند، تشخیص پیشگیرانه ی خطرات و تهدیدات امنیتی آسان تر است. استراتژی های کلیدی که «مدیران فناوری اطلاعات» میتوانند برای جلوگیری از حملات امنیتی و حفظ انعطاف پذیری شبکه استفاده کنند، شامل ارزیابی آسیب پذیری دستگاه، محدود کردن سرویس های غیرضروری، پشتیبان گیری منظم از داده ها، روش های بازیابی شبکه، تقسیم بندی شبکه و ابزارهای نظارت بر شبکه است.

با تقویت امنیت و محافظت از دستگاه ها، می توان از سوءاستفاده از دستگاه برای انجام حملاتی مانند انکار سرویس توزیع شده علیه سایر سازمان ها، شنود ترافیک شبکه و هک کردن سایر دستگاه ها جلوگیری کرد. این کار سبب افزایش حفاظت و امنیت داده ها شده و منجر به محرمانه بودن، یکپارچگی و در دسترس بودن داده های جمع آوری شده، ذخیره شده، پردازش شده و ارسال شده به و از دستگاه های اینترنت اشیاء می شود.

اعمال این «استراتژیهای کلیدی» بر روی تمامی دستگاه هایی که به طور مستقیم و غیرمستقیم به اطلاعات شخصی افراد مرتبط هستند، منجر به حفاظت از حریم خصوصی افراد می شود. سازمان ها باید اطمینان حاصل کنند که ملاحظات و چالش های امنیت سایبری، سوءاستفاده از نقاط آسیب پذیر امنیتی جهت تهدید محرمانگی، یکپارچگی یا در دسترس بودن دستگاه ها یا داده ها را بررسی می کنند. (نوروزی، ۱۴۰۳)

۲-۱۱. زنجیره ی بلوک (بلاک چین)[۴۸] و کاربردهای آن در اینترنت اشیاء

«زنجیره ی بلوک» یک سیستم و تکنولوژی ثبت رمزگذاری شده و توزیع شده ی کامپیوتری است که به آن، «پایگاه داده» نیز گفته می شود. این داده‌ها می‌توانند برای نمونه تراکنش‌های بانکی باشند یا اسناد مالکیت، قرارها، پیام‌های شخصی و یا دیگر اطلاعات.

زنجیره ی بلوک، یک ساختار ذخیره سازی داده برای ثبت اطلاعات و گزارش ها است که به دلیل ثبت شدن همه ی اطلاعات مربوط به تراکنش های سازمان ها در آن، «دفتر کل»[۴۹] نیز نامیده می شود. (افشار و همکاران، ۱۳۹۹)

یکی از ویژگی های زنجیره ی بلوک این است که کار ذخیره ی این داده‌ها بدون وجود یک مدیر و صاحب اختیار مرکزی امکان پذیر است و نمی‌توان با تخریب یک نقطه ی مرکزی، داده‌های ذخیره شده را تحریف یا نابود کرد که نام این ویژگی، «شبکه ی غیرمتمرکز» نام دارد. زنجیره ی بلوک، تراکنش‌های آنلاین امن را ساده می‌کند. (بلاک چین، ۱۴۰۳)

ساختار زنجیره ی بلوک، از یک «دنباله» یا «سلسله بلوک» تشکیل شده که با هم به وسیله ی مقادیر «هش»[۵۰] خود، متصل شده اند.

[۴۸] Blockchain
[۴۹] Ledger
[۵۰] Hash

هر بلوک شامل بخش «سرآیند»[۵۱] و بخش «دنباله» است که در بخش سرآیند، زمان ایجاد بلوک[۵۲]، هش آن بلوک و هش بلوک قبلی است و سایر اطلاعات مربوط به شناسایی آن بلوک قرار می گیرد و در بخش دنباله، داده هایی که قرار است در آن بلوک ذخیره شوند، قرار می گیرد. هش که مجموعه ای از اعداد و حروف تصادفی است، توسط تأییدکنندگان تراکنش[۵۳] با کمک یک تابع ریاضی خاص به دست می آید. هش هر بلوک، مخصوص همان بلوک بوده و مانند «اثر انگشت» برای بلوک است. اگر تغییری در اطلاعات بلوک به وجود آید، هش آن کاملاً عوض میشود و به دلیل وابستگی بلوک ها به یکدیگر، هش بلوک های بعدی نیز تغییر می کنند و بلوک ها نامعتبر می شوند و باعث به هم خوردن شبکه می شود. به همین دلیل، با بررسی هش یک بلوک، به سادگی میتوان اصالت یا عدم اصالت اطلاعات یک بلوک را تشخیص داد. (چراغعلی و تاجفر، ۱۴۰۰)

کاربردهای زنجیره ی بلوک (بلاک چین) برای IoT

فن آوری زنجیره ی بلوک را می توان به طور مؤثر در تقریباً همه ی حیطه های (IoT) به کار گرفت. مسائل مقیاس پذیری که ممکن است به خاطر افزایش تعداد گره های شرکت کننده به وجود بیاید و بنابراین اندازه ی بلوک، بخصوص برای (۵G) و اینترنت وسایل نقلیه که می توانند بر مصرف توان، انتشار شبکه و ازدحام شبکه تأثیر بگذارند.

برخی از کاربردهای «فن آوری زنجیره ی بلوک» شامل موارد زیر است:

۱. اینترنت اشیاء و مراقبت از سلامت

رشد و پیشرفت اینترنت اشیاء نوید دهنده ی جهش های تکنولوژیکی قابل توجه در قرن ۲۱ است. هرچند تاکنون در مورد تأثیر اینترنت اشیاء بر تولید، انبارداری و کارخانه ها صحبت شده است، ولی تنها محدود به این کاربردها نیست. در کنار موارد مذکور، پیشرفت ها در زمینه ی سلامت و بهداشت نیز بسیار چشمگیر بوده است. بر اساس ایده ی پایگاه داده ی آنلاین توزیع شده، طرحی بر پایه ی زنجیره ی بلوک برای (IoT) در مراقبت سلامت را پیشنهاد کردند. در یک مدل از زنجیره ی بلوک کنسرسیومی[۵۴]، یک بلوک جدید ایجاد می شود و توزیع می شود، هنگامی که داده های مراقبت سلامت جدید خلق می شوند. از شبکه ی بلاک چین در کاربردهای مراقب سلامت موبایل برای حفاظت از یکپارچگی، حسابرسی یا بررسی استفاده کرده اند.

۲. اینترنت اشیاء در عصر ۵G

در عصر (IoT)، ۵G یک جامعه ی کاملاً متحرک و متصل به هم را برای میلیاردها اشیاء متصل، فراهم می کند. برای حل مسائل حریم خصوصی در محیط ارتباطات ناهمگن، ۵G یک طرح حفظ کننده ی حریم خصوصی و اشتراک داده بر پایه ی زنجیره ی بلوک پیشنهاد داده است. بر اساس ایده ی افزودن بلوک ها به زنجیره ی بلوک، هر بلوک جدید به وسیله ی مقدار هش خود، به زنجیره ی بلوک متصل می شود. مقدار هش قبلی را می توان از هدر بلوک قبلی فهمید.

---

[۵۱] Header
[۵۲] Timestamp
[۵۳] Miners
[۵۴] Consortium

۳. اینترنت وسایل نقلیه[۵۵]

اینترنت اشیاء یک شبکه ی گسترده است که تمام اشیاء هوشمند را به هم وصل می کند. هر زمان که این اشیاء هوشمند به اینترنت متصل می شوند، تنها به وسایل نقلیه محدود می شوند، سپس آن را «اینترنت وسایل نقلیه» می نامند. بر اساس مدل امنیت غیرمتمرکز، یک مدل اکوسیستم زنجیره ی بلوک به نام (LNSC) برای مدیریت وسایل نقلیه الکترونیکی و مجموعه ی شارژکنندگی، پیشنهاد شده است. این مدل از رمزنگاری منحنی بیضوی (ECC) برای محاسبه ی توابع هش در خودروهای الکتریکی و ایستگاه های شارژ استفاده می کند. برای اجتناب و جلوگیری از ردیابی مکان، (IoV) یک معماری حفظ کننده ی حریم خصوصی غیرمتمرکز پیشنهاد داده است که در آن گره های لایه ی اصلی زنجیره ی بلوک را مدیریت می کند.

۴. اینترنت انرژی

اینترنت انرژی به عنوان یک حوزه ی ترکیبی از فناوری و توزیع انرژی، سازوکارهایی را برای بهبود استفاده از توانمندی های مبتنی بر شبکه ی هوشمند فراهم آورده است. در حوزه ی اینترنت، انرژی از فناوری اینترنت اشیاء به منظور گردآوری و تحلیل داده ها در زمان واقعی جهت مدیریت هوشمند انرژی استفاده می شود.

۵. اینترنت ابری[۵۶]

در اینترنت (IoC)، میلیون ها دستگاه (IoT) داده های خود را از طریق اتصال اینترنت با بهره گیری از فن آوری مجازی سازی به ابر، آپلود می کنند. یک مدیریت منابع هوشمند برای دیتا سنترهای ابری بر اساس فن آوری بلاک چین، معرفی شده است تا هزینه ی کل مصرف انرژی کاهش یابد.

۶. مدیریت دسترسی در (IoT)

برای مدیریت ادوات در (IoT) یک سیستم کنترل دسترسی توزیع شده با استفاده از فن آوری زنجیره ی بلوک پیشنهاد شده است. معماری این سیستم از ۶ جزء تشکیل شده است:

۱. شبکه های حسگر بیسیم؛

۲. مدیران؛

۳. گره ی کارگزار؛

۴. قرارداد هوشمند؛

۵. شبکه ی زنجیره ی بلوک؛

۶. هاب ها[۵۷] یا مراکز مدیریت.

این سیستم مزیت هایی برای کنترل دسترسی در (IoT) فراهم می کند:

۱. تحرک، که در سیستم های مدیریتی ایزوله قابل استفاده است؛

[۵۵] IOV or Internet of vehicles
[۵۶] IOC or Intenet of Cloud
[۵۷] Hub

۲. قابلیت دسترسی که تضمین می کند قوانین کنترل دسترسی همیشه مهیا هستند؛

۳. هم زمانی؛

۴. سبک وزنی، به این معنا که ادوات (IoT)، نیاز به هر گونه اصلاح برای به کارگیری این سیستم را دارد.

دیگر کاربردهای بلاک چین، شامل سنجش تجمع؛ توزیع (P۲P) توزیع شده؛ ذخیره ی داده و «بیت کوین»[۵۸] است. (چراغعلی و تاجفر، ۱۴۰۰)

۱۲. تحولات تکنولوژیکی برای آینده ی اینترنت اشیاء

توسعه ی فناوری های توانمندی مانند الکترونیک نیمه هادی، ارتباطات، حسگرها، تلفن های هوشمند، سیستم های تعبیه شده، شبکه ی ابری، شبکه ی مجازی سازی و نرم افزار، برای اجازه به دستگاه های فیزیکی جهت فعالیت در محیط های متغیر که همیشه و در همه جا متصل باشند، ضروری خواهد بود.

آینده ی توسعه ی تکنولوژی های اینترنت اشیاء شامل موارد زیر می باشد:

۱. دستگاه های سخت افزاری: فناوری نانو، کوچک سازی چیپست ها[۵۹] و مدارهای بسیار کم توان؛

۲. سنسورها: سنسورهای هوشمند، کوچک و کم توان، و شبکه ی حسگر بی سیم برای اتصال حسگر؛

۳. تکنولوژی ارتباطی: آنتن های بر روی تراشه، پروتکل های طیف گسترده و آگاه، پروتکل یکپارچه در طیف گسترده و تراشه های قابل تنظیم مجدد چند منظوره؛

۴. فناوری شبکه: شبکه های خودآگاهی و خودسازماندهی، شبکه های خودترمیم شونده و خود آموز، پروتکل IPV۶ فراگیر مبتنی بر استقرار اینترنت اشیاء، قابلیت مقیاس پذیری IPV۶؛

۵. نرم افزار و الگوریتم ها: نرم افزار هدف گرا، هوش توزیع شده (نامتمرکز) و حل مشکل، نرم افزار استفاده کننده گرا؛

۶. تکنولوژی پردازش داده و سیگنال: پردازش داده بافت آگاه و پاسخ داده ها، پردازش شناختی و بهینه سازی، تجزیه و تحلیل داده های پیچیده ی اینترنت اشیاء، تجسم داده ی هوشمند اینترنت اشیاء، انرژی و طیف فرکانسی پردازش آگاهانه اطلاعات؛

۷. تکنولوژی های کشف و موتور جستجو: برچسب گذاری خودکار مسیر و مراکز شناسایی مدیریت، خدمات برحسب تقاضا (کشف/ادغام)؛

۸. فناوری های امنیت و حریم خصوصی: حریم خصوصی و سیاست های حفظ حریم خصوصی کاربر- محور بافت آگاه، پردازش داده آگاه از حریم خصوصی و پروفایل های امنیتی و حریم خصوصی (انتخاب بر اساس امنیت و نیاز به حریم خصوصی). (Patel, & Co., ۲۰۱۶)

[۵۸] Bitcoin
[۵۹] Chipsets

۱۳. نتیجه گیری

«اینترنت اشیاء»، این انقلاب تکنولوژی، به همه ی حیطه های زندگی افراد به خصوص مهم ترین بخش شکل دهنده ی هویت اشخاص اعم از خانواده، رفتار، دین و تفریحات، کالاهای مصرفی و ... ورود پیدا کرده است و با سرعت زیادی در حال تسخیر بازار و گسترش است. انقلابی که متوقف نخواهد شد و ما در آینده شاهد جهش های غیرمنتظره، عجیب و باورنکردنی در این حیطه خواهیم بود، و امنیت و حریم خصوصی کاربران در استفاده از این اختراعات علمی، به مسأله ای حیاتی برای بشر تبدیل شده و خواهد شد، زیرا فناوری، با وجود آسانتر کردن روش های زیست انسان ها، میتواند به ابزاری بی رحم و تهدیدگر توسط سوءاستفاده کنندگان درآمده و جان، مال و نام افراد را خدشه دار کرده و یا از بین ببرد و در صورت عدم واکنش سریع مسئولان به چالش های مطرح شده یا نبودن استانداردها و قوانین بازدارنده ی کافی، کنش های اجتماعی و سیاسی غیرمنتظره ای را شکل خواهد داد.

همانطور که در این مقاله بررسی شد، اینترنت اشیاء در سازمان های فرهنگی با خطرات و تهدیدات امنیتی زیادی در حوزه هایی نظیر وسعت اینترنت اشیاء، دستگاه های ناامن، نگه داری و به روز رسانی، استقرار غیرمجاز دستگاه ها، انتقال داده های رمزگذاری نشده و تهدیدات خارج از شبکه رو به رو است. همچنین، با چالش هایی در حفاظت از حریم خصوصی مانند چالش انعقاد قراردادهای تولید و مصرف کننده، تعامل بین پردازنده و کنترل کننده، محرمانگی اینترنت اشیاء و اعتماد به اینترنت اشیاء مواجه است. در این میان، روش های حفاظتی نظیر استفاده از «گذرواژه های قوی» برای دستگاه های موجود، «نرم افزارهای تشخیص تهدید» و به کارگیری سیستم رمزگذاری شده ی «زنجیره ی بلوک» به عنوان مؤثرترین راهکارها معرفی شده اند. نادیده گرفتن این تهدیدات و چالش ها می تواند منجر به نقض محرمانگی، افشای حریم شخصی کاربران و از دست رفتن میراث فرهنگی دیجیتال شود. بنابراین، تدوین استانداردهای الزام آور ملی، تصویب قوانین بازدارنده و فرهنگ سازی پیش از ورود فناوری، یک ضرورت فوری برای «سازمان های فرهنگی» است.

۱۴. پیشنهادها برای تحقیقات آینده

موضوعات زیر برای تحقیقات آتی راجع به امنیت و حریم خصوصی اینترنت اشیاء پیشنهاد می گردد که به پیشبرد علم در این زمینه کمک خواهد کرد:

۱. تحقیق در زمینه ی مقایسه ی سیستم های امنیتی (IoT) در سازمان های فرهنگی در کشورهای مختلف؛

۲. تحقیق در زمینه ی مدل های امنیتی خاص برای سازمان های فرهنگی؛

۳. تحقیق در زمینه ی رفتار کاربران و تهدیدات امنیتی اشیاء در سازمان های فرهنگی؛

۴. تحقیق در زمینه ی اثرات قانونی و اخلاقی استفاده از اینترنت اشیاء در سازمان های فرهنگی؛

۵. تحقیق در زمینه ی ارزیابی ریسک های امنیتی و حریم خصوصی در پیاده سازی اینترنت اشیاء در سازمان های فرهنگی.

فهرست منابع و مأخذ

منابع فارسی

۱. آزادی، زهرا؛ کرباسی، مصطفی. (مهرماه ۱۳۹۷). بررسی نقش اینترنت اشیاء در شهر هوشمند و شبکه ی هوشمند. پایان نامه ی کارشناسی ارشد، مؤسسه ی آموزش عالی غیاث الدین جمشید کاشانی، دانشکده ی کامپیوتر و فناوری اطلاعات.

۲. افشار، حمیدرضا؛ حسینی، سید شمس‌الدین؛ موحدی صفت، محمدرضا. (مرداد ۱۳۹۹). ارائه ی مدل مفهومی فرصت‌ها و تهدیدات به کارگیری و توسعه ی فناوری زنجیره ی بلوکی در جمهوری اسلامی ایران. *فصنامه ی علمی امنیت ملی*، دوره ی ۱۰، شماره ی ۳۶، صفحات ۳۴۸-۳۰۷

۳. آقایی طوق، مسلم؛ ناصر، مهدی. (تابستان ۱۳۹۹). چالش های حفاظت از داده های خصوصی در حوزه ی اینترنت اشیاء: مطالعه ی تطبیقی حقوق ایران و اتحادیه ی اروپا. *فصلنامه ی حقوق اداری (علمی- پژوهشی)*، سال هفتم، شماره ی ۲۳، صفحات ۵۵-۳۳

۴. چراغعلی، مرتضی؛ تاجفر، امیر هوشنگ. (۱۰ خرداد ۱۴۰۰). کاربردهای بلاک چین در سیستم های مبتنی بر اینترنت اشیاء. *هفتمین کنفرانس بین المللی فناوری های نوآورانه در زمینه ی علوم، مهندسی و تکنولوژی*، استانبول، ترکیه

۵. زرودی، علی؛ نصرالهی، محمد صادق؛ اسلامی، مهدی. (۱۳۹۶). پیوست فرهنگی اینترنت اشیاء در جمهوری اسلامی. پایان نامه ی کارشناسی ارشد، دانشگاه امام صادق علیه السلام، دانشکده ی معارف و فرهنگ و ارتباطات

۶. زندیار، ریحانه؛ اخترکاوان، احسان؛ رحیم آبادی، علی موقر. (۱۴۰۰). احراز هویت حسگرهای اینترنت اشیاء با استفاده از واترمارکینگ. پایان نامه ی کارشناسی ارشد، دانشگاه خاتم، دانشکده ی فنی و مهندسی

۷. ساکت، توحید. (۱۳۹۸). امنیت اینترنت اشیاء: نقش چالش ها و کاربردها. *مجله ی علمی- پژوهشی در علوم رایانه (سال چهارم)*، شماره ی ۱۳، بهار ۱۳۹۸، گروه کامپیوتر دانشگاه آزاد اسلامی، واحد میانه، ایران، صفحه ی ۳۲-۲۲

۸. سلمانی، محمدرضا؛ خسروی، حمید. (شهریورماه ۱۴۰۰). بررسی روش ها و پروتکل ها در کیفیت سرویس های اینترنت اشیاء، پایان نامه ی کارشناسی ارشد رشته ی مهندسی کامپیوتر گرایش هوش مصنوعی، مؤسسه ی آموزش عالی بهمنیار کرمان (بخش کامپیوتر)

۹. شعبانی پور، حمید؛ ابراهیمی آتانی، رضا. (۱۳۹۷). ارزیابی امنیت در پروتکل های ارتباطی اینترنت اشیاء. پایان نامه ی کارشناسی ارشد، دانشگاه گیلان

۱۰. صفری، مینا؛ و همکاران. (۱۴۰۰). مباحثی در مورد اینترنت اشیاء و کاربردهای آن، پایان نامه ی کارشناسی ارشد، مؤسسه ی آموزش عالی غیاث الدین جمشید کاشانی، دانشکده ی کامپیوتر و فناوری اطلاعات

۱۱. نوروزی، ریحانه. (پاییز ۱۴۰۳). مروری بر مسائل امنیتی و حریم خصوصی اینترنت اشیاء. *فصلنامه ی علمی و تخصصی فناوری های نوین در مهندسی برق و کامپیوتر*. جلد ۴، شماره ۳، دانشگاه آزاد اسلامی، واحد نی ریز، صفحه ی ۱۵۸ تا ۱۶۶

منابع لاتین

۱۲. Astorga González, Elizabeth M.& Noriega Alemán, Maikel & Municio, Esteban, & Johann M., Marquez-Barja (۱۴ September ۲۰۲۰).“Cultural Heritage and Internet of Things”. ۶th Conference EAI on Smart Objects and Technologies for Social Good, GoodTechs ’۲۰, Antwerp, Belgium, Pages ۲۴۸ – ۲۵۱

۱۳. Dabrowska, Magda. (۲۰۲۴). “IoT in cultural preservation: Digitising heritage sites”, Address: https://www.iot-now.com/۲۰۲۴/۱۲/۲۴/۱۴۸۶۹۹-iot-in-cultural-preservation-digitising-heritage-sites/, (Last seen: ۱۴۰۴, ۰۱, ۱۱)

۱۴. Mohamed, A.A.E.W (March ۲۰۲۴). *“Proposed Methodology for Using Internet of Cultural Things (IoCT) in Conservation on Cultural Heritage Sites”.Sohag Engineering Journal (SEJ),*

Volume ۴, NO. ۱, Department of Architecture, Faculty of Fine Arts, Assiut University, Pages ۶۱-۷۲

۱۵. Nasrollahi, Mohammad Sadeq & Zaroodi, Ali (Autumn & Winter ۲۰۲۰). "Recognizing Cultural Consequences of the Internet of Things". *Bi-quarterly scientific journal of Religion and communication*, Volume ۲۷, Issue ۲, Serial Number ۵۸, Pages ۱۶۱-۲۰۱

۱۶. Patel, Keyur K & Patel, Sunil M. & Salazar, Carlos & PG Scholar (May ۲۰۱۶). "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenge". *IJESC (International Journal of Engineering Science and Computing)*, Volume ۶, Issue No.۵, Faculty of Technology and Engineering-MSU, Vadodara, Gujarat, India, Pages ۶۱۲۲-۶۱۳۱

منابع اینترنتی

۱۷. بلاک چین. (۱۴۰۳). ویکی پدیا، دانشنامه ی آزاد، بازیابی شده در (۱۴۰۴/۰۱/۱۵)، درگاه اینترنتی:
https://fa.wikipedia.org/wiki/%D%۸B%۲D%۸۶%۹D%۸AC%DB۸%C%D%۸B%۱D۸۷%۹%D%۸A%۸D%۸۴%۹D%۸۸%۹DA%A۹

۱۸. مرکز اینترنت اشیاء ایران (IoT IRAN). (فروردین ۱۴۰۴). استانداردها و پروتکل ها، درگاه اینترنتی:
https://iotiran.com/about-iot/iot-standard

۱۹. خبرگزاری دانشجویان ایران. (۱۷ مرداد ۱۳۹۷). در آینده عدم ارتباط با اشیاء پذیرفته نیست/اینترنت اشیاء؛ انقلاب صنعتی دوم، قم، کد خبر: (-۵۰۰۶۳qom)، درگاه اینترنتی:
https://www.isna.ir

۲۰. مرکز اینترنت اشیاء ایران (IoT IRAN). (فروردین ۱۴۰۴). امنیت و حریم خصوصی، درگاه اینترنتی:
https://iotiran.com/about-iot/security

۲۱. مرکز اینترنت اشیاء ایران (IoT IRAN). (فروردین ۱۴۰۴). اینترنت اشیاء چیست و انواع مختلف آن کدامند؟ درگاه اینترنتی:
https://www.irisaco.com/internet-of-things

۲۲. مرکز اینترنت اشیاء ایران (IoT IRAN). اینترنت اشیاء، فرصت ادغام دنیای فیزیکی با سیستم های مبتنی بر کامپیوتر. (۱۸خرداد ۱۳۹۹). پایگاه خبری عصر هامون، کد مطلب: ۱۲۵۱۷۱، درگاه اینترنتی:
https://www.asrehamoon.ir